Ansible Galaxy FortiOS Collection

Release 1.0

Jun 26, 2021

FortiOS/Galaxy Version Mapping Guide

The FortiOS Ansible Collection provides Ansible modules for configuring FortiOS appliances.

CHAPTER 1

FortiOS Galaxy Versioning

1.1 FortiOS Galaxy versions

From `v2.0.0` on, FortiOS galaxy collections are unified, there is only one sequential collection at any moment. users who install these collections are expected to find the version compatibility information for each module and its parameters.

FOS version	Galaxy Version	Release date	Path to Install
unified	2.0.0	2021/4/6	`ansible-galaxy collection install fortinet.fortios:2.0.0`
unified	2.0.1	2021/4/7	`ansible-galaxy collection install fortinet.fortios:2.0.1`
unified	2.0.2	2021/5/14	`ansible-galaxy collection install fortinet.fortios:2.0.2`
unified	2.1.0 `latest`	2021/6/25	`ansible-galaxy collection install fortinet.fortios:2.1.0`

1.2 Legacy FortiOS Galaxy Versions

Prior to FortiOS collection `v2.0.0`, FortiOS Galaxy collections were built over three FOS major versions, i.e. `v6.0`, `v6.2` and `v6.4`, thus, users are expected to install the collection according to the following table to avoid potential compatibility issues.

FOS version	Galaxy Version	Release date	Path to Install
6.0.0	1.0.13	2020/5/26	`ansible-galaxy collection install fortinet.fortios:1.0.13`
6.0.0	1.1.2	2020/12/4	`ansible-galaxy collection install fortinet.fortios:1.1.2`
6.0.0	1.1.5	2020/12/7	`ansible-galaxy collection install fortinet.fortios:1.1.5`
6.0.0	1.1.8	2020/12/21	`ansible-galaxy collection install fortinet.fortios:1.1.8`
6.0.0	1.1.9	2020/3/1	`ansible-galaxy collection install fortinet.fortios:1.1.9`
6.2.0	1.0.10	2020/5/6	`ansible-galaxy collection install fortinet.fortios:1.0.10`
6.2.0	1.1.0	2020/12/4	`ansible-galaxy collection install fortinet.fortios:1.1.0`
6.2.0	1.1.3	2020/12/7	`ansible-galaxy collection install fortinet.fortios:1.1.3`
6.2.0	1.1.6	2020/12/21	`ansible-galaxy collection install fortinet.fortios:1.1.6`
6.4.0	1.0.11	2020/5/11	`ansible-galaxy collection install fortinet.fortios:1.0.11`
6.4.0	1.1.1	2020/12/4	`ansible-galaxy collection install fortinet.fortios:1.1.1`
6.4.0	1.1.4	2020/12/7	`ansible-galaxy collection install fortinet.fortios:1.1.4`
6.4.0	1.1.7	2020/12/21	`ansible-galaxy collection install fortinet.fortios:1.1.7`

Note: Use `-f` option (i.e. `ansible-galaxy collection install -f fortinet.fortios:x.x.x`) to renew your existing local installation.

CHAPTER 2

Install FortiOS Ansible Galaxy

This document explains how to install the FortiOS Ansible Galaxy Collection.

2.1 Install Python3

- Follow steps in https://www.python.org/ to install Python3 on your host.

2.2 Install Ansible Core

- Follow instructions in https://docs.ansible.com/ansible/latest/installation_guide/intro_installation.html to install Ansible
- The Ansible core version requirement: >= 2.9.0

2.3 Install FortiOS Galaxy Collection

The FortiOS Ansible Galaxy supports multilple FortiOS major releases, you can install the latest collection by default via command `ansible-galaxy collection install fortinet.fortios`. you can also choose another galaxy version to match your FortiOS device.

Please see the versionig notes for more recently released collections and install the ones which are marked `latest` for your devices.

CHAPTER 3

Run Your First Playbook

This document explains how to run your first FortiOS Ansible playbook.

With FortiOS Galaxy collection, you are always recommended to run FortiOS module in `httpapi` manner. The first step is to prepare your host inventory with which you can use `ansible-vault` to encrypt or decrypt your secrets for the sake of confidentiality.

3.1 Prepare host inventory

in our case we create a file named `hosts`:

```
[fortigates]
fortigate01 ansible_host=192.168.190.130 ansible_user="admin" ansible_password=
↪"password"
fortigate02 ansible_host=192.168.190.131 ansible_user="admin" ansible_password=
↪"password"
fortigate03 ansible_host=192.168.190.132 fortios_access_token=<your access token>

[fortigates:vars]
ansible_network_os=fortinet.fortios.fortios
```

FortiOS supports two ways to authenticate Ansible: `ansible_user` and `ansible_password` pair based; `fortios_access_token` access token based. Access token based way is prefered as it is safer without any password explosure and access token guarantees request source location is wanted.

for how to generate an API token, visit page FortiOS API Spec.

3.2 Write the playbook

in the example: `test.yml` we are going to modify the fortigate device's hostname:

```
- hosts: fortigate03
  connection: httpapi
  collections:
  - fortinet.fortios
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
   - name: Configure global attributes.
     fortios_system_global:
        vdom:  "{{ vdom }}"
        access_token: "{{ fortios_access_token }}" #if you prefer access token based
↪authentication, add this line.
        system_global:
            hostname: 'CustomHostName'
```

there are several options which might need you special care:

- **connection** : `httpapi` is preferred.
- **collections** : The namespace must be `fortinet.fortios`
- **ansible_httpapi_use_ssl** and **ansible_httpapi_port**: by default when your fortiOS device is licensed, the https is enabled. there is one exception: uploading vmlicence to a newly installed FOS instance, where you should set `ansible_httpapi_use_ssl: no` and `ansible_httpapi_port: 80`. Please see Import licence to FOS for more details.

3.3 Run the playbook

```
ansible-playbook -i hosts test.yml
```

you can also observe the verbose output by adding option at the tail: `-vvv`.

CHAPTER 4

Frequently Asked Questions (FAQ)

4.1 What's Access Token?

Access Token here is an API token which is used to authenticate an API request, an api token is associated with an API user once generated in FortiOS. FortiOS Ansible supports api token based authentication, please see Run Your Playbook for how to use `access_token` in Ansible playbook.

Sometimes we also want to dynamically generate an API token via FortiOS ansible module, we have a demo to show how to generate an API token:

```
# to customize privileges for the API user, we can also define an accprofile via␣
↪module fortios_system_accprofile.
- name: Create An API User if not present
  fortios_system_api_user:
     vdom: 'root'
     state: 'present'
     system_api_user:
          name: 'AnsibleAPIUser'
          accprofile: 'super_admin' # This is predefined privilege profile.
          vdom:
             - name: 'root'
          trusthost:
              - id: '1'
                ipv4_trusthost: '192.168.190.0 255.255.255.0'

# To reference the generated token, we can use notation "{{ tokeninfo.meta.results.
↪access_token  }}"in further tasks or keep it somewhere in disk.
- name: Generate The API token
  fortios_monitor:
     vdom: 'root'
     selector: 'generate-key.system.api-user'
```

(continues on next page)

(continued from previous page)

```
    params:
        api-user: 'AnsibleAPIUser'
  register: tokeninfo

- name: do another api request with newly generated access_token
  fortios_configuration_fact:
    access_token: "{{ tokeninfo.meta.results.access_token  }}"
    vdom: 'root'
    selector: 'system_status'
```

4.2 How To Backup And Restore FOS?

Legacy module `fortios_system_config_backup_restore` is deprecated since 2.0.0, new modules are available for doing equivalent jobs. New modules are desined to be very flexible, that requires us to combine modules to do complex task.

Note: operation backup and restore needs administrative privilege, better not choose access token based authentication.

4.2.1 Backup settings to local file.

FortiOS Ansible collection doesn't provide any modules for local file operations, here we use builtin `copy` module to copy plain configuration text into a file.

```
- name: Backup a virtual domain.
  fortios_monitor_fact:
    selector: 'system_config_backup'
    vdom: 'root'
    params:
        scope: 'global'
  register: backupinfo

- name: Save the backup information.
  copy:
    content: '{{ backupinfo.meta.raw }}'
    dest: './local.backup'
```

4.2.2 Restore settings from local file.

FortiOS only accepts base64 encoded text, the configuration text must be encoded before being uploaded.

```
- name: Restore from file.
  fortios_monitor:
    selector: 'restore.system.config'
    vdom: 'root'
    params:
        scope: 'global'
        source: 'upload'
        vdom: 'root'
        file_content: "{{ lookup( 'file', './local.backup') | string | b64encode }}"
```

4.2.3 Restore settings from other sources.

no matter what source is, just make sure content is encoded.

```
- name: Backup a virtual domain.
  fortios_monitor_fact:
     selector: 'system_config_backup'
     vdom: 'root'
     params:
         scope: 'global'
  register: backupinfo

- name: Restore from intermediate result.
  fortios_monitor:
     selector: 'restore.system.config'
     vdom: 'root'
     params:
         scope: 'global'
         source: 'upload'
         vdom: 'root'
         file_content: "{{ backupinfo.meta.raw | string | b64encode}}"
```

For more options to restore, see module `fortios_monitor` and its selector `restore.system.config`, for more options to backup, see module `fortios_monitor_fact` and its selector `system_config_backup`.

4.3 How To Import A License?

4.3.1 Import a license for a newly installed FOS instance.

Make sure the active management port allows access to http service by setting `allowaccess`.

```
FortiGate-VM64 # show system interface port1
config system interface
edit "port1"
    set vdom "root"
    set mode dhcp
    set allowaccess ping https ssh http fgfm
    set type physical
    set snmp-index 1
next
end
```

Then run the following playbook to upload licence for the first time:

```
- hosts: fortigate_new
  connection: httpapi
  collections:
   - fortinet.fortios
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: no
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 80
   ansible_command_timeout: 5
  tasks:
```

(continues on next page)

(continued from previous page)

```
  - name: Upload the license to the newly installed FGT device
    fortios_monitor:
        vdom: "{{ vdom }}"
        selector: 'upload.system.vmlicense'
        params:
            file_content: "{{ lookup( 'file', './FGVM02TM20012347.lic') | string |␣
↪b64encode }}"
    ignore_errors: True
```

In the example, we put license file `FGVM02TM20012347.lic` under current working directory.

Once FOS accepts a valid licence, it reboots immediately and the connection terminates suddenly, as a result, we must not regard connection timeout as errors, we'd better ignore connection timeout exception. and the default connection timeout is 30 seconds, better make it smaller.

Access token based authentication is not allowed in initial license import

4.3.2 Renew a license for a licence-ready FOS instance.

To renew the license for a running FOS instance, we don't have to use http service (by default, after license is activated, http service is redirected to https service, which causes problems for Ansible). by setting `ansible_httpapi_use_ssl` to `True` and `ansible_httpapi_port` to `443`, the task can normally upload the license.

Renewing a license can use access token based authentication as long as associated API user has admin privilege to upload license.

4.4 How does Ansible work with login banner?

4.4.1 what's login banner?

FOS puts a barrier in login process if pre- and(or) post- login bannner are enabled, and ansible authentication is restricted: **only access token based authentication is allowed**.

4.4.2 How to safely generate access token?

For Ansible FOS login banner usage, there could be a `deadlock` if one the of following cases apprears:

- I don't have an API user or access token.
- I have an access token but it has expired.

upon such deadlocks, there is no other way but to disable banners and (re)generate one.

To generate an access token in advance, please see How To Generate Access Token Dynamically, and please do token generation with Ansible with all the login banners disabled(it's not necessay to disable banners if we generate access token from WEB UI).

```
FGVM02TM20012347 # config system global
FGVM02TM20012347 (global) # set post-login-banner disable
FGVM02TM20012347 (global) # set pre-login-banner disable
FGVM02TM20012347 (global) # end
FGVM02TM20012347 #
```

4.4.3 where to keep generated access token?

Normally if we generate an access token from WEB UI, we may put it in inventory file as a variable `fortios_access_token`:

```
[fortigates]
fortigate01 ansible_host=<the address of the host> fortios_access_token=<the access␣
↪token>
```

we can encrypt the inventory file through ansible tool `ansible-vault`, thus avoiding token leaks.

To automate token (re)generation, we might also want to keep it somewhere else in local storage. An example is given below to show how to save and re-use a token later:

```
- name: Generate The API token
  fortios_monitor:
     vdom: 'root'
     selector: 'generate-key.system.api-user'
     params:
         api-user: 'AnsibleAPIUser'
  register: tokeninfo

- name: Save the API token
  copy:
     content: "{{ tokeninfo.meta.results.access_token }}"
     dest: './access_token.save'
```

then in subsequent tasks, we read the token directly from saved file:

```
vars:
 vdom: "root"
 ansible_httpapi_use_ssl: yes
 ansible_httpapi_validate_certs: no
 ansible_httpapi_port: 443
 saved_access_token: "{{ lookup( 'file', './access_token.save') | string }}"

tasks:
 - name: do another api request with saved access_token
   fortios_configuration_fact:
     access_token: "{{ saved_access_token }}"
     vdom: 'root'
     selector: 'system_status'
```

Caveats: saved access token is not guarded by Ansible, once leaked, others may access the FOS illegally. one way to restrict illegal access is to limit source localtion in ipv4_trusthost during creating the API users.

4.5 How To Work With Raw FotiOS CLI?

In FortiOS, some CLI commands are not exported as RestAPI, as a reasult, Ansible FortiOS collection has no identical module for those CLI commands. And FortiOS default CLI shell is not a standard Unix shell, so Ansible builtin modules like `shell` and `command` are of no use. To work this around in Ansible, we use a verbose but very efficient and flexible way to execute some FortiOS CLI commands from Ansible.

Below are two examples of the template:

Append a firewall address member to a group using append command:

```
- hosts: localhost
  vars:
    # ======================== Below are crenditials to connect to Fortigate␣
↪Device========
    fgt_host: '192.168.190.171'
    fgt_user: 'admin'
    fgt_pass: 'password'

    firewall_group_name: 'firwalladdressgroup0'
    firewall_address_name: 'firewalladdress0'
    #␣
↪=============================================================================================
    script_path: '/tmp/fgt.shell.task'
  tasks:
   - name: Prepare The Shell Scrit Template.
     raw: |
            cat > {{script_path }} << EOF_OUTER
            # /bin/bash
            # Please make sure tool sshpass is installed. e.g. on Debian/Ubuntu, apt-
↪get install sshpass.
            # Optionally you can pass some parameters.
            # The character `a` at second line below is to avoid post-login-banner␣
↪barrier.
            sshpass -p '{{ fgt_pass }}' ssh -o StrictHostKeyChecking=no {{ fgt_user }}
↪@{{ fgt_host }} <<EOF
            a
            # ======================= Edit Your Commands Below␣
↪============================================
            config firewall addrgrp
            edit '\$1'
            append member '\$2'
            end
            #␣
↪=============================================================================================================
            EOF
            EOF_OUTER


   - name: Execute The Cli Commands.
     raw: |
            chmod +x {{ script_path }} && {{ script_path }} '{{ firewall_group_name }}
↪' '{{ firewall_address_name }}'
     args:
       executable: /bin/bash
```

Enable/Disable pre-/post- login banners

```
- hosts: localhost
  vars:
    # ======================== Below are crenditials to connect to Fortigate␣
↪Device========
    fgt_host: '192.168.190.171'
    fgt_user: 'admin'
    fgt_pass: 'password'
    #␣
↪=============================================================================================
    script_path: '/tmp/fgt.shell.task'
```

(continues on next page)

(continued from previous page)

```
  tasks:
   - name: Prepare The Shell Scrit Template.
     raw: |
            cat > {{script_path }} << EOF_OUTER
            # /bin/bash
            # Please make sure tool sshpass is installed. e.g. on Debian/Ubuntu, apt-
↪get install sshpass.
            # Optionally you can pass some parameters.
            # The character `a` at second line below is to avoid post-login-banner␣
↪barrier.
            sshpass -p '{{ fgt_pass }}' ssh -o StrictHostKeyChecking=no {{ fgt_user }}
↪@{{ fgt_host }} <<EOF
            a
            # ====================== Edit Your Commands Below␣
↪=============================================
            config system global
            set pre-login-banner '\${1:-disbale}'
            set post-login-banner '\${2:-disable}'
            end
            #␣
↪=============================================================================================================
            EOF
            EOF_OUTER


   - name: Execute The Cli Commands, e.g. enable pre- and post- login banner.
     raw: |
            chmod +x {{ script_path }} && {{ script_path }} enable enable
     args:
       executable: /bin/bash
```

4.6 How to use the set_fact module in a task?

In Ansible, there's an important module that works with variables and is used to get or set variable values, which is `set_fact`. This module is used to set new variables and these variables are available to subsequent plays in a playbook. Using set_fact, we can store the value after preparing it on the fly using certain task.

The following example will show you how set_fact module can be used in a task to configure the firewall address group.

Configuring the firewall address group with a string type of variable that contains all the grouped firewall addresses:

```
- hosts: fortigateslab
  connection: httpapi
  collections:
    - fortinet.fortios
  vars:
    vdom: 'root'
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
    demo_input: 'login.microsoftonline.com, login.microsoft.com, login.windows.net'
    demo_members: []
```

(continues on next page)

(continued from previous page)

```
tasks:
  - name: Process input content
    set_fact:
      demo_members: "{{ demo_members + [{'name': item.strip(' ')}] }}"
    with_items:
      - "{{demo_input.split(',')}}"

  - debug:
      var: demo_members

  - name: Configure Firewall Schedule Recurring
    fortios_firewall_addrgrp:
      vdom:  '{{ vdom }}'
      state: 'present'
      enable_log: True
      access_token: '{{ fortios_access_token }}'
      firewall_addrgrp:
        name: 'group_1'
        comment: 'created via Ansible'
        visibility: 'enable'
        member: '{{ demo_members }}'
```

In the example, the first task is preprocessing the input content. Specifically, it splits the input content with comma to get a list of the firewall addresses. Then it appends the each address to the variable demo_members. So the demo_members variable can be assigned to the variable members in the subsequent play.

CHAPTER 5

Get Help

5.1 Technical and Commuity Support

You can get support from Fortinet Technical Assistance Center.

For Ansible common issue, you can also get support from the community

5.2 Filing issues.

You can get support from the community engineering team via filing an issue in git issues page

CHAPTER 6

Configuration Modules

6.1 fortios_alertemail_setting – Configure alert email settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.1.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify alertemail feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.1.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.1.3 FortiOS Version Compatibility

6.1.4 Parameters

6.1.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.1.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure alert email settings.
    fortios_alertemail_setting:
      vdom:  "{{ vdom }}"
      alertemail_setting:
        admin_login_logs: "enable"
        alert_interval: "4"
        amc_interface_bypass_mode: "enable"
        antivirus_logs: "enable"
        configuration_changes_logs: "enable"
        critical_interval: "8"
        debug_interval: "9"
        email_interval: "10"
        emergency_interval: "11"
        error_interval: "12"
        FDS_license_expiring_days: "13"
        FDS_license_expiring_warning: "enable"
        FDS_update_logs: "enable"
        filter_mode: "category"
        FIPS_CC_errors: "enable"
        firewall_authentication_failure_logs: "enable"
        fortiguard_log_quota_warning: "enable"
        FSSO_disconnect_logs: "enable"
        HA_logs: "enable"
        information_interval: "22"
        IPS_logs: "enable"
```

(continues on next page)

(continued from previous page)

```
        IPsec_errors_logs: "enable"
        local_disk_usage: "25"
        log_disk_usage_warning: "enable"
        mailto1: "<your_own_value>"
        mailto2: "<your_own_value>"
        mailto3: "<your_own_value>"
        notification_interval: "30"
        PPP_errors_logs: "enable"
        severity: "emergency"
        ssh_logs: "enable"
        sslvpn_authentication_errors_logs: "enable"
        username: "<your_own_value>"
        violation_traffic_logs: "enable"
        warning_interval: "37"
        webfilter_logs: "enable"
```

6.1.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.1.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.1.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.2 fortios_antivirus_heuristic – Configure global heuristic options in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.2.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify antivirus feature and heuristic category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.2.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.2.3 FortiOS Version Compatibility

6.2.4 Parameters

6.2.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.2.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure global heuristic options.
```

(continues on next page)

(continued from previous page)

```
    fortios_antivirus_heuristic:
      vdom:  "{{ vdom }}"
      antivirus_heuristic:
        mode: "pass"
```

6.2.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.2.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.2.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.3 fortios_antivirus_mms_checksum – Configure MMS content checksum list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.3.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify antivirus feature and mms_checksum category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.3.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.3.3 FortiOS Version Compatibility

6.3.4 Parameters

6.3.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.3.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure MMS content checksum list.
    fortios_antivirus_mms_checksum:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      antivirus_mms_checksum:
        comment: "Optional comments."
        entries:
         -
            checksum: "<your_own_value>"
            name: "default_name_6"
            status: "enable"
```

(continues on next page)

(continued from previous page)

```
        id:  "8"
        name: "default_name_9"
```

6.3.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.3.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.3.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.4 fortios_antivirus_notification – Configure AntiVirus notification lists in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.4.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify antivirus feature and notification category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.4.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.4.3 FortiOS Version Compatibility

6.4.4 Parameters

6.4.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.4.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure AntiVirus notification lists.
    fortios_antivirus_notification:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      antivirus_notification:
        comment: "Optional comments."
        entries:
         -
            name: "default_name_5"
            prefix: "enable"
            status: "enable"
        id:  "8"
        name: "default_name_9"
```

6.4.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.4.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.4.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.5 fortios_antivirus_profile – Configure AntiVirus profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.5.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify antivirus feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.5.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.5.3 FortiOS Version Compatibility

6.5.4 Parameters

6.5.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.5.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure AntiVirus profiles.
    fortios_antivirus_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      antivirus_profile:
        analytics_accept_filetype: "3 (source dlp.filepattern.id)"
        analytics_bl_filetype: "4 (source dlp.filepattern.id)"
        analytics_db: "disable"
        analytics_ignore_filetype: "6 (source dlp.filepattern.id)"
        analytics_max_upload: "7"
        analytics_wl_filetype: "8 (source dlp.filepattern.id)"
        av_block_log: "enable"
        av_virus_log: "enable"
        cifs:
            archive_block: "encrypted"
            archive_log: "encrypted"
            av_scan: "disable"
            emulator: "enable"
            external_blocklist: "disable"
            options: "scan"
            outbreak_prevention: "disabled"
            quarantine: "disable"
        comment: "Comment."
        content_disarm:
```

(continues on next page)

(continued from previous page)

```
            cover_page: "disable"
            detect_only: "disable"
            error_action: "block"
            office_action: "disable"
            office_dde: "disable"
            office_embed: "disable"
            office_hylink: "disable"
            office_linked: "disable"
            office_macro: "disable"
            original_file_destination: "fortisandbox"
            pdf_act_form: "disable"
            pdf_act_gotor: "disable"
            pdf_act_java: "disable"
            pdf_act_launch: "disable"
            pdf_act_movie: "disable"
            pdf_act_sound: "disable"
            pdf_embedfile: "disable"
            pdf_hyperlink: "disable"
            pdf_javacode: "disable"
        ems_threat_feed: "disable"
        extended_log: "enable"
        external_blocklist:
         -
            name: "default_name_44 (source system.external-resource.name)"
        external_blocklist_archive_scan: "disable"
        external_blocklist_enable_all: "disable"
        feature_set: "flow"
        ftgd_analytics: "disable"
        ftp:
            archive_block: "encrypted"
            archive_log: "encrypted"
            av_scan: "disable"
            emulator: "enable"
            external_blocklist: "disable"
            options: "scan"
            outbreak_prevention: "disabled"
            quarantine: "disable"
        http:
            archive_block: "encrypted"
            archive_log: "encrypted"
            av_scan: "disable"
            content_disarm: "disable"
            emulator: "enable"
            external_blocklist: "disable"
            options: "scan"
            outbreak_prevention: "disabled"
            quarantine: "disable"
        imap:
            archive_block: "encrypted"
            archive_log: "encrypted"
            av_scan: "disable"
            content_disarm: "disable"
            emulator: "enable"
            executables: "default"
            external_blocklist: "disable"
            options: "scan"
            outbreak_prevention: "disabled"
```

(continues on next page)

(continued from previous page)

```
            quarantine: "disable"
        inspection_mode: "proxy"
        mapi:
            archive_block: "encrypted"
            archive_log: "encrypted"
            av_scan: "disable"
            emulator: "enable"
            executables: "default"
            external_blocklist: "disable"
            options: "scan"
            outbreak_prevention: "disabled"
            quarantine: "disable"
        mobile_malware_db: "disable"
        nac_quar:
            expiry: "<your_own_value>"
            infected: "none"
            log: "enable"
        name: "default_name_95"
        nntp:
            archive_block: "encrypted"
            archive_log: "encrypted"
            av_scan: "disable"
            emulator: "enable"
            external_blocklist: "disable"
            options: "scan"
            outbreak_prevention: "disabled"
            quarantine: "disable"
        outbreak_prevention:
            external_blocklist: "disable"
            ftgd_service: "disable"
        outbreak_prevention_archive_scan: "disable"
        pop3:
            archive_block: "encrypted"
            archive_log: "encrypted"
            av_scan: "disable"
            content_disarm: "disable"
            emulator: "enable"
            executables: "default"
            external_blocklist: "disable"
            options: "scan"
            outbreak_prevention: "disabled"
            quarantine: "disable"
        replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
        scan_mode: "quick"
        smb:
            archive_block: "encrypted"
            archive_log: "encrypted"
            emulator: "enable"
            options: "scan"
            outbreak_prevention: "disabled"
        smtp:
            archive_block: "encrypted"
            archive_log: "encrypted"
            av_scan: "disable"
            content_disarm: "disable"
            emulator: "enable"
            executables: "default"
```

(continues on next page)

(continued from previous page)

```
            external_blocklist: "disable"
            options: "scan"
            outbreak_prevention: "disabled"
            quarantine: "disable"
        ssh:
            archive_block: "encrypted"
            archive_log: "encrypted"
            av_scan: "disable"
            emulator: "enable"
            external_blocklist: "disable"
            options: "scan"
            outbreak_prevention: "disabled"
            quarantine: "disable"
```

6.5.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.5.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.5.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.6 fortios_antivirus_quarantine – Configure quarantine options in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.6.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify antivirus feature and quarantine category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.6.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.6.3 FortiOS Version Compatibility

6.6.4 Parameters

6.6.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.6.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure quarantine options.
    fortios_antivirus_quarantine:
      vdom:  "{{ vdom }}"
      antivirus_quarantine:
        agelimit: "3"
```

(continues on next page)

(continued from previous page)

```
        destination: "NULL"
        drop_blocked: "imap"
        drop_heuristic: "imap"
        drop_infected: "imap"
        drop_intercepted: "imap"
        lowspace: "drop-new"
        maxfilesize: "10"
        quarantine_quota: "11"
        store_blocked: "imap"
        store_heuristic: "imap"
        store_infected: "imap"
        store_intercepted: "imap"
```

6.6.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.6.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.6.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.7 fortios_antivirus_settings – Configure AntiVirus settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.7.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify antivirus feature and settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.7.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.7.3 FortiOS Version Compatibility

6.7.4 Parameters

6.7.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.7.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure AntiVirus settings.
    fortios_antivirus_settings:
      vdom:  "{{ vdom }}"
      antivirus_settings:
        default_db: "normal"
```

(continues on next page)

(continued from previous page)

```
        grayware: "enable"
        machine_learning_detection: "enable"
        override_timeout: "6"
        use_extreme_db: "enable"
```

6.7.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.7.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.7.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.8 fortios_application_custom – Configure custom application signatures in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.8.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify application feature and custom category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.8.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.8.3 FortiOS Version Compatibility

6.8.4 Parameters

6.8.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.8.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure custom application signatures.
    fortios_application_custom:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      application_custom:
        behavior: "<your_own_value>"
        category: "4"
        comment: "Comment."
        id:  "6"
        name: "default_name_7"
        protocol: "<your_own_value>"
        signature: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        tag: "<your_own_value>"
        technology: "<your_own_value>"
        vendor: "<your_own_value>"
```

6.8.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.8.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.8.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.9 fortios_application_group – Configure firewall application groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.9.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify application feature and group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.9.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.9.3 FortiOS Version Compatibility

6.9.4 Parameters

6.9.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.9.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure firewall application groups.
    fortios_application_group:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      application_group:
        application:
         -
            id:  "4"
        behavior: "<your_own_value>"
        category:
         -
            id:  "7"
        comment: "Comment"
        name: "default_name_9"
        popularity: "1"
        protocols: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        risk:
         -
            level: "13"
        technology: "<your_own_value>"
        type: "application"
        vendor: "<your_own_value>"
```

6.9.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.9.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.9.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.10 fortios_application_list – Configure application control lists in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.10.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify application feature and list category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.10.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.10.3 FortiOS Version Compatibility

6.10.4 Parameters

6.10.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.10.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure application control lists.
    fortios_application_list:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      application_list:
        app_replacemsg: "disable"
        comment: "comments"
        control_default_network_services: "disable"
        deep_app_inspection: "disable"
        default_network_services:
```

(continues on next page)

(continued from previous page)

```
        -
            id:  "8"
            port: "9"
            services: "http"
            violation_action: "pass"
        enforce_default_app_port: "disable"
        entries:
         -
            action: "pass"
            application:
             -
                id:  "16"
            behavior: "<your_own_value>"
            category:
             -
                id:  "19"
            exclusion:
             -
                id:  "21"
            id:  "22"
            log: "disable"
            log_packet: "disable"
            parameters:
             -
                id:  "26"
                members:
                 -
                    id:  "28"
                    name: "default_name_29"
                    value: "<your_own_value>"
                value: "<your_own_value>"
            per_ip_shaper: "<your_own_value> (source firewall.shaper.per-ip-shaper.
↪name)"
            popularity: "1"
            protocols: "<your_own_value>"
            quarantine: "none"
            quarantine_expiry: "<your_own_value>"
            quarantine_log: "disable"
            rate_count: "38"
            rate_duration: "39"
            rate_mode: "periodical"
            rate_track: "none"
            risk:
             -
                level: "43"
            session_ttl: "44"
            shaper: "<your_own_value> (source firewall.shaper.traffic-shaper.name)"
            shaper_reverse: "<your_own_value> (source firewall.shaper.traffic-shaper.
↪name)"
            sub_category:
             -
                id:  "48"
            technology: "<your_own_value>"
            vendor: "<your_own_value>"
        extended_log: "enable"
        force_inclusion_ssl_di_sigs: "disable"
        name: "default_name_53"
```

(continues on next page)

(continued from previous page)

```
        options: "allow-dns"
        other_application_action: "pass"
        other_application_log: "disable"
        p2p_black_list: "skype"
        p2p_block_list: "skype"
        replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
        unknown_application_action: "pass"
        unknown_application_log: "disable"
```

6.10.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.10.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.10.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.11 fortios_application_name – Configure application signatures in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.11.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify application feature and name category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.11.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.11.3 FortiOS Version Compatibility

6.11.4 Parameters

6.11.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.11.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure application signatures.
    fortios_application_name:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      application_name:
        behavior: "<your_own_value>"
        category: "4"
        id:  "5"
        metadata:
```

(continues on next page)

(continued from previous page)

```
        -
            id:  "7"
            metaid: "8"
            valueid: "9"
        name: "default_name_10"
        parameter: "<your_own_value>"
        parameters:
         -
            default value: "<your_own_value>"
            name: "default_name_14"
        popularity: "15"
        protocol: "<your_own_value>"
        risk: "17"
        sub_category: "18"
        technology: "<your_own_value>"
        vendor: "<your_own_value>"
        weight: "21"
```

6.11.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.11.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.11.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.12 fortios_application_rule_settings – Configure application rule settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.12.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify application feature and rule_settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.12.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.12.3 FortiOS Version Compatibility

6.12.4 Parameters

6.12.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.12.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure application rule settings.
  fortios_application_rule_settings:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    application_rule_settings:
      id:  "3"
```

6.12.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.12.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.12.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.13 fortios_authentication_rule – Configure Authentication Rules in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.13.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify authentication feature and rule category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.13.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.13.3 FortiOS Version Compatibility

6.13.4 Parameters

6.13.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.13.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Authentication Rules.
    fortios_authentication_rule:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      authentication_rule:
        active_auth_method: "<your_own_value> (source authentication.scheme.name)"
        comments: "<your_own_value>"
        dstaddr:
         -
```

(continues on next page)

(continued from previous page)

```
            name: "default_name_6 (source firewall.address.name firewall.addrgrp.name␣
↪firewall.proxy-address.name firewall.proxy-addrgrp.name system
              .external-resource.name)"
        dstaddr6:
          -
            name: "default_name_8 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        ip_based: "enable"
        name: "default_name_10"
        protocol: "http"
        srcaddr:
          -
            name: "default_name_13 (source firewall.address.name firewall.addrgrp.
↪name firewall.proxy-address.name firewall.proxy-addrgrp.name)"
        srcaddr6:
          -
            name: "default_name_15 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        srcintf:
          -
            name: "default_name_17 (source system.interface.name system.zone.name)"
        sso_auth_method: "<your_own_value> (source authentication.scheme.name)"
        status: "enable"
        transaction_based: "enable"
        web_auth_cookie: "enable"
        web_portal: "enable"
```

6.13.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.13.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.13.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.14 fortios_authentication_scheme – Configure Authentication Schemes in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.14.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify authentication feature and scheme category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.14.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.14.3 FortiOS Version Compatibility

6.14.4 Parameters

6.14.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.14.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Authentication Schemes.
    fortios_authentication_scheme:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      authentication_scheme:
        domain_controller: "<your_own_value> (source user.domain-controller.name)"
        ems_device_owner: "enable"
        fsso_agent_for_ntlm: "<your_own_value> (source user.fsso.name)"
        fsso_guest: "enable"
        kerberos_keytab: "<your_own_value> (source user.krb-keytab.name)"
        method: "ntlm"
        name: "default_name_9"
        negotiate_ntlm: "enable"
        require_tfa: "enable"
        saml_server: "<your_own_value> (source user.saml.name)"
        saml_timeout: "13"
        ssh_ca: "<your_own_value> (source firewall.ssh.local-ca.name)"
        user_database:
         -
            name: "default_name_16 (source system.datasource.name user.radius.name␣
↪user.tacacs+.name user.ldap.name user.group.name)"
```

6.14.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.14.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.14.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.15 fortios_authentication_setting – Configure authentication setting in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.15.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify authentication feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.15.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.15.3 FortiOS Version Compatibility

6.15.4 Parameters

6.15.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.15.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure authentication setting.
    fortios_authentication_setting:
      vdom:  "{{ vdom }}"
      authentication_setting:
        active_auth_scheme: "<your_own_value> (source authentication.scheme.name)"
        auth_https: "enable"
        captive_portal: "<your_own_value> (source firewall.address.name)"
        captive_portal_ip: "<your_own_value>"
        captive_portal_ip6: "<your_own_value>"
        captive_portal_port: "8"
        captive_portal_ssl_port: "9"
        captive_portal_type: "fqdn"
        captive_portal6: "<your_own_value> (source firewall.address6.name)"
        dev_range:
         -
            name: "default_name_13 (source firewall.address.name firewall.addrgrp.
↪name)"
        sso_auth_scheme: "<your_own_value> (source authentication.scheme.name)"
        user_cert_ca:
         -
            name: "default_name_16 (source vpn.certificate.ca.name)"
```

6.15.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.15.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.15.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.16 fortios_certificate_ca – CA certificate in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.16.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify certificate feature and ca category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.16.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.16.3 FortiOS Version Compatibility

6.16.4 Parameters

6.16.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.16.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: CA certificate.
    fortios_certificate_ca:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      certificate_ca:
        auto_update_days: "3"
        auto_update_days_warning: "4"
        ca: "<your_own_value>"
        last_updated: "6"
        name: "default_name_7"
        range: "global"
        scep_url: "<your_own_value>"
        source: "factory"
        source_ip: "84.230.14.43"
        ssl_inspection_trusted: "enable"
        trusted: "enable"
```

6.16.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.16.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.16.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.17 fortios_certificate_crl – Certificate Revocation List as a PEM file in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.17.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify certificate feature and crl category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.17.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.17.3 FortiOS Version Compatibility

6.17.4 Parameters

6.17.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.17.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Certificate Revocation List as a PEM file.
    fortios_certificate_crl:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      certificate_crl:
        crl: "<your_own_value>"
        http_url: "<your_own_value>"
        last_updated: "5"
        ldap_password: "<your_own_value>"
        ldap_server: "<your_own_value>"
        ldap_username: "<your_own_value>"
        name: "default_name_9"
        range: "global"
        scep_cert: "<your_own_value> (source certificate.local.name)"
        scep_url: "<your_own_value>"
        source: "factory"
        source_ip: "84.230.14.43"
        update_interval: "15"
        update_vdom: "<your_own_value> (source system.vdom.name)"
```

6.17.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.17.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.17.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.18 fortios_certificate_local – Local keys and certificates in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.18.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify certificate feature and local category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.18.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.18.3 FortiOS Version Compatibility

6.18.4 Parameters

6.18.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.18.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Local keys and certificates.
    fortios_certificate_local:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      certificate_local:
        acme_ca_url: "<your_own_value>"
        acme_domain: "<your_own_value>"
        acme_email: "<your_own_value>"
        acme_renew_window: "6"
        acme_rsa_key_size: "7"
        auto_regenerate_days: "8"
        auto_regenerate_days_warning: "9"
        ca_identifier:  "myId_10"
        certificate: "<your_own_value>"
        cmp_path: "<your_own_value>"
        cmp_regeneration_method: "keyupate"
        cmp_server: "<your_own_value>"
        cmp_server_cert: "<your_own_value> (source certificate.ca.name)"
        comments: "<your_own_value>"
        csr: "<your_own_value>"
        enroll_protocol: "none"
        ike_localid: "<your_own_value>"
        ike_localid_type: "asn1dn"
        last_updated: "21"
        name: "default_name_22"
        name_encoding: "printable"
        password: "<your_own_value>"
        private_key: "<your_own_value>"
        range: "global"
        scep_password: "<your_own_value>"
        scep_url: "<your_own_value>"
        source: "factory"
        source_ip: "84.230.14.43"
        state: "<your_own_value>"
```

6.18.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.18.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.18.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.19 fortios_certificate_remote – Remote certificate as a PEM file in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.19.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify certificate feature and remote category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.19.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.19.3 FortiOS Version Compatibility

6.19.4 Parameters

6.19.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

---

6.19.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Remote certificate as a PEM file.
    fortios_certificate_remote:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      certificate_remote:
        name: "default_name_3"
        range: "global"
        remote: "<your_own_value>"
        source: "factory"
```

6.19.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.19.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.19.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.20 fortios_cifs_domain_controller – Define known domain controller servers in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.20.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify cifs feature and domain_controller category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.20.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.20.3 FortiOS Version Compatibility

6.20.4 Parameters

6.20.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.20.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Define known domain controller servers.
    fortios_cifs_domain_controller:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      cifs_domain_controller:
        domain_name: "<your_own_value>"
        ip: "<your_own_value>"
        ip6: "<your_own_value>"
        password: "<your_own_value>"
        port: "7"
        server_name: "<your_own_value>"
        username: "<your_own_value>"
```

6.20.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.20.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.20.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.21 fortios_cifs_profile – Configure CIFS profile in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.21.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify cifs feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.21.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.21.3 FortiOS Version Compatibility

6.21.4 Parameters

6.21.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.21.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure CIFS profile.
    fortios_cifs_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      cifs_profile:
        domain_controller: "<your_own_value> (source cifs.domain-controller.server-
↪name)"
        file_filter:
            entries:
             -
                action: "log"
                comment: "Comment."
                direction: "incoming"
                file_type:
                 -
                    name: "default_name_10 (source antivirus.filetype.name)"
                filter: "<your_own_value>"
                protocol: "cifs"
            log: "enable"
            status: "enable"
        name: "default_name_15"
        server_credential_type: "none"
        server_keytab:
         -
            keytab: "<your_own_value>"
            password: "<your_own_value>"
            principal: "<your_own_value>"
```

6.21.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.21.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.21.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.22 fortios_credential_store_domain_controller – Define known domain controller servers in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.22.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify credential_store feature and domain_controller category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.22.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.22.3 FortiOS Version Compatibility

6.22.4 Parameters

6.22.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.22.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Define known domain controller servers.
    fortios_credential_store_domain_controller:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      credential_store_domain_controller:
        domain_name: "<your_own_value>"
        hostname: "myhostname"
        ip: "<your_own_value>"
        ip6: "<your_own_value>"
        password: "<your_own_value>"
        port: "8"
        server_name: "<your_own_value>"
        username: "<your_own_value>"
```

6.22.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.22.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.22.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.23 fortios_dlp_filepattern – Configure file patterns used by DLP blocking in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.23.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify dlp feature and filepattern category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.23.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.23.3 FortiOS Version Compatibility

6.23.4 Parameters

6.23.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.23.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure file patterns used by DLP blocking.
    fortios_dlp_filepattern:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      dlp_filepattern:
        comment: "Optional comments."
        entries:
         -
            file_type: "7z"
            filter_type: "pattern"
            pattern: "<your_own_value>"
        id:  "8"
        name: "default_name_9"
```

6.23.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.23.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.23.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.24 fortios_dlp_fp_doc_source – Create a DLP fingerprint database by allowing the FortiGate to access a file server containing files from which to create fingerprints in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.24.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify dlp feature and fp_doc_source category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.24.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.24.3 FortiOS Version Compatibility

6.24.4 Parameters

6.24.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.24.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Create a DLP fingerprint database by allowing the FortiGate to access a␣
↪file server containing files from which to create fingerprints.
    fortios_dlp_fp_doc_source:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      dlp_fp_doc_source:
        date: "3"
        file_path: "<your_own_value>"
        file_pattern: "<your_own_value>"
        keep_modified: "enable"
        name: "default_name_7"
        password: "<your_own_value>"
        period: "none"
        remove_deleted: "enable"
        scan_on_creation: "enable"
        scan_subdirectories: "enable"
        sensitivity: "<your_own_value> (source dlp.fp-sensitivity.name)"
        server: "192.168.100.40"
        server_type: "samba"
        tod_hour: "16"
        tod_min: "17"
        username: "<your_own_value>"
        vdom: "mgmt"
        weekday: "sunday"
```

6.24.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.24.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.24.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.25 fortios_dlp_fp_sensitivity – Create self-explanatory DLP sensitivity levels to be used when setting sensitivity under config fp-doc-source in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.25.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify dlp feature and fp_sensitivity category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.25.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.25.3 FortiOS Version Compatibility

6.25.4 Parameters

6.25.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.25.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Create self-explanatory DLP sensitivity levels to be used when setting␣
↪sensitivity under config fp-doc-source.
    fortios_dlp_fp_sensitivity:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      dlp_fp_sensitivity:
        name: "default_name_3"
```

6.25.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.25.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.25.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.26 fortios_dlp_sensitivity – Create self-explanatory DLP sensitivity levels to be used when setting sensitivity under config fp-doc-source in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.26.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify dlp feature and sensitivity category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.26.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.26.3 FortiOS Version Compatibility

6.26.4 Parameters

6.26.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.26.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Create self-explanatory DLP sensitivity levels to be used when setting␣
↪sensitivity under config fp-doc-source.
    fortios_dlp_sensitivity:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      dlp_sensitivity:
        name: "default_name_3"
```

6.26.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.26.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.26.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.27 fortios_dlp_sensor – Configure DLP sensors in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.27.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify dlp feature and sensor category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.27.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.27.3 FortiOS Version Compatibility

6.27.4 Parameters

6.27.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.27.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure DLP sensors.
    fortios_dlp_sensor:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      dlp_sensor:
        comment: "Comment."
        dlp_log: "enable"
        extended_log: "enable"
        feature_set: "flow"
        filter:
         -
            action: "allow"
            archive: "disable"
            company_identifier:  "myId_10"
            expiry: "<your_own_value>"
            file_size: "12"
            file_type: "13 (source dlp.filepattern.id)"
            filter_by: "credit-card"
            fp_sensitivity:
             -
                name: "default_name_16 (source dlp.fp-sensitivity.name)"
            id:  "17"
            match_percentage: "18"
            name: "default_name_19"
            proto: "smtp"
            regexp: "<your_own_value>"
            sensitivity:
             -
                name: "default_name_23 (source dlp.sensitivity.name)"
            severity: "info"
            type: "file"
        flow_based: "enable"
        full_archive_proto: "smtp"
        nac_quar_log: "enable"
        name: "default_name_29"
        options: "<your_own_value>"
        replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
        summary_proto: "smtp"
```

6.27.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.27.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.27.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.28 fortios_dlp_settings – Designate logical storage for DLP fingerprint database in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.28.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify dlp feature and settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.28.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.28.3 FortiOS Version Compatibility

6.28.4 Parameters

6.28.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.28.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Designate logical storage for DLP fingerprint database.
    fortios_dlp_settings:
      vdom:  "{{ vdom }}"
      dlp_settings:
        cache_mem_percent: "3"
        chunk_size: "4"
        db_mode: "stop-adding"
        size: "6"
        storage_device: "<your_own_value> (source system.storage.name)"
```

6.28.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.28.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.28.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.29 fortios_dnsfilter_domain_filter – Configure DNS domain filters in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.29.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify dnsfilter feature and domain_filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.29.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.29.3 FortiOS Version Compatibility

6.29.4 Parameters

6.29.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.29.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure DNS domain filters.
    fortios_dnsfilter_domain_filter:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      dnsfilter_domain_filter:
        comment: "Optional comments."
        entries:
         -
            action: "block"
            domain: "<your_own_value>"
            id:  "7"
            status: "enable"
            type: "simple"
        id:  "10"
        name: "default_name_11"
```

6.29.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.29.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.29.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.30 fortios_dnsfilter_profile – Configure DNS domain filter profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.30.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify dnsfilter feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.30.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.30.3 FortiOS Version Compatibility

6.30.4 Parameters

6.30.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.30.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure DNS domain filter profiles.
    fortios_dnsfilter_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      dnsfilter_profile:
        block_action: "block"
        block_botnet: "disable"
        comment: "Comment."
        dns_translation:
         -
            addr_type: "ipv4"
            dst: "<your_own_value>"
            dst6: "<your_own_value>"
            id:  "10"
            netmask: "<your_own_value>"
            prefix: "12"
            src: "<your_own_value>"
            src6: "<your_own_value>"
            status: "enable"
        domain_filter:
            domain_filter_table: "17 (source dnsfilter.domain-filter.id)"
        external_ip_blocklist:
         -
            name: "default_name_19 (source system.external-resource.name)"
        ftgd_dns:
            filters:
             -
                action: "block"
                category: "23"
                id:  "24"
                log: "enable"
            options: "error-allow"
        log_all_domain: "enable"
        name: "default_name_28"
        redirect_portal: "<your_own_value>"
        redirect_portal6: "<your_own_value>"
        safe_search: "disable"
        sdns_domain_log: "enable"
        sdns_ftgd_err_log: "enable"
        youtube_restrict: "strict"
```

6.30.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.30.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.30.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.31 fortios_dpdk_cpus – Configure CPUs enabled to run engines in each DPDK stage in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.31.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify dpdk feature and cpus category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.31.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.31.3 FortiOS Version Compatibility

6.31.4 Parameters

6.31.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.31.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure CPUs enabled to run engines in each DPDK stage.
    fortios_dpdk_cpus:
      vdom:  "{{ vdom }}"
      dpdk_cpus:
        ips_cpus: "<your_own_value>"
        rx_cpus: "<your_own_value>"
        tx_cpus: "<your_own_value>"
        vnp_cpus: "<your_own_value>"
```

6.31.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.31.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.31.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.32 fortios_dpdk_global – Configure global DPDK options in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.32.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify dpdk feature and global category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.32.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.32.3 FortiOS Version Compatibility

6.32.4 Parameters

6.32.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.32.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure global DPDK options.
    fortios_dpdk_global:
      vdom:  "{{ vdom }}"
      dpdk_global:
        elasticbuffer: "disable"
        hugepage_percentage: "4"
        interface:
         -
            interface_name: "<your_own_value> (source system.interface.name)"
        mbufpool_percentage: "7"
        multiqueue: "disable"
        per_session_accounting: "disable"
        sleep_on_idle: "disable"
        status: "disable"
```

6.32.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.32.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.32.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.33 fortios_emailfilter_block_allow_list – Configure anti-spam block/allow list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.33.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify emailfilter feature and block_allow_list category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.33.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.33.3 FortiOS Version Compatibility

6.33.4 Parameters

6.33.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.33.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure anti-spam block/allow list.
    fortios_emailfilter_block_allow_list:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      emailfilter_block_allow_list:
        comment: "Optional comments."
        entries:
         -
            action: "reject"
            addr_type: "ipv4"
            email_pattern: "<your_own_value>"
            id:  "8"
            ip4_subnet: "<your_own_value>"
            ip6_subnet: "<your_own_value>"
            pattern_type: "wildcard"
            status: "enable"
            type: "ip"
        id:  "14"
        name: "default_name_15"
```

6.33.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.33.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.33.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.34 fortios_emailfilter_bwl – Configure anti-spam black/white list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.34.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify emailfilter feature and bwl category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.34.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.34.3 FortiOS Version Compatibility

6.34.4 Parameters

6.34.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.34.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure anti-spam black/white list.
    fortios_emailfilter_bwl:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      emailfilter_bwl:
        comment: "Optional comments."
        entries:
         -
            action: "reject"
            addr_type: "ipv4"
            email_pattern: "<your_own_value>"
            id:  "8"
            ip4_subnet: "<your_own_value>"
            ip6_subnet: "<your_own_value>"
            pattern_type: "wildcard"
            status: "enable"
            type: "ip"
        id:  "14"
        name: "default_name_15"
```

6.34.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.34.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.34.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.35 fortios_emailfilter_bword – Configure AntiSpam banned word list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.35.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify emailfilter feature and bword category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.35.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.35.3 FortiOS Version Compatibility

6.35.4 Parameters

6.35.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.35.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure AntiSpam banned word list.
    fortios_emailfilter_bword:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      emailfilter_bword:
        comment: "Optional comments."
        entries:
         -
            action: "spam"
            id:  "6"
            language: "western"
            pattern: "<your_own_value>"
            pattern_type: "wildcard"
            score: "10"
            status: "enable"
            where: "subject"
        id:  "13"
        name: "default_name_14"
```

6.35.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.35.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.35.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.36 fortios_emailfilter_dnsbl – Configure AntiSpam DNSBL/ORBL in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.36.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify emailfilter feature and dnsbl category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.36.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.36.3 FortiOS Version Compatibility

6.36.4 Parameters

6.36.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.36.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure AntiSpam DNSBL/ORBL.
    fortios_emailfilter_dnsbl:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      emailfilter_dnsbl:
        comment: "Optional comments."
        entries:
         -
            action: "reject"
            id:  "6"
            server: "192.168.100.40"
            status: "enable"
        id:  "9"
        name: "default_name_10"
```

6.36.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.36.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.36.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.37 fortios_emailfilter_fortishield – Configure FortiGuard - AntiSpam in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.37.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify emailfilter feature and fortishield category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.37.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.37.3 FortiOS Version Compatibility

6.37.4 Parameters

6.37.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.37.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiGuard - AntiSpam.
    fortios_emailfilter_fortishield:
      vdom:  "{{ vdom }}"
      emailfilter_fortishield:
        spam_submit_force: "enable"
        spam_submit_srv: "<your_own_value>"
        spam_submit_txt2htm: "enable"
```

6.37.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.37.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.37.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.38 fortios_emailfilter_iptrust – Configure AntiSpam IP trust in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.38.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify emailfilter feature and iptrust category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.38.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.38.3 FortiOS Version Compatibility

6.38.4 Parameters

6.38.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.38.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure AntiSpam IP trust.
    fortios_emailfilter_iptrust:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      emailfilter_iptrust:
        comment: "Optional comments."
        entries:
         -
            addr_type: "ipv4"
            id:  "6"
            ip4_subnet: "<your_own_value>"
            ip6_subnet: "<your_own_value>"
            status: "enable"
        id:  "10"
        name: "default_name_11"
```

6.38.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.38.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.38.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.39 fortios_emailfilter_mheader – Configure AntiSpam MIME header in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.39.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify emailfilter feature and mheader category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.39.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.39.3 FortiOS Version Compatibility

6.39.4 Parameters

6.39.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.39.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure AntiSpam MIME header.
    fortios_emailfilter_mheader:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      emailfilter_mheader:
        comment: "Optional comments."
        entries:
         -
            action: "spam"
            fieldbody: "<your_own_value>"
            fieldname: "<your_own_value>"
            id:  "8"
            pattern_type: "wildcard"
            status: "enable"
        id:  "11"
        name: "default_name_12"
```

6.39.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.39.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.39.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.40 fortios_emailfilter_options – Configure AntiSpam options in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.40.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify emailfilter feature and options category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.40.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.40.3 FortiOS Version Compatibility

6.40.4 Parameters

6.40.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.40.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure AntiSpam options.
    fortios_emailfilter_options:
      vdom:  "{{ vdom }}"
      emailfilter_options:
        dns_timeout: "3"
```

6.40.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.40.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.40.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.41 fortios_emailfilter_profile – Configure Email Filter profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.41.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify emailfilter feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.41.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.41.3 FortiOS Version Compatibility

6.41.4 Parameters

6.41.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.41.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Email Filter profiles.
    fortios_emailfilter_profile:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    state: "present"
    access_token: "<your_own_value>"
    emailfilter_profile:
      comment: "Comment."
      external: "enable"
      feature_set: "flow"
      file_filter:
          entries:
           -
              action: "log"
              comment: "Comment."
              file_type:
               -
                  name: "default_name_11 (source antivirus.filetype.name)"
              filter: "<your_own_value>"
              password_protected: "yes"
              protocol: "smtp"
          log: "enable"
          scan_archive_contents: "enable"
          status: "enable"
      gmail:
          log: "enable"
          log_all: "disable"
      imap:
          action: "pass"
          log: "enable"
          log_all: "disable"
          tag_msg: "<your_own_value>"
          tag_type: "subject"
      mapi:
          action: "pass"
          log: "enable"
          log_all: "disable"
      msn_hotmail:
          log: "enable"
          log_all: "disable"
      name: "default_name_34"
      options: "bannedword"
      other_webmails:
          log_all: "disable"
      pop3:
          action: "pass"
          log: "enable"
          log_all: "disable"
          tag_msg: "<your_own_value>"
          tag_type: "subject"
      replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
      smtp:
          action: "pass"
          hdrip: "disable"
          local_override: "disable"
          log: "enable"
          log_all: "disable"
          tag_msg: "<your_own_value>"
          tag_type: "subject"
      spam_bal_table: "53 (source emailfilter.block-allow-list.id)"
      spam_bwl_table: "54 (source emailfilter.bwl.id)"
```

(continues on next page)

(continued from previous page)

```
        spam_bword_table: "55 (source emailfilter.bword.id)"
        spam_bword_threshold: "56"
        spam_filtering: "enable"
        spam_iptrust_table: "58 (source emailfilter.iptrust.id)"
        spam_log: "disable"
        spam_log_fortiguard_response: "disable"
        spam_mheader_table: "61 (source emailfilter.mheader.id)"
        spam_rbl_table: "62 (source emailfilter.dnsbl.id)"
        yahoo_mail:
            log: "enable"
            log_all: "disable"
```

6.41.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.41.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.41.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.42 fortios_endpoint_control_client – Configure endpoint control client lists in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.42.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify endpoint_control feature and client category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.42.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.42.3 FortiOS Version Compatibility

6.42.4 Parameters

6.42.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.42.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure endpoint control client lists.
    fortios_endpoint_control_client:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      endpoint_control_client:
```

(continues on next page)

(continued from previous page)

```
        ad_groups: "<your_own_value>"
        ftcl_uid: "<your_own_value>"
        id:  "5"
        info: "<your_own_value>"
        src_ip: "<your_own_value>"
        src_mac: "<your_own_value>"
```

6.42.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.42.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.42.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.43 fortios_endpoint_control_fctems – Configure FortiClient Enterprise Management Server (EMS) entries in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.43.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify endpoint_control feature and fctems category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.43.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.43.3 FortiOS Version Compatibility

6.43.4 Parameters

6.43.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.43.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiClient Enterprise Management Server (EMS) entries.
    fortios_endpoint_control_fctems:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      endpoint_control_fctems:
        admin_password: "<your_own_value>"
        admin_username: "<your_own_value>"
        call_timeout: "5"
        capabilities: "fabric-auth"
```

(continues on next page)

(continued from previous page)

```
        certificate: "<your_own_value> (source certificate.remote.name)"
        cloud_server_type: "production"
        fortinetone_cloud_authentication: "enable"
        https_port: "10"
        name: "default_name_11"
        pull_avatars: "enable"
        pull_malware_hash: "enable"
        pull_sysinfo: "enable"
        pull_tags: "enable"
        pull_vulnerabilities: "enable"
        serial_number: "<your_own_value>"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        status_check_interval: "20"
        websocket_override: "enable"
```

6.43.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.43.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.43.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.44 fortios_endpoint_control_forticlient_ems – Configure FortiClient Enterprise Management Server (EMS) entries in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.44.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify endpoint_control feature and forticlient_ems category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.44.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.44.3 FortiOS Version Compatibility

6.44.4 Parameters

6.44.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.44.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure FortiClient Enterprise Management Server (EMS) entries.
  fortios_endpoint_control_forticlient_ems:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    endpoint_control_forticlient_ems:
      address: "<your_own_value> (source firewall.address.name)"
      admin_password: "<your_own_value>"
      admin_type: "Windows"
      admin_username: "<your_own_value>"
      https_port: "7"
      listen_port: "8"
      name: "default_name_9"
      rest_api_auth: "disable"
      serial_number: "<your_own_value>"
      upload_port: "12"
```

6.44.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.44.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.44.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.45 fortios_endpoint_control_forticlient_registration_sync – Configure FortiClient registration synchronization settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.45.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify endpoint_control feature and forticlient_registration_sync category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.45.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.45.3 FortiOS Version Compatibility

6.45.4 Parameters

6.45.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.45.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure FortiClient registration synchronization settings.
  fortios_endpoint_control_forticlient_registration_sync:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    endpoint_control_forticlient_registration_sync:
      peer_ip: "<your_own_value>"
      peer_name: "<your_own_value>"
```

6.45.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.45.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.45.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.46 fortios_endpoint_control_profile – Configure FortiClient endpoint control profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.46.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify endpoint_control feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.46.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.46.3 FortiOS Version Compatibility

6.46.4 Parameters

6.46.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.46.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiClient endpoint control profiles.
    fortios_endpoint_control_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      endpoint_control_profile:
```

(continues on next page)

(continued from previous page)

```
        description: "<your_own_value>"
        device_groups:
         -
            name: "default_name_5 (source user.device-group.name user.device-category.
↪name)"
        forticlient_android_settings:
            disable_wf_when_protected: "enable"
            forticlient_advanced_vpn: "enable"
            forticlient_advanced_vpn_buffer: "<your_own_value>"
            forticlient_vpn_provisioning: "enable"
            forticlient_vpn_settings:
             -
                auth_method: "psk"
                name: "default_name_13"
                preshared_key: "<your_own_value>"
                remote_gw: "<your_own_value>"
                sslvpn_access_port: "16"
                sslvpn_require_certificate: "enable"
                type: "ipsec"
            forticlient_wf: "enable"
            forticlient_wf_profile: "<your_own_value> (source webfilter.profile.name)"
        forticlient_ios_settings:
            client_vpn_provisioning: "enable"
            client_vpn_settings:
             -
                auth_method: "psk"
                name: "default_name_25"
                preshared_key: "<your_own_value>"
                remote_gw: "<your_own_value>"
                sslvpn_access_port: "28"
                sslvpn_require_certificate: "enable"
                type: "ipsec"
                vpn_configuration_content: "<your_own_value>"
                vpn_configuration_name: "<your_own_value>"
            configuration_content: "<your_own_value>"
            configuration_name: "<your_own_value>"
            disable_wf_when_protected: "enable"
            distribute_configuration_profile: "enable"
            forticlient_wf: "enable"
            forticlient_wf_profile: "<your_own_value> (source webfilter.profile.name)"
        forticlient_winmac_settings:
            av_realtime_protection: "enable"
            av_signature_up_to_date: "enable"
            forticlient_application_firewall: "enable"
            forticlient_application_firewall_list: "<your_own_value> (source␣
↪application.list.name)"
            forticlient_av: "enable"
            forticlient_ems_compliance: "enable"
            forticlient_ems_compliance_action: "block"
            forticlient_ems_entries:
             -
                name: "default_name_48 (source endpoint-control.forticlient-ems.name)"
            forticlient_linux_ver: "<your_own_value>"
            forticlient_log_upload: "enable"
            forticlient_log_upload_level: "traffic"
            forticlient_log_upload_server: "<your_own_value>"
            forticlient_mac_ver: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
            forticlient_minimum_software_version: "enable"
            forticlient_operating_system:
             -
                id:  "56"
                os_name: "<your_own_value>"
                os_type: "custom"
            forticlient_own_file:
             -
                file: "<your_own_value>"
                id:  "61"
            forticlient_registration_compliance_action: "block"
            forticlient_registry_entry:
             -
                id:  "64"
                registry_entry: "<your_own_value>"
            forticlient_running_app:
             -
                app_name: "<your_own_value>"
                app_sha256_signature: "<your_own_value>"
                app_sha256_signature2: "<your_own_value>"
                app_sha256_signature3: "<your_own_value>"
                app_sha256_signature4: "<your_own_value>"
                application_check_rule: "present"
                id:  "73"
                process_name: "<your_own_value>"
                process_name2: "<your_own_value>"
                process_name3: "<your_own_value>"
                process_name4: "<your_own_value>"
            forticlient_security_posture: "enable"
            forticlient_security_posture_compliance_action: "block"
            forticlient_system_compliance: "enable"
            forticlient_system_compliance_action: "block"
            forticlient_vuln_scan: "enable"
            forticlient_vuln_scan_compliance_action: "block"
            forticlient_vuln_scan_enforce: "critical"
            forticlient_vuln_scan_enforce_grace: "85"
            forticlient_vuln_scan_exempt: "enable"
            forticlient_wf: "enable"
            forticlient_wf_profile: "<your_own_value> (source webfilter.profile.name)"
            forticlient_win_ver: "<your_own_value>"
            os_av_software_installed: "enable"
            sandbox_address: "<your_own_value>"
            sandbox_analysis: "enable"
        on_net_addr:
         -
            name: "default_name_94 (source firewall.address.name firewall.addrgrp.
↪name)"
        profile_name: "<your_own_value>"
        replacemsg_override_group: "<your_own_value> (source system.replacemsg-group.
↪name)"
        src_addr:
         -
            name: "default_name_98 (source firewall.address.name firewall.addrgrp.
↪name)"
        user_groups:
         -
            name: "default_name_100 (source user.group.name)"
```

(continues on next page)

(continued from previous page)

```
        users:
         -
            name: "default_name_102 (source user.local.name)"
```

6.46.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.46.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.46.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.47 fortios_endpoint_control_registered_forticlient – Registered FortiClient list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.47.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify endpoint_control feature and registered_forticlient category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.47.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.47.3 FortiOS Version Compatibility

6.47.4 Parameters

6.47.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.47.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Registered FortiClient list.
    fortios_endpoint_control_registered_forticlient:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      endpoint_control_registered_forticlient:
        flag: "3"
        ip: "<your_own_value>"
        mac: "<your_own_value>"
        reg_fortigate: "<your_own_value>"
        status: "7"
        uid: "<your_own_value>"
        vdom: "<your_own_value>"
```

6.47.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.47.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.47.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.48 fortios_endpoint_control_settings – Configure endpoint control settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.48.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify endpoint_control feature and settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.48.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.48.3 FortiOS Version Compatibility

6.48.4 Parameters

6.48.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.48.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure endpoint control settings.
    fortios_endpoint_control_settings:
      vdom:  "{{ vdom }}"
      endpoint_control_settings:
        download_custom_link: "<your_own_value>"
        download_location: "fortiguard"
        forticlient_avdb_update_interval: "5"
        forticlient_dereg_unsupported_client: "enable"
        forticlient_disconnect_unsupported_client: "enable"
        forticlient_ems_rest_api_call_timeout: "8"
        forticlient_keepalive_interval: "9"
        forticlient_offline_grace: "enable"
        forticlient_offline_grace_interval: "11"
        forticlient_reg_key: "<your_own_value>"
        forticlient_reg_key_enforce: "enable"
        forticlient_reg_timeout: "14"
        forticlient_sys_update_interval: "15"
        forticlient_user_avatar: "enable"
        forticlient_warning_interval: "17"
```

6.48.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.48.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.48.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.49 fortios_extender_controller_dataplan – FortiExtender dataplan configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.49.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify extender_controller feature and dataplan category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.49.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.49.3 FortiOS Version Compatibility

6.49.4 Parameters

6.49.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.49.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: FortiExtender dataplan configuration.
    fortios_extender_controller_dataplan:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      extender_controller_dataplan:
        apn: "<your_own_value>"
        APN: "<your_own_value>"
        auth_type: "none"
        billing_date: "6"
        capacity: "7"
        carrier: "<your_own_value>"
        iccid: "<your_own_value>"
        modem_id: "modem1"
        monthly_fee: "11"
        name: "default_name_12"
        overage: "disable"
        password: "<your_own_value>"
        pdn: "ipv4-only"
        PDN: "ipv4-only"
        preferred_subnet: "17"
        private_network: "disable"
        signal_period: "19"
        signal_threshold: "20"
        slot: "sim1"
        type: "carrier"
        username: "<your_own_value>"
```

6.49.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.49.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.49.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.50 fortios_extender_controller_extender – Extender controller configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.50.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify extender_controller feature and extender category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.50.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.50.3 FortiOS Version Compatibility

6.50.4 Parameters

6.50.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.50.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Extender controller configuration.
    fortios_extender_controller_extender:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      extender_controller_extender:
        aaa_shared_secret: "<your_own_value>"
        access_point_name: "<your_own_value>"
        admin: "disable"
        at_dial_script: "<your_own_value>"
        authorized: "disable"
        billing_start_day: "8"
        cdma_aaa_spi: "<your_own_value>"
        cdma_ha_spi: "<your_own_value>"
        cdma_nai: "<your_own_value>"
        conn_status: "12"
        controller_report:
            interval: "14"
            signal_threshold: "15"
            status: "disable"
        description: "<your_own_value>"
        dial_mode: "dial-on-demand"
        dial_status: "19"
        ext_name: "<your_own_value>"
        ha_shared_secret: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        id:  "22"
        ifname: "<your_own_value> (source system.interface.name)"
        initiated_update: "enable"
        login_password: "<your_own_value>"
        mode: "standalone"
        modem_passwd: "<your_own_value>"
        modem_type: "cdma"
        modem1:
            auto_switch:
                dataplan: "disable"
                disconnect: "disable"
                disconnect_period: "33"
                disconnect_threshold: "34"
                signal: "disable"
                switch_back: "time"
                switch_back_time: "<your_own_value>"
                switch_back_timer: "38"
            conn_status: "39"
            default_sim: "sim1"
            gps: "disable"
            ifname: "<your_own_value> (source system.interface.name)"
            preferred_carrier: "<your_own_value>"
            redundant_intf: "<your_own_value>"
            redundant_mode: "disable"
            sim1_pin: "disable"
            sim1_pin_code: "<your_own_value>"
            sim2_pin: "disable"
            sim2_pin_code: "<your_own_value>"
        modem2:
            auto_switch:
                dataplan: "disable"
                disconnect: "disable"
                disconnect_period: "54"
                disconnect_threshold: "55"
                signal: "disable"
                switch_back: "time"
                switch_back_time: "<your_own_value>"
                switch_back_timer: "59"
            conn_status: "60"
            default_sim: "sim1"
            gps: "disable"
            ifname: "<your_own_value> (source system.interface.name)"
            preferred_carrier: "<your_own_value>"
            redundant_intf: "<your_own_value>"
            redundant_mode: "disable"
            sim1_pin: "disable"
            sim1_pin_code: "<your_own_value>"
            sim2_pin: "disable"
            sim2_pin_code: "<your_own_value>"
        multi_mode: "auto"
        name: "default_name_72"
        ppp_auth_protocol: "auto"
        ppp_echo_request: "enable"
        ppp_password: "<your_own_value>"
        ppp_username: "<your_own_value>"
        primary_ha: "<your_own_value>"
        quota_limit_mb: "78"
```

(continues on next page)

(continued from previous page)

```
        redial: "none"
        redundant_intf: "<your_own_value>"
        roaming: "enable"
        role: "none"
        secondary_ha: "<your_own_value>"
        sim_pin: "<your_own_value>"
        vdom: "85"
        wimax_auth_protocol: "tls"
        wimax_carrier: "<your_own_value>"
        wimax_realm: "<your_own_value>"
```

6.50.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.50.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.50.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.51 fortios_extender_extender_info – Display extender struct information in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.51.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify extender feature and extender_info category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.51.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.51.3 FortiOS Version Compatibility

6.51.4 Parameters

6.51.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.51.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Display extender struct information.
    fortios_extender_extender_info:
      vdom:  "{{ vdom }}"
      extender_extender_info:
        <sn>: "<your_own_value> (source extender-controller.extender.id)"
```

6.51.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.51.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.51.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.52 fortios_extender_lte_carrier_by_mcc_mnc – Display extender modem carrier based on MCC and MNC in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.52.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify extender feature and lte_carrier_by_mcc_mnc category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.52.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.52.3 FortiOS Version Compatibility

6.52.4 Parameters

6.52.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.52.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Display extender modem carrier based on MCC and MNC.
    fortios_extender_lte_carrier_by_mcc_mnc:
      vdom:  "{{ vdom }}"
      extender_lte_carrier_by_mcc_mnc:
        <sn>: "<your_own_value> (source extender-controller.extender.id)"
```

6.52.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.52.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.52.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.53 fortios_extender_lte_carrier_list – Display extender modem carrier list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.53.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify extender feature and lte_carrier_list category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.53.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.53.3 FortiOS Version Compatibility

6.53.4 Parameters

6.53.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.53.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Display extender modem carrier list.
    fortios_extender_lte_carrier_list:
      vdom:  "{{ vdom }}"
      extender_lte_carrier_list:
        <sn>: "<your_own_value> (source extender-controller.extender.id)"
```

6.53.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.53.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.53.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.54 fortios_extender_modem_status – Display detailed extender modem status in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.54.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify extender feature and modem_status category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.54.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.54.3 FortiOS Version Compatibility

6.54.4 Parameters

6.54.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.54.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Display detailed extender modem status.
    fortios_extender_modem_status:
      vdom:  "{{ vdom }}"
      extender_modem_status:
        <sn>: "<your_own_value> (source extender-controller.extender.id)"
```

6.54.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.54.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.54.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.55 fortios_extender_sys_info – Display detailed extender system information in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.55.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify extender feature and sys_info category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.55.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.55.3 FortiOS Version Compatibility

6.55.4 Parameters

6.55.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.55.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Display detailed extender system information.
  fortios_extender_sys_info:
    vdom:  "{{ vdom }}"
    extender_sys_info:
      <sn>: "<your_own_value> (source extender-controller.extender.id)"
```

6.55.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.55.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.55.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.56 fortios_file_filter_profile – Configure file-filter profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.56.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify file_filter feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.56.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.56.3 FortiOS Version Compatibility

6.56.4 Parameters

6.56.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.56.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure file-filter profiles.
    fortios_file_filter_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      file_filter_profile:
        comment: "Comment."
        extended_log: "disable"
        feature_set: "flow"
        log: "disable"
        name: "default_name_7"
```

(continues on next page)

(continued from previous page)

```
        replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
        rules:
         -
            action: "log-only"
            comment: "Comment."
            direction: "incoming"
            file_type:
             -
                name: "default_name_14 (source antivirus.filetype.name)"
            name: "default_name_15"
            password_protected: "yes"
            protocol: "http"
        scan_archive_contents: "disable"
```

6.56.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.56.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.56.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.57 fortios_firewall_access_proxy – Configure Access Proxy in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.57.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and access_proxy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.57.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.57.3 FortiOS Version Compatibility

6.57.4 Parameters

6.57.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.57.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Access Proxy.
    fortios_firewall_access_proxy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
      firewall_access_proxy:
        api_gateway:
         -
            http_cookie_age: "4"
            http_cookie_domain: "<your_own_value>"
            http_cookie_domain_from_host: "disable"
            http_cookie_generation: "7"
            http_cookie_path: "<your_own_value>"
            http_cookie_share: "disable"
            https_cookie_secure: "disable"
            id:  "11"
            ldb_method: "static"
            persistence: "none"
            realservers:
             -
                address: "<your_own_value> (source firewall.address.name firewall.
↪addrgrp.name)"
                health_check: "disable"
                health_check_proto: "ping"
                http_host: "myhostname"
                id:  "19"
                ip: "<your_own_value>"
                mappedport: "<your_own_value>"
                port: "22"
                status: "active"
                weight: "24"
            saml_server: "<your_own_value> (source user.saml.name)"
            service: "http"
            ssl_algorithm: "high"
            ssl_cipher_suites:
             -
                cipher: "TLS-AES-128-GCM-SHA256"
                priority: "30"
                versions: "tls-1.0"
            ssl_dh_bits: "768"
            ssl_max_version: "tls-1.0"
            ssl_min_version: "tls-1.0"
            url_map: "<your_own_value>"
            url_map_type: "sub-string"
            virtual_host: "myhostname (source firewall.access-proxy-virtual-host.name)
↪"
        client_cert: "disable"
        empty_cert_action: "accept"
        ldb_method: "static"
        name: "default_name_41"
        realservers:
         -
            id:  "43"
            ip: "<your_own_value>"
            port: "45"
            status: "active"
            weight: "47"
        server_pubkey_auth: "disable"
        server_pubkey_auth_settings:
            auth_ca: "<your_own_value> (source firewall.ssh.local-ca.name)"
            cert_extension:
             -
```

(continues on next page)

(continued from previous page)

```
            critical: "no"
            data: "<your_own_value>"
            name: "default_name_54"
            type: "fixed"
        permit_agent_forwarding: "enable"
        permit_port_forwarding: "enable"
        permit_pty: "enable"
        permit_user_rc: "enable"
        permit_x11_forwarding: "enable"
        source_address: "enable"
    vip: "<your_own_value> (source firewall.vip.name)"
```

6.57.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.57.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.57.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.58 fortios_firewall_access_proxy_virtual_host – Configure Access Proxy virtual hosts in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.58.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and access_proxy_virtual_host category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.58.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.58.3 FortiOS Version Compatibility

6.58.4 Parameters

6.58.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.58.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Access Proxy virtual hosts.
    fortios_firewall_access_proxy_virtual_host:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_access_proxy_virtual_host:
```

(continues on next page)

(continued from previous page)

```
        host: "myhostname"
        host_type: "sub-string"
        name: "default_name_5"
        ssl_certificate: "<your_own_value> (source vpn.certificate.local.name)"
```

6.58.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.58.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.58.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.59 fortios_firewall_acl – Configure IPv4 access control list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.59.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and acl category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.59.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.59.3 FortiOS Version Compatibility

6.59.4 Parameters

6.59.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.59.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv4 access control list.
    fortios_firewall_acl:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_acl:
        comments: "<your_own_value>"
        dstaddr:
         -
            name: "default_name_5 (source firewall.address.name firewall.addrgrp.name)
↪"
        interface: "<your_own_value> (source system.zone.name system.interface.name)"
        name: "default_name_7"
```

(continues on next page)

(continued from previous page)

```
        policyid: "8"
        service:
         -
            name: "default_name_10 (source firewall.service.custom.name firewall.
↪service.group.name)"
        srcaddr:
         -
            name: "default_name_12 (source firewall.address.name firewall.addrgrp.
↪name)"
        status: "enable"
```

6.59.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.59.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.59.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.60 fortios_firewall_acl6 – Configure IPv6 access control list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.60.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and acl6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.60.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.60.3 FortiOS Version Compatibility

6.60.4 Parameters

6.60.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.60.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 access control list.
    fortios_firewall_acl6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_acl6:
```

(continues on next page)

(continued from previous page)

```
        comments: "<your_own_value>"
        dstaddr:
         -
            name: "default_name_5 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        interface: "<your_own_value> (source system.zone.name system.interface.name)"
        name: "default_name_7"
        policyid: "8"
        service:
         -
            name: "default_name_10 (source firewall.service.custom.name firewall.
↪service.group.name)"
        srcaddr:
         -
            name: "default_name_12 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        status: "enable"
```

6.60.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.60.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.60.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.61 fortios_firewall_address – Configure IPv4 addresses in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.61.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and address category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.61.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.61.3 FortiOS Version Compatibility

6.61.4 Parameters

6.61.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.61.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
  tasks:
  - name: Configure IPv4 addresses.
    fortios_firewall_address:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_address:
        allow_routing: "enable"
        associated_interface: "<your_own_value> (source system.interface.name system.
↪zone.name)"
        cache_ttl: "5"
        clearpass_spt: "unknown"
        color: "7"
        comment: "Comment."
        country: "<your_own_value>"
        end_ip: "<your_own_value>"
        end_mac: "<your_own_value>"
        epg_name: "<your_own_value>"
        fabric_object: "enable"
        filter: "<your_own_value>"
        fqdn: "<your_own_value>"
        fsso_group:
         -
            name: "default_name_17 (source user.adgrp.name)"
        interface: "<your_own_value> (source system.interface.name)"
        list:
         -
            ip: "<your_own_value>"
            net_id: "<your_own_value>"
            obj_id: "<your_own_value>"
        macaddr:
         -
            macaddr: "<your_own_value>"
        name: "default_name_25"
        node_ip_only: "enable"
        obj_id: "<your_own_value>"
        obj_tag: "<your_own_value>"
        obj_type: "ip"
        organization: "<your_own_value>"
        policy_group: "<your_own_value>"
        sdn: "aci"
        sdn_addr_type: "private"
        sdn_tag: "<your_own_value>"
        start_ip: "<your_own_value>"
        start_mac: "<your_own_value>"
        sub_type: "sdn"
        subnet: "<your_own_value>"
        subnet_name: "<your_own_value>"
        tagging:
         -
            category: "<your_own_value> (source system.object-tagging.category)"
            name: "default_name_42"
            tags:
             -
                name: "default_name_44 (source system.object-tagging.tags.name)"
        tenant: "<your_own_value>"
        type: "ipmask"
```

(continues on next page)

(continued from previous page)

```
        uuid: "<your_own_value>"
        visibility: "enable"
        wildcard: "<your_own_value>"
        wildcard_fqdn: "<your_own_value>"
```

6.61.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.61.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.61.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.62 fortios_firewall_address6 – Configure IPv6 firewall addresses in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.62.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and address6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.62.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.62.3 FortiOS Version Compatibility

6.62.4 Parameters

6.62.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.62.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 firewall addresses.
    fortios_firewall_address6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_address6:
        cache_ttl: "3"
        color: "4"
        comment: "Comment."
        country: "<your_own_value>"
        end_ip: "<your_own_value>"
        end_mac: "<your_own_value>"
        fabric_object: "enable"
```

(continues on next page)

(continued from previous page)

```
        fqdn: "<your_own_value>"
        host: "<your_own_value>"
        host_type: "any"
        ip6: "<your_own_value>"
        list:
         -
            ip: "<your_own_value>"
            net_id: "<your_own_value>"
            obj_id: "<your_own_value>"
        macaddr:
         -
            macaddr: "<your_own_value>"
        name: "default_name_20"
        obj_id: "<your_own_value>"
        sdn: "nsx"
        start_ip: "<your_own_value>"
        start_mac: "<your_own_value>"
        subnet_segment:
         -
            name: "default_name_26"
            type: "any"
            value: "<your_own_value>"
        tagging:
         -
            category: "<your_own_value> (source system.object-tagging.category)"
            name: "default_name_31"
            tags:
             -
                name: "default_name_33 (source system.object-tagging.tags.name)"
        template: "<your_own_value> (source firewall.address6-template.name)"
        type: "ipprefix"
        uuid: "<your_own_value>"
        visibility: "enable"
```

6.62.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.62.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.62.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.63 fortios_firewall_address6_template – Configure IPv6 address templates in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.63.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and address6_template category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.63.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.63.3 FortiOS Version Compatibility

6.63.4 Parameters

6.63.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.63.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 address templates.
    fortios_firewall_address6_template:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_address6_template:
        fabric_object: "enable"
        ip6: "<your_own_value>"
        name: "default_name_5"
        subnet_segment:
         -
            bits: "7"
            exclusive: "enable"
            id:  "9"
            name: "default_name_10"
            values:
             -
                name: "default_name_12"
                value: "<your_own_value>"
        subnet_segment_count: "14"
```

6.63.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.63.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.63.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.64 fortios_firewall_addrgrp – Configure IPv4 address groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.64.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and addrgrp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.64.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.64.3 FortiOS Version Compatibility

6.64.4 Parameters

6.64.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.64.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv4 address groups.
    fortios_firewall_addrgrp:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_addrgrp:
        allow_routing: "enable"
        category: "default"
        color: "5"
        comment: "Comment."
        exclude: "enable"
        exclude_member:
         -
            name: "default_name_9 (source firewall.address.name firewall.addrgrp.name)
↪"
        fabric_object: "enable"
        member:
         -
            name: "default_name_12 (source firewall.address.name firewall.addrgrp.
↪name)"
        name: "default_name_13"
        tagging:
         -
            category: "<your_own_value> (source system.object-tagging.category)"
            name: "default_name_16"
            tags:
             -
                name: "default_name_18 (source system.object-tagging.tags.name)"
        type: "default"
        uuid: "<your_own_value>"
        visibility: "enable"
```

6.64.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.64.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.64.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.65 fortios_firewall_addrgrp6 – Configure IPv6 address groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.65.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and addrgrp6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.65.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.65.3 FortiOS Version Compatibility

6.65.4 Parameters

6.65.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.65.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 address groups.
    fortios_firewall_addrgrp6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_addrgrp6:
        color: "3"
        comment: "Comment."
        fabric_object: "enable"
        member:
         -
            name: "default_name_7 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        name: "default_name_8"
        tagging:
         -
            category: "<your_own_value> (source system.object-tagging.category)"
            name: "default_name_11"
            tags:
             -
                name: "default_name_13 (source system.object-tagging.tags.name)"
        uuid: "<your_own_value>"
        visibility: "enable"
```

6.65.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.65.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.65.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.66 fortios_firewall_auth_portal – Configure firewall authentication portals in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.66.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and auth_portal category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.66.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.66.3 FortiOS Version Compatibility

6.66.4 Parameters

6.66.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

---

6.66.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure firewall authentication portals.
    fortios_firewall_auth_portal:
      vdom:  "{{ vdom }}"
      firewall_auth_portal:
        groups:
         -
            name: "default_name_4 (source user.group.name)"
        identity_based_route: "<your_own_value> (source firewall.identity-based-route.
↪name)"
        portal_addr: "<your_own_value>"
        portal_addr6: "<your_own_value>"
```

6.66.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.66.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.66.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.67 fortios_firewall_carrier_endpoint_bwl – Carrier end point black/white list tables in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.67.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and carrier_endpoint_bwl category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.67.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.67.3 FortiOS Version Compatibility

6.67.4 Parameters

6.67.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.67.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Carrier end point black/white list tables.
    fortios_firewall_carrier_endpoint_bwl:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_carrier_endpoint_bwl:
        comment: "Optional comments."
        entries:
         -
            action: "block"
            carrier_endpoint: "<your_own_value>"
            log_action: "archive"
            pattern_type: "wildcard"
            status: "enable"
        id:  "10"
        name: "default_name_11"
```

6.67.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.67.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.67.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.68 fortios_firewall_central_snat_map – Configure central SNAT policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.68.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and central_snat_map category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.68.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.68.3 FortiOS Version Compatibility

6.68.4 Parameters

6.68.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
- Adjust object order by moving self after(before) another.
- Only one of [after, before] must be specified when action is moving an object.

6.68.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure central SNAT policies.
    fortios_firewall_central_snat_map:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_central_snat_map:
        comments: "<your_own_value>"
        dst_addr:
         -
            name: "default_name_5 (source firewall.address.name firewall.addrgrp.name)
↪"
        dst_addr6:
         -
            name: "default_name_7 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        dstintf:
         -
            name: "default_name_9 (source system.interface.name system.zone.name)"
        nat: "disable"
        nat_ippool:
         -
            name: "default_name_12 (source firewall.ippool.name)"
        nat_ippool6:
         -
            name: "default_name_14 (source firewall.ippool6.name)"
        nat_port: "<your_own_value>"
        orig_addr:
         -
```

(continues on next page)

(continued from previous page)

```
            name: "default_name_17 (source firewall.address.name firewall.addrgrp.
↪name)"
        orig_addr6:
         -
            name: "default_name_19 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        orig_port: "<your_own_value>"
        policyid: "21"
        protocol: "22"
        srcintf:
         -
            name: "default_name_24 (source system.interface.name system.zone.name)"
        status: "enable"
        type: "ipv4"
        uuid: "<your_own_value>"

  - name: move firewall.central_snat_map
    fortios_firewall_central_snat_map:
      vdom:  "root"
      action: "move"
      self: "<mkey of self identifier>"
      after: "<mkey of target identifier>"
     #before: "<mkey of target identifier>"
```

6.68.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.68.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.68.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.69 fortios_firewall_city – Define city table in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.69.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and city category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.69.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.69.3 FortiOS Version Compatibility

6.69.4 Parameters

6.69.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.69.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Define city table.
    fortios_firewall_city:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_city:
        id:  "3"
        name: "default_name_4"
```

6.69.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.69.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.69.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.70 fortios_firewall_consolidated_policy – Configure consolidated IPv4/IPv6 policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.70.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_consolidated feature and policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.70.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.70.3 FortiOS Version Compatibility

6.70.4 Parameters

6.70.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.70.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
  tasks:
  - name: Configure consolidated IPv4/IPv6 policies.
    fortios_firewall_consolidated_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_consolidated_policy:
        action: "accept"
        application_list: "<your_own_value> (source application.list.name)"
        auto_asic_offload: "enable"
        av_profile: "<your_own_value> (source antivirus.profile.name)"
        captive_portal_exempt: "enable"
        cifs_profile: "<your_own_value> (source cifs.profile.name)"
        comments: "<your_own_value>"
        diffserv_forward: "enable"
        diffserv_reverse: "enable"
        diffservcode_forward: "<your_own_value>"
        diffservcode_rev: "<your_own_value>"
        dlp_sensor: "<your_own_value> (source dlp.sensor.name)"
        dnsfilter_profile: "<your_own_value> (source dnsfilter.profile.name)"
        dstaddr_negate: "enable"
        dstaddr4:
         -
            name: "default_name_18 (source firewall.address.name firewall.addrgrp.
↪name firewall.vip.name firewall.vipgrp.name system.external-resource.name)"
        dstaddr6:
         -
            name: "default_name_20 (source firewall.address6.name firewall.addrgrp6.
↪name firewall.vip6.name firewall.vipgrp6.name system.external-resource
              .name)"
        dstintf:
         -
            name: "default_name_22 (source system.interface.name system.zone.name)"
        emailfilter_profile: "<your_own_value> (source emailfilter.profile.name)"
        fixedport: "enable"
        fsso_groups:
         -
            name: "default_name_26 (source user.adgrp.name)"
        global_label: "<your_own_value>"
        groups:
         -
            name: "default_name_29 (source user.group.name)"
        http_policy_redirect: "enable"
        icap_profile: "<your_own_value> (source icap.profile.name)"
        inbound: "enable"
        inspection_mode: "proxy"
        internet_service: "enable"
        internet_service_custom:
         -
            name: "default_name_36 (source firewall.internet-service-custom.name)"
        internet_service_custom_group:
         -
            name: "default_name_38 (source firewall.internet-service-custom-group.
↪name)"
        internet_service_group:
         -
            name: "default_name_40 (source firewall.internet-service-group.name)"
```

(continues on next page)

(continued from previous page)

```
        internet_service_id:
         -
            id:  "42 (source firewall.internet-service.id)"
        internet_service_negate: "enable"
        internet_service_src: "enable"
        internet_service_src_custom:
         -
            name: "default_name_46 (source firewall.internet-service-custom.name)"
        internet_service_src_custom_group:
         -
            name: "default_name_48 (source firewall.internet-service-custom-group.
↪name)"
        internet_service_src_group:
         -
            name: "default_name_50 (source firewall.internet-service-group.name)"
        internet_service_src_id:
         -
            id:  "52 (source firewall.internet-service.id)"
        internet_service_src_negate: "enable"
        ippool: "enable"
        ips_sensor: "<your_own_value> (source ips.sensor.name)"
        logtraffic: "all"
        logtraffic_start: "enable"
        mms_profile: "<your_own_value> (source firewall.mms-profile.name)"
        name: "default_name_59"
        nat: "enable"
        outbound: "enable"
        per_ip_shaper: "<your_own_value> (source firewall.shaper.per-ip-shaper.name)"
        policyid: "63"
        poolname4:
         -
            name: "default_name_65 (source firewall.ippool.name)"
        poolname6:
         -
            name: "default_name_67 (source firewall.ippool6.name)"
        profile_group: "<your_own_value> (source firewall.profile-group.name)"
        profile_protocol_options: "<your_own_value> (source firewall.profile-protocol-
↪options.name)"
        profile_type: "single"
        schedule: "<your_own_value> (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name firewall.schedule.group.name)"
        service:
         -
            name: "default_name_73 (source firewall.service.custom.name firewall.
↪service.group.name)"
        service_negate: "enable"
        session_ttl: "75"
        srcaddr_negate: "enable"
        srcaddr4:
         -
            name: "default_name_78 (source firewall.address.name firewall.addrgrp.
↪name system.external-resource.name)"
        srcaddr6:
         -
            name: "default_name_80 (source firewall.address6.name firewall.addrgrp6.
↪name system.external-resource.name)"
        srcintf:
```

(continues on next page)

(continued from previous page)

```
        -
            name: "default_name_82 (source system.interface.name system.zone.name)"
        ssh_filter_profile: "<your_own_value> (source ssh-filter.profile.name)"
        ssh_policy_redirect: "enable"
        ssl_ssh_profile: "<your_own_value> (source firewall.ssl-ssh-profile.name)"
        status: "enable"
        tcp_mss_receiver: "87"
        tcp_mss_sender: "88"
        traffic_shaper: "<your_own_value> (source firewall.shaper.traffic-shaper.name)
↪"
        traffic_shaper_reverse: "<your_own_value> (source firewall.shaper.traffic-
↪shaper.name)"
        users:
        -
            name: "default_name_92 (source user.local.name)"
        utm_status: "enable"
        uuid: "<your_own_value>"
        voip_profile: "<your_own_value> (source voip.profile.name)"
        vpntunnel: "<your_own_value> (source vpn.ipsec.phase1.name vpn.ipsec.
↪manualkey.name)"
        waf_profile: "<your_own_value> (source waf.profile.name)"
        wanopt: "enable"
        wanopt_detection: "active"
        wanopt_passive_opt: "default"
        wanopt_peer: "<your_own_value> (source wanopt.peer.peer-host-id)"
        wanopt_profile: "<your_own_value> (source wanopt.profile.name)"
        webcache: "enable"
        webcache_https: "disable"
        webfilter_profile: "<your_own_value> (source webfilter.profile.name)"
        webproxy_forward_server: "<your_own_value> (source web-proxy.forward-server.
↪name web-proxy.forward-server-group.name)"
        webproxy_profile: "<your_own_value> (source web-proxy.profile.name)"
```

6.70.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.70.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.70.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.71 fortios_firewall_country – Define country table in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.71.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and country category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.71.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.71.3 FortiOS Version Compatibility

6.71.4 Parameters

6.71.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.71.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Define country table.
    fortios_firewall_country:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_country:
        id:  "3"
        name: "default_name_4"
        region:
         -
            id:  "6"
```

6.71.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.71.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.71.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.72 fortios_firewall_decrypted_traffic_mirror – Configure decrypted traffic mirror in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.72.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and decrypted_traffic_mirror category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.72.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.72.3 FortiOS Version Compatibility

6.72.4 Parameters

6.72.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.72.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure decrypted traffic mirror.
    fortios_firewall_decrypted_traffic_mirror:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_decrypted_traffic_mirror:
        dstmac: "<your_own_value>"
        interface:
         -
            name: "default_name_5 (source system.interface.name system.zone.name)"
        name: "default_name_6"
        traffic_source: "client"
        traffic_type: "ssl"
```

6.72.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.72.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.72.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.73 fortios_firewall_dnstranslation – Configure DNS translation in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.73.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and dnstranslation category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.73.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.73.3 FortiOS Version Compatibility

6.73.4 Parameters

6.73.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.73.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure DNS translation.
    fortios_firewall_dnstranslation:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_dnstranslation:
        dst: "<your_own_value>"
        id:  "4"
        netmask: "<your_own_value>"
        src: "<your_own_value>"
```

6.73.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.73.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.73.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.74 fortios_firewall_dos_policy – Configure IPv4 DoS policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.74.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and dos_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.74.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.74.3 FortiOS Version Compatibility

6.74.4 Parameters

6.74.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.74.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv4 DoS policies.
    fortios_firewall_dos_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_dos_policy:
        anomaly:
         -
            action: "pass"
            log: "enable"
            name: "default_name_6"
            quarantine: "none"
            quarantine_expiry: "<your_own_value>"
            quarantine_log: "disable"
            status: "disable"
            threshold: "11"
            threshold(default): "12"
        comments: "<your_own_value>"
        dstaddr:
         -
            name: "default_name_15 (source firewall.address.name firewall.addrgrp.
↪name)"
        interface: "<your_own_value> (source system.zone.name system.interface.name)"
        name: "default_name_17"
        policyid: "18"
        service:
         -
            name: "default_name_20 (source firewall.service.custom.name firewall.
↪service.group.name)"
        srcaddr:
         -
            name: "default_name_22 (source firewall.address.name firewall.addrgrp.
↪name)"
        status: "enable"
```

6.74.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.74.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.74.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.75 fortios_firewall_dos_policy6 – Configure IPv6 DoS policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.75.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and dos_policy6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.75.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.75.3 FortiOS Version Compatibility

6.75.4 Parameters

6.75.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.75.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 DoS policies.
    fortios_firewall_dos_policy6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_dos_policy6:
        anomaly:
         -
            action: "pass"
            log: "enable"
            name: "default_name_6"
            quarantine: "none"
            quarantine_expiry: "<your_own_value>"
            quarantine_log: "disable"
            status: "disable"
            threshold: "11"
            threshold(default): "12"
        comments: "<your_own_value>"
        dstaddr:
         -
            name: "default_name_15 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        interface: "<your_own_value> (source system.zone.name system.interface.name)"
        name: "default_name_17"
        policyid: "18"
        service:
         -
            name: "default_name_20 (source firewall.service.custom.name firewall.
↪service.group.name)"
        srcaddr:
         -
            name: "default_name_22 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        status: "enable"
```

6.75.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.75.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.75.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.76 fortios_firewall_gtp – Configure GTP in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.76.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and gtp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.76.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.76.3 FortiOS Version Compatibility

6.76.4 Parameters

6.76.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.76.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure GTP.
    fortios_firewall_gtp:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_gtp:
        addr_notify: "<your_own_value>"
        apn:
         -
            action: "allow"
            apnmember:
             -
                name: "default_name_7 (source gtp.apn.name gtp.apngrp.name)"
            id:  "8"
            selection_mode: "ms"
        apn_filter: "enable"
        authorized_ggsns: "<your_own_value> (source firewall.address.name firewall.
↪addrgrp.name)"
        authorized_ggsns6: "<your_own_value> (source firewall.address6.name firewall.
↪addrgrp6.name)"
        authorized_sgsns: "<your_own_value> (source firewall.address.name firewall.
↪addrgrp.name)"
        authorized_sgsns6: "<your_own_value> (source firewall.address6.name firewall.
↪addrgrp6.name)"
        comment: "Comment."
        context_id: "16"
        control_plane_message_rate_limit: "17"
        default_apn_action: "allow"
```

(continues on next page)

(continued from previous page)

```
        default_imsi_action: "allow"
        default_ip_action: "allow"
        default_noip_action: "allow"
        default_policy_action: "allow"
        denied_log: "enable"
        echo_request_interval: "24"
        extension_log: "enable"
        forwarded_log: "enable"
        global_tunnel_limit: "<your_own_value> (source gtp.tunnel-limit.name)"
        gtp_in_gtp: "allow"
        gtpu_denied_log: "enable"
        gtpu_forwarded_log: "enable"
        gtpu_log_freq: "31"
        half_close_timeout: "32"
        half_open_timeout: "33"
        handover_group: "<your_own_value> (source firewall.address.name firewall.
↪addrgrp.name)"
        handover_group6: "<your_own_value> (source firewall.address6.name firewall.
↪addrgrp6.name)"
        ie_allow_list_v0v1: "<your_own_value> (source gtp.ie-allow-list.name)"
        ie_allow_list_v2: "<your_own_value> (source gtp.ie-allow-list.name)"
        ie_remove_policy:
         -
            id:  "39"
            remove_ies: "apn-restriction"
            sgsn_addr: "<your_own_value> (source firewall.address.name firewall.
↪addrgrp.name)"
            sgsn_addr6: "<your_own_value> (source firewall.address6.name firewall.
↪addrgrp6.name)"
        ie_remover: "enable"
        ie_validation:
            apn_restriction: "enable"
            charging_gateway_addr: "enable"
            charging_ID: "enable"
            end_user_addr: "enable"
            gsn_addr: "enable"
            imei: "enable"
            imsi: "enable"
            mm_context: "enable"
            ms_tzone: "enable"
            ms_validated: "enable"
            msisdn: "enable"
            nsapi: "enable"
            pdp_context: "enable"
            qos_profile: "enable"
            rai: "enable"
            rat_type: "enable"
            reordering_required: "enable"
            selection_mode: "enable"
            uli: "enable"
        ie_white_list_v0v1: "<your_own_value> (source gtp.ie-white-list.name)"
        ie_white_list_v2: "<your_own_value> (source gtp.ie-white-list.name)"
        imsi:
         -
            action: "allow"
            apnmember:
             -
```

(continues on next page)

(continued from previous page)

```
                name: "default_name_69 (source gtp.apn.name gtp.apngrp.name)"
            id:  "70"
            mcc_mnc: "<your_own_value>"
            msisdn_prefix: "<your_own_value>"
            selection_mode: "ms"
        imsi_filter: "enable"
        interface_notify: "<your_own_value> (source system.interface.name)"
        invalid_reserved_field: "allow"
        invalid_sgsns_to_log: "<your_own_value> (source firewall.address.name␣
↪firewall.addrgrp.name)"
        invalid_sgsns6_to_log: "<your_own_value> (source firewall.address6.name␣
↪firewall.addrgrp6.name)"
        ip_filter: "enable"
        ip_policy:
         -
            action: "allow"
            dstaddr: "<your_own_value> (source firewall.address.name firewall.addrgrp.
↪name)"
            dstaddr6: "<your_own_value> (source firewall.address6.name firewall.
↪addrgrp6.name)"
            id:  "84"
            srcaddr: "<your_own_value> (source firewall.address.name firewall.addrgrp.
↪name)"
            srcaddr6: "<your_own_value> (source firewall.address6.name firewall.
↪addrgrp6.name)"
        log_freq: "87"
        log_gtpu_limit: "88"
        log_imsi_prefix: "<your_own_value>"
        log_msisdn_prefix: "<your_own_value>"
        max_message_length: "91"
        message_filter_v0v1: "<your_own_value> (source gtp.message-filter-v0v1.name)"
        message_filter_v2: "<your_own_value> (source gtp.message-filter-v2.name)"
        message_rate_limit:
            create_aa_pdp_request: "95"
            create_aa_pdp_response: "96"
            create_mbms_request: "97"
            create_mbms_response: "98"
            create_pdp_request: "99"
            create_pdp_response: "100"
            delete_aa_pdp_request: "101"
            delete_aa_pdp_response: "102"
            delete_mbms_request: "103"
            delete_mbms_response: "104"
            delete_pdp_request: "105"
            delete_pdp_response: "106"
            echo_reponse: "107"
            echo_request: "108"
            error_indication: "109"
            failure_report_request: "110"
            failure_report_response: "111"
            fwd_reloc_complete_ack: "112"
            fwd_relocation_complete: "113"
            fwd_relocation_request: "114"
            fwd_relocation_response: "115"
            fwd_srns_context: "116"
            fwd_srns_context_ack: "117"
            g_pdu: "118"
```

(continues on next page)

(continued from previous page)

```
            identification_request: "119"
            identification_response: "120"
            mbms_de_reg_request: "121"
            mbms_de_reg_response: "122"
            mbms_notify_rej_request: "123"
            mbms_notify_rej_response: "124"
            mbms_notify_request: "125"
            mbms_notify_response: "126"
            mbms_reg_request: "127"
            mbms_reg_response: "128"
            mbms_ses_start_request: "129"
            mbms_ses_start_response: "130"
            mbms_ses_stop_request: "131"
            mbms_ses_stop_response: "132"
            note_ms_request: "133"
            note_ms_response: "134"
            pdu_notify_rej_request: "135"
            pdu_notify_rej_response: "136"
            pdu_notify_request: "137"
            pdu_notify_response: "138"
            ran_info: "139"
            relocation_cancel_request: "140"
            relocation_cancel_response: "141"
            send_route_request: "142"
            send_route_response: "143"
            sgsn_context_ack: "144"
            sgsn_context_request: "145"
            sgsn_context_response: "146"
            support_ext_hdr_notify: "147"
            update_mbms_request: "148"
            update_mbms_response: "149"
            update_pdp_request: "150"
            update_pdp_response: "151"
            version_not_support: "152"
        message_rate_limit_v0:
            create_pdp_request: "154"
            delete_pdp_request: "155"
            echo_request: "156"
        message_rate_limit_v1:
            create_pdp_request: "158"
            delete_pdp_request: "159"
            echo_request: "160"
        message_rate_limit_v2:
            create_session_request: "162"
            delete_session_request: "163"
            echo_request: "164"
        min_message_length: "165"
        miss_must_ie: "allow"
        monitor_mode: "enable"
        name: "default_name_168"
        noip_filter: "enable"
        noip_policy:
         -
            action: "allow"
            end: "172"
            id:  "173"
            start: "174"
```

(continues on next page)

(continued from previous page)

```
        type: "etsi"
    out_of_state_ie: "allow"
    out_of_state_message: "allow"
    per_apn_shaper:
     -
        apn: "<your_own_value> (source gtp.apn.name)"
        id:  "180"
        rate_limit: "181"
        version: "182"
    policy:
     -
        action: "allow"
        apn_sel_mode: "ms"
        apnmember:
         -
            name: "default_name_187 (source gtp.apn.name gtp.apngrp.name)"
        id:  "188"
        imei: "<your_own_value>"
        imsi: "<your_own_value>"
        imsi_prefix: "<your_own_value>"
        max_apn_restriction: "all"
        messages: "create-req"
        msisdn: "<your_own_value>"
        msisdn_prefix: "<your_own_value>"
        rai: "<your_own_value>"
        rat_type: "any"
        uli: "<your_own_value>"
    policy_filter: "enable"
    policy_v2:
     -
        action: "allow"
        apn_sel_mode: "ms"
        apnmember:
         -
            name: "default_name_204 (source gtp.apn.name gtp.apngrp.name)"
        id:  "205"
        imsi_prefix: "<your_own_value>"
        max_apn_restriction: "all"
        mei: "<your_own_value>"
        messages: "create-ses-req"
        msisdn_prefix: "<your_own_value>"
        rat_type: "any"
        uli: "<your_own_value>"
    port_notify: "213"
    rate_limit_mode: "per-profile"
    rate_limited_log: "enable"
    rate_sampling_interval: "216"
    remove_if_echo_expires: "enable"
    remove_if_recovery_differ: "enable"
    reserved_ie: "allow"
    send_delete_when_timeout: "enable"
    send_delete_when_timeout_v2: "enable"
    spoof_src_addr: "allow"
    state_invalid_log: "enable"
    sub_second_interval: "0.5"
    sub_second_sampling: "enable"
    traffic_count_log: "enable"
```

(continues on next page)

(continued from previous page)

```
        tunnel_limit: "227"
        tunnel_limit_log: "enable"
        tunnel_timeout: "229"
        unknown_version_action: "allow"
        user_plane_message_rate_limit: "231"
        warning_threshold: "232"
```

6.76.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.76.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.76.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.77 fortios_firewall_identity_based_route – Configure identity based routing in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.77.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and identity_based_route category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.77.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.77.3 FortiOS Version Compatibility

6.77.4 Parameters

6.77.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.77.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure identity based routing.
    fortios_firewall_identity_based_route:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_identity_based_route:
        comments: "<your_own_value>"
        name: "default_name_4"
        rule:
         -
            device: "<your_own_value> (source system.interface.name)"
```

(continues on next page)

(continued from previous page)

```
            gateway: "<your_own_value>"
            groups:
             -
                name: "default_name_9 (source user.group.name)"
            id:  "10"
```

6.77.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.77.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.77.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.78 fortios_firewall_interface_policy – Configure IPv4 interface policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.78.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and interface_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.78.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.78.3 FortiOS Version Compatibility

6.78.4 Parameters

6.78.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.78.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv4 interface policies.
    fortios_firewall_interface_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_interface_policy:
        address_type: "ipv4"
        application_list: "<your_own_value> (source application.list.name)"
        application_list_status: "enable"
        av_profile: "<your_own_value> (source antivirus.profile.name)"
        av_profile_status: "enable"
        comments: "<your_own_value>"
        dlp_sensor: "<your_own_value> (source dlp.sensor.name)"
```

(continues on next page)

(continued from previous page)

```
        dlp_sensor_status: "enable"
        dsri: "enable"
        dstaddr:
         -
            name: "default_name_13 (source firewall.address.name firewall.addrgrp.
↪name)"
        emailfilter_profile: "<your_own_value> (source emailfilter.profile.name)"
        emailfilter_profile_status: "enable"
        interface: "<your_own_value> (source system.zone.name system.interface.name)"
        ips_sensor: "<your_own_value> (source ips.sensor.name)"
        ips_sensor_status: "enable"
        label: "<your_own_value>"
        logtraffic: "all"
        policyid: "21"
        scan_botnet_connections: "disable"
        service:
         -
            name: "default_name_24 (source firewall.service.custom.name firewall.
↪service.group.name)"
        spamfilter_profile: "<your_own_value> (source spamfilter.profile.name)"
        spamfilter_profile_status: "enable"
        srcaddr:
         -
            name: "default_name_28 (source firewall.address.name firewall.addrgrp.
↪name)"
        status: "enable"
        webfilter_profile: "<your_own_value> (source webfilter.profile.name)"
        webfilter_profile_status: "enable"
```

6.78.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.78.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.78.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.79 fortios_firewall_interface_policy6 – Configure IPv6 interface policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.79.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and interface_policy6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.79.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.79.3 FortiOS Version Compatibility

6.79.4 Parameters

6.79.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.79.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 interface policies.
    fortios_firewall_interface_policy6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_interface_policy6:
        address_type: "ipv4"
        application_list: "<your_own_value> (source application.list.name)"
        application_list_status: "enable"
        av_profile: "<your_own_value> (source antivirus.profile.name)"
        av_profile_status: "enable"
        comments: "<your_own_value>"
        dlp_sensor: "<your_own_value> (source dlp.sensor.name)"
        dlp_sensor_status: "enable"
        dsri: "enable"
        dstaddr6:
         -
            name: "default_name_13 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        emailfilter_profile: "<your_own_value> (source emailfilter.profile.name)"
        emailfilter_profile_status: "enable"
        interface: "<your_own_value> (source system.zone.name system.interface.name)"
        ips_sensor: "<your_own_value> (source ips.sensor.name)"
        ips_sensor_status: "enable"
        label: "<your_own_value>"
        logtraffic: "all"
        policyid: "21"
        scan_botnet_connections: "disable"
        service6:
         -
            name: "default_name_24 (source firewall.service.custom.name firewall.
↪service.group.name)"
        spamfilter_profile: "<your_own_value> (source spamfilter.profile.name)"
        spamfilter_profile_status: "enable"
        srcaddr6:
         -
            name: "default_name_28 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        status: "enable"
        webfilter_profile: "<your_own_value> (source webfilter.profile.name)"
        webfilter_profile_status: "enable"
```

6.79.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.79.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.79.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.80 fortios_firewall_internet_service – Show Internet Service application in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.80.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.80.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.80.3 FortiOS Version Compatibility

6.80.4 Parameters

6.80.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.80.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Show Internet Service application.
    fortios_firewall_internet_service:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_internet_service:
        database: "isdb"
        direction: "src"
        entry:
         -
            id:  "6"
            ip_number: "7"
            ip_range_number: "8"
            port: "9"
            protocol: "10"
        extra_ip_range_number: "11"
        icon_id: "12"
        id:  "13"
        ip_number: "14"
        ip_range_number: "15"
        name: "default_name_16"
        obsolete: "17"
        offset: "18"
        reputation: "19"
        singularity: "20"
        sld_id: "21"
```

6.80.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.80.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.80.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.81 fortios_firewall_internet_service_addition – Configure Internet Services Addition in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.81.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_addition category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.81.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.81.3 FortiOS Version Compatibility

6.81.4 Parameters

6.81.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.81.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Internet Services Addition.
    fortios_firewall_internet_service_addition:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_internet_service_addition:
        comment: "Comment."
        entry:
         -
            id:  "5"
            port_range:
             -
                end_port: "7"
                id:  "8"
                start_port: "9"
            protocol: "10"
        id:  "11 (source firewall.internet-service.id)"
```

6.81.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.81.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.81.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.82 fortios_firewall_internet_service_append – Configure additional port mappings for Internet Services in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.82.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_append category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.82.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.82.3 FortiOS Version Compatibility

6.82.4 Parameters

6.82.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.82.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure additional port mappings for Internet Services.
    fortios_firewall_internet_service_append:
      vdom:  "{{ vdom }}"
      firewall_internet_service_append:
        append_port: "3"
        match_port: "4"
```

6.82.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.82.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.82.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.83 fortios_firewall_internet_service_botnet – Show Internet Service botnet in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.83.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_botnet category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.83.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.83.3 FortiOS Version Compatibility

6.83.4 Parameters

6.83.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.83.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Show Internet Service botnet.
    fortios_firewall_internet_service_botnet:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_internet_service_botnet:
        id:  "3"
        name: "default_name_4"
```

6.83.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.83.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.83.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.84 fortios_firewall_internet_service_custom – Configure custom Internet Services in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.84.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_custom category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.84.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.84.3 FortiOS Version Compatibility

6.84.4 Parameters

6.84.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.84.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure custom Internet Services.
    fortios_firewall_internet_service_custom:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_internet_service_custom:
        comment: "Comment."
        disable_entry:
         -
            id:  "5"
            ip_range:
             -
                end_ip: "<your_own_value>"
                id:  "8"
                start_ip: "<your_own_value>"
            port: "10"
            protocol: "11"
        entry:
         -
            dst:
             -
                name: "default_name_14 (source firewall.address.name firewall.addrgrp.
↪name)"
            id:  "15"
            port_range:
             -
                end_port: "17"
                id:  "18"
                start_port: "19"
            protocol: "20"
        master_service_id: "21 (source firewall.internet-service.id)"
        name: "default_name_22"
        reputation: "23 (source firewall.internet-service-reputation.id)"
```

6.84.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.84.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.84.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.85 fortios_firewall_internet_service_custom_group – Configure custom Internet Service group in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.85.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_custom_group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.85.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.85.3 FortiOS Version Compatibility

6.85.4 Parameters

6.85.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.85.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure custom Internet Service group.
    fortios_firewall_internet_service_custom_group:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_internet_service_custom_group:
        comment: "Comment."
        member:
         -
            name: "default_name_5 (source firewall.internet-service-custom.name)"
        name: "default_name_6"
```

6.85.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.85.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.85.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.86 fortios_firewall_internet_service_definition – Configure Internet Service definition in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.86.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_definition category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.86.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.86.3 FortiOS Version Compatibility

6.86.4 Parameters

6.86.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.86.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Internet Service definition.
    fortios_firewall_internet_service_definition:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_internet_service_definition:
        entry:
         -
            category_id: "4"
            name: "default_name_5"
            port_range:
             -
                end_port: "7"
                id:  "8"
                start_port: "9"
            protocol: "10"
            seq_num: "11"
        id:  "12"
```

6.86.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.86.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.86.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.87 fortios_firewall_internet_service_extension – Configure Internet Services Extension in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.87.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_extension category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.87.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.87.3 FortiOS Version Compatibility

6.87.4 Parameters

6.87.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.87.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Internet Services Extension.
    fortios_firewall_internet_service_extension:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_internet_service_extension:
        comment: "Comment."
        disable_entry:
         -
            id:  "5"
            ip_range:
             -
                end_ip: "<your_own_value>"
                id:  "8"
                start_ip: "<your_own_value>"
            port_range:
             -
                end_port: "11"
                id:  "12"
                start_port: "13"
            protocol: "14"
        entry:
         -
            dst:
             -
                name: "default_name_17 (source firewall.address.name firewall.addrgrp.
↪name)"
            id:  "18"
            port_range:
             -
                end_port: "20"
                id:  "21"
                start_port: "22"
            protocol: "23"
        id:  "24 (source firewall.internet-service.id)"
```

6.87.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.87.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.87.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.88 fortios_firewall_internet_service_group – Configure group of Internet Service in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.88.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.88.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.88.3 FortiOS Version Compatibility

6.88.4 Parameters

6.88.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.88.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure group of Internet Service.
    fortios_firewall_internet_service_group:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_internet_service_group:
        comment: "Comment."
        direction: "source"
        member:
         -
            id:  "6 (source firewall.internet-service.id)"
            name: "default_name_7 (source firewall.internet-service-name.name)"
        name: "default_name_8"
```

6.88.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.88.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.88.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.89 fortios_firewall_internet_service_ipbl_reason – IP blacklist reason in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.89.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_ipbl_reason category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.89.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.89.3 FortiOS Version Compatibility

6.89.4 Parameters

6.89.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

---

6.89.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: IP blacklist reason.
    fortios_firewall_internet_service_ipbl_reason:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_internet_service_ipbl_reason:
        id:  "3"
        name: "default_name_4"
```

6.89.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.89.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.89.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.90 fortios_firewall_internet_service_ipbl_vendor – IP blacklist vendor in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.90.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_ipbl_vendor category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.90.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.90.3 FortiOS Version Compatibility

6.90.4 Parameters

6.90.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.90.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: IP blacklist vendor.
    fortios_firewall_internet_service_ipbl_vendor:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_internet_service_ipbl_vendor:
        id:  "3"
        name: "default_name_4"
```

6.90.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.90.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.90.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.91 fortios_firewall_internet_service_list – Internet Service list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.91.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_list category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.91.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.91.3 FortiOS Version Compatibility

6.91.4 Parameters

6.91.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.91.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Internet Service list.
  fortios_firewall_internet_service_list:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    firewall_internet_service_list:
      id:  "3"
      name: "default_name_4"
```

6.91.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.91.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.91.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.92 fortios_firewall_internet_service_name – Define internet service names in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.92.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_name category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.92.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.92.3 FortiOS Version Compatibility

6.92.4 Parameters

6.92.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.92.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Define internet service names.
    fortios_firewall_internet_service_name:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_internet_service_name:
```

(continues on next page)

(continued from previous page)

```
        city_id: "3 (source firewall.city.id)"
        country_id: "4 (source firewall.country.id)"
        internet_service_id: "5 (source firewall.internet-service.id)"
        name: "default_name_6"
        region_id: "7 (source firewall.region.id)"
        type: "default"
```

6.92.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.92.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.92.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.93 fortios_firewall_internet_service_owner – Internet Service owner in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.93.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_owner category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.93.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.93.3 FortiOS Version Compatibility

6.93.4 Parameters

6.93.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.93.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Internet Service owner.
    fortios_firewall_internet_service_owner:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_internet_service_owner:
        id:  "3"
        name: "default_name_4"
```

6.93.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.93.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.93.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.94 fortios_firewall_internet_service_reputation – Show Internet Service reputation in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.94.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_reputation category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.94.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.94.3 FortiOS Version Compatibility

6.94.4 Parameters

6.94.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.94.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Show Internet Service reputation.
    fortios_firewall_internet_service_reputation:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_internet_service_reputation:
        description: "<your_own_value>"
        id:  "4"
```

6.94.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.94.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.94.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.95 fortios_firewall_internet_service_sld – Internet Service Second Level Domain in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.95.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and internet_service_sld category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.95.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.95.3 FortiOS Version Compatibility

6.95.4 Parameters

6.95.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.95.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Internet Service Second Level Domain.
    fortios_firewall_internet_service_sld:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_internet_service_sld:
        id:  "3"
        name: "default_name_4"
```

6.95.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.95.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.95.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.96 fortios_firewall_ip_translation – Configure firewall IP-translation in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.96.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and ip_translation category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.96.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.96.3 FortiOS Version Compatibility

6.96.4 Parameters

6.96.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.96.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure firewall IP-translation.
    fortios_firewall_ip_translation:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_ip_translation:
        endip: "<your_own_value>"
        map_startip: "<your_own_value>"
        startip: "<your_own_value>"
        transid: "6"
        type: "SCTP"
```

6.96.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.96.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.96.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.97 fortios_firewall_ipmacbinding_setting – Configure IP to MAC binding settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.97.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_ipmacbinding feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.97.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.97.3 FortiOS Version Compatibility

6.97.4 Parameters

6.97.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.97.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IP to MAC binding settings.
    fortios_firewall_ipmacbinding_setting:
      vdom:  "{{ vdom }}"
      firewall_ipmacbinding_setting:
        bindthroughfw: "enable"
        bindtofw: "enable"
        undefinedhost: "allow"
```

6.97.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.97.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.97.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.98 fortios_firewall_ipmacbinding_table – Configure IP to MAC address pairs in the IP/MAC binding table in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.98.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_ipmacbinding feature and table category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.98.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.98.3 FortiOS Version Compatibility

6.98.4 Parameters

6.98.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.98.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure IP to MAC address pairs in the IP/MAC binding table.
  fortios_firewall_ipmacbinding_table:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    firewall_ipmacbinding_table:
      ip: "<your_own_value>"
      mac: "<your_own_value>"
      name: "default_name_5"
      seq_num: "6"
      status: "enable"
```

6.98.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.98.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.98.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.99 fortios_firewall_ippool – Configure IPv4 IP pools in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.99.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and ippool category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.99.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.99.3 FortiOS Version Compatibility

6.99.4 Parameters

6.99.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.99.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv4 IP pools.
    fortios_firewall_ippool:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
    firewall_ippool:
      arp_intf: "<your_own_value> (source system.interface.name)"
      arp_reply: "disable"
      associated_interface: "<your_own_value> (source system.interface.name)"
      block_size: "6"
      comments: "<your_own_value>"
      endip: "<your_own_value>"
      endport: "9"
      name: "default_name_10"
      num_blocks_per_user: "11"
      pba_timeout: "12"
      permit_any_host: "disable"
      port_per_user: "14"
      source_endip: "<your_own_value>"
      source_startip: "<your_own_value>"
      startip: "<your_own_value>"
      startport: "18"
      type: "overload"
```

6.99.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.99.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.99.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.100 fortios_firewall_ippool6 – Configure IPv6 IP pools in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.100.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and ippool6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.100.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.100.3 FortiOS Version Compatibility

6.100.4 Parameters

6.100.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.100.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure IPv6 IP pools.
  fortios_firewall_ippool6:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    firewall_ippool6:
      comments: "<your_own_value>"
      endip: "<your_own_value>"
      name: "default_name_5"
      startip: "<your_own_value>"
```

6.100.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.100.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.100.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.101 fortios_firewall_iprope_list – lis in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.101.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_iprope feature and list category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.101.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.101.3 FortiOS Version Compatibility

6.101.4 Parameters

6.101.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.101.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: list
    fortios_firewall_iprope_list:
      vdom:  "{{ vdom }}"
      firewall_iprope_list:
        <group_number>: "<your_own_value>"
```

6.101.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.101.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.101.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.102 fortios_firewall_ipv6_eh_filter – Configure IPv6 extension header filter in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.102.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and ipv6_eh_filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.102.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.102.3 FortiOS Version Compatibility

6.102.4 Parameters

6.102.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.102.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 extension header filter.
    fortios_firewall_ipv6_eh_filter:
      vdom:  "{{ vdom }}"
      firewall_ipv6_eh_filter:
        auth: "enable"
        dest_opt: "enable"
        fragment: "enable"
        hdopt_type: "6"
        hop_opt: "enable"
        no_next: "enable"
        routing: "enable"
        routing_type: "10"
```

6.102.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.102.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.102.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.103 fortios_firewall_ldb_monitor – Configure server load balancing health monitors in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.103.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and ldb_monitor category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.103.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.103.3 FortiOS Version Compatibility

6.103.4 Parameters

6.103.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.103.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure server load balancing health monitors.
    fortios_firewall_ldb_monitor:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_ldb_monitor:
        dns_match_ip: "<your_own_value>"
        dns_protocol: "udp"
        dns_request_domain: "<your_own_value>"
        http_get: "<your_own_value>"
        http_match: "<your_own_value>"
        http_max_redirects: "8"
        interval: "9"
        name: "default_name_10"
        port: "11"
        retry: "12"
        src_ip: "<your_own_value>"
        timeout: "14"
        type: "ping"
```

6.103.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.103.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.103.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.104 fortios_firewall_local_in_policy – Configure user defined IPv4 local-in policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.104.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and local_in_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.104.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.104.3 FortiOS Version Compatibility

6.104.4 Parameters

6.104.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.104.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure user defined IPv4 local-in policies.
    fortios_firewall_local_in_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_local_in_policy:
        action: "accept"
        comments: "<your_own_value>"
        dstaddr:
         -
            name: "default_name_6 (source firewall.address.name firewall.addrgrp.name)
↪"
        dstaddr_negate: "enable"
        ha_mgmt_intf_only: "enable"
        intf: "<your_own_value> (source system.zone.name system.interface.name)"
        policyid: "10"
        schedule: "<your_own_value> (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name firewall.schedule.group.name)"
        service:
         -
            name: "default_name_13 (source firewall.service.custom.name firewall.
↪service.group.name)"
        service_negate: "enable"
        srcaddr:
         -
            name: "default_name_16 (source firewall.address.name firewall.addrgrp.
↪name)"
        srcaddr_negate: "enable"
        status: "enable"
        uuid: "<your_own_value>"
```

6.104.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.104.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.104.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.105 fortios_firewall_local_in_policy6 – Configure user defined IPv6 local-in policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.105.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and local_in_policy6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.105.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.105.3 FortiOS Version Compatibility

6.105.4 Parameters

6.105.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.105.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure user defined IPv6 local-in policies.
    fortios_firewall_local_in_policy6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_local_in_policy6:
        action: "accept"
        comments: "<your_own_value>"
        dstaddr:
         -
            name: "default_name_6 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        dstaddr_negate: "enable"
        intf: "<your_own_value> (source system.zone.name system.interface.name)"
        policyid: "9"
        schedule: "<your_own_value> (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name firewall.schedule.group.name)"
        service:
         -
            name: "default_name_12 (source firewall.service.custom.name firewall.
↪service.group.name)"
        service_negate: "enable"
        srcaddr:
         -
            name: "default_name_15 (source firewall.address6.name firewall.addrgrp6.
↪name)"
```

(continues on next page)

(continued from previous page)

```
        srcaddr_negate: "enable"
        status: "enable"
        uuid: "<your_own_value>"
```

6.105.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.105.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.105.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.106 fortios_firewall_mms_profile – Configure MMS profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.106.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and mms_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.106.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.106.3 FortiOS Version Compatibility

6.106.4 Parameters

6.106.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.106.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure MMS profiles.
    fortios_firewall_mms_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_mms_profile:
        avnotificationtable: "3 (source antivirus.notification.id)"
        bwordtable: "4 (source webfilter.content.id)"
        carrier_endpoint_prefix: "enable"
        carrier_endpoint_prefix_range_max: "6"
        carrier_endpoint_prefix_range_min: "7"
        carrier_endpoint_prefix_string: "<your_own_value>"
        carrierendpointbwltable: "9 (source firewall.carrier-endpoint-bwl.id)"
        comment: "Comment."
        dupe:
         -
            action1: "block"
```

(continues on next page)

(continued from previous page)

```
            action2: "block"
            action3: "block"
            block_time1: "15"
            block_time2: "16"
            block_time3: "17"
            limit1: "18"
            limit2: "19"
            limit3: "20"
            protocol: "<your_own_value>"
            status1: "enable"
            status2: "enable"
            status3: "enable"
            window1: "25"
            window2: "26"
            window3: "27"
        extended_utm_log: "<your_own_value>"
        flood:
         -
            action1: "block"
            action2: "block"
            action3: "block"
            block_time1: "33"
            block_time2: "34"
            block_time3: "35"
            limit1: "36"
            limit2: "37"
            limit3: "38"
            protocol: "<your_own_value>"
            status1: "enable"
            status2: "enable"
            status3: "enable"
            window1: "43"
            window2: "44"
            window3: "45"
        mm1: "avmonitor"
        mm1_addr_hdr: "<your_own_value>"
        mm1_addr_source: "http-header"
        mm1_convert_hex: "enable"
        mm1_outbreak_prevention: "disabled"
        mm1_retr_dupe: "enable"
        mm1_retrieve_scan: "enable"
        mm1comfortamount: "53"
        mm1comfortinterval: "54"
        mm1oversizelimit: "55"
        mm3: "avmonitor"
        mm3_outbreak_prevention: "disabled"
        mm3oversizelimit: "58"
        mm4: "avmonitor"
        mm4_outbreak_prevention: "disabled"
        mm4oversizelimit: "61"
        mm7: "avmonitor"
        mm7_addr_hdr: "<your_own_value>"
        mm7_addr_source: "http-header"
        mm7_convert_hex: "enable"
        mm7_outbreak_prevention: "disabled"
        mm7comfortamount: "67"
        mm7comfortinterval: "68"
```

(continues on next page)

(continued from previous page)

```
        mm7oversizelimit: "69"
        mms_antispam_mass_log: "enable"
        mms_av_block_log: "enable"
        mms_av_oversize_log: "enable"
        mms_av_virus_log: "enable"
        mms_carrier_endpoint_filter_log: "enable"
        mms_checksum_log: "enable"
        mms_checksum_table: "76 (source antivirus.mms-checksum.id)"
        mms_notification_log: "enable"
        mms_web_content_log: "enable"
        mmsbwordthreshold: "79"
        name: "default_name_80"
        notif_msisdn:
         -
            msisdn: "<your_own_value>"
            threshold: "flood-thresh-1"
        notification:
         -
            alert_int: "85"
            alert_int_mode: "hours"
            alert_src_msisdn: "<your_own_value>"
            alert_status: "enable"
            bword_int: "89"
            bword_int_mode: "hours"
            bword_status: "enable"
            carrier_endpoint_bwl_int: "92"
            carrier_endpoint_bwl_int_mode: "hours"
            carrier_endpoint_bwl_status: "enable"
            days_allowed: "sunday"
            detect_server: "enable"
            dupe_int: "97"
            dupe_int_mode: "hours"
            dupe_status: "enable"
            file_block_int: "100"
            file_block_int_mode: "hours"
            file_block_status: "enable"
            flood_int: "103"
            flood_int_mode: "hours"
            flood_status: "enable"
            from_in_header: "enable"
            mms_checksum_int: "107"
            mms_checksum_int_mode: "hours"
            mms_checksum_status: "enable"
            mmsc_hostname: "myhostname"
            mmsc_password: "<your_own_value>"
            mmsc_port: "112"
            mmsc_url: "<your_own_value>"
            mmsc_username: "<your_own_value>"
            msg_protocol: "mm1"
            msg_type: "submit-req"
            protocol: "<your_own_value>"
            rate_limit: "118"
            tod_window_duration: "<your_own_value>"
            tod_window_end: "<your_own_value>"
            tod_window_start: "<your_own_value>"
            user_domain: "<your_own_value>"
            vas_id: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
            vasp_id: "<your_own_value>"
            virus_int: "125"
            virus_int_mode: "hours"
            virus_status: "enable"
        outbreak_prevention:
            external_blocklist: "disable"
            ftgd_service: "disable"
        remove_blocked_const_length: "enable"
        replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
```

6.106.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.106.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.106.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.107 fortios_firewall_multicast_address – Configure multicast addresses in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.107.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and multicast_address category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.107.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.107.3 FortiOS Version Compatibility

6.107.4 Parameters

6.107.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.107.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure multicast addresses.
    fortios_firewall_multicast_address:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_multicast_address:
        associated_interface: "<your_own_value> (source system.interface.name)"
        color: "4"
```

(continues on next page)

(continued from previous page)

```
        comment: "Comment."
        end_ip: "<your_own_value>"
        name: "default_name_7"
        start_ip: "<your_own_value>"
        subnet: "<your_own_value>"
        tagging:
         -
            category: "<your_own_value> (source system.object-tagging.category)"
            name: "default_name_12"
            tags:
             -
                name: "default_name_14 (source system.object-tagging.tags.name)"
        type: "multicastrange"
        visibility: "enable"
```

6.107.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.107.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.107.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.108 fortios_firewall_multicast_address6 – Configure IPv6 multicast address in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.108.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and multicast_address6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.108.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.108.3 FortiOS Version Compatibility

6.108.4 Parameters

6.108.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.108.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 multicast address.
    fortios_firewall_multicast_address6:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    state: "present"
    access_token: "<your_own_value>"
    firewall_multicast_address6:
      color: "3"
      comment: "Comment."
      ip6: "<your_own_value>"
      name: "default_name_6"
      tagging:
       -
          category: "<your_own_value> (source system.object-tagging.category)"
          name: "default_name_9"
          tags:
           -
              name: "default_name_11 (source system.object-tagging.tags.name)"
      visibility: "enable"
```

6.108.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.108.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.108.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.109 fortios_firewall_multicast_policy – Configure multicast NAT policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.109.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and multicast_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.109.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.109.3 FortiOS Version Compatibility

6.109.4 Parameters

6.109.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.109.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure multicast NAT policies.
```

(continues on next page)

(continued from previous page)

```
    fortios_firewall_multicast_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_multicast_policy:
        action: "accept"
        auto_asic_offload: "enable"
        comments: "<your_own_value>"
        dnat: "<your_own_value>"
        dstaddr:
         -
            name: "default_name_8 (source firewall.multicast-address.name)"
        dstintf: "<your_own_value> (source system.interface.name system.zone.name)"
        end_port: "10"
        id:  "11"
        logtraffic: "enable"
        name: "default_name_13"
        protocol: "14"
        snat: "enable"
        snat_ip: "<your_own_value>"
        srcaddr:
         -
            name: "default_name_18 (source firewall.address.name firewall.addrgrp.
↪name)"
        srcintf: "<your_own_value> (source system.interface.name system.zone.name)"
        start_port: "20"
        status: "enable"
        uuid: "<your_own_value>"
```

6.109.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.109.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.109.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.110 fortios_firewall_multicast_policy6 – Configure IPv6 multicast NAT policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.110.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and multicast_policy6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.110.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.110.3 FortiOS Version Compatibility

6.110.4 Parameters

6.110.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.110.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 multicast NAT policies.
    fortios_firewall_multicast_policy6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_multicast_policy6:
        action: "accept"
        auto_asic_offload: "enable"
        comments: "<your_own_value>"
        dstaddr:
         -
            name: "default_name_7 (source firewall.multicast-address6.name)"
        dstintf: "<your_own_value> (source system.interface.name system.zone.name)"
        end_port: "9"
        id:  "10"
        logtraffic: "enable"
        name: "default_name_12"
        protocol: "13"
        srcaddr:
         -
            name: "default_name_15 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        srcintf: "<your_own_value> (source system.interface.name system.zone.name)"
        start_port: "17"
        status: "enable"
        uuid: "<your_own_value>"
```

6.110.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.110.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.110.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.111 fortios_firewall_policy – Configure IPv4 policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.111.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.111.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.111.3 FortiOS Version Compatibility

6.111.4 Parameters

6.111.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

- Adjust object order by moving self after(before) another.
- Only one of [after, before] must be specified when action is moving an object.

6.111.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv4 policies.
    fortios_firewall_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_policy:
        action: "accept"
        anti_replay: "enable"
        app_category:
         -
            id:  "6"
        app_group:
         -
            name: "default_name_8 (source application.group.name)"
        application:
         -
            id:  "10"
        application_list: "<your_own_value> (source application.list.name)"
        auth_cert: "<your_own_value> (source vpn.certificate.local.name)"
        auth_path: "enable"
        auth_redirect_addr: "<your_own_value>"
        auto_asic_offload: "enable"
        av_profile: "<your_own_value> (source antivirus.profile.name)"
        block_notification: "enable"
        captive_portal_exempt: "enable"
        capture_packet: "enable"
        cifs_profile: "<your_own_value> (source cifs.profile.name)"
        comments: "<your_own_value>"
        custom_log_fields:
         -
            field_id: "<your_own_value> (source log.custom-field.id)"
        decrypted_traffic_mirror: "<your_own_value> (source firewall.decrypted-
↪traffic-mirror.name)"
        delay_tcp_npu_session: "enable"
        devices:
         -
            name: "default_name_27 (source user.device.alias user.device-group.name␣
↪user.device-category.name)"
        diffserv_forward: "enable"
        diffserv_reverse: "enable"
```

(continues on next page)

(continued from previous page)

```
        diffservcode_forward: "<your_own_value>"
        diffservcode_rev: "<your_own_value>"
        disclaimer: "enable"
        dlp_sensor: "<your_own_value> (source dlp.sensor.name)"
        dnsfilter_profile: "<your_own_value> (source dnsfilter.profile.name)"
        dscp_match: "enable"
        dscp_negate: "enable"
        dscp_value: "<your_own_value>"
        dsri: "enable"
        dstaddr:
         -
            name: "default_name_40 (source firewall.address.name firewall.addrgrp.
↪name firewall.vip.name firewall.vipgrp.name)"
        dstaddr_negate: "enable"
        dstaddr6:
         -
            name: "default_name_43 (source firewall.address6.name firewall.addrgrp6.
↪name firewall.vipgrp6.name firewall.vip6.name system.external-resource
              .name)"
        dstintf:
         -
            name: "default_name_45 (source system.interface.name system.zone.name)"
        dynamic_shaping: "enable"
        email_collect: "enable"
        emailfilter_profile: "<your_own_value> (source emailfilter.profile.name)"
        file_filter_profile: "<your_own_value> (source file-filter.profile.name)"
        firewall_session_dirty: "check-all"
        fixedport: "enable"
        fsso: "enable"
        fsso_agent_for_ntlm: "<your_own_value> (source user.fsso.name)"
        fsso_groups:
         -
            name: "default_name_55 (source user.adgrp.name)"
        geoip_anycast: "enable"
        geoip_match: "physical-location"
        global_label: "<your_own_value>"
        groups:
         -
            name: "default_name_60 (source user.group.name)"
        gtp_profile: "<your_own_value> (source firewall.gtp.name)"
        http_policy_redirect: "enable"
        icap_profile: "<your_own_value> (source icap.profile.name)"
        identity_based_route: "<your_own_value> (source firewall.identity-based-route.
↪name)"
        inbound: "enable"
        inspection_mode: "proxy"
        internet_service: "enable"
        internet_service_custom:
         -
            name: "default_name_69 (source firewall.internet-service-custom.name)"
        internet_service_custom_group:
         -
            name: "default_name_71 (source firewall.internet-service-custom-group.
↪name)"
        internet_service_group:
         -
            name: "default_name_73 (source firewall.internet-service-group.name)"
```

(continues on next page)

(continued from previous page)

```
        internet_service_id:
         -
            id:  "75 (source firewall.internet-service.id)"
        internet_service_name:
         -
            name: "default_name_77 (source firewall.internet-service-name.name)"
        internet_service_negate: "enable"
        internet_service_src: "enable"
        internet_service_src_custom:
         -
            name: "default_name_81 (source firewall.internet-service-custom.name)"
        internet_service_src_custom_group:
         -
            name: "default_name_83 (source firewall.internet-service-custom-group.
↪name)"
        internet_service_src_group:
         -
            name: "default_name_85 (source firewall.internet-service-group.name)"
        internet_service_src_id:
         -
            id:  "87 (source firewall.internet-service.id)"
        internet_service_src_name:
         -
            name: "default_name_89 (source firewall.internet-service-name.name)"
        internet_service_src_negate: "enable"
        ippool: "enable"
        ips_sensor: "<your_own_value> (source ips.sensor.name)"
        label: "<your_own_value>"
        learning_mode: "enable"
        logtraffic: "all"
        logtraffic_start: "enable"
        match_vip: "enable"
        match_vip_only: "enable"
        mms_profile: "<your_own_value> (source firewall.mms-profile.name)"
        name: "default_name_100"
        nat: "enable"
        natinbound: "enable"
        natip: "<your_own_value>"
        natoutbound: "enable"
        np_acceleration: "enable"
        ntlm: "enable"
        ntlm_enabled_browsers:
         -
            user_agent_string: "<your_own_value>"
        ntlm_guest: "enable"
        outbound: "enable"
        passive_wan_health_measurement: "enable"
        per_ip_shaper: "<your_own_value> (source firewall.shaper.per-ip-shaper.name)"
        permit_any_host: "enable"
        permit_stun_host: "enable"
        policyid: "115"
        poolname:
         -
            name: "default_name_117 (source firewall.ippool.name)"
        poolname6:
         -
            name: "default_name_119 (source firewall.ippool6.name)"
```

(continues on next page)

(continued from previous page)

```
        profile_group: "<your_own_value> (source firewall.profile-group.name)"
        profile_protocol_options: "<your_own_value> (source firewall.profile-protocol-
↪options.name)"
        profile_type: "single"
        radius_mac_auth_bypass: "enable"
        redirect_url: "<your_own_value>"
        replacemsg_override_group: "<your_own_value> (source system.replacemsg-group.
↪name)"
        reputation_direction: "source"
        reputation_minimum: "127 (source firewall.internet-service-reputation.id)"
        rsso: "enable"
        rtp_addr:
         -
            name: "default_name_130 (source firewall.address.name firewall.addrgrp.
↪name)"
        rtp_nat: "disable"
        scan_botnet_connections: "disable"
        schedule: "<your_own_value> (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name firewall.schedule.group.name)"
        schedule_timeout: "enable"
        send_deny_packet: "disable"
        service:
         -
            name: "default_name_137 (source firewall.service.custom.name firewall.
↪service.group.name)"
        service_negate: "enable"
        session_ttl: "139"
        spamfilter_profile: "<your_own_value> (source spamfilter.profile.name)"
        src_vendor_mac:
         -
            id:  "142 (source firewall.vendor-mac.id)"
        srcaddr:
         -
            name: "default_name_144 (source firewall.address.name firewall.addrgrp.
↪name)"
        srcaddr_negate: "enable"
        srcaddr6:
         -
            name: "default_name_147 (source firewall.address6.name firewall.addrgrp6.
↪name system.external-resource.name)"
        srcintf:
         -
            name: "default_name_149 (source system.interface.name system.zone.name)"
        ssh_filter_profile: "<your_own_value> (source ssh-filter.profile.name)"
        ssh_policy_redirect: "enable"
        ssl_mirror: "enable"
        ssl_mirror_intf:
         -
            name: "default_name_154 (source system.interface.name system.zone.name)"
        ssl_ssh_profile: "<your_own_value> (source firewall.ssl-ssh-profile.name)"
        status: "enable"
        tcp_mss_receiver: "157"
        tcp_mss_sender: "158"
        tcp_session_without_syn: "all"
        timeout_send_rst: "enable"
        tos: "<your_own_value>"
        tos_mask: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        tos_negate: "enable"
        traffic_shaper: "<your_own_value> (source firewall.shaper.traffic-shaper.name)
↪"
        traffic_shaper_reverse: "<your_own_value> (source firewall.shaper.traffic-
↪shaper.name)"
        url_category:
         -
            id:  "167"
        users:
         -
            name: "default_name_169 (source user.local.name)"
        utm_status: "enable"
        uuid: "<your_own_value>"
        videofilter_profile: "<your_own_value> (source videofilter.profile.name)"
        vlan_cos_fwd: "173"
        vlan_cos_rev: "174"
        vlan_filter: "<your_own_value>"
        voip_profile: "<your_own_value> (source voip.profile.name)"
        vpntunnel: "<your_own_value> (source vpn.ipsec.phase1.name vpn.ipsec.
↪manualkey.name)"
        waf_profile: "<your_own_value> (source waf.profile.name)"
        wanopt: "enable"
        wanopt_detection: "active"
        wanopt_passive_opt: "default"
        wanopt_peer: "<your_own_value> (source wanopt.peer.peer-host-id)"
        wanopt_profile: "<your_own_value> (source wanopt.profile.name)"
        wccp: "enable"
        webcache: "enable"
        webcache_https: "disable"
        webfilter_profile: "<your_own_value> (source webfilter.profile.name)"
        webproxy_forward_server: "<your_own_value> (source web-proxy.forward-server.
↪name web-proxy.forward-server-group.name)"
        webproxy_profile: "<your_own_value> (source web-proxy.profile.name)"
        wsso: "enable"
        ztna_ems_tag:
         -
            name: "default_name_192 (source firewall.address.name firewall.addrgrp.
↪name)"
        ztna_geo_tag:
         -
            name: "default_name_194 (source firewall.address.name firewall.addrgrp.
↪name)"
        ztna_status: "enable"

  - name: move firewall.policy
    fortios_firewall_policy:
      vdom:  "root"
      action: "move"
      self: "<mkey of self identifier>"
      after: "<mkey of target identifier>"
     #before: "<mkey of target identifier>"
```

6.111.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.111.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.111.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.112 fortios_firewall_policy46 – Configure IPv4 to IPv6 policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.112.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and policy46 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.112.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.112.3 FortiOS Version Compatibility

6.112.4 Parameters

6.112.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.112.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv4 to IPv6 policies.
    fortios_firewall_policy46:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_policy46:
        action: "accept"
        comments: "<your_own_value>"
        dstaddr:
         -
            name: "default_name_6 (source firewall.vip46.name firewall.vipgrp46.name)"
        dstintf: "<your_own_value> (source system.interface.name system.zone.name)"
        fixedport: "enable"
        ippool: "enable"
        logtraffic: "enable"
        logtraffic_start: "enable"
        name: "default_name_12"
        per_ip_shaper: "<your_own_value> (source firewall.shaper.per-ip-shaper.name)"
        permit_any_host: "enable"
        policyid: "15"
        poolname:
         -
            name: "default_name_17 (source firewall.ippool6.name)"
        schedule: "<your_own_value> (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name firewall.schedule.group.name)"
        service:
         -
            name: "default_name_20 (source firewall.service.custom.name firewall.
↪service.group.name)"
```

(continues on next page)

(continued from previous page)

```
        srcaddr:
         -
            name: "default_name_22 (source firewall.address.name firewall.addrgrp.
↪name)"
        srcintf: "<your_own_value> (source system.zone.name system.interface.name)"
        status: "enable"
        tcp_mss_receiver: "25"
        tcp_mss_sender: "26"
        traffic_shaper: "<your_own_value> (source firewall.shaper.traffic-shaper.name)
↪"
        traffic_shaper_reverse: "<your_own_value> (source firewall.shaper.traffic-
↪shaper.name)"
        uuid: "<your_own_value>"
```

6.112.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.112.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.112.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.113 fortios_firewall_policy6 – Configure IPv6 policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.113.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and policy6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.113.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.113.3 FortiOS Version Compatibility

6.113.4 Parameters

6.113.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.113.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 policies.
    fortios_firewall_policy6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
      firewall_policy6:
        action: "accept"
        anti_replay: "enable"
        app_category:
         -
            id:  "6"
        app_group:
         -
            name: "default_name_8 (source application.group.name)"
        application:
         -
            id:  "10"
        application_list: "<your_own_value> (source application.list.name)"
        auto_asic_offload: "enable"
        av_profile: "<your_own_value> (source antivirus.profile.name)"
        cifs_profile: "<your_own_value> (source cifs.profile.name)"
        comments: "<your_own_value>"
        custom_log_fields:
         -
            field_id: "<your_own_value> (source log.custom-field.id)"
        devices:
         -
            name: "default_name_19 (source user.device.alias user.device-group.name␣
↪user.device-category.name)"
        diffserv_forward: "enable"
        diffserv_reverse: "enable"
        diffservcode_forward: "<your_own_value>"
        diffservcode_rev: "<your_own_value>"
        dlp_sensor: "<your_own_value> (source dlp.sensor.name)"
        dnsfilter_profile: "<your_own_value> (source dnsfilter.profile.name)"
        dscp_match: "enable"
        dscp_negate: "enable"
        dscp_value: "<your_own_value>"
        dsri: "enable"
        dstaddr:
         -
            name: "default_name_31 (source firewall.address6.name firewall.addrgrp6.
↪name firewall.vip6.name firewall.vipgrp6.name)"
        dstaddr_negate: "enable"
        dstintf:
         -
            name: "default_name_34 (source system.interface.name system.zone.name)"
        emailfilter_profile: "<your_own_value> (source emailfilter.profile.name)"
        firewall_session_dirty: "check-all"
        fixedport: "enable"
        fsso_groups:
         -
            name: "default_name_39 (source user.adgrp.name)"
        global_label: "<your_own_value>"
        groups:
         -
            name: "default_name_42 (source user.group.name)"
        http_policy_redirect: "enable"
        icap_profile: "<your_own_value> (source icap.profile.name)"
        inbound: "enable"
        inspection_mode: "proxy"
        ippool: "enable"
```

(continues on next page)

(continued from previous page)

```
        ips_sensor: "<your_own_value> (source ips.sensor.name)"
        label: "<your_own_value>"
        logtraffic: "all"
        logtraffic_start: "enable"
        mms_profile: "<your_own_value> (source firewall.mms-profile.name)"
        name: "default_name_53"
        nat: "enable"
        natinbound: "enable"
        natoutbound: "enable"
        np_acceleration: "enable"
        outbound: "enable"
        per_ip_shaper: "<your_own_value> (source firewall.shaper.per-ip-shaper.name)"
        policyid: "60"
        poolname:
         -
            name: "default_name_62 (source firewall.ippool6.name)"
        profile_group: "<your_own_value> (source firewall.profile-group.name)"
        profile_protocol_options: "<your_own_value> (source firewall.profile-protocol-
↪options.name)"
        profile_type: "single"
        replacemsg_override_group: "<your_own_value> (source system.replacemsg-group.
↪name)"
        rsso: "enable"
        schedule: "<your_own_value> (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name firewall.schedule.group.name)"
        send_deny_packet: "enable"
        service:
         -
            name: "default_name_71 (source firewall.service.custom.name firewall.
↪service.group.name)"
        service_negate: "enable"
        session_ttl: "73"
        spamfilter_profile: "<your_own_value> (source spamfilter.profile.name)"
        srcaddr:
         -
            name: "default_name_76 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        srcaddr_negate: "enable"
        srcintf:
         -
            name: "default_name_79 (source system.zone.name system.interface.name)"
        ssh_filter_profile: "<your_own_value> (source ssh-filter.profile.name)"
        ssh_policy_redirect: "enable"
        ssl_mirror: "enable"
        ssl_mirror_intf:
         -
            name: "default_name_84 (source system.zone.name system.interface.name)"
        ssl_ssh_profile: "<your_own_value> (source firewall.ssl-ssh-profile.name)"
        status: "enable"
        tcp_mss_receiver: "87"
        tcp_mss_sender: "88"
        tcp_session_without_syn: "all"
        timeout_send_rst: "enable"
        tos: "<your_own_value>"
        tos_mask: "<your_own_value>"
        tos_negate: "enable"
        traffic_shaper: "<your_own_value> (source firewall.shaper.traffic-shaper.name)
↪"
```

(continues on next page)

(continued from previous page)

```
        traffic_shaper_reverse: "<your_own_value> (source firewall.shaper.traffic-
↪shaper.name)"
        url_category:
         -
            id:  "97"
        users:
         -
            name: "default_name_99 (source user.local.name)"
        utm_status: "enable"
        uuid: "<your_own_value>"
        vlan_cos_fwd: "102"
        vlan_cos_rev: "103"
        vlan_filter: "<your_own_value>"
        voip_profile: "<your_own_value> (source voip.profile.name)"
        vpntunnel: "<your_own_value> (source vpn.ipsec.phase1.name vpn.ipsec.
↪manualkey.name)"
        waf_profile: "<your_own_value> (source waf.profile.name)"
        webcache: "enable"
        webcache_https: "disable"
        webfilter_profile: "<your_own_value> (source webfilter.profile.name)"
        webproxy_forward_server: "<your_own_value> (source web-proxy.forward-server.
↪name web-proxy.forward-server-group.name)"
        webproxy_profile: "<your_own_value> (source web-proxy.profile.name)"
```

6.113.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.113.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.113.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.114 fortios_firewall_policy64 – Configure IPv6 to IPv4 policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.114.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and policy64 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.114.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.114.3 FortiOS Version Compatibility

6.114.4 Parameters

6.114.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.114.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 to IPv4 policies.
    fortios_firewall_policy64:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_policy64:
        action: "accept"
        comments: "<your_own_value>"
        dstaddr:
         -
            name: "default_name_6 (source firewall.address.name firewall.addrgrp.name␣
↪firewall.vip64.name firewall.vipgrp64.name)"
        dstintf: "<your_own_value> (source system.interface.name system.zone.name)"
        fixedport: "enable"
        ippool: "enable"
        logtraffic: "enable"
        logtraffic_start: "enable"
        name: "default_name_12"
        per_ip_shaper: "<your_own_value> (source firewall.shaper.per-ip-shaper.name)"
        permit_any_host: "enable"
        policyid: "15"
        poolname:
         -
            name: "default_name_17 (source firewall.ippool.name)"
        schedule: "<your_own_value> (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name firewall.schedule.group.name)"
        service:
         -
            name: "default_name_20 (source firewall.service.custom.name firewall.
↪service.group.name)"
        srcaddr:
         -
            name: "default_name_22 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        srcintf: "<your_own_value> (source system.zone.name system.interface.name)"
        status: "enable"
        tcp_mss_receiver: "25"
        tcp_mss_sender: "26"
        traffic_shaper: "<your_own_value> (source firewall.shaper.traffic-shaper.name)
↪"
        traffic_shaper_reverse: "<your_own_value> (source firewall.shaper.traffic-
↪shaper.name)"
        uuid: "<your_own_value>"
```

6.114.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.114.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.114.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.115 fortios_firewall_profile_group – Configure profile groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.115.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and profile_group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.115.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.115.3 FortiOS Version Compatibility

6.115.4 Parameters

6.115.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.115.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure profile groups.
    fortios_firewall_profile_group:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_profile_group:
        application_list: "<your_own_value> (source application.list.name)"
        av_profile: "<your_own_value> (source antivirus.profile.name)"
        cifs_profile: "<your_own_value> (source cifs.profile.name)"
        dlp_sensor: "<your_own_value> (source dlp.sensor.name)"
        dnsfilter_profile: "<your_own_value> (source dnsfilter.profile.name)"
        emailfilter_profile: "<your_own_value> (source emailfilter.profile.name)"
        file_filter_profile: "<your_own_value> (source file-filter.profile.name)"
        icap_profile: "<your_own_value> (source icap.profile.name)"
        ips_sensor: "<your_own_value> (source ips.sensor.name)"
        mms_profile: "<your_own_value> (source firewall.mms-profile.name)"
        name: "default_name_13"
        profile_protocol_options: "<your_own_value> (source firewall.profile-protocol-
↪options.name)"
        spamfilter_profile: "<your_own_value> (source spamfilter.profile.name)"
        ssh_filter_profile: "<your_own_value> (source ssh-filter.profile.name)"
        ssl_ssh_profile: "<your_own_value> (source firewall.ssl-ssh-profile.name)"
        videofilter_profile: "<your_own_value> (source videofilter.profile.name)"
        voip_profile: "<your_own_value> (source voip.profile.name)"
```

(continues on next page)

(continued from previous page)

```
        waf_profile: "<your_own_value> (source waf.profile.name)"
        webfilter_profile: "<your_own_value> (source webfilter.profile.name)"
```

6.115.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.115.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.115.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.116 fortios_firewall_profile_protocol_options – Configure protocol options in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.116.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and profile_protocol_options category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.116.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.116.3 FortiOS Version Compatibility

6.116.4 Parameters

6.116.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.116.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure protocol options.
    fortios_firewall_profile_protocol_options:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_profile_protocol_options:
        cifs:
            domain_controller: "<your_own_value> (source credential-store.domain-
↪controller.server-name)"
            options: "oversize"
            oversize_limit: "6"
            ports: "7"
            scan_bzip2: "enable"
            server_credential_type: "none"
            server_keytab:
             -
                keytab: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
            principal: "<your_own_value>"
        status: "enable"
        tcp_window_maximum: "14"
        tcp_window_minimum: "15"
        tcp_window_size: "16"
        tcp_window_type: "system"
        uncompressed_nest_limit: "18"
        uncompressed_oversize_limit: "19"
    comment: "Optional comments."
    dns:
        ports: "22"
        status: "enable"
    ftp:
        comfort_amount: "25"
        comfort_interval: "26"
        inspect_all: "enable"
        options: "clientcomfort"
        oversize_limit: "29"
        ports: "30"
        scan_bzip2: "enable"
        ssl_offloaded: "no"
        status: "enable"
        stream_based_uncompressed_limit: "34"
        tcp_window_maximum: "35"
        tcp_window_minimum: "36"
        tcp_window_size: "37"
        tcp_window_type: "system"
        uncompressed_nest_limit: "39"
        uncompressed_oversize_limit: "40"
    http:
        block_page_status_code: "42"
        comfort_amount: "43"
        comfort_interval: "44"
        fortinet_bar: "enable"
        fortinet_bar_port: "46"
        http_policy: "disable"
        inspect_all: "enable"
        options: "clientcomfort"
        oversize_limit: "50"
        ports: "51"
        post_lang: "jisx0201"
        proxy_after_tcp_handshake: "enable"
        range_block: "disable"
        retry_count: "55"
        scan_bzip2: "enable"
        ssl_offloaded: "no"
        status: "enable"
        stream_based_uncompressed_limit: "59"
        streaming_content_bypass: "enable"
        strip_x_forwarded_for: "disable"
        switching_protocols: "bypass"
        tcp_window_maximum: "63"
        tcp_window_minimum: "64"
        tcp_window_size: "65"
        tcp_window_type: "system"
        tunnel_non_http: "enable"
        uncompressed_nest_limit: "68"
```

(continues on next page)

(continued from previous page)

```
            uncompressed_oversize_limit: "69"
            unknown_http_version: "reject"
        imap:
            inspect_all: "enable"
            options: "fragmail"
            oversize_limit: "74"
            ports: "75"
            proxy_after_tcp_handshake: "enable"
            scan_bzip2: "enable"
            ssl_offloaded: "no"
            status: "enable"
            uncompressed_nest_limit: "80"
            uncompressed_oversize_limit: "81"
        mail_signature:
            signature: "<your_own_value>"
            status: "disable"
        mapi:
            options: "fragmail"
            oversize_limit: "87"
            ports: "88"
            scan_bzip2: "enable"
            status: "enable"
            uncompressed_nest_limit: "91"
            uncompressed_oversize_limit: "92"
        name: "default_name_93"
        nntp:
            inspect_all: "enable"
            options: "oversize"
            oversize_limit: "97"
            ports: "98"
            proxy_after_tcp_handshake: "enable"
            scan_bzip2: "enable"
            status: "enable"
            uncompressed_nest_limit: "102"
            uncompressed_oversize_limit: "103"
        oversize_log: "disable"
        pop3:
            inspect_all: "enable"
            options: "fragmail"
            oversize_limit: "108"
            ports: "109"
            proxy_after_tcp_handshake: "enable"
            scan_bzip2: "enable"
            ssl_offloaded: "no"
            status: "enable"
            uncompressed_nest_limit: "114"
            uncompressed_oversize_limit: "115"
        replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
        rpc_over_http: "enable"
        smtp:
            inspect_all: "enable"
            options: "fragmail"
            oversize_limit: "121"
            ports: "122"
            proxy_after_tcp_handshake: "enable"
            scan_bzip2: "enable"
            server_busy: "enable"
```

(continues on next page)

(continued from previous page)

```
            ssl_offloaded: "no"
            status: "enable"
            uncompressed_nest_limit: "128"
            uncompressed_oversize_limit: "129"
        ssh:
            comfort_amount: "131"
            comfort_interval: "132"
            options: "oversize"
            oversize_limit: "134"
            scan_bzip2: "enable"
            ssl_offloaded: "no"
            stream_based_uncompressed_limit: "137"
            tcp_window_maximum: "138"
            tcp_window_minimum: "139"
            tcp_window_size: "140"
            tcp_window_type: "system"
            uncompressed_nest_limit: "142"
            uncompressed_oversize_limit: "143"
        switching_protocols_log: "disable"
```

6.116.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.116.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.116.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.117 fortios_firewall_proute – List policy routing in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.117.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and proute category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.117.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.117.3 FortiOS Version Compatibility

6.117.4 Parameters

6.117.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.117.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: List policy routing.
  fortios_firewall_proute:
    vdom:  "{{ vdom }}"
    firewall_proute:
      <policy route id>: "<your_own_value>"
```

6.117.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.117.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.117.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.118 fortios_firewall_proxy_address – Web proxy address configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.118.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and proxy_address category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.118.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.118.3 FortiOS Version Compatibility

6.118.4 Parameters

6.118.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.118.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Web proxy address configuration.
    fortios_firewall_proxy_address:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_proxy_address:
        case_sensitivity: "disable"
        category:
          -
            id:  "5"
```

(continues on next page)

(continued from previous page)

```
        color: "6"
        comment: "Optional comments."
        header: "<your_own_value>"
        header_group:
         -
            case_sensitivity: "disable"
            header: "<your_own_value>"
            header_name: "<your_own_value>"
            id:  "13"
        header_name: "<your_own_value>"
        host: "myhostname (source firewall.address.name firewall.addrgrp.name␣
↪firewall.proxy-address.name)"
        host_regex: "myhostname"
        method: "get"
        name: "default_name_18"
        path: "<your_own_value>"
        query: "<your_own_value>"
        referrer: "enable"
        tagging:
         -
            category: "<your_own_value> (source system.object-tagging.category)"
            name: "default_name_24"
            tags:
             -
                name: "default_name_26 (source system.object-tagging.tags.name)"
        type: "host-regex"
        ua: "chrome"
        uuid: "<your_own_value>"
        visibility: "enable"
```

6.118.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.118.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.118.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.119 fortios_firewall_proxy_addrgrp – Web proxy address group configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.119.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and proxy_addrgrp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.119.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.119.3 FortiOS Version Compatibility

6.119.4 Parameters

6.119.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.119.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Web proxy address group configuration.
    fortios_firewall_proxy_addrgrp:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_proxy_addrgrp:
        color: "3"
        comment: "Optional comments."
        member:
         -
            name: "default_name_6 (source firewall.proxy-address.name firewall.proxy-
↪addrgrp.name)"
        name: "default_name_7"
        tagging:
         -
            category: "<your_own_value> (source system.object-tagging.category)"
            name: "default_name_10"
            tags:
             -
                name: "default_name_12 (source system.object-tagging.tags.name)"
        type: "src"
        uuid: "<your_own_value>"
        visibility: "enable"
```

6.119.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.119.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.119.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.120 fortios_firewall_proxy_policy – Configure proxy policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.120.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and proxy_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.120.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.120.3 FortiOS Version Compatibility

6.120.4 Parameters

6.120.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.120.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure proxy policies.
    fortios_firewall_proxy_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_proxy_policy:
        access_proxy:
         -
            name: "default_name_4 (source firewall.access-proxy.name)"
        action: "accept"
        application_list: "<your_own_value> (source application.list.name)"
        av_profile: "<your_own_value> (source antivirus.profile.name)"
        cifs_profile: "<your_own_value> (source cifs.profile.name)"
        comments: "<your_own_value>"
        decrypted_traffic_mirror: "<your_own_value> (source firewall.decrypted-
↪traffic-mirror.name)"
        device_ownership: "enable"
        disclaimer: "disable"
        dlp_sensor: "<your_own_value> (source dlp.sensor.name)"
        dstaddr:
         -
            name: "default_name_15 (source firewall.address.name firewall.addrgrp.
↪name firewall.proxy-address.name firewall.proxy-addrgrp.name firewall.vip
              .name firewall.vipgrp.name firewall.vip46.name firewall.vipgrp46.name␣
↪system.external-resource.name)"
        dstaddr_negate: "enable"
        dstaddr6:
         -
            name: "default_name_18 (source firewall.address6.name firewall.addrgrp6.
↪name firewall.vip6.name firewall.vipgrp6.name firewall.vip64.name firewall
              .vipgrp64.name system.external-resource.name)"
        dstintf:
         -
            name: "default_name_20 (source system.interface.name system.zone.name)"
        emailfilter_profile: "<your_own_value> (source emailfilter.profile.name)"
        file_filter_profile: "<your_own_value> (source file-filter.profile.name)"
        global_label: "<your_own_value>"
        groups:
         -
            name: "default_name_25 (source user.group.name)"
        http_tunnel_auth: "enable"
        icap_profile: "<your_own_value> (source icap.profile.name)"
```

(continues on next page)

(continued from previous page)

```
        internet_service: "enable"
        internet_service_custom:
         -
            name: "default_name_30 (source firewall.internet-service-custom.name)"
        internet_service_custom_group:
         -
            name: "default_name_32 (source firewall.internet-service-custom-group.
↪name)"
        internet_service_group:
         -
            name: "default_name_34 (source firewall.internet-service-group.name)"
        internet_service_id:
         -
            id:  "36 (source firewall.internet-service.id)"
        internet_service_name:
         -
            name: "default_name_38 (source firewall.internet-service-name.name)"
        internet_service_negate: "enable"
        ips_sensor: "<your_own_value> (source ips.sensor.name)"
        label: "<your_own_value>"
        logtraffic: "all"
        logtraffic_start: "enable"
        mms_profile: "<your_own_value> (source firewall.mms-profile.name)"
        name: "default_name_45"
        policyid: "46"
        poolname:
         -
            name: "default_name_48 (source firewall.ippool.name)"
        profile_group: "<your_own_value> (source firewall.profile-group.name)"
        profile_protocol_options: "<your_own_value> (source firewall.profile-protocol-
↪options.name)"
        profile_type: "single"
        proxy: "explicit-web"
        redirect_url: "<your_own_value>"
        replacemsg_override_group: "<your_own_value> (source system.replacemsg-group.
↪name)"
        scan_botnet_connections: "disable"
        schedule: "<your_own_value> (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name firewall.schedule.group.name)"
        service:
         -
            name: "default_name_58 (source firewall.service.custom.name firewall.
↪service.group.name)"
        service_negate: "enable"
        session_ttl: "60"
        spamfilter_profile: "<your_own_value> (source spamfilter.profile.name)"
        srcaddr:
         -
            name: "default_name_63 (source firewall.address.name firewall.addrgrp.
↪name firewall.proxy-address.name firewall.proxy-addrgrp.name system
                .external-resource.name)"
        srcaddr_negate: "enable"
        srcaddr6:
         -
            name: "default_name_66 (source firewall.address6.name firewall.addrgrp6.
↪name system.external-resource.name)"
        srcintf:
```

(continues on next page)

(continued from previous page)

```
        -
            name: "default_name_68 (source system.interface.name system.zone.name)"
        ssh_filter_profile: "<your_own_value> (source ssh-filter.profile.name)"
        ssh_policy_redirect: "enable"
        ssl_ssh_profile: "<your_own_value> (source firewall.ssl-ssh-profile.name)"
        status: "enable"
        transparent: "enable"
        users:
         -
            name: "default_name_75 (source user.local.name)"
        utm_status: "enable"
        uuid: "<your_own_value>"
        videofilter_profile: "<your_own_value> (source videofilter.profile.name)"
        voip_profile: "<your_own_value> (source voip.profile.name)"
        waf_profile: "<your_own_value> (source waf.profile.name)"
        webcache: "enable"
        webcache_https: "disable"
        webfilter_profile: "<your_own_value> (source webfilter.profile.name)"
        webproxy_forward_server: "<your_own_value> (source web-proxy.forward-server.
↪name web-proxy.forward-server-group.name)"
        webproxy_profile: "<your_own_value> (source web-proxy.profile.name)"
        ztna_ems_tag:
         -
            name: "default_name_87 (source firewall.address.name firewall.addrgrp.
↪name)"
```

6.120.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.120.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.120.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.121 fortios_firewall_region – Define region table in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.121.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and region category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.121.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.121.3 FortiOS Version Compatibility

6.121.4 Parameters

6.121.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.121.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Define region table.
    fortios_firewall_region:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_region:
        city:
         -
            id:  "4"
        id:  "5"
        name: "default_name_6"
```

6.121.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.121.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.121.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.122 fortios_firewall_schedule_group – Schedule group configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.122.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_schedule feature and group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.122.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.122.3 FortiOS Version Compatibility

6.122.4 Parameters

6.122.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.122.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
 tasks:
 - name: Schedule group configuration.
   fortios_firewall_schedule_group:
     vdom:  "{{ vdom }}"
     state: "present"
     access_token: "<your_own_value>"
     firewall_schedule_group:
       color: "3"
       fabric_object: "enable"
       member:
        -
           name: "default_name_6 (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name)"
       name: "default_name_7"
```

6.122.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.122.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.122.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.123 fortios_firewall_schedule_onetime – Onetime schedule configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Synopsis*

6.123.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_schedule feature and onetime category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.123.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.123.3 FortiOS Version Compatibility

6.123.4 Parameters

6.123.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.123.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Onetime schedule configuration.
```

(continues on next page)

(continued from previous page)

```
    fortios_firewall_schedule_onetime:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_schedule_onetime:
        color: "3"
        end: "<your_own_value>"
        expiration_days: "5"
        fabric_object: "enable"
        name: "default_name_7"
        start: "<your_own_value>"
```

6.123.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.123.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.123.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.124 fortios_firewall_schedule_recurring – Recurring schedule configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.124.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_schedule feature and recurring category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.124.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.124.3 FortiOS Version Compatibility

6.124.4 Parameters

6.124.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.124.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Recurring schedule configuration.
    fortios_firewall_schedule_recurring:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_schedule_recurring:
```

(continues on next page)

(continued from previous page)

```
        color: "3"
        day: "sunday"
        end: "<your_own_value>"
        fabric_object: "enable"
        name: "default_name_7"
        start: "<your_own_value>"
```

6.124.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.124.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.124.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.125 fortios_firewall_security_policy – Configure NGFW IPv4/IPv6 application policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.125.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and security_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.125.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.125.3 FortiOS Version Compatibility

6.125.4 Parameters

6.125.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.125.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure NGFW IPv4/IPv6 application policies.
    fortios_firewall_security_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_security_policy:
        action: "accept"
        app_category:
         -
            id:  "5"
        app_group:
```

(continues on next page)

(continued from previous page)

```
        -
            name: "default_name_7 (source application.group.name)"
        application:
        -
            id:  "9"
        application_list: "<your_own_value> (source application.list.name)"
        av_profile: "<your_own_value> (source antivirus.profile.name)"
        cifs_profile: "<your_own_value> (source cifs.profile.name)"
        comments: "<your_own_value>"
        dlp_sensor: "<your_own_value> (source dlp.sensor.name)"
        dnsfilter_profile: "<your_own_value> (source dnsfilter.profile.name)"
        dstaddr:
        -
            name: "default_name_17 (source firewall.address.name firewall.addrgrp.
↪name firewall.vip.name firewall.vipgrp.name system.external-resource.name)"
        dstaddr_negate: "enable"
        dstaddr4:
        -
            name: "default_name_20 (source firewall.address.name firewall.addrgrp.
↪name firewall.vip.name firewall.vipgrp.name)"
        dstaddr6:
        -
            name: "default_name_22 (source firewall.address6.name firewall.addrgrp6.
↪name firewall.vip6.name firewall.vipgrp6.name)"
        dstintf:
        -
            name: "default_name_24 (source system.interface.name system.zone.name)"
        emailfilter_profile: "<your_own_value> (source emailfilter.profile.name)"
        enforce_default_app_port: "enable"
        file_filter_profile: "<your_own_value> (source file-filter.profile.name)"
        fsso_groups:
        -
            name: "default_name_29 (source user.adgrp.name)"
        global_label: "<your_own_value>"
        groups:
        -
            name: "default_name_32 (source user.group.name)"
        icap_profile: "<your_own_value> (source icap.profile.name)"
        internet_service: "enable"
        internet_service_custom:
        -
            name: "default_name_36 (source firewall.internet-service-custom.name)"
        internet_service_custom_group:
        -
            name: "default_name_38 (source firewall.internet-service-custom-group.
↪name)"
        internet_service_group:
        -
            name: "default_name_40 (source firewall.internet-service-group.name)"
        internet_service_id:
        -
            id:  "42 (source firewall.internet-service.id)"
        internet_service_name:
        -
            name: "default_name_44 (source firewall.internet-service-name.name)"
        internet_service_negate: "enable"
        internet_service_src: "enable"
```

(continues on next page)

(continued from previous page)

```
        internet_service_src_custom:
         -
            name: "default_name_48 (source firewall.internet-service-custom.name)"
        internet_service_src_custom_group:
         -
            name: "default_name_50 (source firewall.internet-service-custom-group.
↪name)"
        internet_service_src_group:
         -
            name: "default_name_52 (source firewall.internet-service-group.name)"
        internet_service_src_id:
         -
            id:  "54 (source firewall.internet-service.id)"
        internet_service_src_name:
         -
            name: "default_name_56 (source firewall.internet-service-name.name)"
        internet_service_src_negate: "enable"
        ips_sensor: "<your_own_value> (source ips.sensor.name)"
        learning_mode: "enable"
        logtraffic: "all"
        logtraffic_start: "enable"
        mms_profile: "<your_own_value> (source firewall.mms-profile.name)"
        name: "default_name_63"
        policyid: "64"
        profile_group: "<your_own_value> (source firewall.profile-group.name)"
        profile_protocol_options: "<your_own_value> (source firewall.profile-protocol-
↪options.name)"
        profile_type: "single"
        schedule: "<your_own_value> (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name firewall.schedule.group.name)"
        send_deny_packet: "disable"
        service:
         -
            name: "default_name_71 (source firewall.service.custom.name firewall.
↪service.group.name)"
        service_negate: "enable"
        srcaddr:
         -
            name: "default_name_74 (source firewall.address.name firewall.addrgrp.
↪name system.external-resource.name)"
        srcaddr_negate: "enable"
        srcaddr4:
         -
            name: "default_name_77 (source firewall.address.name firewall.addrgrp.
↪name)"
        srcaddr6:
         -
            name: "default_name_79 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        srcintf:
         -
            name: "default_name_81 (source system.interface.name system.zone.name)"
        ssh_filter_profile: "<your_own_value> (source ssh-filter.profile.name)"
        ssl_ssh_profile: "<your_own_value> (source firewall.ssl-ssh-profile.name)"
        status: "enable"
        url_category:
         -
```

(continues on next page)

(continued from previous page)

```
        id:  "86"
    users:
     -
        name: "default_name_88 (source user.local.name)"
    utm_status: "enable"
    uuid: "<your_own_value>"
    uuid_idx: "91"
    videofilter_profile: "<your_own_value> (source videofilter.profile.name)"
    voip_profile: "<your_own_value> (source voip.profile.name)"
    webfilter_profile: "<your_own_value> (source webfilter.profile.name)"
```

6.125.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.125.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.125.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.126 fortios_firewall_service_category – Configure service categories in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.126.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_service feature and category category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.126.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.126.3 FortiOS Version Compatibility

6.126.4 Parameters

6.126.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.126.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure service categories.
    fortios_firewall_service_category:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_service_category:
```

(continues on next page)

(continued from previous page)

```
        comment: "Comment."
        fabric_object: "enable"
        name: "default_name_5"
```

6.126.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.126.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.126.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.127 fortios_firewall_service_custom – Configure custom services in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.127.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_service feature and custom category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.127.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.127.3 FortiOS Version Compatibility

6.127.4 Parameters

6.127.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.127.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure custom services.
    fortios_firewall_service_custom:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_service_custom:
        app_category:
         -
            id:  "4"
        app_service_type: "disable"
        application:
         -
            id:  "7"
        category: "<your_own_value> (source firewall.service.category.name)"
        check_reset_range: "disable"
        color: "10"
        comment: "Comment."
```

(continues on next page)

(continued from previous page)

```
        fabric_object: "enable"
        fqdn: "<your_own_value>"
        helper: "auto"
        icmpcode: "15"
        icmptype: "16"
        iprange: "<your_own_value>"
        name: "default_name_18"
        protocol: "TCP/UDP/SCTP"
        protocol_number: "20"
        proxy: "enable"
        sctp_portrange: "<your_own_value>"
        session_ttl: "23"
        tcp_halfclose_timer: "24"
        tcp_halfopen_timer: "25"
        tcp_portrange: "<your_own_value>"
        tcp_rst_timer: "27"
        tcp_timewait_timer: "28"
        udp_idle_timer: "29"
        udp_portrange: "<your_own_value>"
        visibility: "enable"
```

6.127.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.127.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.127.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.128 fortios_firewall_service_group – Configure service groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.128.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_service feature and group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.128.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.128.3 FortiOS Version Compatibility

6.128.4 Parameters

6.128.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.128.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
   ansible_httpapi_port: 443
  tasks:
  - name: Configure service groups.
    fortios_firewall_service_group:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_service_group:
        color: "3"
        comment: "Comment."
        fabric_object: "enable"
        member:
         -
            name: "default_name_7 (source firewall.service.custom.name firewall.
↪service.group.name)"
        name: "default_name_8"
        proxy: "enable"
```

6.128.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.128.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.128.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.129 fortios_firewall_shaper_per_ip_shaper – Configure per-IP traffic shaper in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.129.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_shaper feature and per_ip_shaper category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.129.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.129.3 FortiOS Version Compatibility

6.129.4 Parameters

6.129.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.129.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure per-IP traffic shaper.
  fortios_firewall_shaper_per_ip_shaper:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    firewall_shaper_per_ip_shaper:
      bandwidth_unit: "kbps"
      diffserv_forward: "enable"
      diffserv_reverse: "enable"
      diffservcode_forward: "<your_own_value>"
      diffservcode_rev: "<your_own_value>"
      max_bandwidth: "8"
      max_concurrent_session: "9"
      max_concurrent_tcp_session: "10"
      max_concurrent_udp_session: "11"
      name: "default_name_12"
```

6.129.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.129.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.129.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.130 fortios_firewall_shaper_traffic_shaper – Configure shared traffic shaper in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.130.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_shaper feature and traffic_shaper category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.130.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.130.3 FortiOS Version Compatibility

6.130.4 Parameters

6.130.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.130.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure shared traffic shaper.
  fortios_firewall_shaper_traffic_shaper:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    firewall_shaper_traffic_shaper:
      bandwidth_unit: "kbps"
      diffserv: "enable"
      diffservcode: "<your_own_value>"
      dscp_marking_method: "multi-stage"
      exceed_bandwidth: "7"
      exceed_class_id: "8 (source firewall.traffic-class.class-id)"
      exceed_dscp: "<your_own_value>"
      guaranteed_bandwidth: "10"
      maximum_bandwidth: "11"
      maximum_dscp: "<your_own_value>"
      name: "default_name_13"
      overhead: "14"
      per_policy: "disable"
      priority: "low"
```

6.130.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.130.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.130.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.131 fortios_firewall_shaping_policy – Configure shaping policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.131.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and shaping_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.131.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.131.3 FortiOS Version Compatibility

6.131.4 Parameters

6.131.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.131.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure shaping policies.
    fortios_firewall_shaping_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_shaping_policy:
        app_category:
         -
            id:  "4"
        app_group:
         -
            name: "default_name_6 (source application.group.name)"
        application:
         -
            id:  "8"
        class_id: "9 (source firewall.traffic-class.class-id)"
        comment: "Comments."
        diffserv_forward: "enable"
        diffserv_reverse: "enable"
        diffservcode_forward: "<your_own_value>"
        diffservcode_rev: "<your_own_value>"
        dstaddr:
         -
            name: "default_name_16 (source firewall.address.name firewall.addrgrp.
↪name)"
        dstaddr6:
         -
            name: "default_name_18 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        dstintf:
         -
            name: "default_name_20 (source system.interface.name system.zone.name)"
        groups:
         -
            name: "default_name_22 (source user.group.name)"
        id:  "23"
        internet_service: "enable"
        internet_service_custom:
         -
            name: "default_name_26 (source firewall.internet-service-custom.name)"
        internet_service_custom_group:
         -
            name: "default_name_28 (source firewall.internet-service-custom-group.
↪name)"
        internet_service_group:
         -
            name: "default_name_30 (source firewall.internet-service-group.name)"
```

(continues on next page)

(continued from previous page)

```
        internet_service_id:
         -
            id:  "32 (source firewall.internet-service.id)"
        internet_service_name:
         -
            name: "default_name_34 (source firewall.internet-service-name.name)"
        internet_service_src: "enable"
        internet_service_src_custom:
         -
            name: "default_name_37 (source firewall.internet-service-custom.name)"
        internet_service_src_custom_group:
         -
            name: "default_name_39 (source firewall.internet-service-custom-group.
↪name)"
        internet_service_src_group:
         -
            name: "default_name_41 (source firewall.internet-service-group.name)"
        internet_service_src_id:
         -
            id:  "43 (source firewall.internet-service.id)"
        internet_service_src_name:
         -
            name: "default_name_45 (source firewall.internet-service-name.name)"
        ip_version: "4"
        name: "default_name_47"
        per_ip_shaper: "<your_own_value> (source firewall.shaper.per-ip-shaper.name)"
        schedule: "<your_own_value> (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name firewall.schedule.group.name)"
        service:
         -
            name: "default_name_51 (source firewall.service.custom.name firewall.
↪service.group.name)"
        srcaddr:
         -
            name: "default_name_53 (source firewall.address.name firewall.addrgrp.
↪name)"
        srcaddr6:
         -
            name: "default_name_55 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        srcintf:
         -
            name: "default_name_57 (source system.interface.name system.zone.name)"
        status: "enable"
        tos: "<your_own_value>"
        tos_mask: "<your_own_value>"
        tos_negate: "enable"
        traffic_shaper: "<your_own_value> (source firewall.shaper.traffic-shaper.name)
↪"
        traffic_shaper_reverse: "<your_own_value> (source firewall.shaper.traffic-
↪shaper.name)"
        url_category:
         -
            id:  "65"
        users:
         -
            name: "default_name_67 (source user.local.name)"
```

6.131.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.131.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.131.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.132 fortios_firewall_shaping_profile – Configure shaping profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.132.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and shaping_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.132.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.132.3 FortiOS Version Compatibility

6.132.4 Parameters

6.132.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.132.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure shaping profiles.
    fortios_firewall_shaping_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_shaping_profile:
        comment: "Comment."
        default_class_id: "4 (source firewall.traffic-class.class-id)"
        profile_name: "<your_own_value>"
        shaping_entries:
         -
            burst_in_msec: "7"
            cburst_in_msec: "8"
            class_id: "9 (source firewall.traffic-class.class-id)"
            guaranteed_bandwidth_percentage: "10"
            id:  "11"
            limit: "12"
            max: "13"
            maximum_bandwidth_percentage: "14"
            min: "15"
            priority: "high"
            red_probability: "17"
        type: "policing"
```

6.132.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.132.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.132.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.133 fortios_firewall_sniffer – Configure sniffer in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.133.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and sniffer category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.133.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.133.3 FortiOS Version Compatibility

6.133.4 Parameters

6.133.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.133.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure sniffer.
    fortios_firewall_sniffer:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_sniffer:
        anomaly:
         -
            action: "pass"
            log: "enable"
            name: "default_name_6"
            quarantine: "none"
            quarantine_expiry: "<your_own_value>"
            quarantine_log: "disable"
            status: "disable"
            threshold: "11"
            threshold(default): "12"
        application_list: "<your_own_value> (source application.list.name)"
        application_list_status: "enable"
        av_profile: "<your_own_value> (source antivirus.profile.name)"
        av_profile_status: "enable"
        dlp_sensor: "<your_own_value> (source dlp.sensor.name)"
        dlp_sensor_status: "enable"
        dsri: "enable"
        emailfilter_profile: "<your_own_value> (source emailfilter.profile.name)"
```

(continues on next page)

(continued from previous page)

```
        emailfilter_profile_status: "enable"
        file_filter_profile: "<your_own_value> (source file-filter.profile.name)"
        file_filter_profile_status: "enable"
        host: "myhostname"
        id:  "25"
        interface: "<your_own_value> (source system.interface.name)"
        ip_threatfeed:
         -
            name: "default_name_28 (source system.external-resource.name)"
        ip_threatfeed_status: "enable"
        ips_dos_status: "enable"
        ips_sensor: "<your_own_value> (source ips.sensor.name)"
        ips_sensor_status: "enable"
        ipv6: "enable"
        logtraffic: "all"
        max_packet_count: "35"
        non_ip: "enable"
        port: "<your_own_value>"
        protocol: "<your_own_value>"
        scan_botnet_connections: "disable"
        spamfilter_profile: "<your_own_value> (source spamfilter.profile.name)"
        spamfilter_profile_status: "enable"
        status: "enable"
        vlan: "<your_own_value>"
        webfilter_profile: "<your_own_value> (source webfilter.profile.name)"
        webfilter_profile_status: "enable"
```

6.133.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.133.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.133.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.134 fortios_firewall_ssh_host_key – SSH proxy host public keys in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.134.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_ssh feature and host_key category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.134.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.134.3 FortiOS Version Compatibility

6.134.4 Parameters

6.134.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.134.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: SSH proxy host public keys.
    fortios_firewall_ssh_host_key:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_ssh_host_key:
        hostname: "myhostname"
        ip: "<your_own_value>"
        name: "default_name_5"
        nid: "256"
        port: "7"
        public_key: "<your_own_value>"
        status: "trusted"
        type: "RSA"
```

6.134.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.134.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.134.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.135 fortios_firewall_ssh_local_ca – SSH proxy local CA in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.135.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_ssh feature and local_ca category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.135.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.135.3 FortiOS Version Compatibility

6.135.4 Parameters

6.135.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.135.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: SSH proxy local CA.
    fortios_firewall_ssh_local_ca:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_ssh_local_ca:
        name: "default_name_3"
        password: "<your_own_value>"
        private_key: "<your_own_value>"
        public_key: "<your_own_value>"
        source: "built-in"
```

6.135.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.135.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.135.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.136 fortios_firewall_ssh_local_key – SSH proxy local keys in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.136.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_ssh feature and local_key category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.136.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.136.3 FortiOS Version Compatibility

6.136.4 Parameters

6.136.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.136.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: SSH proxy local keys.
  fortios_firewall_ssh_local_key:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    firewall_ssh_local_key:
      name: "default_name_3"
      password: "<your_own_value>"
      private_key: "<your_own_value>"
      public_key: "<your_own_value>"
      source: "built-in"
```

6.136.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.136.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.136.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.137 fortios_firewall_ssh_setting – SSH proxy settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.137.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_ssh feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.137.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.137.3 FortiOS Version Compatibility

6.137.4 Parameters

6.137.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.137.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: SSH proxy settings.
    fortios_firewall_ssh_setting:
      vdom:  "{{ vdom }}"
      firewall_ssh_setting:
        caname: "<your_own_value> (source firewall.ssh.local-ca.name)"
```

(continues on next page)

(continued from previous page)

```
        host_trusted_checking: "enable"
        hostkey_dsa1024: "myhostname (source firewall.ssh.local-key.name)"
        hostkey_ecdsa256: "myhostname (source firewall.ssh.local-key.name)"
        hostkey_ecdsa384: "myhostname (source firewall.ssh.local-key.name)"
        hostkey_ecdsa521: "myhostname (source firewall.ssh.local-key.name)"
        hostkey_ed25519: "myhostname (source firewall.ssh.local-key.name)"
        hostkey_rsa2048: "myhostname (source firewall.ssh.local-key.name)"
        untrusted_caname: "<your_own_value> (source firewall.ssh.local-ca.name)"
```

6.137.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.137.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.137.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.138 fortios_firewall_ssl_server – Configure SSL servers in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.138.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and ssl_server category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.138.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.138.3 FortiOS Version Compatibility

6.138.4 Parameters

6.138.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.138.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure SSL servers.
    fortios_firewall_ssl_server:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_ssl_server:
        add_header_x_forwarded_proto: "enable"
        ip: "<your_own_value>"
        mapped_port: "5"
        name: "default_name_6"
```

(continues on next page)

(continued from previous page)

```
        port: "7"
        ssl_algorithm: "high"
        ssl_cert: "<your_own_value> (source vpn.certificate.local.name)"
        ssl_client_renegotiation: "allow"
        ssl_dh_bits: "768"
        ssl_max_version: "tls-1.0"
        ssl_min_version: "tls-1.0"
        ssl_mode: "half"
        ssl_send_empty_frags: "enable"
        url_rewrite: "enable"
```

6.138.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.138.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.138.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.139 fortios_firewall_ssl_setting – SSL proxy settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.139.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_ssl feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.139.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.139.3 FortiOS Version Compatibility

6.139.4 Parameters

6.139.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.139.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: SSL proxy settings.
    fortios_firewall_ssl_setting:
      vdom:  "{{ vdom }}"
      firewall_ssl_setting:
        abbreviate_handshake: "enable"
        cert_cache_capacity: "4"
```

(continues on next page)

(continued from previous page)

```
        cert_cache_timeout: "5"
        kxp_queue_threshold: "6"
        no_matching_cipher_action: "bypass"
        proxy_connect_timeout: "8"
        session_cache_capacity: "9"
        session_cache_timeout: "10"
        ssl_dh_bits: "768"
        ssl_queue_threshold: "12"
        ssl_send_empty_frags: "enable"
```

6.139.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.139.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.139.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.140 fortios_firewall_ssl_ssh_profile – Configure SSL/SSH protocol options in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.140.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and ssl_ssh_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.140.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.140.3 FortiOS Version Compatibility

6.140.4 Parameters

6.140.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.140.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure SSL/SSH protocol options.
    fortios_firewall_ssl_ssh_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_ssl_ssh_profile:
        allowlist: "enable"
        block_blacklisted_certificates: "disable"
```

(continues on next page)

(continued from previous page)

```
        block_blocklisted_certificates: "disable"
        caname: "<your_own_value> (source vpn.certificate.local.name)"
        comment: "Optional comments."
        dot:
            cert_validation_failure: "allow"
            cert_validation_timeout: "allow"
            client_certificate: "bypass"
            expired_server_cert: "allow"
            proxy_after_tcp_handshake: "enable"
            revoked_server_cert: "allow"
            sni_server_cert_check: "enable"
            status: "disable"
            unsupported_ssl_cipher: "allow"
            unsupported_ssl_negotiation: "allow"
            untrusted_server_cert: "allow"
        ftps:
            allow_invalid_server_cert: "enable"
            cert_validation_failure: "allow"
            cert_validation_timeout: "allow"
            client_cert_request: "bypass"
            client_certificate: "bypass"
            expired_server_cert: "allow"
            invalid_server_cert: "allow"
            ports: "28"
            revoked_server_cert: "allow"
            sni_server_cert_check: "enable"
            status: "disable"
            unsupported_ssl: "bypass"
            unsupported_ssl_cipher: "allow"
            unsupported_ssl_negotiation: "allow"
            untrusted_cert: "allow"
            untrusted_server_cert: "allow"
        https:
            allow_invalid_server_cert: "enable"
            cert_probe_failure: "allow"
            cert_validation_failure: "allow"
            cert_validation_timeout: "allow"
            client_cert_request: "bypass"
            client_certificate: "bypass"
            expired_server_cert: "allow"
            invalid_server_cert: "allow"
            ports: "46"
            proxy_after_tcp_handshake: "enable"
            revoked_server_cert: "allow"
            sni_server_cert_check: "enable"
            status: "disable"
            unsupported_ssl: "bypass"
            unsupported_ssl_cipher: "allow"
            unsupported_ssl_negotiation: "allow"
            untrusted_cert: "allow"
            untrusted_server_cert: "allow"
        imaps:
            allow_invalid_server_cert: "enable"
            cert_validation_failure: "allow"
            cert_validation_timeout: "allow"
            client_cert_request: "bypass"
            client_certificate: "bypass"
```

(continues on next page)

(continued from previous page)

```
            expired_server_cert: "allow"
            invalid_server_cert: "allow"
            ports: "64"
            proxy_after_tcp_handshake: "enable"
            revoked_server_cert: "allow"
            sni_server_cert_check: "enable"
            status: "disable"
            unsupported_ssl: "bypass"
            unsupported_ssl_cipher: "allow"
            unsupported_ssl_negotiation: "allow"
            untrusted_cert: "allow"
            untrusted_server_cert: "allow"
        mapi_over_https: "enable"
        name: "default_name_75"
        pop3s:
            allow_invalid_server_cert: "enable"
            cert_validation_failure: "allow"
            cert_validation_timeout: "allow"
            client_cert_request: "bypass"
            client_certificate: "bypass"
            expired_server_cert: "allow"
            invalid_server_cert: "allow"
            ports: "84"
            proxy_after_tcp_handshake: "enable"
            revoked_server_cert: "allow"
            sni_server_cert_check: "enable"
            status: "disable"
            unsupported_ssl: "bypass"
            unsupported_ssl_cipher: "allow"
            unsupported_ssl_negotiation: "allow"
            untrusted_cert: "allow"
            untrusted_server_cert: "allow"
        rpc_over_https: "enable"
        server_cert: "<your_own_value> (source vpn.certificate.local.name)"
        server_cert_mode: "re-sign"
        smtps:
            allow_invalid_server_cert: "enable"
            cert_validation_failure: "allow"
            cert_validation_timeout: "allow"
            client_cert_request: "bypass"
            client_certificate: "bypass"
            expired_server_cert: "allow"
            invalid_server_cert: "allow"
            ports: "105"
            proxy_after_tcp_handshake: "enable"
            revoked_server_cert: "allow"
            sni_server_cert_check: "enable"
            status: "disable"
            unsupported_ssl: "bypass"
            unsupported_ssl_cipher: "allow"
            unsupported_ssl_negotiation: "allow"
            untrusted_cert: "allow"
            untrusted_server_cert: "allow"
        ssh:
            inspect_all: "disable"
            ports: "117"
            proxy_after_tcp_handshake: "enable"
```

(continues on next page)

(continued from previous page)

```
            ssh_algorithm: "compatible"
            ssh_policy_check: "disable"
            ssh_tun_policy_check: "disable"
            status: "disable"
            unsupported_version: "bypass"
        ssl:
            allow_invalid_server_cert: "enable"
            cert_validation_failure: "allow"
            cert_validation_timeout: "allow"
            client_cert_request: "bypass"
            client_certificate: "bypass"
            expired_server_cert: "allow"
            inspect_all: "disable"
            invalid_server_cert: "allow"
            revoked_server_cert: "allow"
            sni_server_cert_check: "enable"
            unsupported_ssl: "bypass"
            unsupported_ssl_cipher: "allow"
            unsupported_ssl_negotiation: "allow"
            untrusted_cert: "allow"
            untrusted_server_cert: "allow"
        ssl_anomalies_log: "disable"
        ssl_exempt:
         -
            address: "<your_own_value> (source firewall.address.name firewall.addrgrp.
↪name)"
            address6: "<your_own_value> (source firewall.address6.name firewall.
↪addrgrp6.name)"
            fortiguard_category: "144"
            id:  "145"
            regex: "<your_own_value>"
            type: "fortiguard-category"
            wildcard_fqdn: "<your_own_value> (source firewall.wildcard-fqdn.custom.
↪name firewall.wildcard-fqdn.group.name)"
        ssl_exemptions_log: "disable"
        ssl_negotiation_log: "disable"
        ssl_server:
         -
            ftps_client_cert_request: "bypass"
            ftps_client_certificate: "bypass"
            https_client_cert_request: "bypass"
            https_client_certificate: "bypass"
            id:  "156"
            imaps_client_cert_request: "bypass"
            imaps_client_certificate: "bypass"
            ip: "<your_own_value>"
            pop3s_client_cert_request: "bypass"
            pop3s_client_certificate: "bypass"
            smtps_client_cert_request: "bypass"
            smtps_client_certificate: "bypass"
            ssl_other_client_cert_request: "bypass"
            ssl_other_client_certificate: "bypass"
        supported_alpn: "http1-1"
        untrusted_caname: "<your_own_value> (source vpn.certificate.local.name)"
        use_ssl_server: "disable"
        whitelist: "enable"
```

6.140.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.140.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.140.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.141 fortios_firewall_traffic_class – Configure names for shaping classes in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.141.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and traffic_class category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.141.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.141.3 FortiOS Version Compatibility

6.141.4 Parameters

6.141.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.141.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure names for shaping classes.
    fortios_firewall_traffic_class:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_traffic_class:
        class_id: "3"
        class_name: "<your_own_value>"
```

6.141.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.141.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.141.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.142 fortios_firewall_ttl_policy – Configure TTL policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.142.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and ttl_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.142.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.142.3 FortiOS Version Compatibility

6.142.4 Parameters

6.142.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.142.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure TTL policies.
    fortios_firewall_ttl_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_ttl_policy:
        action: "accept"
        id:  "4"
        schedule: "<your_own_value> (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name firewall.schedule.group.name)"
        service:
         -
            name: "default_name_7 (source firewall.service.custom.name firewall.
↪service.group.name)"
        srcaddr:
         -
            name: "default_name_9 (source firewall.address.name firewall.addrgrp.name)
↪"
        srcintf: "<your_own_value> (source system.zone.name system.interface.name)"
        status: "enable"
        ttl: "<your_own_value>"
```

6.142.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.142.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.142.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.143 fortios_firewall_vendor_mac – Show vendor and the MAC address they have in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.143.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vendor_mac category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.143.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.143.3 FortiOS Version Compatibility

6.143.4 Parameters

6.143.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.143.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Show vendor and the MAC address they have.
    fortios_firewall_vendor_mac:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_vendor_mac:
        id:  "3"
        mac_number: "4"
        name: "default_name_5"
```

6.143.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.143.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.143.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.144 fortios_firewall_vip – Configure virtual IP for IPv4 in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.144.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vip category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.144.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.144.3 FortiOS Version Compatibility

6.144.4 Parameters

6.144.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.144.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure virtual IP for IPv4.
    fortios_firewall_vip:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_vip:
        arp_reply: "disable"
        color: "4"
        comment: "Comment."
        dns_mapping_ttl: "6"
        extaddr:
         -
            name: "default_name_8 (source firewall.address.name firewall.addrgrp.name)
↪"
        extintf: "<your_own_value> (source system.interface.name)"
        extip: "<your_own_value>"
        extport: "<your_own_value>"
        gratuitous_arp_interval: "12"
        http_cookie_age: "13"
        http_cookie_domain: "<your_own_value>"
        http_cookie_domain_from_host: "disable"
        http_cookie_generation: "16"
        http_cookie_path: "<your_own_value>"
        http_cookie_share: "disable"
        http_ip_header: "enable"
        http_ip_header_name: "<your_own_value>"
        http_multiplex: "enable"
        http_redirect: "enable"
        https_cookie_secure: "disable"
        id:  "24"
        ldb_method: "static"
        mapped_addr: "<your_own_value> (source firewall.address.name)"
        mappedip:
         -
            range: "<your_own_value>"
        mappedport: "<your_own_value>"
        max_embryonic_connections: "30"
        monitor:
         -
            name: "default_name_32 (source firewall.ldb-monitor.name)"
        name: "default_name_33"
```

(continues on next page)

(continued from previous page)

```
        nat_source_vip: "disable"
        outlook_web_access: "disable"
        persistence: "none"
        portforward: "disable"
        portmapping_type: "1-to-1"
        protocol: "tcp"
        realservers:
         -
            address: "<your_own_value> (source firewall.address.name)"
            client_ip: "<your_own_value>"
            healthcheck: "disable"
            holddown_interval: "44"
            http_host: "myhostname"
            id:  "46"
            ip: "<your_own_value>"
            max_connections: "48"
            monitor: "<your_own_value> (source firewall.ldb-monitor.name)"
            port: "50"
            status: "active"
            type: "ip"
            weight: "53"
        server_type: "http"
        service:
         -
            name: "default_name_56 (source firewall.service.custom.name firewall.
↪service.group.name)"
        src_filter:
         -
            range: "<your_own_value>"
        srcintf_filter:
         -
            interface_name: "<your_own_value> (source system.interface.name)"
        ssl_algorithm: "high"
        ssl_certificate: "<your_own_value> (source vpn.certificate.local.name)"
        ssl_cipher_suites:
         -
            cipher: "TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256"
            priority: "65"
            versions: "ssl-3.0"
        ssl_client_fallback: "disable"
        ssl_client_rekey_count: "68"
        ssl_client_renegotiation: "allow"
        ssl_client_session_state_max: "70"
        ssl_client_session_state_timeout: "71"
        ssl_client_session_state_type: "disable"
        ssl_dh_bits: "768"
        ssl_hpkp: "disable"
        ssl_hpkp_age: "75"
        ssl_hpkp_backup: "<your_own_value> (source vpn.certificate.local.name vpn.
↪certificate.ca.name)"
        ssl_hpkp_include_subdomains: "disable"
        ssl_hpkp_primary: "<your_own_value> (source vpn.certificate.local.name vpn.
↪certificate.ca.name)"
        ssl_hpkp_report_uri: "<your_own_value>"
        ssl_hsts: "disable"
        ssl_hsts_age: "81"
        ssl_hsts_include_subdomains: "disable"
```

(continues on next page)

(continued from previous page)

```
        ssl_http_location_conversion: "enable"
        ssl_http_match_host: "enable"
        ssl_max_version: "ssl-3.0"
        ssl_min_version: "ssl-3.0"
        ssl_mode: "half"
        ssl_pfs: "require"
        ssl_send_empty_frags: "enable"
        ssl_server_algorithm: "high"
        ssl_server_cipher_suites:
         -
            cipher: "TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256"
            priority: "93"
            versions: "ssl-3.0"
        ssl_server_max_version: "ssl-3.0"
        ssl_server_min_version: "ssl-3.0"
        ssl_server_session_state_max: "97"
        ssl_server_session_state_timeout: "98"
        ssl_server_session_state_type: "disable"
        status: "disable"
        type: "static-nat"
        uuid: "<your_own_value>"
        weblogic_server: "disable"
        websphere_server: "disable"
```

6.144.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.144.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.144.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.145 fortios_firewall_vip46 – Configure IPv4 to IPv6 virtual IPs in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.145.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vip46 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.145.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.145.3 FortiOS Version Compatibility

6.145.4 Parameters

6.145.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.145.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv4 to IPv6 virtual IPs.
    fortios_firewall_vip46:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_vip46:
        arp_reply: "disable"
        color: "4"
        comment: "Comment."
        extip: "<your_own_value>"
        extport: "<your_own_value>"
        id:  "8"
        ldb_method: "static"
        mappedip: "<your_own_value>"
        mappedport: "<your_own_value>"
        monitor:
         -
            name: "default_name_13 (source firewall.ldb-monitor.name)"
        name: "default_name_14"
        portforward: "disable"
        protocol: "tcp"
        realservers:
         -
            client_ip: "<your_own_value>"
            healthcheck: "disable"
            holddown_interval: "20"
            id:  "21"
            ip: "<your_own_value>"
            max_connections: "23"
            monitor: "<your_own_value> (source firewall.ldb-monitor.name)"
            port: "25"
            status: "active"
            weight: "27"
        server_type: "http"
        src_filter:
         -
            range: "<your_own_value>"
        srcintf_filter:
         -
            interface_name: "<your_own_value> (source system.interface.name)"
        type: "static-nat"
        uuid: "<your_own_value>"
```

6.145.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.145.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.145.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.146 fortios_firewall_vip6 – Configure virtual IP for IPv6 in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.146.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vip6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.146.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.146.3 FortiOS Version Compatibility

6.146.4 Parameters

6.146.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.146.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure virtual IP for IPv6.
    fortios_firewall_vip6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_vip6:
        arp_reply: "disable"
        color: "4"
        comment: "Comment."
        extip: "<your_own_value>"
        extport: "<your_own_value>"
        http_cookie_age: "8"
        http_cookie_domain: "<your_own_value>"
        http_cookie_domain_from_host: "disable"
        http_cookie_generation: "11"
        http_cookie_path: "<your_own_value>"
        http_cookie_share: "disable"
        http_ip_header: "enable"
        http_ip_header_name: "<your_own_value>"
        http_multiplex: "enable"
        http_redirect: "enable"
        https_cookie_secure: "disable"
        id:  "19"
        ldb_method: "static"
        mappedip: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        mappedport: "<your_own_value>"
        max_embryonic_connections: "23"
        monitor:
         -
            name: "default_name_25 (source firewall.ldb-monitor.name)"
        name: "default_name_26"
        nat_source_vip: "disable"
        outlook_web_access: "disable"
        persistence: "none"
        portforward: "disable"
        protocol: "tcp"
        realservers:
         -
            client_ip: "<your_own_value>"
            healthcheck: "disable"
            holddown_interval: "35"
            http_host: "myhostname"
            id:  "37"
            ip: "<your_own_value>"
            max_connections: "39"
            monitor: "<your_own_value> (source firewall.ldb-monitor.name)"
            port: "41"
            status: "active"
            weight: "43"
        server_type: "http"
        src_filter:
         -
            range: "<your_own_value>"
        ssl_algorithm: "high"
        ssl_certificate: "<your_own_value> (source vpn.certificate.local.name)"
        ssl_cipher_suites:
         -
            cipher: "TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256"
            priority: "51"
            versions: "ssl-3.0"
        ssl_client_fallback: "disable"
        ssl_client_rekey_count: "54"
        ssl_client_renegotiation: "allow"
        ssl_client_session_state_max: "56"
        ssl_client_session_state_timeout: "57"
        ssl_client_session_state_type: "disable"
        ssl_dh_bits: "768"
        ssl_hpkp: "disable"
        ssl_hpkp_age: "61"
        ssl_hpkp_backup: "<your_own_value> (source vpn.certificate.local.name vpn.
↪certificate.ca.name)"
        ssl_hpkp_include_subdomains: "disable"
        ssl_hpkp_primary: "<your_own_value> (source vpn.certificate.local.name vpn.
↪certificate.ca.name)"
        ssl_hpkp_report_uri: "<your_own_value>"
        ssl_hsts: "disable"
        ssl_hsts_age: "67"
        ssl_hsts_include_subdomains: "disable"
        ssl_http_location_conversion: "enable"
        ssl_http_match_host: "enable"
        ssl_max_version: "ssl-3.0"
        ssl_min_version: "ssl-3.0"
```

(continues on next page)

(continued from previous page)

```
        ssl_mode: "half"
        ssl_pfs: "require"
        ssl_send_empty_frags: "enable"
        ssl_server_algorithm: "high"
        ssl_server_cipher_suites:
         -
            cipher: "TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256"
            priority: "79"
            versions: "ssl-3.0"
        ssl_server_max_version: "ssl-3.0"
        ssl_server_min_version: "ssl-3.0"
        ssl_server_session_state_max: "83"
        ssl_server_session_state_timeout: "84"
        ssl_server_session_state_type: "disable"
        type: "static-nat"
        uuid: "<your_own_value>"
        weblogic_server: "disable"
        websphere_server: "disable"
```

6.146.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.146.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.146.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.147 fortios_firewall_vip64 – Configure IPv6 to IPv4 virtual IPs in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.147.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vip64 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.147.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.147.3 FortiOS Version Compatibility

6.147.4 Parameters

6.147.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.147.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure IPv6 to IPv4 virtual IPs.
  fortios_firewall_vip64:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    firewall_vip64:
      arp_reply: "disable"
      color: "4"
      comment: "Comment."
      extip: "<your_own_value>"
      extport: "<your_own_value>"
      id:  "8"
      ldb_method: "static"
      mappedip: "<your_own_value>"
      mappedport: "<your_own_value>"
      monitor:
       -
          name: "default_name_13 (source firewall.ldb-monitor.name)"
      name: "default_name_14"
      portforward: "disable"
      protocol: "tcp"
      realservers:
       -
          client_ip: "<your_own_value>"
          healthcheck: "disable"
          holddown_interval: "20"
          id:  "21"
          ip: "<your_own_value>"
          max_connections: "23"
          monitor: "<your_own_value> (source firewall.ldb-monitor.name)"
          port: "25"
          status: "active"
          weight: "27"
      server_type: "http"
      src_filter:
       -
          range: "<your_own_value>"
      type: "static-nat"
      uuid: "<your_own_value>"
```

6.147.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.147.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.147.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.148 fortios_firewall_vipgrp – Configure IPv4 virtual IP groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.148.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vipgrp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.148.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.148.3 FortiOS Version Compatibility

6.148.4 Parameters

6.148.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.148.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv4 virtual IP groups.
    fortios_firewall_vipgrp:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_vipgrp:
        color: "3"
        comments: "<your_own_value>"
        interface: "<your_own_value> (source system.interface.name)"
        member:
         -
            name: "default_name_7 (source firewall.vip.name)"
        name: "default_name_8"
        uuid: "<your_own_value>"
```

6.148.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.148.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.148.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.149 fortios_firewall_vipgrp46 – Configure IPv4 to IPv6 virtual IP groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.149.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vipgrp46 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.149.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.149.3 FortiOS Version Compatibility

6.149.4 Parameters

6.149.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.149.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv4 to IPv6 virtual IP groups.
    fortios_firewall_vipgrp46:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_vipgrp46:
        color: "3"
        comments: "<your_own_value>"
        member:
         -
            name: "default_name_6 (source firewall.vip46.name)"
        name: "default_name_7"
        uuid: "<your_own_value>"
```

6.149.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.149.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.149.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.150 fortios_firewall_vipgrp6 – Configure IPv6 virtual IP groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.150.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vipgrp6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.150.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.150.3 FortiOS Version Compatibility

6.150.4 Parameters

6.150.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.150.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 virtual IP groups.
    fortios_firewall_vipgrp6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_vipgrp6:
        color: "3"
        comments: "<your_own_value>"
        member:
         -
            name: "default_name_6 (source firewall.vip6.name)"
        name: "default_name_7"
        uuid: "<your_own_value>"
```

6.150.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.150.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.150.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.151 fortios_firewall_vipgrp64 – Configure IPv6 to IPv4 virtual IP groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.151.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vipgrp64 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.151.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.151.3 FortiOS Version Compatibility

6.151.4 Parameters

6.151.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.151.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 to IPv4 virtual IP groups.
    fortios_firewall_vipgrp64:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_vipgrp64:
        color: "3"
        comments: "<your_own_value>"
        member:
         -
            name: "default_name_6 (source firewall.vip64.name)"
        name: "default_name_7"
        uuid: "<your_own_value>"
```

6.151.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.151.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.151.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.152 fortios_firewall_wildcard_fqdn_custom – Config global/VDOM Wildcard FQDN address in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.152.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_wildcard_fqdn feature and custom category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.152.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.152.3 FortiOS Version Compatibility

6.152.4 Parameters

6.152.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.152.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Config global/VDOM Wildcard FQDN address.
    fortios_firewall_wildcard_fqdn_custom:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_wildcard_fqdn_custom:
        color: "3"
        comment: "Comment."
        name: "default_name_5"
        uuid: "<your_own_value>"
        visibility: "enable"
        wildcard_fqdn: "<your_own_value>"
```

6.152.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.152.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.152.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.153 fortios_firewall_wildcard_fqdn_group – Config global Wildcard FQDN address groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.153.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall_wildcard_fqdn feature and group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.153.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.153.3 FortiOS Version Compatibility

6.153.4 Parameters

6.153.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.153.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Config global Wildcard FQDN address groups.
    fortios_firewall_wildcard_fqdn_group:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_wildcard_fqdn_group:
        color: "3"
        comment: "Comment."
        member:
         -
            name: "default_name_6 (source firewall.wildcard-fqdn.custom.name)"
        name: "default_name_7"
        uuid: "<your_own_value>"
        visibility: "enable"
```

6.153.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.153.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.153.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.154 fortios_ftp_proxy_explicit – Configure explicit FTP proxy settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.154.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify ftp_proxy feature and explicit category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.154.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.154.3 FortiOS Version Compatibility

6.154.4 Parameters

6.154.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.154.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure explicit FTP proxy settings.
    fortios_ftp_proxy_explicit:
      vdom:  "{{ vdom }}"
      ftp_proxy_explicit:
        incoming_ip: "<your_own_value>"
        incoming_port: "<your_own_value>"
        outgoing_ip: "<your_own_value>"
        sec_default_action: "accept"
        ssl: "enable"
        ssl_algorithm: "high"
        ssl_cert: "<your_own_value> (source certificate.local.name)"
        ssl_dh_bits: "768"
        status: "enable"
```

6.154.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.154.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.154.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.155 fortios_gtp_apn – Configure APN for GTP in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.155.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify gtp feature and apn category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.155.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.155.3 FortiOS Version Compatibility

6.155.4 Parameters

6.155.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.155.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure APN for GTP.
    fortios_gtp_apn:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      gtp_apn:
        apn: "<your_own_value>"
        name: "default_name_4"
```

6.155.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.155.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.155.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.156 fortios_gtp_apn_shaper – Global per-APN shaper in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.156.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify gtp feature and apn_shaper category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.156.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.156.3 FortiOS Version Compatibility

6.156.4 Parameters

6.156.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.156.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Global per-APN shaper.
  fortios_gtp_apn_shaper:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    gtp_apn_shaper:
      action: "drop"
      apn: "<your_own_value> (source gtp.apn.name)"
      back_off_time: "5"
      id:  "6"
      rate_limit: "7"
```

6.156.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.156.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.156.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.157 fortios_gtp_apngrp – Configure APN groups for GTP in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.157.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify gtp feature and apngrp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.157.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.157.3 FortiOS Version Compatibility

6.157.4 Parameters

6.157.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.157.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure APN groups for GTP.
    fortios_gtp_apngrp:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
    gtp_apngrp:
      member:
       -
          name: "default_name_4 (source gtp.apn.name gtp.apngrp.name)"
      name: "default_name_5"
```

6.157.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.157.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.157.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.158 fortios_gtp_ie_allow_list – IE allow list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.158.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify gtp feature and ie_allow_list category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.158.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.158.3 FortiOS Version Compatibility

6.158.4 Parameters

6.158.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.158.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: IE allow list.
    fortios_gtp_ie_allow_list:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      gtp_ie_allow_list:
        entries:
         -
            id:  "4"
            ie: "5"
            message: "6"
        name: "default_name_7"
```

6.158.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.158.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.158.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.159 fortios_gtp_ie_white_list – IE white list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.159.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify gtp feature and ie_white_list category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.159.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.159.3 FortiOS Version Compatibility

6.159.4 Parameters

6.159.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.159.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: IE white list.
    fortios_gtp_ie_white_list:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      gtp_ie_white_list:
        entries:
         -
            id:  "4"
            ie: "5"
            message: "6"
        name: "default_name_7"
```

6.159.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.159.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.159.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.160 fortios_gtp_message_filter_v0v1 – Message filter for GTPv0/v1 messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.160.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify gtp feature and message_filter_v0v1 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.160.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.160.3 FortiOS Version Compatibility

6.160.4 Parameters

6.160.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.160.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Message filter for GTPv0/v1 messages.
    fortios_gtp_message_filter_v0v1:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      gtp_message_filter_v0v1:
        create_mbms: "allow"
        create_pdp: "allow"
        data_record: "allow"
        delete_aa_pdp: "allow"
        delete_mbms: "allow"
        delete_pdp: "allow"
        echo: "allow"
        end_marker: "allow"
        error_indication: "allow"
        failure_report: "allow"
        fwd_relocation: "allow"
        fwd_srns_context: "allow"
        gtp_pdu: "allow"
        identification: "allow"
        mbms_de_registration: "allow"
        mbms_notification: "allow"
        mbms_registration: "allow"
        mbms_session_start: "allow"
        mbms_session_stop: "allow"
        mbms_session_update: "allow"
        ms_info_change_notif: "allow"
        name: "default_name_24"
        node_alive: "allow"
        note_ms_present: "allow"
        pdu_notification: "allow"
```

(continues on next page)

(continued from previous page)

```
        ran_info: "allow"
        redirection: "allow"
        relocation_cancel: "allow"
        send_route: "allow"
        sgsn_context: "allow"
        support_extension: "allow"
        unknown_message: "allow"
        unknown_message_white_list:
         -
            id:  "36"
        update_mbms: "allow"
        update_pdp: "allow"
        v0_create_aa_pdp__v1_init_pdp_ctx: "allow"
        version_not_support: "allow"
```

6.160.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.160.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.160.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.161 fortios_gtp_message_filter_v2 – Message filter for GTPv2 messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.161.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify gtp feature and message_filter_v2 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.161.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.161.3 FortiOS Version Compatibility

6.161.4 Parameters

6.161.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.161.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Message filter for GTPv2 messages.
    fortios_gtp_message_filter_v2:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    state: "present"
    access_token: "<your_own_value>"
    gtp_message_filter_v2:
      bearer_resource_cmd_fail: "allow"
      change_notification: "allow"
      create_bearer: "allow"
      create_session: "allow"
      delete_bearer_cmd_fail: "allow"
      delete_bearer_req_resp: "allow"
      delete_pdn_connection_set: "allow"
      delete_session: "allow"
      echo: "allow"
      modify_bearer_cmd_fail: "allow"
      modify_bearer_req_resp: "allow"
      name: "default_name_14"
      resume: "allow"
      suspend: "allow"
      trace_session: "allow"
      unknown_message: "allow"
      unknown_message_white_list:
       -
          id:  "20"
      update_bearer: "allow"
      update_pdn_connection_set: "allow"
      version_not_support: "allow"
```

6.161.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.161.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.161.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.162 fortios_gtp_tunnel_limit – GTP tunnel limiter in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.162.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify gtp feature and tunnel_limit category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.162.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.162.3 FortiOS Version Compatibility

6.162.4 Parameters

6.162.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.162.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: GTP tunnel limiter.
    fortios_gtp_tunnel_limit:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      gtp_tunnel_limit:
        name: "default_name_3"
        tunnel_limit: "4"
```

6.162.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.162.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.162.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.163 fortios_hardware_nic – Display NIC information in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.163.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify hardware feature and nic category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.163.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.163.3 FortiOS Version Compatibility

6.163.4 Parameters

6.163.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.163.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Display NIC information.
  fortios_hardware_nic:
    vdom:  "{{ vdom }}"
    hardware_nic:
      <nic>: "<your_own_value>"
```

6.163.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.163.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.163.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.164 fortios_hardware_npu_np6_dce – Show NP6 non-zero subengine drop counters in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.164.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify hardware_npu_np6 feature and dce category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.164.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.164.3 FortiOS Version Compatibility

6.164.4 Parameters

6.164.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.164.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Show NP6 non-zero subengine drop counters.
    fortios_hardware_npu_np6_dce:
      vdom:  "{{ vdom }}"
      hardware_npu_np6_dce:
        <dev_id>: "<your_own_value>"
```

6.164.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.164.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.164.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.165 fortios_hardware_npu_np6_session_stats – Show NP6 session offloading statistics counters in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.165.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify hardware_npu_np6 feature and session_stats category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.165.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.165.3 FortiOS Version Compatibility

6.165.4 Parameters

6.165.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.165.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Show NP6 session offloading statistics counters.
    fortios_hardware_npu_np6_session_stats:
      vdom:  "{{ vdom }}"
      hardware_npu_np6_session_stats:
        <dev_id>: "<your_own_value>"
```

6.165.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.165.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.165.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.166 fortios_hardware_npu_np6_sse_stats – Show NP6 hardware session statistics counters in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.166.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify hardware_npu_np6 feature and sse_stats category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.166.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.166.3 FortiOS Version Compatibility

6.166.4 Parameters

6.166.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.166.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Show NP6 hardware session statistics counters.
    fortios_hardware_npu_np6_sse_stats:
      vdom:  "{{ vdom }}"
      hardware_npu_np6_sse_stats:
        <dev_id>: "<your_own_value>"
```

6.166.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.166.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.166.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.167 fortios_icap_profile – Configure ICAP profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.167.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify icap feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.167.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.167.3 FortiOS Version Compatibility

6.167.4 Parameters

6.167.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.167.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
 tasks:
 - name: Configure ICAP profiles.
   fortios_icap_profile:
     vdom:  "{{ vdom }}"
     state: "present"
     access_token: "<your_own_value>"
     icap_profile:
       icap_headers:
        -
           base64_encoding: "disable"
           content: "<your_own_value>"
           id:  "6"
           name: "default_name_7"
       methods: "delete"
       name: "default_name_9"
       preview: "disable"
       preview_data_length: "11"
       replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
       request: "disable"
       request_failure: "error"
       request_path: "<your_own_value>"
       request_server: "<your_own_value> (source icap.server.name)"
       respmod_default_action: "forward"
       respmod_forward_rules:
        -
           action: "forward"
           header_group:
            -
               case_sensitivity: "disable"
               header: "<your_own_value>"
               header_name: "<your_own_value>"
               id:  "24"
           host: "myhostname (source firewall.address.name firewall.addrgrp.name␣
↪firewall.proxy-address.name)"
           http_resp_status_code:
            -
               code: "27"
           name: "default_name_28"
       response: "disable"
       response_failure: "error"
       response_path: "<your_own_value>"
       response_req_hdr: "disable"
       response_server: "<your_own_value> (source icap.server.name)"
       streaming_content_bypass: "disable"
```

6.167.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.167.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.167.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.168 fortios_icap_server – Configure ICAP servers in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.168.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify icap feature and server category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.168.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.168.3 FortiOS Version Compatibility

6.168.4 Parameters

6.168.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.168.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure ICAP servers.
    fortios_icap_server:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      icap_server:
        ip_address: "<your_own_value>"
        ip_version: "4"
        ip6_address: "<your_own_value>"
        max_connections: "6"
        name: "default_name_7"
        port: "8"
        secure: "enable"
        ssl_cert: "<your_own_value> (source vpn.certificate.ca.name)"
```

6.168.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.168.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.168.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.169 fortios_ips_custom – Configure IPS custom signature in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.169.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify ips feature and custom category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.169.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.169.3 FortiOS Version Compatibility

6.169.4 Parameters

6.169.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.169.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPS custom signature.
    fortios_ips_custom:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      ips_custom:
        action: "pass"
        application: "<your_own_value>"
        comment: "Comment."
        location: "<your_own_value>"
        log: "disable"
        log_packet: "disable"
        os: "<your_own_value>"
        protocol: "<your_own_value>"
        rule_id: "11"
        severity: "<your_own_value>"
        sig_name: "<your_own_value>"
        signature: "<your_own_value>"
        status: "disable"
        tag: "<your_own_value>"
```

6.169.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.169.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.169.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.170 fortios_ips_decoder – Configure IPS decoder in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.170.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify ips feature and decoder category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.170.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.170.3 FortiOS Version Compatibility

6.170.4 Parameters

6.170.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.170.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPS decoder.
    fortios_ips_decoder:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      ips_decoder:
        name: "default_name_3"
        parameter:
         -
            name: "default_name_5"
            value: "<your_own_value>"
```

6.170.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.170.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.170.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.171 fortios_ips_global – Configure IPS global parameter in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.171.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify ips feature and global category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.171.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.171.3 FortiOS Version Compatibility

6.171.4 Parameters

6.171.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.171.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPS global parameter.
    fortios_ips_global:
      vdom:  "{{ vdom }}"
      ips_global:
        anomaly_mode: "periodical"
        cp_accel_mode: "none"
        database: "regular"
        deep_app_insp_db_limit: "6"
        deep_app_insp_timeout: "7"
        engine_count: "8"
        exclude_signatures: "none"
        fail_open: "enable"
        intelligent_mode: "enable"
        ips_reserve_cpu: "disable"
        ngfw_max_scan_range: "13"
        np_accel_mode: "none"
        packet_log_queue_depth: "15"
        session_limit_mode: "accurate"
        skype_client_public_ipaddr: "<your_own_value>"
        socket_size: "18"
        sync_session_ttl: "enable"
        tls_active_probe:
            interface: "<your_own_value> (source system.interface.name)"
            interface_select_method: "auto"
            source_ip: "84.230.14.43"
            source_ip6: "<your_own_value>"
            vdom: "<your_own_value> (source system.vdom.name)"
        traffic_submit: "enable"
```

6.171.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.171.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.171.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.172 fortios_ips_rule – Configure IPS rules in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.172.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify ips feature and rule category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.172.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.172.3 FortiOS Version Compatibility

6.172.4 Parameters

6.172.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.172.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPS rules.
    fortios_ips_rule:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      ips_rule:
        action: "pass"
        application: "<your_own_value>"
        date: "5"
        group: "<your_own_value>"
        location: "<your_own_value>"
        log: "disable"
        log_packet: "disable"
        metadata:
         -
            id:  "11"
            metaid: "12"
            valueid: "13"
        name: "default_name_14"
        os: "<your_own_value>"
        rev: "16"
        rule_id: "17"
        service: "<your_own_value>"
        severity: "<your_own_value>"
        status: "disable"
```

6.172.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.172.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.172.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.173 fortios_ips_rule_settings – Configure IPS rule setting in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.173.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify ips feature and rule_settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.173.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.173.3 FortiOS Version Compatibility

6.173.4 Parameters

6.173.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.173.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPS rule setting.
    fortios_ips_rule_settings:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      ips_rule_settings:
        id:  "3"
```

6.173.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.173.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.173.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.174 fortios_ips_sensor – Configure IPS sensor in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.174.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify ips feature and sensor category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.174.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.174.3 FortiOS Version Compatibility

6.174.4 Parameters

6.174.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.174.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPS sensor.
    fortios_ips_sensor:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      ips_sensor:
        block_malicious_url: "disable"
        comment: "Comment."
        entries:
         -
            action: "pass"
            application: "<your_own_value>"
            cve:
             -
                cve_entry: "<your_own_value>"
            exempt_ip:
             -
                dst_ip: "<your_own_value>"
                id:  "12"
                src_ip: "<your_own_value>"
            id:  "14"
            location: "<your_own_value>"
            log: "disable"
            log_attack_context: "disable"
            log_packet: "disable"
            os: "<your_own_value>"
            protocol: "<your_own_value>"
            quarantine: "none"
            quarantine_expiry: "<your_own_value>"
            quarantine_log: "disable"
            rate_count: "24"
            rate_duration: "25"
            rate_mode: "periodical"
            rate_track: "none"
            rule:
             -
                id:  "29"
            severity: "<your_own_value>"
            status: "disable"
        extended_log: "enable"
        filter:
         -
```

(continues on next page)

(continued from previous page)

```
            action: "pass"
            application: "<your_own_value>"
            location: "<your_own_value>"
            log: "disable"
            log_packet: "disable"
            name: "default_name_39"
            os: "<your_own_value>"
            protocol: "<your_own_value>"
            quarantine: "none"
            quarantine_expiry: "43"
            quarantine_log: "disable"
            severity: "<your_own_value>"
            status: "disable"
        name: "default_name_47"
        override:
         -
            action: "pass"
            exempt_ip:
             -
                dst_ip: "<your_own_value>"
                id:  "52"
                src_ip: "<your_own_value>"
            log: "disable"
            log_packet: "disable"
            quarantine: "none"
            quarantine_expiry: "57"
            quarantine_log: "disable"
            rule_id: "59"
            status: "disable"
        replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
        scan_botnet_connections: "disable"
```

6.174.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.174.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.174.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.175 fortios_ips_settings – Configure IPS VDOM parameter in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.175.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify ips feature and settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.175.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.175.3 FortiOS Version Compatibility

6.175.4 Parameters

6.175.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.175.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPS VDOM parameter.
    fortios_ips_settings:
      vdom:  "{{ vdom }}"
      ips_settings:
        ips_packet_quota: "3"
        packet_log_history: "4"
        packet_log_memory: "5"
        packet_log_post_attack: "6"
```

6.175.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.175.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.175.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.176 fortios_ips_view_map – configure ips view-ma in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.176.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify ips feature and view_map category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.176.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.176.3 FortiOS Version Compatibility

6.176.4 Parameters

6.176.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.176.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: configure ips view-map
  fortios_ips_view_map:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    ips_view_map:
      id:  "3"
      id_policy_id: "4"
      policy_id: "5"
      vdom_id: "6"
      which: "firewall"
```

6.176.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.176.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.176.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.177 fortios_log_custom_field – Configure custom log fields in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.177.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log feature and custom_field category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.177.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.177.3 FortiOS Version Compatibility

6.177.4 Parameters

6.177.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.177.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure custom log fields.
    fortios_log_custom_field:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
    log_custom_field:
      id:  "3"
      name: "default_name_4"
      value: "<your_own_value>"
```

6.177.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.177.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.177.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.178 fortios_log_disk_filter – Configure filters for local disk logging. Use these filters to determine the log messages to record according to severity and type in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.178.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_disk feature and filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.178.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.178.3 FortiOS Version Compatibility

6.178.4 Parameters

6.178.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.178.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure filters for local disk logging. Use these filters to determine␣
↪the log messages to record according to severity and type.
    fortios_log_disk_filter:
      vdom:  "{{ vdom }}"
      log_disk_filter:
        admin: "enable"
        anomaly: "enable"
        auth: "enable"
        cpu_memory_usage: "enable"
        dhcp: "enable"
```

(continues on next page)

(continued from previous page)

```
        dlp_archive: "enable"
        dns: "enable"
        event: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "18"
        gtp: "enable"
        ha: "enable"
        ipsec: "enable"
        ldb_monitor: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        notification: "enable"
        pattern: "enable"
        ppp: "enable"
        radius: "enable"
        severity: "emergency"
        sniffer_traffic: "enable"
        ssh: "enable"
        sslvpn_log_adm: "enable"
        sslvpn_log_auth: "enable"
        sslvpn_log_session: "enable"
        system: "enable"
        vip_ssl: "enable"
        voip: "enable"
        wan_opt: "enable"
        wireless_activity: "enable"
```

6.178.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.178.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.178.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.179 fortios_log_disk_setting – Settings for local disk logging in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.179.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_disk feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.179.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.179.3 FortiOS Version Compatibility

6.179.4 Parameters

6.179.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.179.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Settings for local disk logging.
    fortios_log_disk_setting:
      vdom:  "{{ vdom }}"
      log_disk_setting:
        diskfull: "overwrite"
        dlp_archive_quota: "4"
        full_final_warning_threshold: "5"
        full_first_warning_threshold: "6"
        full_second_warning_threshold: "7"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        ips_archive: "enable"
        log_quota: "11"
        max_log_file_size: "12"
        max_policy_packet_capture_size: "13"
        maximum_log_age: "14"
        report_quota: "15"
        roll_day: "sunday"
        roll_schedule: "daily"
        roll_time: "<your_own_value>"
        source_ip: "84.230.14.43"
        status: "enable"
        upload: "enable"
        upload_delete_files: "enable"
        upload_destination: "ftp-server"
        upload_ssl_conn: "default"
        uploaddir: "<your_own_value>"
        uploadip: "<your_own_value>"
        uploadpass: "<your_own_value>"
        uploadport: "28"
        uploadsched: "disable"
        uploadtime: "<your_own_value>"
        uploadtype: "traffic"
        uploaduser: "<your_own_value>"
```

6.179.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.179.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.179.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.180 fortios_log_eventfilter – Configure log event filters in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.180.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log feature and eventfilter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.180.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.180.3 FortiOS Version Compatibility

6.180.4 Parameters

6.180.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.180.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure log event filters.
    fortios_log_eventfilter:
      vdom:  "{{ vdom }}"
      log_eventfilter:
        cifs: "enable"
        compliance_check: "enable"
        connector: "enable"
        endpoint: "enable"
        event: "enable"
        fortiextender: "enable"
        ha: "enable"
        router: "enable"
        sdwan: "enable"
        security_rating: "enable"
        switch_controller: "enable"
        system: "enable"
        user: "enable"
        vpn: "enable"
        wan_opt: "enable"
        wireless_activity: "enable"
```

6.180.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.180.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.180.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.181 fortios_log_fortianalyzer2_filter – Filters for FortiAnalyzer in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.181.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer2 feature and filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.181.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.181.3 FortiOS Version Compatibility

6.181.4 Parameters

6.181.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.181.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Filters for FortiAnalyzer.
    fortios_log_fortianalyzer2_filter:
      vdom:  "{{ vdom }}"
      log_fortianalyzer2_filter:
        anomaly: "enable"
        dlp_archive: "enable"
        dns: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "13"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        severity: "emergency"
        sniffer_traffic: "enable"
        ssh: "enable"
        voip: "enable"
```

6.181.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.181.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.181.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.182 fortios_log_fortianalyzer2_override_filter – Override filters for FortiAnalyzer in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.182.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer2 feature and override_filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.182.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.182.3 FortiOS Version Compatibility

6.182.4 Parameters

6.182.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.182.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override filters for FortiAnalyzer.
    fortios_log_fortianalyzer2_override_filter:
      vdom:  "{{ vdom }}"
      log_fortianalyzer2_override_filter:
        anomaly: "enable"
        dlp_archive: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "12"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        severity: "emergency"
        sniffer_traffic: "enable"
        voip: "enable"
```

6.182.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.182.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.182.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.183 fortios_log_fortianalyzer2_override_setting – Override FortiAnalyzer settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.183.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer2 feature and override_setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.183.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.183.3 FortiOS Version Compatibility

6.183.4 Parameters

6.183.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.183.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override FortiAnalyzer settings.
    fortios_log_fortianalyzer2_override_setting:
      vdom:  "{{ vdom }}"
      log_fortianalyzer2_override_setting:
        __change_ip: "3"
        access_config: "enable"
        certificate: "<your_own_value> (source certificate.local.name)"
        certificate_verification: "enable"
        conn_timeout: "7"
        enc_algorithm: "high-medium"
        faz_type: "9"
        hmac_algorithm: "sha256"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        ips_archive: "enable"
        max_log_rate: "14"
        mgmt_name: "<your_own_value>"
        monitor_failure_retry_period: "16"
        monitor_keepalive_period: "17"
        override: "enable"
        preshared_key: "<your_own_value>"
        priority: "default"
        reliable: "enable"
        serial:
         -
```

(continues on next page)

(continued from previous page)

```
        name: "default_name_23"
    server: "192.168.100.40"
    source_ip: "84.230.14.43"
    ssl_min_proto_version: "default"
    status: "enable"
    upload_day: "<your_own_value>"
    upload_interval: "daily"
    upload_option: "store-and-upload"
    upload_time: "<your_own_value>"
    use_management_vdom: "enable"
```

6.183.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.183.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.183.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.184 fortios_log_fortianalyzer2_setting – Global FortiAnalyzer settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.184.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer2 feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.184.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.184.3 FortiOS Version Compatibility

6.184.4 Parameters

6.184.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.184.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Global FortiAnalyzer settings.
    fortios_log_fortianalyzer2_setting:
      vdom:  "{{ vdom }}"
      log_fortianalyzer2_setting:
        __change_ip: "3"
        access_config: "enable"
```

(continues on next page)

(continued from previous page)

```
        certificate: "<your_own_value> (source certificate.local.name)"
        certificate_verification: "enable"
        conn_timeout: "7"
        enc_algorithm: "high-medium"
        faz_type: "9"
        hmac_algorithm: "sha256"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        ips_archive: "enable"
        max_log_rate: "14"
        mgmt_name: "<your_own_value>"
        monitor_failure_retry_period: "16"
        monitor_keepalive_period: "17"
        preshared_key: "<your_own_value>"
        priority: "default"
        reliable: "enable"
        serial:
         -
            name: "default_name_22"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
        status: "enable"
        upload_day: "<your_own_value>"
        upload_interval: "daily"
        upload_option: "store-and-upload"
        upload_time: "<your_own_value>"
```

6.184.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.184.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.184.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.185 fortios_log_fortianalyzer3_filter – Filters for FortiAnalyzer in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.185.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer3 feature and filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.185.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.185.3 FortiOS Version Compatibility

6.185.4 Parameters

6.185.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.185.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Filters for FortiAnalyzer.
    fortios_log_fortianalyzer3_filter:
      vdom:  "{{ vdom }}"
      log_fortianalyzer3_filter:
        anomaly: "enable"
        dlp_archive: "enable"
        dns: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "13"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        severity: "emergency"
        sniffer_traffic: "enable"
        ssh: "enable"
        voip: "enable"
```

6.185.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.185.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.185.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.186 fortios_log_fortianalyzer3_override_filter – Override filters for FortiAnalyzer in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.186.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer3 feature and override_filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.186.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.186.3 FortiOS Version Compatibility

6.186.4 Parameters

6.186.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.186.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override filters for FortiAnalyzer.
    fortios_log_fortianalyzer3_override_filter:
      vdom:  "{{ vdom }}"
      log_fortianalyzer3_override_filter:
        anomaly: "enable"
        dlp_archive: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "12"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        severity: "emergency"
        sniffer_traffic: "enable"
        voip: "enable"
```

6.186.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.186.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.186.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.187 fortios_log_fortianalyzer3_override_setting – Override FortiAnalyzer settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.187.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer3 feature and override_setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.187.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.187.3 FortiOS Version Compatibility

6.187.4 Parameters

6.187.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.187.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override FortiAnalyzer settings.
    fortios_log_fortianalyzer3_override_setting:
      vdom:  "{{ vdom }}"
      log_fortianalyzer3_override_setting:
        __change_ip: "3"
        access_config: "enable"
        certificate: "<your_own_value> (source certificate.local.name)"
        certificate_verification: "enable"
        conn_timeout: "7"
        enc_algorithm: "high-medium"
        faz_type: "9"
        hmac_algorithm: "sha256"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        ips_archive: "enable"
        max_log_rate: "14"
        mgmt_name: "<your_own_value>"
        monitor_failure_retry_period: "16"
        monitor_keepalive_period: "17"
        override: "enable"
        preshared_key: "<your_own_value>"
        priority: "default"
        reliable: "enable"
        serial:
         -
            name: "default_name_23"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
        status: "enable"
        upload_day: "<your_own_value>"
        upload_interval: "daily"
        upload_option: "store-and-upload"
        upload_time: "<your_own_value>"
        use_management_vdom: "enable"
```

6.187.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.187.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.187.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.188 fortios_log_fortianalyzer3_setting – Global FortiAnalyzer settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.188.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer3 feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.188.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.188.3 FortiOS Version Compatibility

6.188.4 Parameters

6.188.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.188.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Global FortiAnalyzer settings.
    fortios_log_fortianalyzer3_setting:
      vdom:  "{{ vdom }}"
      log_fortianalyzer3_setting:
        __change_ip: "3"
        access_config: "enable"
        certificate: "<your_own_value> (source certificate.local.name)"
        certificate_verification: "enable"
        conn_timeout: "7"
        enc_algorithm: "high-medium"
        faz_type: "9"
        hmac_algorithm: "sha256"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        ips_archive: "enable"
        max_log_rate: "14"
        mgmt_name: "<your_own_value>"
        monitor_failure_retry_period: "16"
        monitor_keepalive_period: "17"
        preshared_key: "<your_own_value>"
        priority: "default"
        reliable: "enable"
        serial:
         -
            name: "default_name_22"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
```

(continues on next page)

(continued from previous page)

```
        status: "enable"
        upload_day: "<your_own_value>"
        upload_interval: "daily"
        upload_option: "store-and-upload"
        upload_time: "<your_own_value>"
```

6.188.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.188.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.188.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.189 fortios_log_fortianalyzer_cloud_filter – Filters for FortiAnalyzer Cloud in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.189.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer_cloud feature and filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.189.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.189.3 FortiOS Version Compatibility

6.189.4 Parameters

6.189.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.189.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Filters for FortiAnalyzer Cloud.
    fortios_log_fortianalyzer_cloud_filter:
      vdom:  "{{ vdom }}"
      log_fortianalyzer_cloud_filter:
        anomaly: "enable"
        dlp_archive: "enable"
        dns: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
```

(continues on next page)

(continued from previous page)

```
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "13"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        severity: "emergency"
        sniffer_traffic: "enable"
        ssh: "enable"
        voip: "enable"
```

6.189.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.189.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.189.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.190 fortios_log_fortianalyzer_cloud_override_filter – Override filters for FortiAnalyzer Cloud in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.190.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer_cloud feature and override_filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.190.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.190.3 FortiOS Version Compatibility

6.190.4 Parameters

6.190.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.190.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override filters for FortiAnalyzer Cloud.
    fortios_log_fortianalyzer_cloud_override_filter:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    log_fortianalyzer_cloud_override_filter:
      anomaly: "enable"
      dlp_archive: "enable"
      dns: "enable"
      filter: "<your_own_value>"
      filter_type: "include"
      forward_traffic: "enable"
      free_style:
       -
          category: "traffic"
          filter: "<your_own_value>"
          filter_type: "include"
          id:  "13"
      gtp: "enable"
      local_traffic: "enable"
      multicast_traffic: "enable"
      netscan_discovery: "<your_own_value>"
      netscan_vulnerability: "<your_own_value>"
      severity: "emergency"
      sniffer_traffic: "enable"
      ssh: "enable"
      voip: "enable"
```

6.190.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.190.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.190.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.191 fortios_log_fortianalyzer_cloud_override_setting – Override FortiAnalyzer Cloud settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.191.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer_cloud feature and override_setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.191.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.191.3 FortiOS Version Compatibility

6.191.4 Parameters

6.191.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.191.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override FortiAnalyzer Cloud settings.
    fortios_log_fortianalyzer_cloud_override_setting:
      vdom:  "{{ vdom }}"
      log_fortianalyzer_cloud_override_setting:
        faz_type: "3"
        override: "enable"
        status: "enable"
```

6.191.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.191.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.191.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.192 fortios_log_fortianalyzer_cloud_setting – Global FortiAnalyzer Cloud settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.192.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer_cloud feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.192.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.192.3 FortiOS Version Compatibility

6.192.4 Parameters

6.192.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.192.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Global FortiAnalyzer Cloud settings.
  fortios_log_fortianalyzer_cloud_setting:
    vdom:  "{{ vdom }}"
    log_fortianalyzer_cloud_setting:
      __change_ip: "3"
      access_config: "enable"
      certificate: "<your_own_value> (source certificate.local.name)"
      conn_timeout: "6"
      enc_algorithm: "high-medium"
      faz_type: "8"
      hmac_algorithm: "sha256"
      interface: "<your_own_value> (source system.interface.name)"
      interface_select_method: "auto"
      ips_archive: "enable"
      max_log_rate: "13"
      mgmt_name: "<your_own_value>"
      monitor_failure_retry_period: "15"
      monitor_keepalive_period: "16"
      preshared_key: "<your_own_value>"
      priority: "default"
      source_ip: "84.230.14.43"
      ssl_min_proto_version: "default"
      status: "enable"
      upload_day: "<your_own_value>"
      upload_interval: "daily"
      upload_option: "store-and-upload"
      upload_time: "<your_own_value>"
```

6.192.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.192.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.192.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.193 fortios_log_fortianalyzer_filter – Filters for FortiAnalyzer in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.193.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer feature and filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.193.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.193.3 FortiOS Version Compatibility

6.193.4 Parameters

6.193.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.193.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Filters for FortiAnalyzer.
    fortios_log_fortianalyzer_filter:
      vdom:  "{{ vdom }}"
      log_fortianalyzer_filter:
        anomaly: "enable"
        dlp_archive: "enable"
        dns: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "13"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        severity: "emergency"
        sniffer_traffic: "enable"
        ssh: "enable"
        voip: "enable"
```

6.193.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.193.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.193.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.194 fortios_log_fortianalyzer_override_filter – Override filters for FortiAnalyzer in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.194.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer feature and override_filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.194.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.194.3 FortiOS Version Compatibility

6.194.4 Parameters

6.194.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.194.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override filters for FortiAnalyzer.
    fortios_log_fortianalyzer_override_filter:
      vdom:  "{{ vdom }}"
      log_fortianalyzer_override_filter:
        anomaly: "enable"
        dlp_archive: "enable"
        dns: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "13"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        severity: "emergency"
        sniffer_traffic: "enable"
        ssh: "enable"
        voip: "enable"
```

6.194.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.194.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.194.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.195 fortios_log_fortianalyzer_override_setting – Override FortiAnalyzer settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.195.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer feature and override_setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.195.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.195.3 FortiOS Version Compatibility

6.195.4 Parameters

6.195.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.195.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override FortiAnalyzer settings.
    fortios_log_fortianalyzer_override_setting:
      vdom:  "{{ vdom }}"
      log_fortianalyzer_override_setting:
        __change_ip: "3"
        access_config: "enable"
        certificate: "<your_own_value> (source certificate.local.name)"
        certificate_verification: "enable"
        conn_timeout: "7"
        enc_algorithm: "high-medium"
        faz_type: "9"
        hmac_algorithm: "sha256"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        ips_archive: "enable"
        max_log_rate: "14"
        mgmt_name: "<your_own_value>"
        monitor_failure_retry_period: "16"
        monitor_keepalive_period: "17"
        override: "enable"
        preshared_key: "<your_own_value>"
        priority: "default"
        reliable: "enable"
        serial:
         -
            name: "default_name_23"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
        status: "enable"
        upload_day: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        upload_interval: "daily"
        upload_option: "store-and-upload"
        upload_time: "<your_own_value>"
        use_management_vdom: "enable"
```

6.195.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.195.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.195.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.196 fortios_log_fortianalyzer_setting – Global FortiAnalyzer settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.196.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortianalyzer feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.196.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.196.3 FortiOS Version Compatibility

6.196.4 Parameters

6.196.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.196.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Global FortiAnalyzer settings.
    fortios_log_fortianalyzer_setting:
      vdom:  "{{ vdom }}"
      log_fortianalyzer_setting:
        __change_ip: "3"
        access_config: "enable"
        certificate: "<your_own_value> (source certificate.local.name)"
        certificate_verification: "enable"
        conn_timeout: "7"
        enc_algorithm: "high-medium"
        faz_type: "9"
        hmac_algorithm: "sha256"
        interface: "<your_own_value> (source system.interface.name)"
```

(continues on next page)

(continued from previous page)

```
        interface_select_method: "auto"
        ips_archive: "enable"
        max_log_rate: "14"
        mgmt_name: "<your_own_value>"
        monitor_failure_retry_period: "16"
        monitor_keepalive_period: "17"
        preshared_key: "<your_own_value>"
        priority: "default"
        reliable: "enable"
        serial:
         -
            name: "default_name_22"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
        status: "enable"
        upload_day: "<your_own_value>"
        upload_interval: "daily"
        upload_option: "store-and-upload"
        upload_time: "<your_own_value>"
```

6.196.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.196.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.196.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.197 fortios_log_fortiguard_filter – Filters for FortiCloud in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.197.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortiguard feature and filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.197.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.197.3 FortiOS Version Compatibility

6.197.4 Parameters

6.197.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.197.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Filters for FortiCloud.
  fortios_log_fortiguard_filter:
    vdom:  "{{ vdom }}"
    log_fortiguard_filter:
      anomaly: "enable"
      dlp_archive: "enable"
      dns: "enable"
      filter: "<your_own_value>"
      filter_type: "include"
      forward_traffic: "enable"
      free_style:
       -
          category: "traffic"
          filter: "<your_own_value>"
          filter_type: "include"
          id:  "13"
      gtp: "enable"
      local_traffic: "enable"
      multicast_traffic: "enable"
      netscan_discovery: "<your_own_value>"
      netscan_vulnerability: "<your_own_value>"
      severity: "emergency"
      sniffer_traffic: "enable"
      ssh: "enable"
      voip: "enable"
```

6.197.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.197.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.197.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.198 fortios_log_fortiguard_override_filter – Override filters for FortiCloud in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.198.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortiguard feature and override_filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.198.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.198.3 FortiOS Version Compatibility

6.198.4 Parameters

6.198.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.198.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override filters for FortiCloud.
    fortios_log_fortiguard_override_filter:
      vdom:  "{{ vdom }}"
      log_fortiguard_override_filter:
        anomaly: "enable"
        dlp_archive: "enable"
        dns: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "13"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        severity: "emergency"
        sniffer_traffic: "enable"
        ssh: "enable"
        voip: "enable"
```

6.198.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.198.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.198.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.199 fortios_log_fortiguard_override_setting – Override global FortiCloud logging settings for this VDOM in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.199.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortiguard feature and override_setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.199.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.199.3 FortiOS Version Compatibility

6.199.4 Parameters

6.199.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.199.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override global FortiCloud logging settings for this VDOM.
    fortios_log_fortiguard_override_setting:
      vdom:  "{{ vdom }}"
      log_fortiguard_override_setting:
        max_log_rate: "3"
        override: "enable"
        priority: "default"
        status: "enable"
        upload_day: "<your_own_value>"
        upload_interval: "daily"
        upload_option: "store-and-upload"
        upload_time: "<your_own_value>"
```

6.199.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.199.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.199.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.200 fortios_log_fortiguard_setting – Configure logging to FortiCloud in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.200.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_fortiguard feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.200.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.200.3 FortiOS Version Compatibility

6.200.4 Parameters

6.200.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.200.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure logging to FortiCloud.
    fortios_log_fortiguard_setting:
      vdom:  "{{ vdom }}"
      log_fortiguard_setting:
        conn_timeout: "3"
        enc_algorithm: "high-medium"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        max_log_rate: "7"
        priority: "default"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
        status: "enable"
        upload_day: "<your_own_value>"
        upload_interval: "daily"
        upload_option: "store-and-upload"
        upload_time: "<your_own_value>"
```

6.200.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.200.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.200.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.201 fortios_log_gui_display – Configure how log messages are displayed on the GUI in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.201.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log feature and gui_display category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.201.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.201.3 FortiOS Version Compatibility

6.201.4 Parameters

6.201.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.201.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure how log messages are displayed on the GUI.
    fortios_log_gui_display:
      vdom:  "{{ vdom }}"
      log_gui_display:
        fortiview_unscanned_apps: "enable"
        resolve_apps: "enable"
        resolve_hosts: "enable"
```

6.201.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.201.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.201.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.202 fortios_log_memory_filter – Filters for memory buffer in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.202.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_memory feature and filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.202.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.202.3 FortiOS Version Compatibility

6.202.4 Parameters

6.202.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.202.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Filters for memory buffer.
  fortios_log_memory_filter:
    vdom:  "{{ vdom }}"
    log_memory_filter:
      admin: "enable"
      anomaly: "enable"
      auth: "enable"
      cpu_memory_usage: "enable"
      dhcp: "enable"
      dns: "enable"
      event: "enable"
      filter: "<your_own_value>"
      filter_type: "include"
      forward_traffic: "enable"
      free_style:
       -
          category: "traffic"
          filter: "<your_own_value>"
          filter_type: "include"
          id:  "17"
      gtp: "enable"
      ha: "enable"
      ipsec: "enable"
      ldb_monitor: "enable"
      local_traffic: "enable"
      multicast_traffic: "enable"
      netscan_discovery: "<your_own_value>"
      netscan_vulnerability: "<your_own_value>"
      notification: "enable"
      pattern: "enable"
      ppp: "enable"
      radius: "enable"
      severity: "emergency"
      sniffer_traffic: "enable"
      ssh: "enable"
      sslvpn_log_adm: "enable"
      sslvpn_log_auth: "enable"
      sslvpn_log_session: "enable"
      system: "enable"
      vip_ssl: "enable"
      voip: "enable"
      wan_opt: "enable"
      wireless_activity: "enable"
```

6.202.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.202.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.202.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.203 fortios_log_memory_global_setting – Global settings for memory logging in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.203.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_memory feature and global_setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.203.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.203.3 FortiOS Version Compatibility

6.203.4 Parameters

6.203.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.203.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Global settings for memory logging.
    fortios_log_memory_global_setting:
      vdom:  "{{ vdom }}"
      log_memory_global_setting:
        full_final_warning_threshold: "3"
        full_first_warning_threshold: "4"
        full_second_warning_threshold: "5"
        max_size: "6"
```

6.203.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.203.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.203.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.204 fortios_log_memory_setting – Settings for memory buffer in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.204.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_memory feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.204.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.204.3 FortiOS Version Compatibility

6.204.4 Parameters

6.204.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.204.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Settings for memory buffer.
    fortios_log_memory_setting:
      vdom:  "{{ vdom }}"
      log_memory_setting:
        diskfull: "overwrite"
        status: "enable"
```

6.204.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.204.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.204.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.205 fortios_log_null_device_filter – Filters for null device logging in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.205.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_null_device feature and filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.205.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.205.3 FortiOS Version Compatibility

6.205.4 Parameters

6.205.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.205.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Filters for null device logging.
  fortios_log_null_device_filter:
    vdom:  "{{ vdom }}"
    log_null_device_filter:
      anomaly: "enable"
      dns: "enable"
      filter: "<your_own_value>"
      filter_type: "include"
      forward_traffic: "enable"
      free_style:
       -
          category: "traffic"
          filter: "<your_own_value>"
          filter_type: "include"
          id:  "12"
      gtp: "enable"
      local_traffic: "enable"
      multicast_traffic: "enable"
      netscan_discovery: "<your_own_value>"
      netscan_vulnerability: "<your_own_value>"
      severity: "emergency"
      sniffer_traffic: "enable"
      ssh: "enable"
      voip: "enable"
```

6.205.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.205.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.205.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.206 fortios_log_null_device_setting – Settings for null device logging in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.206.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_null_device feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.206.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.206.3 FortiOS Version Compatibility

6.206.4 Parameters

6.206.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.206.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Settings for null device logging.
    fortios_log_null_device_setting:
      vdom:  "{{ vdom }}"
      log_null_device_setting:
        status: "enable"
```

6.206.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.206.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.206.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.207 fortios_log_setting – Configure general log settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.207.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.207.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.207.3 FortiOS Version Compatibility

6.207.4 Parameters

6.207.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.207.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure general log settings.
    fortios_log_setting:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    log_setting:
      brief_traffic_format: "enable"
      custom_log_fields:
       -
          field_id: "<your_own_value> (source log.custom-field.id)"
      daemon_log: "enable"
      expolicy_implicit_log: "enable"
      faz_override: "enable"
      fortiview_weekly_data: "enable"
      fwpolicy_implicit_log: "enable"
      fwpolicy6_implicit_log: "enable"
      local_in_allow: "enable"
      local_in_deny_broadcast: "enable"
      local_in_deny_unicast: "enable"
      local_out: "enable"
      log_invalid_packet: "enable"
      log_policy_comment: "enable"
      log_policy_name: "enable"
      log_user_in_upper: "enable"
      neighbor_event: "enable"
      resolve_ip: "enable"
      resolve_port: "enable"
      syslog_override: "enable"
      user_anonymize: "enable"
```

6.207.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.207.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.207.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.208 fortios_log_syslogd2_filter – Filters for remote system server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.208.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd2 feature and filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.208.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.208.3 FortiOS Version Compatibility

6.208.4 Parameters

6.208.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.208.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Filters for remote system server.
    fortios_log_syslogd2_filter:
      vdom:  "{{ vdom }}"
      log_syslogd2_filter:
        anomaly: "enable"
        dns: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "12"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        severity: "emergency"
        sniffer_traffic: "enable"
        ssh: "enable"
        voip: "enable"
```

6.208.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.208.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.208.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.209 fortios_log_syslogd2_override_filter – Override filters for remote system server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.209.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd2 feature and override_filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.209.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.209.3 FortiOS Version Compatibility

6.209.4 Parameters

6.209.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.209.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override filters for remote system server.
    fortios_log_syslogd2_override_filter:
      vdom:  "{{ vdom }}"
      log_syslogd2_override_filter:
        anomaly: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "11"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        severity: "emergency"
        sniffer_traffic: "enable"
        voip: "enable"
```

6.209.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.209.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.209.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.210 fortios_log_syslogd2_override_setting – Override settings for remote syslog server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.210.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd2 feature and override_setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.210.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.210.3 FortiOS Version Compatibility

6.210.4 Parameters

6.210.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.210.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override settings for remote syslog server.
    fortios_log_syslogd2_override_setting:
      vdom:  "{{ vdom }}"
      log_syslogd2_override_setting:
        certificate: "<your_own_value> (source certificate.local.name)"
        custom_field_name:
         -
            custom: "<your_own_value>"
            id:  "6"
            name: "default_name_7"
        enc_algorithm: "high-medium"
        facility: "kernel"
        format: "default"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        max_log_rate: "13"
        mode: "udp"
        override: "enable"
        port: "16"
        priority: "default"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
        status: "enable"
        syslog_type: "22"
```

6.210.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.210.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.210.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.211 fortios_log_syslogd2_setting – Global settings for remote syslog server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.211.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd2 feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.211.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.211.3 FortiOS Version Compatibility

6.211.4 Parameters

6.211.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.211.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Global settings for remote syslog server.
    fortios_log_syslogd2_setting:
      vdom:  "{{ vdom }}"
      log_syslogd2_setting:
        certificate: "<your_own_value> (source certificate.local.name)"
        custom_field_name:
         -
            custom: "<your_own_value>"
            id:  "6"
            name: "default_name_7"
        enc_algorithm: "high-medium"
        facility: "kernel"
        format: "default"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        max_log_rate: "13"
        mode: "udp"
        port: "15"
        priority: "default"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
        status: "enable"
        syslog_type: "21"
```

6.211.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.211.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.211.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.212 fortios_log_syslogd3_filter – Filters for remote system server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.212.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd3 feature and filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.212.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.212.3 FortiOS Version Compatibility

6.212.4 Parameters

6.212.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.212.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Filters for remote system server.
    fortios_log_syslogd3_filter:
      vdom:  "{{ vdom }}"
      log_syslogd3_filter:
        anomaly: "enable"
        dns: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "12"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        severity: "emergency"
        sniffer_traffic: "enable"
        ssh: "enable"
        voip: "enable"
```

6.212.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.212.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.212.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.213 fortios_log_syslogd3_override_filter – Override filters for remote system server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.213.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd3 feature and override_filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.213.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.213.3 FortiOS Version Compatibility

6.213.4 Parameters

6.213.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.213.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override filters for remote system server.
    fortios_log_syslogd3_override_filter:
      vdom:  "{{ vdom }}"
      log_syslogd3_override_filter:
        anomaly: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "11"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        severity: "emergency"
        sniffer_traffic: "enable"
        voip: "enable"
```

6.213.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.213.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.213.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.214 fortios_log_syslogd3_override_setting – Override settings for remote syslog server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.214.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd3 feature and override_setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.214.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.214.3 FortiOS Version Compatibility

6.214.4 Parameters

6.214.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.214.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override settings for remote syslog server.
    fortios_log_syslogd3_override_setting:
      vdom:  "{{ vdom }}"
      log_syslogd3_override_setting:
        certificate: "<your_own_value> (source certificate.local.name)"
        custom_field_name:
         -
            custom: "<your_own_value>"
            id:  "6"
            name: "default_name_7"
        enc_algorithm: "high-medium"
        facility: "kernel"
        format: "default"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        max_log_rate: "13"
        mode: "udp"
        override: "enable"
        port: "16"
        priority: "default"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
        status: "enable"
        syslog_type: "22"
```

6.214.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.214.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.214.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.215 fortios_log_syslogd3_setting – Global settings for remote syslog server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.215.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd3 feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.215.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.215.3 FortiOS Version Compatibility

6.215.4 Parameters

6.215.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.215.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Global settings for remote syslog server.
    fortios_log_syslogd3_setting:
      vdom:  "{{ vdom }}"
      log_syslogd3_setting:
        certificate: "<your_own_value> (source certificate.local.name)"
        custom_field_name:
         -
            custom: "<your_own_value>"
            id:  "6"
            name: "default_name_7"
        enc_algorithm: "high-medium"
        facility: "kernel"
        format: "default"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        max_log_rate: "13"
        mode: "udp"
        port: "15"
        priority: "default"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
        status: "enable"
        syslog_type: "21"
```

6.215.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.215.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.215.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.216 fortios_log_syslogd4_filter – Filters for remote system server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.216.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd4 feature and filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.216.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.216.3 FortiOS Version Compatibility

6.216.4 Parameters

6.216.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.216.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Filters for remote system server.
    fortios_log_syslogd4_filter:
      vdom:  "{{ vdom }}"
      log_syslogd4_filter:
        anomaly: "enable"
        dns: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "12"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        severity: "emergency"
        sniffer_traffic: "enable"
        ssh: "enable"
        voip: "enable"
```

6.216.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.216.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.216.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.217 fortios_log_syslogd4_override_filter – Override filters for remote system server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.217.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd4 feature and override_filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.217.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.217.3 FortiOS Version Compatibility

6.217.4 Parameters

6.217.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.217.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override filters for remote system server.
    fortios_log_syslogd4_override_filter:
      vdom:  "{{ vdom }}"
      log_syslogd4_override_filter:
        anomaly: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "11"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        severity: "emergency"
        sniffer_traffic: "enable"
        voip: "enable"
```

6.217.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.217.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.217.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.218 fortios_log_syslogd4_override_setting – Override settings for remote syslog server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.218.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd4 feature and override_setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.218.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.218.3 FortiOS Version Compatibility

6.218.4 Parameters

6.218.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.218.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override settings for remote syslog server.
    fortios_log_syslogd4_override_setting:
      vdom:  "{{ vdom }}"
      log_syslogd4_override_setting:
        certificate: "<your_own_value> (source certificate.local.name)"
        custom_field_name:
         -
            custom: "<your_own_value>"
            id:  "6"
            name: "default_name_7"
        enc_algorithm: "high-medium"
        facility: "kernel"
        format: "default"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        max_log_rate: "13"
        mode: "udp"
        override: "enable"
        port: "16"
        priority: "default"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
        status: "enable"
        syslog_type: "22"
```

6.218.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.218.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.218.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.219 fortios_log_syslogd4_setting – Global settings for remote syslog server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.219.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd4 feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.219.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.219.3 FortiOS Version Compatibility

6.219.4 Parameters

6.219.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.219.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Global settings for remote syslog server.
    fortios_log_syslogd4_setting:
      vdom:  "{{ vdom }}"
      log_syslogd4_setting:
        certificate: "<your_own_value> (source certificate.local.name)"
        custom_field_name:
         -
            custom: "<your_own_value>"
            id:  "6"
            name: "default_name_7"
        enc_algorithm: "high-medium"
        facility: "kernel"
        format: "default"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        max_log_rate: "13"
        mode: "udp"
        port: "15"
        priority: "default"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
        status: "enable"
        syslog_type: "21"
```

6.219.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.219.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.219.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.220 fortios_log_syslogd_filter – Filters for remote system server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.220.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd feature and filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.220.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.220.3 FortiOS Version Compatibility

6.220.4 Parameters

6.220.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.220.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Filters for remote system server.
    fortios_log_syslogd_filter:
      vdom:  "{{ vdom }}"
      log_syslogd_filter:
        anomaly: "enable"
        dns: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "12"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        severity: "emergency"
        sniffer_traffic: "enable"
        ssh: "enable"
        voip: "enable"
```

6.220.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.220.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.220.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.221 fortios_log_syslogd_override_filter – Override filters for remote system server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.221.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd feature and override_filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.221.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.221.3 FortiOS Version Compatibility

6.221.4 Parameters

6.221.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.221.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override filters for remote system server.
    fortios_log_syslogd_override_filter:
      vdom:  "{{ vdom }}"
      log_syslogd_override_filter:
        anomaly: "enable"
        dns: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "12"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        severity: "emergency"
        sniffer_traffic: "enable"
        ssh: "enable"
        voip: "enable"
```

6.221.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.221.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.221.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.222 fortios_log_syslogd_override_setting – Override settings for remote syslog server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.222.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd feature and override_setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.222.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.222.3 FortiOS Version Compatibility

6.222.4 Parameters

6.222.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.222.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Override settings for remote syslog server.
    fortios_log_syslogd_override_setting:
      vdom:  "{{ vdom }}"
      log_syslogd_override_setting:
        certificate: "<your_own_value> (source certificate.local.name)"
        custom_field_name:
         -
            custom: "<your_own_value>"
            id:  "6"
            name: "default_name_7"
        enc_algorithm: "high-medium"
        facility: "kernel"
        format: "default"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        max_log_rate: "13"
        mode: "udp"
        override: "enable"
        port: "16"
        priority: "default"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
        status: "enable"
        syslog_type: "22"
```

6.222.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.222.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.222.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.223 fortios_log_syslogd_setting – Global settings for remote syslog server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.223.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_syslogd feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.223.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.223.3 FortiOS Version Compatibility

6.223.4 Parameters

6.223.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.223.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Global settings for remote syslog server.
    fortios_log_syslogd_setting:
      vdom:  "{{ vdom }}"
      log_syslogd_setting:
        certificate: "<your_own_value> (source certificate.local.name)"
        custom_field_name:
         -
            custom: "<your_own_value>"
            id:  "6"
            name: "default_name_7"
        enc_algorithm: "high-medium"
        facility: "kernel"
        format: "default"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        max_log_rate: "13"
        mode: "udp"
        port: "15"
        priority: "default"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
        status: "enable"
        syslog_type: "21"
```

6.223.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.223.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.223.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.224 fortios_log_threat_weight – Configure threat weight settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.224.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log feature and threat_weight category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.224.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.224.3 FortiOS Version Compatibility

6.224.4 Parameters

6.224.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.224.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure threat weight settings.
    fortios_log_threat_weight:
      vdom:  "{{ vdom }}"
      log_threat_weight:
        application:
         -
            category: "4"
            id:  "5"
            level: "disable"
        blocked_connection: "disable"
        botnet_connection_detected: "disable"
        failed_connection: "disable"
        geolocation:
         -
            country: "<your_own_value>"
            id:  "12"
            level: "disable"
        ips:
            critical_severity: "disable"
            high_severity: "disable"
            info_severity: "disable"
            low_severity: "disable"
            medium_severity: "disable"
        level:
            critical: "21"
```

(continues on next page)

(continued from previous page)

```
            high: "22"
            low: "23"
            medium: "24"
        malware:
            botnet_connection: "disable"
            command_blocked: "disable"
            content_disarm: "disable"
            ems_threat_feed: "disable"
            file_blocked: "disable"
            fsa_high_risk: "disable"
            fsa_malicious: "disable"
            fsa_medium_risk: "disable"
            malware_list: "disable"
            mimefragmented: "disable"
            oversized: "disable"
            switch_proto: "disable"
            virus_blocked: "disable"
            virus_file_type_executable: "disable"
            virus_infected: "disable"
            virus_outbreak_prevention: "disable"
            virus_scan_error: "disable"
        status: "enable"
        url_block_detected: "disable"
        web:
         -
            category: "46"
            id:  "47"
            level: "disable"
```

6.224.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.224.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.224.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.225 fortios_log_webtrends_filter – Filters for WebTrends in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.225.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_webtrends feature and filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.225.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.225.3 FortiOS Version Compatibility

6.225.4 Parameters

6.225.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.225.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Filters for WebTrends.
    fortios_log_webtrends_filter:
      vdom:  "{{ vdom }}"
      log_webtrends_filter:
        anomaly: "enable"
        dns: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        free_style:
         -
            category: "traffic"
            filter: "<your_own_value>"
            filter_type: "include"
            id:  "12"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        severity: "emergency"
        sniffer_traffic: "enable"
        ssh: "enable"
        voip: "enable"
```

6.225.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.225.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.225.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.226 fortios_log_webtrends_setting – Settings for WebTrends in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.226.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify log_webtrends feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.226.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.226.3 FortiOS Version Compatibility

6.226.4 Parameters

6.226.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.226.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Settings for WebTrends.
    fortios_log_webtrends_setting:
      vdom:  "{{ vdom }}"
      log_webtrends_setting:
        server: "192.168.100.40"
        status: "enable"
```

6.226.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.226.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.226.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.227 fortios_monitoring_np6_ipsec_engine – Configure NP6 IPsec engine status monitoring in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.227.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify monitoring feature and np6_ipsec_engine category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.227.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.227.3 FortiOS Version Compatibility

6.227.4 Parameters

6.227.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.227.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure NP6 IPsec engine status monitoring.
  fortios_monitoring_np6_ipsec_engine:
    vdom:  "{{ vdom }}"
    monitoring_np6_ipsec_engine:
      interval: "3"
      status: "enable"
      threshold: "<your_own_value>"
```

6.227.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.227.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.227.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.228 fortios_monitoring_npu_hpe – Configure npu-hpe status monitoring in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.228.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify monitoring feature and npu_hpe category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.228.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.228.3 FortiOS Version Compatibility

6.228.4 Parameters

6.228.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.228.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure npu-hpe status monitoring.
    fortios_monitoring_npu_hpe:
      vdom:  "{{ vdom }}"
      monitoring_npu_hpe:
        interval: "3"
        multipliers: "<your_own_value>"
        status: "enable"
```

6.228.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.228.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.228.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.229 fortios_nsxt_service_chain – Configure NSX-T service chain in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.229.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify nsxt feature and service_chain category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.229.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.229.3 FortiOS Version Compatibility

6.229.4 Parameters

6.229.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.229.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure NSX-T service chain.
    fortios_nsxt_service_chain:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      nsxt_service_chain:
        id:  "3"
        name: "default_name_4"
        service_index:
         -
            id:  "6"
            name: "default_name_7"
            reverse_index: "8"
            vd: "<your_own_value> (source system.vdom.name)"
```

6.229.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.229.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.229.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.230 fortios_nsxt_setting – Configure NSX-T setting in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.230.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify nsxt feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.230.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.230.3 FortiOS Version Compatibility

6.230.4 Parameters

6.230.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.230.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure NSX-T setting.
    fortios_nsxt_setting:
      vdom:  "{{ vdom }}"
      nsxt_setting:
        liveness: "enable"
        service: "<your_own_value>"
```

6.230.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.230.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.230.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.231 fortios_report_chart – Report chart widget configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.231.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify report feature and chart category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.231.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.231.3 FortiOS Version Compatibility

6.231.4 Parameters

6.231.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.231.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Report chart widget configuration.
    fortios_report_chart:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      report_chart:
        background: "<your_own_value>"
        category: "misc"
        category_series:
            databind: "<your_own_value>"
            font_size: "7"
        color_palette: "<your_own_value>"
        column:
         -
            detail_unit: "<your_own_value>"
            detail_value: "<your_own_value>"
            footer_unit: "<your_own_value>"
            footer_value: "<your_own_value>"
            header_value: "<your_own_value>"
            id:  "15"
            mapping:
             -
                displayname: "<your_own_value>"
                id:  "18"
                op: "none"
                value_type: "integer"
                value1: "<your_own_value>"
                value2: "<your_own_value>"
        comments: "<your_own_value>"
        dataset: "<your_own_value>"
        dimension: "2D"
        drill_down_charts:
         -
            chart_name: "<your_own_value>"
            id:  "28"
            status: "enable"
        favorite: "no"
        graph_type: "none"
        legend: "enable"
        legend_font_size: "33"
        name: "default_name_34"
        period: "last24h"
```

(continues on next page)

(continued from previous page)

```
        policy: "36"
        style: "auto"
        title: "<your_own_value>"
        title_font_size: "39"
        type: "graph"
        value_series:
            databind: "<your_own_value>"
        x_series:
            caption: "<your_own_value>"
            caption_font_size: "45"
            databind: "<your_own_value>"
            font_size: "47"
            is_category: "yes"
            label_angle: "45-degree"
            scale_direction: "decrease"
            scale_format: "YYYY-MM-DD-HH-MM"
            scale_step: "52"
            scale_unit: "minute"
            unit: "<your_own_value>"
        y_series:
            caption: "<your_own_value>"
            caption_font_size: "57"
            databind: "<your_own_value>"
            extra_databind: "<your_own_value>"
            extra_y: "enable"
            extra_y_legend: "<your_own_value>"
            font_size: "62"
            group: "<your_own_value>"
            label_angle: "45-degree"
            unit: "<your_own_value>"
            y_legend: "<your_own_value>"
```

6.231.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.231.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.231.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.232 fortios_report_dataset – Report dataset configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.232.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify report feature and dataset category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.232.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.232.3 FortiOS Version Compatibility

6.232.4 Parameters

6.232.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.232.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Report dataset configuration.
    fortios_report_dataset:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      report_dataset:
        field:
         -
            displayname: "<your_own_value>"
            id:  "5"
            name: "default_name_6"
            type: "text"
        name: "default_name_8"
        parameters:
         -
            data_type: "text"
            display_name: "<your_own_value>"
            field: "<your_own_value>"
            id:  "13"
        policy: "14"
        query: "<your_own_value>"
```

6.232.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.232.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.232.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.233 fortios_report_layout – Report layout configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.233.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify report feature and layout category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.233.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.233.3 FortiOS Version Compatibility

6.233.4 Parameters

6.233.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.233.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Report layout configuration.
    fortios_report_layout:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      report_layout:
        body_item:
         -
            chart: "<your_own_value>"
            chart_options: "include-no-data"
            column: "6"
            content: "<your_own_value>"
            description: "<your_own_value>"
            drill_down_items: "<your_own_value>"
            drill_down_types: "<your_own_value>"
            hide: "enable"
            id:  "12"
            img_src: "<your_own_value>"
            list:
             -
                content: "<your_own_value>"
                id:  "16"
            list_component: "bullet"
            misc_component: "hline"
            parameters:
             -
                id:  "20"
                name: "default_name_21"
                value: "<your_own_value>"
            style: "<your_own_value>"
            table_caption_style: "<your_own_value>"
            table_column_widths: "<your_own_value>"
            table_even_row_style: "<your_own_value>"
            table_head_style: "<your_own_value>"
            table_odd_row_style: "<your_own_value>"
            text_component: "text"
            title: "<your_own_value>"
            top_n: "31"
            type: "text"
        cutoff_option: "run-time"
        cutoff_time: "<your_own_value>"
        day: "sunday"
        description: "<your_own_value>"
        email_recipients: "<your_own_value>"
        email_send: "enable"
```

(continues on next page)

(continued from previous page)

```
        format: "pdf"
        max_pdf_report: "40"
        name: "default_name_41"
        options: "include-table-of-content"
        page:
            column_break_before: "heading1"
            footer:
                footer_item:
                 -
                    content: "<your_own_value>"
                    description: "<your_own_value>"
                    id:  "49"
                    img_src: "<your_own_value>"
                    style: "<your_own_value>"
                    type: "text"
                style: "<your_own_value>"
            header:
                header_item:
                 -
                    content: "<your_own_value>"
                    description: "<your_own_value>"
                    id:  "58"
                    img_src: "<your_own_value>"
                    style: "<your_own_value>"
                    type: "text"
                style: "<your_own_value>"
            options: "header-on-first-page"
            page_break_before: "heading1"
            paper: "a4"
        schedule_type: "demand"
        style_theme: "<your_own_value>"
        subtitle: "<your_own_value>"
        time: "<your_own_value>"
        title: "<your_own_value>"
```

6.233.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.233.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.233.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.234 fortios_report_setting – Report setting configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.234.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify report feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.234.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.234.3 FortiOS Version Compatibility

6.234.4 Parameters

6.234.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.234.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Report setting configuration.
    fortios_report_setting:
      vdom:  "{{ vdom }}"
      report_setting:
        fortiview: "enable"
        pdf_report: "enable"
        report_source: "forward-traffic"
        top_n: "6"
        web_browsing_threshold: "7"
```

6.234.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.234.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.234.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.235 fortios_report_style – Report style configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.235.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify report feature and style category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.235.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.235.3 FortiOS Version Compatibility

6.235.4 Parameters

6.235.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.235.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Report style configuration.
    fortios_report_style:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      report_style:
        align: "left"
        bg_color: "<your_own_value>"
        border_bottom: "<your_own_value>"
        border_left: "<your_own_value>"
        border_right: "<your_own_value>"
        border_top: "<your_own_value>"
        column_gap: "<your_own_value>"
        column_span: "none"
        fg_color: "<your_own_value>"
        font_family: "Verdana"
        font_size: "<your_own_value>"
        font_style: "normal"
        font_weight: "normal"
        height: "<your_own_value>"
        line_height: "<your_own_value>"
        margin_bottom: "<your_own_value>"
        margin_left: "<your_own_value>"
        margin_right: "<your_own_value>"
        margin_top: "<your_own_value>"
        name: "default_name_22"
        options: "font"
        padding_bottom: "<your_own_value>"
        padding_left: "<your_own_value>"
        padding_right: "<your_own_value>"
        padding_top: "<your_own_value>"
        width: "<your_own_value>"
```

6.235.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.235.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.235.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.236 fortios_report_theme – Report themes configuratio in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.236.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify report feature and theme category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.236.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.236.3 FortiOS Version Compatibility

6.236.4 Parameters

6.236.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.236.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Report themes configuration
    fortios_report_theme:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      report_theme:
        bullet_list_style: "<your_own_value>"
        column_count: "1"
        default_html_style: "<your_own_value>"
        default_pdf_style: "<your_own_value>"
        graph_chart_style: "<your_own_value>"
        heading1_style: "<your_own_value>"
        heading2_style: "<your_own_value>"
        heading3_style: "<your_own_value>"
        heading4_style: "<your_own_value>"
        hline_style: "<your_own_value>"
        image_style: "<your_own_value>"
        name: "default_name_14"
        normal_text_style: "<your_own_value>"
        numbered_list_style: "<your_own_value>"
        page_footer_style: "<your_own_value>"
        page_header_style: "<your_own_value>"
        page_orient: "portrait"
        page_style: "<your_own_value>"
        report_subtitle_style: "<your_own_value>"
        report_title_style: "<your_own_value>"
        table_chart_caption_style: "<your_own_value>"
        table_chart_even_row_style: "<your_own_value>"
        table_chart_head_style: "<your_own_value>"
        table_chart_odd_row_style: "<your_own_value>"
        table_chart_style: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        toc_heading1_style: "<your_own_value>"
        toc_heading2_style: "<your_own_value>"
        toc_heading3_style: "<your_own_value>"
        toc_heading4_style: "<your_own_value>"
        toc_title_style: "<your_own_value>"
```

6.236.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.236.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.236.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.237 fortios_router_access_list – Configure access lists in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.237.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and access_list category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.237.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.237.3 FortiOS Version Compatibility

6.237.4 Parameters

6.237.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.237.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure access lists.
    fortios_router_access_list:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      router_access_list:
        comments: "<your_own_value>"
        name: "default_name_4"
        rule:
         -
            action: "permit"
            exact_match: "enable"
            flags: "8"
```

(continues on next page)

(continued from previous page)

```
            id:  "9"
            prefix: "<your_own_value>"
            wildcard: "<your_own_value>"
```

6.237.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.237.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.237.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.238 fortios_router_access_list6 – Configure IPv6 access lists in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.238.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and access_list6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.238.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.238.3 FortiOS Version Compatibility

6.238.4 Parameters

6.238.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.238.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 access lists.
    fortios_router_access_list6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      router_access_list6:
        comments: "<your_own_value>"
        name: "default_name_4"
        rule:
         -
            action: "permit"
            exact_match: "enable"
            flags: "8"
            id:  "9"
            prefix6: "<your_own_value>"
```

6.238.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.238.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.238.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.239 fortios_router_aspath_list – Configure Autonomous System (AS) path lists in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.239.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and aspath_list category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.239.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.239.3 FortiOS Version Compatibility

6.239.4 Parameters

6.239.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.239.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Autonomous System (AS) path lists.
    fortios_router_aspath_list:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      router_aspath_list:
        name: "default_name_3"
        rule:
         -
            action: "deny"
            id:  "6"
            regexp: "<your_own_value>"
```

6.239.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.239.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.239.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.240 fortios_router_auth_path – Configure authentication based routing in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.240.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and auth_path category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.240.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.240.3 FortiOS Version Compatibility

6.240.4 Parameters

6.240.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.240.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure authentication based routing.
    fortios_router_auth_path:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      router_auth_path:
        device: "<your_own_value> (source system.interface.name)"
        gateway: "<your_own_value>"
        name: "default_name_5"
```

6.240.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.240.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.240.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.241 fortios_router_bfd – Configure BFD in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.241.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and bfd category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.241.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.241.3 FortiOS Version Compatibility

6.241.4 Parameters

6.241.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.241.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure BFD.
    fortios_router_bfd:
      vdom:  "{{ vdom }}"
      router_bfd:
        neighbor:
         -
            interface: "<your_own_value> (source system.interface.name)"
            ip: "<your_own_value>"
```

6.241.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.241.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.241.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.242 fortios_router_bfd6 – Configure IPv6 BFD in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.242.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and bfd6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.242.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.242.3 FortiOS Version Compatibility

6.242.4 Parameters

6.242.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.242.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 BFD.
    fortios_router_bfd6:
      vdom:  "{{ vdom }}"
      router_bfd6:
        neighbor:
         -
            interface: "<your_own_value> (source system.interface.name)"
            ip6_address: "<your_own_value>"
```

6.242.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.242.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.242.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.243 fortios_router_bgp – Configure BGP in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.243.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and bgp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.243.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.243.3 FortiOS Version Compatibility

6.243.4 Parameters

6.243.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.243.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure BGP.
  fortios_router_bgp:
    vdom:  "{{ vdom }}"
    router_bgp:
      additional_path: "enable"
      additional_path_select: "4"
      additional_path_select6: "5"
      additional_path6: "enable"
      admin_distance:
       -
          distance: "8"
          id:  "9"
          neighbour_prefix: "<your_own_value>"
          route_list: "<your_own_value> (source router.access-list.name)"
      aggregate_address:
       -
          as_set: "enable"
          id:  "14"
          prefix: "<your_own_value>"
          summary_only: "enable"
      aggregate_address6:
       -
          as_set: "enable"
          id:  "19"
          prefix6: "<your_own_value>"
          summary_only: "enable"
      always_compare_med: "enable"
      as: "23"
      bestpath_as_path_ignore: "enable"
      bestpath_cmp_confed_aspath: "enable"
      bestpath_cmp_routerid: "enable"
      bestpath_med_confed: "enable"
      bestpath_med_missing_as_worst: "enable"
      client_to_client_reflection: "enable"
      cluster_id: "<your_own_value>"
      confederation_identifier: "31"
      confederation_peers:
       -
          peer: "<your_own_value>"
      dampening: "enable"
      dampening_max_suppress_time: "35"
      dampening_reachability_half_life: "36"
      dampening_reuse: "37"
      dampening_route_map: "<your_own_value> (source router.route-map.name)"
      dampening_suppress: "39"
      dampening_unreachability_half_life: "40"
      default_local_preference: "41"
      deterministic_med: "enable"
      distance_external: "43"
      distance_internal: "44"
      distance_local: "45"
      ebgp_multipath: "enable"
      enforce_first_as: "enable"
      fast_external_failover: "enable"
      graceful_end_on_timer: "enable"
      graceful_restart: "enable"
```

(continues on next page)

(continued from previous page)

```
        graceful_restart_time: "51"
        graceful_stalepath_time: "52"
        graceful_update_delay: "53"
        holdtime_timer: "54"
        ibgp_multipath: "enable"
        ignore_optional_capability: "enable"
        keepalive_timer: "57"
        log_neighbour_changes: "enable"
        multipath_recursive_distance: "enable"
        neighbor:
         -
            activate: "enable"
            activate6: "enable"
            additional_path: "send"
            additional_path6: "send"
            adv_additional_path: "65"
            adv_additional_path6: "66"
            advertisement_interval: "67"
            allowas_in: "68"
            allowas_in_enable: "enable"
            allowas_in_enable6: "enable"
            allowas_in6: "71"
            as_override: "enable"
            as_override6: "enable"
            attribute_unchanged: "as-path"
            attribute_unchanged6: "as-path"
            bfd: "enable"
            capability_default_originate: "enable"
            capability_default_originate6: "enable"
            capability_dynamic: "enable"
            capability_graceful_restart: "enable"
            capability_graceful_restart6: "enable"
            capability_orf: "none"
            capability_orf6: "none"
            capability_route_refresh: "enable"
            conditional_advertise:
             -
                advertise_routemap: "<your_own_value> (source router.route-map.name)"
                condition_routemap: "<your_own_value> (source router.route-map.name)"
                condition_type: "exist"
            connect_timer: "89"
            default_originate_routemap: "<your_own_value> (source router.route-map.
↪name)"
            default_originate_routemap6: "<your_own_value> (source router.route-map.
↪name)"
            description: "<your_own_value>"
            distribute_list_in: "<your_own_value> (source router.access-list.name)"
            distribute_list_in6: "<your_own_value> (source router.access-list6.name)"
            distribute_list_out: "<your_own_value> (source router.access-list.name)"
            distribute_list_out6: "<your_own_value> (source router.access-list6.name)"
            dont_capability_negotiate: "enable"
            ebgp_enforce_multihop: "enable"
            ebgp_multihop_ttl: "99"
            filter_list_in: "<your_own_value> (source router.aspath-list.name)"
            filter_list_in6: "<your_own_value> (source router.aspath-list.name)"
            filter_list_out: "<your_own_value> (source router.aspath-list.name)"
            filter_list_out6: "<your_own_value> (source router.aspath-list.name)"
```

(continues on next page)

(continued from previous page)

```
            holdtime_timer: "104"
            interface: "<your_own_value> (source system.interface.name)"
            ip: "<your_own_value>"
            keep_alive_timer: "107"
            link_down_failover: "enable"
            local_as: "109"
            local_as_no_prepend: "enable"
            local_as_replace_as: "enable"
            maximum_prefix: "112"
            maximum_prefix_threshold: "113"
            maximum_prefix_threshold6: "114"
            maximum_prefix_warning_only: "enable"
            maximum_prefix_warning_only6: "enable"
            maximum_prefix6: "117"
            next_hop_self: "enable"
            next_hop_self_rr: "enable"
            next_hop_self_rr6: "enable"
            next_hop_self6: "enable"
            override_capability: "enable"
            passive: "enable"
            password: "<your_own_value>"
            prefix_list_in: "<your_own_value> (source router.prefix-list.name)"
            prefix_list_in6: "<your_own_value> (source router.prefix-list6.name)"
            prefix_list_out: "<your_own_value> (source router.prefix-list.name)"
            prefix_list_out6: "<your_own_value> (source router.prefix-list6.name)"
            remote_as: "129"
            remove_private_as: "enable"
            remove_private_as6: "enable"
            restart_time: "132"
            retain_stale_time: "133"
            route_map_in: "<your_own_value> (source router.route-map.name)"
            route_map_in6: "<your_own_value> (source router.route-map.name)"
            route_map_out: "<your_own_value> (source router.route-map.name)"
            route_map_out_preferable: "<your_own_value> (source router.route-map.name)
↪"
            route_map_out6: "<your_own_value> (source router.route-map.name)"
            route_map_out6_preferable: "<your_own_value> (source router.route-map.
↪name)"
            route_reflector_client: "enable"
            route_reflector_client6: "enable"
            route_server_client: "enable"
            route_server_client6: "enable"
            send_community: "standard"
            send_community6: "standard"
            shutdown: "enable"
            soft_reconfiguration: "enable"
            soft_reconfiguration6: "enable"
            stale_route: "enable"
            strict_capability_match: "enable"
            unsuppress_map: "<your_own_value> (source router.route-map.name)"
            unsuppress_map6: "<your_own_value> (source router.route-map.name)"
            update_source: "<your_own_value> (source system.interface.name)"
            weight: "154"
        neighbor_group:
         -
            activate: "enable"
            activate6: "enable"
```

(continues on next page)

(continued from previous page)

```
            additional_path: "send"
            additional_path6: "send"
            adv_additional_path: "160"
            adv_additional_path6: "161"
            advertisement_interval: "162"
            allowas_in: "163"
            allowas_in_enable: "enable"
            allowas_in_enable6: "enable"
            allowas_in6: "166"
            as_override: "enable"
            as_override6: "enable"
            attribute_unchanged: "as-path"
            attribute_unchanged6: "as-path"
            bfd: "enable"
            capability_default_originate: "enable"
            capability_default_originate6: "enable"
            capability_dynamic: "enable"
            capability_graceful_restart: "enable"
            capability_graceful_restart6: "enable"
            capability_orf: "none"
            capability_orf6: "none"
            capability_route_refresh: "enable"
            connect_timer: "180"
            default_originate_routemap: "<your_own_value> (source router.route-map.
↪name)"
            default_originate_routemap6: "<your_own_value> (source router.route-map.
↪name)"
            description: "<your_own_value>"
            distribute_list_in: "<your_own_value> (source router.access-list.name)"
            distribute_list_in6: "<your_own_value> (source router.access-list6.name)"
            distribute_list_out: "<your_own_value> (source router.access-list.name)"
            distribute_list_out6: "<your_own_value> (source router.access-list6.name)"
            dont_capability_negotiate: "enable"
            ebgp_enforce_multihop: "enable"
            ebgp_multihop_ttl: "190"
            filter_list_in: "<your_own_value> (source router.aspath-list.name)"
            filter_list_in6: "<your_own_value> (source router.aspath-list.name)"
            filter_list_out: "<your_own_value> (source router.aspath-list.name)"
            filter_list_out6: "<your_own_value> (source router.aspath-list.name)"
            holdtime_timer: "195"
            interface: "<your_own_value> (source system.interface.name)"
            keep_alive_timer: "197"
            link_down_failover: "enable"
            local_as: "199"
            local_as_no_prepend: "enable"
            local_as_replace_as: "enable"
            maximum_prefix: "202"
            maximum_prefix_threshold: "203"
            maximum_prefix_threshold6: "204"
            maximum_prefix_warning_only: "enable"
            maximum_prefix_warning_only6: "enable"
            maximum_prefix6: "207"
            name: "default_name_208"
            next_hop_self: "enable"
            next_hop_self_rr: "enable"
            next_hop_self_rr6: "enable"
            next_hop_self6: "enable"
```

(continues on next page)

(continued from previous page)

```
            override_capability: "enable"
            passive: "enable"
            prefix_list_in: "<your_own_value> (source router.prefix-list.name)"
            prefix_list_in6: "<your_own_value> (source router.prefix-list6.name)"
            prefix_list_out: "<your_own_value> (source router.prefix-list.name)"
            prefix_list_out6: "<your_own_value> (source router.prefix-list6.name)"
            remote_as: "219"
            remove_private_as: "enable"
            remove_private_as6: "enable"
            restart_time: "222"
            retain_stale_time: "223"
            route_map_in: "<your_own_value> (source router.route-map.name)"
            route_map_in6: "<your_own_value> (source router.route-map.name)"
            route_map_out: "<your_own_value> (source router.route-map.name)"
            route_map_out_preferable: "<your_own_value> (source router.route-map.name)
↪"
            route_map_out6: "<your_own_value> (source router.route-map.name)"
            route_map_out6_preferable: "<your_own_value> (source router.route-map.
↪name)"
            route_reflector_client: "enable"
            route_reflector_client6: "enable"
            route_server_client: "enable"
            route_server_client6: "enable"
            send_community: "standard"
            send_community6: "standard"
            shutdown: "enable"
            soft_reconfiguration: "enable"
            soft_reconfiguration6: "enable"
            stale_route: "enable"
            strict_capability_match: "enable"
            unsuppress_map: "<your_own_value> (source router.route-map.name)"
            unsuppress_map6: "<your_own_value> (source router.route-map.name)"
            update_source: "<your_own_value> (source system.interface.name)"
            weight: "244"
        neighbor_range:
         -
            id:  "246"
            max_neighbor_num: "247"
            neighbor_group: "<your_own_value> (source router.bgp.neighbor-group.name)"
            prefix: "<your_own_value>"
        neighbor_range6:
         -
            id:  "251"
            max_neighbor_num: "252"
            neighbor_group: "<your_own_value> (source router.bgp.neighbor-group.name)"
            prefix6: "<your_own_value>"
        network:
         -
            backdoor: "enable"
            id:  "257"
            prefix: "<your_own_value>"
            route_map: "<your_own_value> (source router.route-map.name)"
        network_import_check: "enable"
        network6:
         -
            backdoor: "enable"
            id:  "263"
```

(continues on next page)

(continued from previous page)

```
        prefix6: "<your_own_value>"
        route_map: "<your_own_value> (source router.route-map.name)"
    recursive_next_hop: "enable"
    redistribute:
     -
        name: "default_name_268"
        route_map: "<your_own_value> (source router.route-map.name)"
        status: "enable"
    redistribute6:
     -
        name: "default_name_272"
        route_map: "<your_own_value> (source router.route-map.name)"
        status: "enable"
    router_id: "<your_own_value>"
    scan_time: "276"
    synchronization: "enable"
    vrf_leak:
     -
        target:
         -
            interface: "<your_own_value> (source system.interface.name)"
            route_map: "<your_own_value> (source router.route-map.name)"
            vrf: "<your_own_value>"
        vrf: "<your_own_value>"
```

6.243.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.243.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.243.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.244 fortios_router_community_list – Configure community lists in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.244.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and community_list category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.244.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.244.3 FortiOS Version Compatibility

6.244.4 Parameters

6.244.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.244.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure community lists.
    fortios_router_community_list:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      router_community_list:
        name: "default_name_3"
        rule:
         -
            action: "deny"
            id:  "6"
            match: "<your_own_value>"
            regexp: "<your_own_value>"
        type: "standard"
```

6.244.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.244.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.244.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.245 fortios_router_isis – Configure IS-IS in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.245.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and isis category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.245.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.245.3 FortiOS Version Compatibility

6.245.4 Parameters

6.245.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.245.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IS-IS.
    fortios_router_isis:
      vdom:  "{{ vdom }}"
      router_isis:
        adjacency_check: "enable"
        adjacency_check6: "enable"
        adv_passive_only: "enable"
        adv_passive_only6: "enable"
        auth_keychain_l1: "<your_own_value> (source router.key-chain.name)"
        auth_keychain_l2: "<your_own_value> (source router.key-chain.name)"
        auth_mode_l1: "password"
        auth_mode_l2: "password"
        auth_password_l1: "<your_own_value>"
        auth_password_l2: "<your_own_value>"
        auth_sendonly_l1: "enable"
        auth_sendonly_l2: "enable"
        default_originate: "enable"
        default_originate6: "enable"
        dynamic_hostname: "enable"
        ignore_lsp_errors: "enable"
        is_type: "level-1-2"
        isis_interface:
         -
            auth_keychain_l1: "<your_own_value> (source router.key-chain.name)"
            auth_keychain_l2: "<your_own_value> (source router.key-chain.name)"
            auth_mode_l1: "md5"
            auth_mode_l2: "md5"
            auth_password_l1: "<your_own_value>"
            auth_password_l2: "<your_own_value>"
            auth_send_only_l1: "enable"
            auth_send_only_l2: "enable"
            circuit_type: "level-1-2"
            csnp_interval_l1: "30"
            csnp_interval_l2: "31"
            hello_interval_l1: "32"
            hello_interval_l2: "33"
            hello_multiplier_l1: "34"
            hello_multiplier_l2: "35"
            hello_padding: "enable"
            lsp_interval: "37"
            lsp_retransmit_interval: "38"
            mesh_group: "enable"
            mesh_group_id: "40"
            metric_l1: "41"
            metric_l2: "42"
            name: "default_name_43 (source system.interface.name)"
            network_type: "broadcast"
```

(continues on next page)

(continued from previous page)

```
            priority_l1: "45"
            priority_l2: "46"
            status: "enable"
            status6: "enable"
            wide_metric_l1: "49"
            wide_metric_l2: "50"
        isis_net:
         -
            id:  "52"
            net: "<your_own_value>"
        lsp_gen_interval_l1: "54"
        lsp_gen_interval_l2: "55"
        lsp_refresh_interval: "56"
        max_lsp_lifetime: "57"
        metric_style: "narrow"
        overload_bit: "enable"
        overload_bit_on_startup: "60"
        overload_bit_suppress: "external"
        redistribute:
         -
            level: "level-1-2"
            metric: "64"
            metric_type: "external"
            protocol: "<your_own_value>"
            routemap: "<your_own_value> (source router.route-map.name)"
            status: "enable"
        redistribute_l1: "enable"
        redistribute_l1_list: "<your_own_value> (source router.access-list.name)"
        redistribute_l2: "enable"
        redistribute_l2_list: "<your_own_value> (source router.access-list.name)"
        redistribute6:
         -
            level: "level-1-2"
            metric: "75"
            metric_type: "external"
            protocol: "<your_own_value>"
            routemap: "<your_own_value> (source router.route-map.name)"
            status: "enable"
        redistribute6_l1: "enable"
        redistribute6_l1_list: "<your_own_value> (source router.access-list6.name)"
        redistribute6_l2: "enable"
        redistribute6_l2_list: "<your_own_value> (source router.access-list6.name)"
        spf_interval_exp_l1: "<your_own_value>"
        spf_interval_exp_l2: "<your_own_value>"
        summary_address:
         -
            id:  "87"
            level: "level-1-2"
            prefix: "<your_own_value>"
        summary_address6:
         -
            id:  "91"
            level: "level-1-2"
            prefix6: "<your_own_value>"
```

6.245.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.245.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.245.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.246 fortios_router_key_chain – Configure key-chain in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.246.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and key_chain category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.246.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.246.3 FortiOS Version Compatibility

6.246.4 Parameters

6.246.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.246.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure key-chain.
    fortios_router_key_chain:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      router_key_chain:
        key:
         -
            accept_lifetime: "<your_own_value>"
            id:  "5"
            key_string: "<your_own_value>"
            send_lifetime: "<your_own_value>"
        name: "default_name_8"
```

6.246.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.246.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.246.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.247 fortios_router_multicast – Configure router multicast in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.247.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and multicast category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.247.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.247.3 FortiOS Version Compatibility

6.247.4 Parameters

6.247.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.247.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure router multicast.
    fortios_router_multicast:
      vdom:  "{{ vdom }}"
      router_multicast:
        interface:
         -
            bfd: "enable"
            cisco_exclude_genid: "enable"
            dr_priority: "6"
            hello_holdtime: "7"
            hello_interval: "8"
            igmp:
                access_group: "<your_own_value> (source router.access-list.name)"
                immediate_leave_group: "<your_own_value> (source router.access-list.
↪name)"
                last_member_query_count: "12"
                last_member_query_interval: "13"
                query_interval: "14"
                query_max_response_time: "15"
                query_timeout: "16"
                router_alert_check: "enable"
                version: "3"
            join_group:
             -
                address: "<your_own_value>"
            multicast_flow: "<your_own_value> (source router.multicast-flow.name)"
            name: "default_name_22 (source system.interface.name)"
            neighbour_filter: "<your_own_value> (source router.access-list.name)"
            passive: "enable"
            pim_mode: "sparse-mode"
            propagation_delay: "26"
```

(continues on next page)

(continued from previous page)

```
            rp_candidate: "enable"
            rp_candidate_group: "<your_own_value> (source router.access-list.name)"
            rp_candidate_interval: "29"
            rp_candidate_priority: "30"
            rpf_nbr_fail_back: "enable"
            rpf_nbr_fail_back_filter: "<your_own_value> (source router.access-list.
↪name)"
            state_refresh_interval: "33"
            static_group: "<your_own_value> (source router.multicast-flow.name)"
            ttl_threshold: "35"
        multicast_routing: "enable"
        pim_sm_global:
            accept_register_list: "<your_own_value> (source router.access-list.name)"
            accept_source_list: "<your_own_value> (source router.access-list.name)"
            bsr_allow_quick_refresh: "enable"
            bsr_candidate: "enable"
            bsr_hash: "42"
            bsr_interface: "<your_own_value> (source system.interface.name)"
            bsr_priority: "44"
            cisco_crp_prefix: "enable"
            cisco_ignore_rp_set_priority: "enable"
            cisco_register_checksum: "enable"
            cisco_register_checksum_group: "<your_own_value> (source router.access-
↪list.name)"
            join_prune_holdtime: "49"
            message_interval: "50"
            null_register_retries: "51"
            register_rate_limit: "52"
            register_rp_reachability: "enable"
            register_source: "disable"
            register_source_interface: "<your_own_value> (source system.interface.
↪name)"
            register_source_ip: "<your_own_value>"
            register_supression: "57"
            rp_address:
             -
                group: "<your_own_value> (source router.access-list.name)"
                id:  "60"
                ip_address: "<your_own_value>"
            rp_register_keepalive: "62"
            spt_threshold: "enable"
            spt_threshold_group: "<your_own_value> (source router.access-list.name)"
            ssm: "enable"
            ssm_range: "<your_own_value> (source router.access-list.name)"
        route_limit: "67"
        route_threshold: "68"
```

6.247.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.247.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.247.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.248 fortios_router_multicast6 – Configure IPv6 multicast in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.248.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and multicast6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.248.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.248.3 FortiOS Version Compatibility

6.248.4 Parameters

6.248.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.248.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 multicast.
    fortios_router_multicast6:
      vdom:  "{{ vdom }}"
      router_multicast6:
        interface:
         -
            hello_holdtime: "4"
            hello_interval: "5"
            name: "default_name_6 (source system.interface.name)"
        multicast_pmtu: "enable"
        multicast_routing: "enable"
        pim_sm_global:
            register_rate_limit: "10"
            rp_address:
             -
                id:  "12"
                ip6_address: "<your_own_value>"
```

6.248.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.248.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.248.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.249 fortios_router_multicast_flow – Configure multicast-flow in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.249.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and multicast_flow category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.249.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.249.3 FortiOS Version Compatibility

6.249.4 Parameters

6.249.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.249.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure multicast-flow.
    fortios_router_multicast_flow:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      router_multicast_flow:
        comments: "<your_own_value>"
        flows:
         -
            group_addr: "<your_own_value>"
            id:  "6"
            source_addr: "<your_own_value>"
        name: "default_name_8"
```

6.249.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.249.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.249.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.250 fortios_router_ospf – Configure OSPF in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.250.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and ospf category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.250.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.250.3 FortiOS Version Compatibility

6.250.4 Parameters

6.250.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.250.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure OSPF.
    fortios_router_ospf:
      vdom:  "{{ vdom }}"
      router_ospf:
        abr_type: "cisco"
        area:
         -
            authentication: "none"
            comments: "<your_own_value>"
            default_cost: "7"
            filter_list:
             -
                direction: "in"
                id:  "10"
                list: "<your_own_value> (source router.access-list.name router.prefix-
↪list.name)"
            id:  "12"
            nssa_default_information_originate: "enable"
            nssa_default_information_originate_metric: "14"
            nssa_default_information_originate_metric_type: "1"
            nssa_redistribution: "enable"
            nssa_translator_role: "candidate"
            range:
             -
                advertise: "disable"
                id:  "20"
                prefix: "<your_own_value>"
                substitute: "<your_own_value>"
                substitute_status: "enable"
            shortcut: "disable"
            stub_type: "no-summary"
            type: "regular"
            virtual_link:
             -
                authentication: "none"
                authentication_key: "<your_own_value>"
                dead_interval: "30"
                hello_interval: "31"
                md5_key: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
                md5_keychain: "<your_own_value> (source router.key-chain.name)"
                md5_keys:
                 -
                    id:  "35"
                    key_string: "<your_own_value>"
                name: "default_name_37"
                peer: "<your_own_value>"
                retransmit_interval: "39"
                transmit_delay: "40"
        auto_cost_ref_bandwidth: "41"
        bfd: "enable"
        database_overflow: "enable"
        database_overflow_max_lsas: "44"
        database_overflow_time_to_recover: "45"
        default_information_metric: "46"
        default_information_metric_type: "1"
        default_information_originate: "enable"
        default_information_route_map: "<your_own_value> (source router.route-map.
↪name)"
        default_metric: "50"
        distance: "51"
        distance_external: "52"
        distance_inter_area: "53"
        distance_intra_area: "54"
        distribute_list:
         -
            access_list: "<your_own_value> (source router.access-list.name)"
            id:  "57"
            protocol: "connected"
        distribute_list_in: "<your_own_value> (source router.access-list.name router.
↪prefix-list.name)"
        distribute_route_map_in: "<your_own_value> (source router.route-map.name)"
        log_neighbour_changes: "enable"
        neighbor:
         -
            cost: "63"
            id:  "64"
            ip: "<your_own_value>"
            poll_interval: "66"
            priority: "67"
        network:
         -
            area: "<your_own_value>"
            comments: "<your_own_value>"
            id:  "71"
            prefix: "<your_own_value>"
        ospf_interface:
         -
            authentication: "none"
            authentication_key: "<your_own_value>"
            bfd: "global"
            comments: "<your_own_value>"
            cost: "78"
            database_filter_out: "enable"
            dead_interval: "80"
            hello_interval: "81"
            hello_multiplier: "82"
```

(continues on next page)

(continued from previous page)

```
            interface: "<your_own_value> (source system.interface.name)"
            ip: "<your_own_value>"
            md5_key: "<your_own_value>"
            md5_keychain: "<your_own_value> (source router.key-chain.name)"
            md5_keys:
             -
                id:  "88"
                key_string: "<your_own_value>"
            mtu: "90"
            mtu_ignore: "enable"
            name: "default_name_92"
            network_type: "broadcast"
            prefix_length: "94"
            priority: "95"
            resync_timeout: "96"
            retransmit_interval: "97"
            status: "disable"
            transmit_delay: "99"
        passive_interface:
         -
            name: "default_name_101 (source system.interface.name)"
        redistribute:
         -
            metric: "103"
            metric_type: "1"
            name: "default_name_105"
            routemap: "<your_own_value> (source router.route-map.name)"
            status: "enable"
            tag: "108"
        restart_mode: "none"
        restart_period: "110"
        rfc1583_compatible: "enable"
        router_id: "<your_own_value>"
        spf_timers: "<your_own_value>"
        summary_address:
         -
            advertise: "disable"
            id:  "116"
            prefix: "<your_own_value>"
            tag: "118"
```

6.250.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.250.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.250.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.251 fortios_router_ospf6 – Configure IPv6 OSPF in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.251.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and ospf6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.251.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.251.3 FortiOS Version Compatibility

6.251.4 Parameters

6.251.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.251.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 OSPF.
    fortios_router_ospf6:
      vdom:  "{{ vdom }}"
      router_ospf6:
        abr_type: "cisco"
        area:
         -
            authentication: "none"
            default_cost: "6"
            id:  "7"
            ipsec_auth_alg: "md5"
            ipsec_enc_alg: "null"
            ipsec_keys:
             -
                auth_key: "<your_own_value>"
                enc_key: "<your_own_value>"
                spi: "13"
            key_rollover_interval: "14"
            nssa_default_information_originate: "enable"
            nssa_default_information_originate_metric: "16"
            nssa_default_information_originate_metric_type: "1"
            nssa_redistribution: "enable"
            nssa_translator_role: "candidate"
            range:
             -
                advertise: "disable"
                id:  "22"
                prefix6: "<your_own_value>"
            stub_type: "no-summary"
            type: "regular"
            virtual_link:
```

(continues on next page)

(continued from previous page)

```
            -
                authentication: "none"
                dead_interval: "28"
                hello_interval: "29"
                ipsec_auth_alg: "md5"
                ipsec_enc_alg: "null"
                ipsec_keys:
                 -
                    auth_key: "<your_own_value>"
                    enc_key: "<your_own_value>"
                    spi: "35"
                key_rollover_interval: "36"
                name: "default_name_37"
                peer: "<your_own_value>"
                retransmit_interval: "39"
                transmit_delay: "40"
        auto_cost_ref_bandwidth: "41"
        bfd: "enable"
        default_information_metric: "43"
        default_information_metric_type: "1"
        default_information_originate: "enable"
        default_information_route_map: "<your_own_value> (source router.route-map.
↪name)"
        default_metric: "47"
        log_neighbour_changes: "enable"
        ospf6_interface:
         -
            area_id: "<your_own_value>"
            authentication: "none"
            bfd: "global"
            cost: "53"
            dead_interval: "54"
            hello_interval: "55"
            interface: "<your_own_value> (source system.interface.name)"
            ipsec_auth_alg: "md5"
            ipsec_enc_alg: "null"
            ipsec_keys:
             -
                auth_key: "<your_own_value>"
                enc_key: "<your_own_value>"
                spi: "62"
            key_rollover_interval: "63"
            mtu: "64"
            mtu_ignore: "enable"
            name: "default_name_66"
            neighbor:
             -
                cost: "68"
                ip6: "<your_own_value>"
                poll_interval: "70"
                priority: "71"
            network_type: "broadcast"
            priority: "73"
            retransmit_interval: "74"
            status: "disable"
            transmit_delay: "76"
        passive_interface:
```

(continues on next page)

(continued from previous page)

```
        -
            name: "default_name_78 (source system.interface.name)"
        redistribute:
         -
            metric: "80"
            metric_type: "1"
            name: "default_name_82"
            routemap: "<your_own_value> (source router.route-map.name)"
            status: "enable"
        router_id: "<your_own_value>"
        spf_timers: "<your_own_value>"
        summary_address:
         -
            advertise: "disable"
            id:  "89"
            prefix6: "<your_own_value>"
            tag: "91"
```

6.251.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.251.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.251.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.252 fortios_router_policy – Configure IPv4 routing policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.252.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.252.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.252.3 FortiOS Version Compatibility

6.252.4 Parameters

6.252.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.252.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
  tasks:
  - name: Configure IPv4 routing policies.
    fortios_router_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      router_policy:
        action: "deny"
        comments: "<your_own_value>"
        dst:
         -
            subnet: "<your_own_value>"
        dst_negate: "enable"
        dstaddr:
         -
            name: "default_name_9 (source firewall.address.name firewall.addrgrp.name)
↪"
        end_port: "10"
        end_source_port: "11"
        gateway: "<your_own_value>"
        input_device:
         -
            name: "default_name_14 (source system.interface.name)"
        input_device_negate: "enable"
        internet_service_custom:
         -
            name: "default_name_17 (source firewall.internet-service-custom.name)"
        internet_service_id:
         -
            id:  "19 (source firewall.internet-service.id)"
        output_device: "<your_own_value> (source system.interface.name)"
        protocol: "21"
        seq_num: "22"
        src:
         -
            subnet: "<your_own_value>"
        src_negate: "enable"
        srcaddr:
         -
            name: "default_name_27 (source firewall.address.name firewall.addrgrp.
↪name)"
        start_port: "28"
        start_source_port: "29"
        status: "enable"
        tos: "<your_own_value>"
        tos_mask: "<your_own_value>"
```

6.252.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.252.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.252.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.253 fortios_router_policy6 – Configure IPv6 routing policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.253.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and policy6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.253.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.253.3 FortiOS Version Compatibility

6.253.4 Parameters

6.253.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.253.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 routing policies.
    fortios_router_policy6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      router_policy6:
        comments: "<your_own_value>"
        dst: "<your_own_value>"
        end_port: "5"
        gateway: "<your_own_value>"
        input_device: "<your_own_value> (source system.interface.name)"
        output_device: "<your_own_value> (source system.interface.name)"
        protocol: "9"
        seq_num: "10"
        src: "<your_own_value>"
        start_port: "12"
        status: "enable"
        tos: "<your_own_value>"
        tos_mask: "<your_own_value>"
```

6.253.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.253.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.253.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.254 fortios_router_prefix_list – Configure IPv4 prefix lists in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.254.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and prefix_list category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.254.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.254.3 FortiOS Version Compatibility

6.254.4 Parameters

6.254.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.254.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv4 prefix lists.
    fortios_router_prefix_list:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      router_prefix_list:
        comments: "<your_own_value>"
        name: "default_name_4"
        rule:
         -
            action: "permit"
            flags: "7"
            ge: "8"
            id:  "9"
            le: "10"
            prefix: "<your_own_value>"
```

6.254.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.254.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.254.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.255 fortios_router_prefix_list6 – Configure IPv6 prefix lists in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.255.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and prefix_list6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.255.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.255.3 FortiOS Version Compatibility

6.255.4 Parameters

6.255.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.255.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 prefix lists.
    fortios_router_prefix_list6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      router_prefix_list6:
        comments: "<your_own_value>"
        name: "default_name_4"
        rule:
         -
            action: "permit"
            flags: "7"
            ge: "8"
            id:  "9"
            le: "10"
            prefix6: "<your_own_value>"
```

6.255.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.255.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.255.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.256 fortios_router_rip – Configure RIP in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.256.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and rip category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.256.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.256.3 FortiOS Version Compatibility

6.256.4 Parameters

6.256.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.256.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure RIP.
    fortios_router_rip:
      vdom:  "{{ vdom }}"
      router_rip:
        default_information_originate: "enable"
        default_metric: "4"
        distance:
         -
            access_list: "<your_own_value> (source router.access-list.name)"
            distance: "7"
            id:  "8"
            prefix: "<your_own_value>"
        distribute_list:
         -
            direction: "in"
            id:  "12"
            interface: "<your_own_value> (source system.interface.name)"
            listname: "<your_own_value> (source router.access-list.name router.prefix-
↪list.name)"
            status: "enable"
        garbage_timer: "16"
        interface:
         -
            auth_keychain: "<your_own_value> (source router.key-chain.name)"
            auth_mode: "none"
            auth_string: "<your_own_value>"
            flags: "21"
            name: "default_name_22 (source system.interface.name)"
            receive_version: "1"
            send_version: "1"
            send_version2_broadcast: "disable"
```

(continues on next page)

(continued from previous page)

```
        split_horizon: "poisoned"
        split_horizon_status: "enable"
    max_out_metric: "28"
    neighbor:
     -
        id:  "30"
        ip: "<your_own_value>"
    network:
     -
        id:  "33"
        prefix: "<your_own_value>"
    offset_list:
     -
        access_list: "<your_own_value> (source router.access-list.name)"
        direction: "in"
        id:  "38"
        interface: "<your_own_value> (source system.interface.name)"
        offset: "40"
        status: "enable"
    passive_interface:
     -
        name: "default_name_43 (source system.interface.name)"
    recv_buffer_size: "44"
    redistribute:
     -
        metric: "46"
        name: "default_name_47"
        routemap: "<your_own_value> (source router.route-map.name)"
        status: "enable"
    timeout_timer: "50"
    update_timer: "51"
    version: "1"
```

6.256.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.256.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.256.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.257 fortios_router_ripng – Configure RIPng in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.257.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and ripng category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.257.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.257.3 FortiOS Version Compatibility

6.257.4 Parameters

6.257.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.257.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure RIPng.
    fortios_router_ripng:
      vdom:  "{{ vdom }}"
      router_ripng:
        aggregate_address:
         -
            id:  "4"
            prefix6: "<your_own_value>"
        default_information_originate: "enable"
        default_metric: "7"
        distance:
         -
            access_list6: "<your_own_value> (source router.access-list6.name)"
            distance: "10"
            id:  "11"
            prefix6: "<your_own_value>"
        distribute_list:
         -
            direction: "in"
            id:  "15"
            interface: "<your_own_value> (source system.interface.name)"
            listname: "<your_own_value> (source router.access-list6.name router.
↪prefix-list6.name)"
            status: "enable"
        garbage_timer: "19"
        interface:
         -
            flags: "21"
            name: "default_name_22 (source system.interface.name)"
            split_horizon: "poisoned"
            split_horizon_status: "enable"
        max_out_metric: "25"
        neighbor:
         -
            id:  "27"
            interface: "<your_own_value> (source system.interface.name)"
            ip6: "<your_own_value>"
        network:
         -
            id:  "31"
            prefix: "<your_own_value>"
        offset_list:
         -
            access_list6: "<your_own_value> (source router.access-list6.name)"
            direction: "in"
```

(continues on next page)

(continued from previous page)

```
        id:  "36"
        interface: "<your_own_value> (source system.interface.name)"
        offset: "38"
        status: "enable"
    passive_interface:
     -
        name: "default_name_41 (source system.interface.name)"
    redistribute:
     -
        metric: "43"
        name: "default_name_44"
        routemap: "<your_own_value> (source router.route-map.name)"
        status: "enable"
    timeout_timer: "47"
    update_timer: "48"
```

6.257.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.257.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.257.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.258 fortios_router_route_map – Configure route maps in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Synopsis*

6.258.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and route_map category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.258.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.258.3 FortiOS Version Compatibility

6.258.4 Parameters

6.258.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.258.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure route maps.
```

(continues on next page)

(continued from previous page)

```
    fortios_router_route_map:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      router_route_map:
        comments: "<your_own_value>"
        name: "default_name_4"
        rule:
         -
            action: "permit"
            id:  "7"
            match_as_path: "<your_own_value> (source router.aspath-list.name)"
            match_community: "<your_own_value> (source router.community-list.name)"
            match_community_exact: "enable"
            match_flags: "11"
            match_interface: "<your_own_value> (source system.interface.name)"
            match_ip_address: "<your_own_value> (source router.access-list.name␣
↪router.prefix-list.name)"
            match_ip_nexthop: "<your_own_value> (source router.access-list.name␣
↪router.prefix-list.name)"
            match_ip6_address: "<your_own_value> (source router.access-list6.name␣
↪router.prefix-list6.name)"
            match_ip6_nexthop: "<your_own_value> (source router.access-list6.name␣
↪router.prefix-list6.name)"
            match_metric: "17"
            match_origin: "none"
            match_route_type: "1"
            match_tag: "20"
            match_vrf: "21"
            set_aggregator_as: "22"
            set_aggregator_ip: "<your_own_value>"
            set_aspath:
             -
                as: "<your_own_value>"
            set_aspath_action: "prepend"
            set_atomic_aggregate: "enable"
            set_community:
             -
                community: "<your_own_value>"
            set_community_additive: "enable"
            set_community_delete: "<your_own_value> (source router.community-list.
↪name)"
            set_dampening_max_suppress: "32"
            set_dampening_reachability_half_life: "33"
            set_dampening_reuse: "34"
            set_dampening_suppress: "35"
            set_dampening_unreachability_half_life: "36"
            set_extcommunity_rt:
             -
                community: "<your_own_value>"
            set_extcommunity_soo:
             -
                community: "<your_own_value>"
            set_flags: "41"
            set_ip_nexthop: "<your_own_value>"
            set_ip6_nexthop: "<your_own_value>"
            set_ip6_nexthop_local: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
            set_local_preference: "45"
            set_metric: "46"
            set_metric_type: "1"
            set_origin: "none"
            set_originator_id: "<your_own_value>"
            set_route_tag: "50"
            set_tag: "51"
            set_weight: "52"
```

6.258.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.258.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.258.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.259 fortios_router_setting – Configure router settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.259.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.259.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.259.3 FortiOS Version Compatibility

6.259.4 Parameters

6.259.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.259.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure router settings.
    fortios_router_setting:
      vdom:  "{{ vdom }}"
      router_setting:
        bgp_debug_flags: "<your_own_value>"
        hostname: "myhostname"
        igmp_debug_flags: "<your_own_value>"
        imi_debug_flags: "<your_own_value>"
        isis_debug_flags: "<your_own_value>"
        ospf6_debug_events_flags: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        ospf6_debug_ifsm_flags: "<your_own_value>"
        ospf6_debug_lsa_flags: "<your_own_value>"
        ospf6_debug_nfsm_flags: "<your_own_value>"
        ospf6_debug_nsm_flags: "<your_own_value>"
        ospf6_debug_packet_flags: "<your_own_value>"
        ospf6_debug_route_flags: "<your_own_value>"
        ospf_debug_events_flags: "<your_own_value>"
        ospf_debug_ifsm_flags: "<your_own_value>"
        ospf_debug_lsa_flags: "<your_own_value>"
        ospf_debug_nfsm_flags: "<your_own_value>"
        ospf_debug_nsm_flags: "<your_own_value>"
        ospf_debug_packet_flags: "<your_own_value>"
        ospf_debug_route_flags: "<your_own_value>"
        pimdm_debug_flags: "<your_own_value>"
        pimsm_debug_joinprune_flags: "<your_own_value>"
        pimsm_debug_simple_flags: "<your_own_value>"
        pimsm_debug_timer_flags: "<your_own_value>"
        rip_debug_flags: "<your_own_value>"
        ripng_debug_flags: "<your_own_value>"
        show_filter: "<your_own_value> (source router.prefix-list.name)"
```

6.259.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.259.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.259.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.260 fortios_router_static – Configure IPv4 static routing tables in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.260.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and static category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.260.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.260.3 FortiOS Version Compatibility

6.260.4 Parameters

6.260.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.260.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
    ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv4 static routing tables.
    fortios_router_static:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      router_static:
        bfd: "enable"
        blackhole: "enable"
        comment: "Optional comments."
        device: "<your_own_value> (source system.interface.name)"
        distance: "7"
        dst: "<your_own_value>"
        dstaddr: "<your_own_value> (source firewall.address.name firewall.addrgrp.
↪name)"
        dynamic_gateway: "enable"
        gateway: "<your_own_value>"
        internet_service: "12 (source firewall.internet-service.id)"
        internet_service_custom: "<your_own_value> (source firewall.internet-service-
↪custom.name)"
        link_monitor_exempt: "enable"
        priority: "15"
        sdwan: "enable"
        seq_num: "17"
        src: "<your_own_value>"
        status: "enable"
        virtual_wan_link: "enable"
        vrf: "21"
        weight: "22"
```

6.260.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.260.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.260.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.261 fortios_router_static6 – Configure IPv6 static routing tables in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.261.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify router feature and static6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.261.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.261.3 FortiOS Version Compatibility

6.261.4 Parameters

6.261.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.261.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 static routing tables.
    fortios_router_static6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      router_static6:
        bfd: "enable"
        blackhole: "enable"
        comment: "Optional comments."
        device: "<your_own_value> (source system.interface.name)"
        devindex: "7"
        distance: "8"
        dst: "<your_own_value>"
        dynamic_gateway: "enable"
        gateway: "<your_own_value>"
        link_monitor_exempt: "enable"
        priority: "13"
        sdwan: "enable"
        seq_num: "15"
        status: "enable"
        virtual_wan_link: "enable"
```

6.261.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.261.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.261.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.262 fortios_spamfilter_bwl – Configure anti-spam black/white list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.262.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify spamfilter feature and bwl category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.262.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.262.3 FortiOS Version Compatibility

6.262.4 Parameters

6.262.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.262.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure anti-spam black/white list.
    fortios_spamfilter_bwl:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      spamfilter_bwl:
        comment: "Optional comments."
        entries:
         -
            action: "reject"
            addr_type: "ipv4"
            email_pattern: "<your_own_value>"
            id:  "8"
            ip4_subnet: "<your_own_value>"
            ip6_subnet: "<your_own_value>"
            pattern_type: "wildcard"
            status: "enable"
            type: "ip"
        id:  "14"
        name: "default_name_15"
```

6.262.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.262.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.262.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.263 fortios_spamfilter_bword – Configure AntiSpam banned word list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.263.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify spamfilter feature and bword category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.263.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.263.3 FortiOS Version Compatibility

6.263.4 Parameters

6.263.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.263.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure AntiSpam banned word list.
    fortios_spamfilter_bword:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      spamfilter_bword:
        comment: "Optional comments."
        entries:
         -
            action: "spam"
            id:  "6"
            language: "western"
            pattern: "<your_own_value>"
            pattern_type: "wildcard"
            score: "10"
            status: "enable"
            where: "subject"
        id:  "13"
        name: "default_name_14"
```

6.263.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.263.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.263.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.264 fortios_spamfilter_dnsbl – Configure AntiSpam DNSBL/ORBL in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.264.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify spamfilter feature and dnsbl category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.264.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.264.3 FortiOS Version Compatibility

6.264.4 Parameters

6.264.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.264.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure AntiSpam DNSBL/ORBL.
    fortios_spamfilter_dnsbl:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      spamfilter_dnsbl:
        comment: "Optional comments."
        entries:
         -
            action: "reject"
            id:  "6"
            server: "192.168.100.40"
            status: "enable"
        id:  "9"
        name: "default_name_10"
```

6.264.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.264.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.264.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.265 fortios_spamfilter_fortishield – Configure FortiGuard - Anti-Spam in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.265.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify spamfilter feature and fortishield category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.265.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.265.3 FortiOS Version Compatibility

6.265.4 Parameters

6.265.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.265.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiGuard - AntiSpam.
    fortios_spamfilter_fortishield:
      vdom:  "{{ vdom }}"
      spamfilter_fortishield:
        spam_submit_force: "enable"
        spam_submit_srv: "<your_own_value>"
        spam_submit_txt2htm: "enable"
```

6.265.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.265.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.265.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.266 fortios_spamfilter_iptrust – Configure AntiSpam IP trust in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.266.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify spamfilter feature and iptrust category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.266.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.266.3 FortiOS Version Compatibility

6.266.4 Parameters

6.266.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.266.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure AntiSpam IP trust.
  fortios_spamfilter_iptrust:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    spamfilter_iptrust:
      comment: "Optional comments."
      entries:
       -
          addr_type: "ipv4"
          id:  "6"
          ip4_subnet: "<your_own_value>"
          ip6_subnet: "<your_own_value>"
          status: "enable"
      id:  "10"
      name: "default_name_11"
```

6.266.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.266.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.266.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.267 fortios_spamfilter_mheader – Configure AntiSpam MIME header in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.267.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify spamfilter feature and mheader category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.267.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.267.3 FortiOS Version Compatibility

6.267.4 Parameters

6.267.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.267.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure AntiSpam MIME header.
  fortios_spamfilter_mheader:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    spamfilter_mheader:
      comment: "Optional comments."
      entries:
       -
          action: "spam"
          fieldbody: "<your_own_value>"
          fieldname: "<your_own_value>"
          id:  "8"
          pattern_type: "wildcard"
          status: "enable"
      id:  "11"
      name: "default_name_12"
```

6.267.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.267.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.267.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.268 fortios_spamfilter_options – Configure AntiSpam options in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.268.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify spamfilter feature and options category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.268.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.268.3 FortiOS Version Compatibility

6.268.4 Parameters

6.268.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.268.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure AntiSpam options.
  fortios_spamfilter_options:
    vdom:  "{{ vdom }}"
    spamfilter_options:
      dns_timeout: "3"
```

6.268.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.268.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.268.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.269 fortios_spamfilter_profile – Configure AntiSpam profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.269.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify spamfilter feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.269.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.269.3 FortiOS Version Compatibility

6.269.4 Parameters

6.269.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.269.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure AntiSpam profiles.
    fortios_spamfilter_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      spamfilter_profile:
        comment: "Comment."
        external: "enable"
        flow_based: "enable"
        gmail:
```

(continues on next page)

(continued from previous page)

```
            log: "enable"
        imap:
            action: "pass"
            log: "enable"
            tag_msg: "<your_own_value>"
            tag_type: "subject"
        mapi:
            action: "pass"
            log: "enable"
        msn_hotmail:
            log: "enable"
        name: "default_name_18"
        options: "bannedword"
        pop3:
            action: "pass"
            log: "enable"
            tag_msg: "<your_own_value>"
            tag_type: "subject"
        replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
        smtp:
            action: "pass"
            hdrip: "disable"
            local_override: "disable"
            log: "enable"
            tag_msg: "<your_own_value>"
            tag_type: "subject"
        spam_bwl_table: "33 (source spamfilter.bwl.id)"
        spam_bword_table: "34 (source spamfilter.bword.id)"
        spam_bword_threshold: "35"
        spam_filtering: "enable"
        spam_iptrust_table: "37 (source spamfilter.iptrust.id)"
        spam_log: "disable"
        spam_log_fortiguard_response: "disable"
        spam_mheader_table: "40 (source spamfilter.mheader.id)"
        spam_rbl_table: "41 (source spamfilter.dnsbl.id)"
        yahoo_mail:
            log: "enable"
```

6.269.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.269.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.269.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.270 fortios_ssh_filter_profile – SSH filter profile in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.270.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify ssh_filter feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.270.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.270.3 FortiOS Version Compatibility

6.270.4 Parameters

6.270.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.270.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: SSH filter profile.
    fortios_ssh_filter_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      ssh_filter_profile:
        block: "x11"
        default_command_log: "enable"
        file_filter:
            entries:
             -
                action: "log"
                comment: "Comment."
                direction: "incoming"
                file_type:
                 -
                    name: "default_name_11 (source antivirus.filetype.name)"
                filter: "<your_own_value>"
                password_protected: "yes"
                protocol: "ssh"
            log: "enable"
            scan_archive_contents: "enable"
            status: "enable"
        log: "x11"
        name: "default_name_19"
        shell_commands:
         -
            action: "block"
            alert: "enable"
            id:  "23"
            log: "enable"
            pattern: "<your_own_value>"
            severity: "low"
            type: "simple"
```

6.270.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.270.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.270.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.271 fortios_switch_controller_802_1x_settings – Configure global 802.1X settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.271.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and 802_1x_settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.271.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.271.3 FortiOS Version Compatibility

6.271.4 Parameters

6.271.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.271.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure global 802.1X settings.
    fortios_switch_controller_802_1x_settings:
      vdom:  "{{ vdom }}"
      switch_controller_802_1x_settings:
        link_down_auth: "set-unauth"
        max_reauth_attempt: "4"
        reauth_period: "5"
        tx_period: "6"
```

6.271.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.271.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.271.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.272 fortios_switch_controller_auto_config_custom – Policies which can override the 'default' for specific ISL/ICL/FortiLink interface in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.272.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller_auto_config feature and custom category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.272.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.272.3 FortiOS Version Compatibility

6.272.4 Parameters

6.272.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.272.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Policies which can override the 'default' for specific ISL/ICL/FortiLink␣
↪interface.
    fortios_switch_controller_auto_config_custom:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_auto_config_custom:
        name: "default_name_3"
        switch_binding:
         -
            policy: "<your_own_value> (source switch-controller.auto-config.policy.
↪name)"
            switch_id: "<your_own_value>"
```

6.272.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.272.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.272.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.273 fortios_switch_controller_auto_config_default – Policies which are applied automatically to all ISL/ICL/FortiLink interfaces in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.273.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller_auto_config feature and default category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.273.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.273.3 FortiOS Version Compatibility

6.273.4 Parameters

6.273.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.273.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Policies which are applied automatically to all ISL/ICL/FortiLink␣
↪interfaces.
    fortios_switch_controller_auto_config_default:
      vdom:  "{{ vdom }}"
      switch_controller_auto_config_default:
        fgt_policy: "<your_own_value> (source switch-controller.auto-config.policy.
↪name)"
        icl_policy: "<your_own_value> (source switch-controller.auto-config.policy.
↪name)"
        isl_policy: "<your_own_value> (source switch-controller.auto-config.policy.
↪name)"
```

6.273.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.273.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.273.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.274 fortios_switch_controller_auto_config_policy – Policy definitions which can define the behavior on auto configured interfaces in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.274.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller_auto_config feature and policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.274.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.274.3 FortiOS Version Compatibility

6.274.4 Parameters

6.274.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.274.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Policy definitions which can define the behavior on auto configured␣
↪interfaces.
    fortios_switch_controller_auto_config_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_auto_config_policy:
        igmp_flood_report: "enable"
        igmp_flood_traffic: "enable"
        name: "default_name_5"
        poe_status: "enable"
        qos_policy: "<your_own_value> (source switch-controller.qos.qos-policy.name)"
        storm_control_policy: "<your_own_value> (source switch-controller.storm-
↪control-policy.name)"
```

6.274.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.274.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.274.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.275 fortios_switch_controller_custom_command – Configure the FortiGate switch controller to send custom commands to managed FortiSwitch devices in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.275.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and custom_command category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.275.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.275.3 FortiOS Version Compatibility

6.275.4 Parameters

6.275.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.275.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure the FortiGate switch controller to send custom commands to␣
↪managed FortiSwitch devices.
    fortios_switch_controller_custom_command:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_custom_command:
        command: "<your_own_value>"
        command_name: "<your_own_value>"
        description: "<your_own_value>"
```

6.275.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.275.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.275.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.276 fortios_switch_controller_dynamic_port_policy – Configure Dynamic port policy to be applied on the managed FortiSwitch ports through DPP device in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.276.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and dynamic_port_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.276.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.276.3 FortiOS Version Compatibility

6.276.4 Parameters

6.276.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.276.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Dynamic port policy to be applied on the managed FortiSwitch␣
↪ports through DPP device.
    fortios_switch_controller_dynamic_port_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_dynamic_port_policy:
        description: "<your_own_value>"
        fortilink: "<your_own_value> (source system.interface.name)"
        name: "default_name_5"
        policy:
         -
            802_1x: "<your_own_value> (source switch-controller.security-policy.802-
↪1X.name switch-controller.security-policy.captive-portal.name)"
            bounce_port_link: "disable"
            category: "device"
            description: "<your_own_value>"
            family: "<your_own_value>"
            host: "myhostname"
            interface_tags:
             -
                tag_name: "<your_own_value> (source switch-controller.switch-
↪interface-tag.name)"
            lldp_profile: "<your_own_value> (source switch-controller.lldp-profile.
↪name)"
            mac: "<your_own_value>"
            name: "default_name_17"
            qos_policy: "<your_own_value> (source switch-controller.qos.qos-policy.
↪name)"
            status: "enable"
            type: "<your_own_value>"
            vlan_policy: "<your_own_value> (source switch-controller.vlan-policy.name)
↪"
```

6.276.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.276.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.276.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.277 fortios_switch_controller_flow_tracking – Configure FortiSwitch flow tracking and export via ipfix/netflow in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.277.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and flow_tracking category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.277.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.277.3 FortiOS Version Compatibility

6.277.4 Parameters

6.277.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.277.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch flow tracking and export via ipfix/netflow.
    fortios_switch_controller_flow_tracking:
      vdom:  "{{ vdom }}"
      switch_controller_flow_tracking:
        aggregates:
         -
            id:  "4"
            ip: "<your_own_value>"
        collector_ip: "<your_own_value>"
        collector_port: "7"
        format: "netflow1"
        level: "vlan"
        max_export_pkt_size: "10"
        sample_mode: "local"
        sample_rate: "12"
        timeout_general: "13"
        timeout_icmp: "14"
        timeout_max: "15"
        timeout_tcp: "16"
        timeout_tcp_fin: "17"
        timeout_tcp_rst: "18"
        timeout_udp: "19"
        transport: "udp"
```

6.277.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.277.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.277.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.278 fortios_switch_controller_fortilink_settings – Configure integrated FortiLink settings for FortiSwitch in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.278.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and fortilink_settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.278.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.278.3 FortiOS Version Compatibility

6.278.4 Parameters

6.278.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.278.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure integrated FortiLink settings for FortiSwitch.
    fortios_switch_controller_fortilink_settings:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_fortilink_settings:
        inactive_timer: "3"
        link_down_flush: "disable"
        nac_ports:
            bounce_nac_port: "disable"
            onboarding_vlan: "<your_own_value> (source system.interface.name)"
        name: "default_name_8"
```

6.278.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.278.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.278.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.279 fortios_switch_controller_global – Configure FortiSwitch global settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.279.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and global category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.279.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.279.3 FortiOS Version Compatibility

6.279.4 Parameters

6.279.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.279.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch global settings.
    fortios_switch_controller_global:
      vdom:  "{{ vdom }}"
      switch_controller_global:
        allow_multiple_interfaces: "enable"
        bounce_quarantined_link: "disable"
        custom_command:
         -
            command_entry: "<your_own_value>"
            command_name: "<your_own_value> (source switch-controller.custom-command.
↪command-name)"
        default_virtual_switch_vlan: "<your_own_value> (source system.interface.name)"
        disable_discovery:
         -
            name: "default_name_10"
        fips_enforce: "disable"
        https_image_push: "enable"
        log_mac_limit_violations: "enable"
        mac_aging_interval: "14"
        mac_event_logging: "enable"
        mac_retention_period: "16"
        mac_violation_timer: "17"
        quarantine_mode: "by-vlan"
        sn_dns_resolution: "enable"
        update_user_device: "mac-cache"
        vlan_all_mode: "all"
        vlan_optimization: "enable"
```

6.279.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.279.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.279.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.280 fortios_switch_controller_igmp_snooping – Configure FortiSwitch IGMP snooping global settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.280.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and igmp_snooping category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.280.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.280.3 FortiOS Version Compatibility

6.280.4 Parameters

6.280.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.280.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch IGMP snooping global settings.
    fortios_switch_controller_igmp_snooping:
      vdom:  "{{ vdom }}"
      switch_controller_igmp_snooping:
        aging_time: "3"
        flood_unknown_multicast: "enable"
```

6.280.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.280.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.280.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.281 fortios_switch_controller_initial_config_template – Configure template for auto-generated VLANs in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.281.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller_initial_config feature and template category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.281.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.281.3 FortiOS Version Compatibility

6.281.4 Parameters

6.281.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.281.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure template for auto-generated VLANs.
    fortios_switch_controller_initial_config_template:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_initial_config_template:
        allowaccess: "ping"
        auto_ip: "enable"
        dhcp_server: "enable"
        ip: "<your_own_value>"
        name: "default_name_7"
        vlanid: "8"
```

6.281.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.281.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.281.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.282 fortios_switch_controller_initial_config_vlans – Configure initial template for auto-generated VLAN interfaces in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.282.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller_initial_config feature and vlans category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.282.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.282.3 FortiOS Version Compatibility

6.282.4 Parameters

6.282.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.282.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure initial template for auto-generated VLAN interfaces.
    fortios_switch_controller_initial_config_vlans:
      vdom:  "{{ vdom }}"
      switch_controller_initial_config_vlans:
        default_vlan: "<your_own_value> (source switch-controller.initial-config.
↪template.name)"
        nac: "<your_own_value> (source switch-controller.initial-config.template.name)
↪"
        quarantine: "<your_own_value> (source switch-controller.initial-config.
↪template.name)"
        rspan: "<your_own_value> (source switch-controller.initial-config.template.
↪name)"
        video: "<your_own_value> (source switch-controller.initial-config.template.
↪name)"
        voice: "<your_own_value> (source switch-controller.initial-config.template.
↪name)"
```

6.282.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.282.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.282.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.283 fortios_switch_controller_lldp_profile – Configure FortiSwitch LLDP profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.283.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and lldp_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.283.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.283.3 FortiOS Version Compatibility

6.283.4 Parameters

6.283.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.283.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch LLDP profiles.
    fortios_switch_controller_lldp_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_lldp_profile:
        tlvs_802dot1: "port-vlan-id"
        tlvs_802dot3: "max-frame-size"
        auto_isl: "disable"
        auto_isl_hello_timer: "6"
        auto_isl_port_group: "7"
        auto_isl_receive_timeout: "8"
        auto_mclag_icl: "disable"
        custom_tlvs:
         -
            information_string: "<your_own_value>"
            name: "default_name_12"
            oui: "<your_own_value>"
            subtype: "14"
        med_location_service:
         -
            name: "default_name_16"
            status: "disable"
            sys_location_id: "<your_own_value> (source switch-controller.location.
↪name)"
        med_network_policy:
         -
            assign_vlan: "disable"
            dscp: "21"
            name: "default_name_22"
            priority: "23"
            status: "disable"
            vlan: "25"
            vlan_intf: "<your_own_value> (source system.interface.name)"
        med_tlvs: "inventory-management"
        name: "default_name_28"
```

6.283.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.283.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.283.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.284 fortios_switch_controller_lldp_settings – Configure FortiSwitch LLDP settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.284.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and lldp_settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.284.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.284.3 FortiOS Version Compatibility

6.284.4 Parameters

6.284.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

---

6.284.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch LLDP settings.
    fortios_switch_controller_lldp_settings:
      vdom:  "{{ vdom }}"
      switch_controller_lldp_settings:
        device_detection: "disable"
        fast_start_interval: "4"
        management_interface: "internal"
        status: "enable"
        tx_hold: "7"
        tx_interval: "8"
```

6.284.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.284.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.284.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.285 fortios_switch_controller_location – Configure FortiSwitch location services in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.285.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and location category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.285.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.285.3 FortiOS Version Compatibility

6.285.4 Parameters

6.285.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.285.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch location services.
    fortios_switch_controller_location:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_location:
        address_civic:
            additional: "<your_own_value>"
            additional_code: "<your_own_value>"
            block: "<your_own_value>"
            branch_road: "<your_own_value>"
            building: "<your_own_value>"
            city: "<your_own_value>"
            city_division: "<your_own_value>"
            country: "<your_own_value>"
            country_subdivision: "<your_own_value>"
            county: "<your_own_value>"
            direction: "<your_own_value>"
            floor: "<your_own_value>"
            landmark: "<your_own_value>"
            language: "<your_own_value>"
            name: "default_name_18"
            number: "<your_own_value>"
            number_suffix: "<your_own_value>"
            parent_key: "<your_own_value>"
            place_type: "<your_own_value>"
            post_office_box: "<your_own_value>"
            postal_community: "<your_own_value>"
            primary_road: "<your_own_value>"
            road_section: "<your_own_value>"
            room: "<your_own_value>"
            script: "<your_own_value>"
            seat: "<your_own_value>"
            street: "<your_own_value>"
            street_name_post_mod: "<your_own_value>"
            street_name_pre_mod: "<your_own_value>"
            street_suffix: "<your_own_value>"
            sub_branch_road: "<your_own_value>"
            trailing_str_suffix: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        unit: "<your_own_value>"
        zip: "<your_own_value>"
    coordinates:
        altitude: "<your_own_value>"
        altitude_unit: "m"
        datum: "WGS84"
        latitude: "<your_own_value>"
        longitude: "<your_own_value>"
        parent_key: "<your_own_value>"
    elin_number:
        elin_num: "<your_own_value>"
        parent_key: "<your_own_value>"
    name: "default_name_48"
```

6.285.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.285.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.285.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.286 fortios_switch_controller_mac_policy – Configure MAC policy to be applied on the managed FortiSwitch devices through NAC device in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.286.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and mac_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.286.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.286.3 FortiOS Version Compatibility

6.286.4 Parameters

6.286.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.286.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure MAC policy to be applied on the managed FortiSwitch devices␣
↪through NAC device.
    fortios_switch_controller_mac_policy:
```

(continues on next page)

(continued from previous page)

```
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_mac_policy:
        bounce_port_link: "disable"
        count: "disable"
        description: "<your_own_value>"
        drop: "disable"
        fortilink: "<your_own_value> (source system.interface.name)"
        name: "default_name_8"
        traffic_policy: "<your_own_value> (source switch-controller.traffic-policy.
↪name)"
        vlan: "<your_own_value> (source system.interface.name)"
```

6.286.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.286.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.286.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.287 fortios_switch_controller_mac_sync_settings – Configure global MAC synchronization settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.287.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and mac_sync_settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.287.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.287.3 FortiOS Version Compatibility

6.287.4 Parameters

6.287.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.287.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure global MAC synchronization settings.
    fortios_switch_controller_mac_sync_settings:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    switch_controller_mac_sync_settings:
      mac_sync_interval: "3"
```

6.287.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.287.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.287.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.288 fortios_switch_controller_managed_switch – Configure FortiSwitch devices that are managed by this FortiGate in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.288.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and managed_switch category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.288.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.288.3 FortiOS Version Compatibility

6.288.4 Parameters

6.288.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.288.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch devices that are managed by this FortiGate.
    fortios_switch_controller_managed_switch:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_managed_switch:
        settings_802_1X:
            link_down_auth: "set-unauth"
            local_override: "enable"
            max_reauth_attempt: "6"
            reauth_period: "7"
            tx_period: "8"
        access_profile: "<your_own_value> (source switch-controller.security-policy.
↪local-access.name)"
```

(continues on next page)

(continued from previous page)

```
        custom_command:
         -
            command_entry: "<your_own_value>"
            command_name: "<your_own_value> (source switch-controller.custom-command.
↪command-name)"
        delayed_restart_trigger: "13"
        description: "<your_own_value>"
        directly_connected: "15"
        dynamic_capability: "16"
        dynamically_discovered: "17"
        firmware_provision: "enable"
        firmware_provision_version: "<your_own_value>"
        flow_identity: "<your_own_value>"
        fsw_wan1_admin: "discovered"
        fsw_wan1_peer: "<your_own_value> (source system.interface.name)"
        fsw_wan2_admin: "discovered"
        fsw_wan2_peer: "<your_own_value>"
        igmp_snooping:
            aging_time: "26"
            flood_unknown_multicast: "enable"
            local_override: "enable"
        ip_source_guard:
         -
            binding_entry:
             -
                entry_name: "<your_own_value>"
                ip: "<your_own_value>"
                mac: "<your_own_value>"
            description: "<your_own_value>"
            port: "<your_own_value>"
        l3_discovered: "36"
        max_allowed_trunk_members: "37"
        mclag_igmp_snooping_aware: "enable"
        mirror:
         -
            dst: "<your_own_value>"
            name: "default_name_41"
            src_egress:
             -
                name: "default_name_43"
            src_ingress:
             -
                name: "default_name_45"
            status: "active"
            switching_packet: "enable"
        name: "default_name_48"
        override_snmp_community: "enable"
        override_snmp_sysinfo: "disable"
        override_snmp_trap_threshold: "enable"
        override_snmp_user: "enable"
        owner_vdom: "<your_own_value>"
        poe_detection_type: "54"
        poe_lldp_detection: "enable"
        poe_pre_standard_detection: "enable"
        ports:
         -
            access_mode: "normal"
```

(continues on next page)

(continued from previous page)

```
            aggregator_mode: "bandwidth"
            allowed_vlans:
             -
                vlan_name: "<your_own_value> (source system.interface.name)"
            allowed_vlans_all: "enable"
            arp_inspection_trust: "untrusted"
            bundle: "enable"
            description: "<your_own_value>"
            dhcp_snoop_option82_trust: "enable"
            dhcp_snooping: "untrusted"
            discard_mode: "none"
            edge_port: "enable"
            export_tags:
             -
                tag_name: "<your_own_value> (source switch-controller.switch-
↪interface-tag.name)"
            export_to: "<your_own_value> (source system.vdom.name)"
            export_to_pool: "<your_own_value> (source switch-controller.virtual-port-
↪pool.name)"
            export_to_pool_flag: "74"
            export_to_pool_flag: "75"
            fec_capable: "76"
            fec_state: "disabled"
            fgt_peer_device_name: "<your_own_value>"
            fgt_peer_port_name: "<your_own_value>"
            fiber_port: "80"
            flags: "81"
            flow_control: "disable"
            fortilink_port: "83"
            igmp_snooping: "enable"
            igmps_flood_reports: "enable"
            igmps_flood_traffic: "enable"
            ip_source_guard: "disable"
            isl_local_trunk_name: "<your_own_value>"
            isl_peer_device_name: "<your_own_value>"
            isl_peer_port_name: "<your_own_value>"
            lacp_speed: "slow"
            learning_limit: "92"
            lldp_profile: "<your_own_value> (source switch-controller.lldp-profile.
↪name)"
            lldp_status: "disable"
            loop_guard: "enabled"
            loop_guard_timeout: "96"
            mac_addr: "<your_own_value>"
            matched_dpp_intf_tags: "<your_own_value>"
            matched_dpp_policy: "<your_own_value>"
            max_bundle: "100"
            mclag: "enable"
            mclag_icl_port: "102"
            media_type: "<your_own_value>"
            member_withdrawal_behavior: "forward"
            members:
             -
                member_name: "<your_own_value>"
            min_bundle: "107"
            mode: "static"
            p2p_port: "109"
```

(continues on next page)

(continued from previous page)

```
            packet_sample_rate: "110"
            packet_sampler: "enabled"
            pause_meter: "112"
            pause_meter_resume: "75%"
            poe_capable: "114"
            poe_pre_standard_detection: "enable"
            poe_status: "enable"
            port_name: "<your_own_value>"
            port_number: "118"
            port_owner: "<your_own_value>"
            port_policy: "<your_own_value> (source switch-controller.dynamic-port-
↪policy.name)"
            port_prefix_type: "121"
            port_security_policy: "<your_own_value> (source switch-controller.
↪security-policy.802-1X.name switch-controller.security-policy.captive-portal
              .name)"
            port_selection_criteria: "src-mac"
            ptp_policy: "<your_own_value> (source switch-controller.ptp.policy.name)"
            qos_policy: "<your_own_value> (source switch-controller.qos.qos-policy.
↪name)"
            rpvst_port: "disabled"
            sample_direction: "tx"
            sflow_counter_interval: "128"
            sflow_sample_rate: "129"
            sflow_sampler: "enabled"
            speed: "10half"
            speed_mask: "132"
            stacking_port: "133"
            status: "up"
            sticky_mac: "enable"
            storm_control_policy: "<your_own_value> (source switch-controller.storm-
↪control-policy.name)"
            stp_bpdu_guard: "enabled"
            stp_bpdu_guard_timeout: "138"
            stp_root_guard: "enabled"
            stp_state: "enabled"
            switch_id: "<your_own_value>"
            type: "physical"
            untagged_vlans:
             -
                vlan_name: "<your_own_value> (source system.interface.name)"
            virtual_port: "145"
            vlan: "<your_own_value> (source system.interface.name)"
        pre_provisioned: "147"
        qos_drop_policy: "taildrop"
        qos_red_probability: "149"
        remote_log:
         -
            csv: "enable"
            facility: "kernel"
            name: "default_name_153"
            port: "154"
            server: "192.168.100.40"
            severity: "emergency"
            status: "enable"
        snmp_community:
         -
```

(continues on next page)

(continued from previous page)

```
            events: "cpu-high"
            hosts:
             -
                id:  "161"
                ip: "<your_own_value>"
            id:  "163"
            name: "default_name_164"
            query_v1_port: "165"
            query_v1_status: "disable"
            query_v2c_port: "167"
            query_v2c_status: "disable"
            status: "disable"
            trap_v1_lport: "170"
            trap_v1_rport: "171"
            trap_v1_status: "disable"
            trap_v2c_lport: "173"
            trap_v2c_rport: "174"
            trap_v2c_status: "disable"
        snmp_sysinfo:
            contact_info: "<your_own_value>"
            description: "<your_own_value>"
            engine_id: "<your_own_value>"
            location: "<your_own_value>"
            status: "disable"
        snmp_trap_threshold:
            trap_high_cpu_threshold: "183"
            trap_log_full_threshold: "184"
            trap_low_memory_threshold: "185"
        snmp_user:
         -
            auth_proto: "md5"
            auth_pwd: "<your_own_value>"
            name: "default_name_189"
            priv_proto: "aes"
            priv_pwd: "<your_own_value>"
            queries: "disable"
            query_port: "193"
            security_level: "no-auth-no-priv"
        staged_image_version: "<your_own_value>"
        static_mac:
         -
            description: "<your_own_value>"
            id:  "198"
            interface: "<your_own_value>"
            mac: "<your_own_value>"
            type: "static"
            vlan: "<your_own_value> (source system.interface.name)"
        storm_control:
            broadcast: "enable"
            local_override: "enable"
            rate: "206"
            unknown_multicast: "enable"
            unknown_unicast: "enable"
        stp_instance:
         -
            id:  "210"
            priority: "0"
```

(continues on next page)

(continued from previous page)

```
        stp_settings:
            forward_time: "213"
            hello_time: "214"
            local_override: "enable"
            max_age: "216"
            max_hops: "217"
            name: "default_name_218"
            pending_timer: "219"
            revision: "220"
            status: "enable"
        switch_device_tag: "<your_own_value>"
        switch_dhcp_opt43_key: "<your_own_value>"
        switch_id: "<your_own_value>"
        switch_log:
            local_override: "enable"
            severity: "emergency"
            status: "enable"
        switch_profile: "<your_own_value> (source switch-controller.switch-profile.
↪name)"
        switch_stp_settings:
            status: "enable"
        tdr_supported: "<your_own_value>"
        type: "virtual"
        version: "234"
```

6.288.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.288.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.288.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.289 fortios_switch_controller_nac_device – Configure/list NAC devices learned on the managed FortiSwitch ports which matches NAC policy in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.289.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and nac_device category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.289.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.289.3 FortiOS Version Compatibility

6.289.4 Parameters

6.289.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.289.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure/list NAC devices learned on the managed FortiSwitch ports which␣
↪matches NAC policy.
    fortios_switch_controller_nac_device:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_nac_device:
        description: "<your_own_value>"
        id:  "4"
        last_known_port: "<your_own_value>"
        last_known_switch: "<your_own_value> (source switch-controller.managed-switch.
↪switch-id)"
        last_seen: "7"
        mac: "<your_own_value>"
        mac_policy: "<your_own_value> (source switch-controller.mac-policy.name)"
        matched_nac_policy: "<your_own_value> (source user.nac-policy.name)"
        port_policy: "<your_own_value> (source switch-controller.port-policy.name)"
        status: "enable"
```

6.289.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.289.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.289.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.290 fortios_switch_controller_nac_settings – Configure integrated NAC settings for FortiSwitch in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.290.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and nac_settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.290.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.290.3 FortiOS Version Compatibility

6.290.4 Parameters

6.290.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.290.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure integrated NAC settings for FortiSwitch.
    fortios_switch_controller_nac_settings:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_nac_settings:
        auto_auth: "disable"
        bounce_nac_port: "disable"
        inactive_timer: "5"
        link_down_flush: "disable"
        mode: "local"
        name: "default_name_8"
        onboarding_vlan: "<your_own_value> (source system.interface.name)"
```

6.290.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.290.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.290.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.291 fortios_switch_controller_network_monitor_settings – Configure network monitor settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.291.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and network_monitor_settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.291.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.291.3 FortiOS Version Compatibility

6.291.4 Parameters

6.291.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.291.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure network monitor settings.
    fortios_switch_controller_network_monitor_settings:
      vdom:  "{{ vdom }}"
      switch_controller_network_monitor_settings:
        network_monitoring: "enable"
```

6.291.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.291.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.291.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.292 fortios_switch_controller_poe – List PoE end-points status in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.292.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and poe category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.292.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.292.3 FortiOS Version Compatibility

6.292.4 Parameters

6.292.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.292.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: List PoE end-points status.
  fortios_switch_controller_poe:
    vdom:  "{{ vdom }}"
    switch_controller_poe:
      <fortiswitch_id>: "<your_own_value>"
```

6.292.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.292.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.292.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.293 fortios_switch_controller_port_policy – Configure port policy to be applied on the managed FortiSwitch ports through NAC device in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.293.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and port_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.293.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.293.3 FortiOS Version Compatibility

6.293.4 Parameters

6.293.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.293.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure port policy to be applied on the managed FortiSwitch ports␣
↪through NAC device.
    fortios_switch_controller_port_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_port_policy:
        802_1x: "<your_own_value> (source switch-controller.security-policy.802-1X.
↪name switch-controller.security-policy.captive-portal.name)"
        bounce_port_link: "disable"
```

(continues on next page)

(continued from previous page)

```
        description: "<your_own_value>"
        fortilink: "<your_own_value> (source system.interface.name)"
        lldp_profile: "<your_own_value> (source switch-controller.lldp-profile.name)"
        name: "default_name_8"
        qos_policy: "<your_own_value> (source switch-controller.qos.qos-policy.name)"
        vlan_policy: "<your_own_value> (source switch-controller.vlan-policy.name)"
```

6.293.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.293.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.293.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.294 fortios_switch_controller_ptp_policy – PTP policy configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.294.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller_ptp feature and policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.294.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.294.3 FortiOS Version Compatibility

6.294.4 Parameters

6.294.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.294.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: PTP policy configuration.
    fortios_switch_controller_ptp_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_ptp_policy:
        name: "default_name_3"
        status: "disable"
```

6.294.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.294.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.294.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.295 fortios_switch_controller_ptp_settings – Global PTP settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.295.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller_ptp feature and settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.295.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.295.3 FortiOS Version Compatibility

6.295.4 Parameters

6.295.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

---

6.295.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Global PTP settings.
    fortios_switch_controller_ptp_settings:
      vdom:  "{{ vdom }}"
      switch_controller_ptp_settings:
        mode: "disable"
```

6.295.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.295.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.295.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.296 fortios_switch_controller_qos_dot1p_map – Configure FortiSwitch QoS 802.1p in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.296.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller_qos feature and dot1p_map category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.296.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.296.3 FortiOS Version Compatibility

6.296.4 Parameters

6.296.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.296.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch QoS 802.1p.
    fortios_switch_controller_qos_dot1p_map:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_qos_dot1p_map:
        description: "<your_own_value>"
        egress_pri_tagging: "disable"
        name: "default_name_5"
        priority_0: "queue-0"
        priority_1: "queue-0"
        priority_2: "queue-0"
        priority_3: "queue-0"
        priority_4: "queue-0"
        priority_5: "queue-0"
        priority_6: "queue-0"
        priority_7: "queue-0"
```

6.296.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.296.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.296.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.297 fortios_switch_controller_qos_ip_dscp_map – Configure FortiSwitch QoS IP precedence/DSCP in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.297.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller_qos feature and ip_dscp_map category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.297.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.297.3 FortiOS Version Compatibility

6.297.4 Parameters

6.297.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.297.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch QoS IP precedence/DSCP.
    fortios_switch_controller_qos_ip_dscp_map:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_qos_ip_dscp_map:
        description: "<your_own_value>"
        map:
         -
            cos_queue: "5"
            diffserv: "CS0"
            ip_precedence: "network-control"
            name: "default_name_8"
            value: "<your_own_value>"
        name: "default_name_10"
```

6.297.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.297.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.297.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.298 fortios_switch_controller_qos_qos_policy – Configure FortiSwitch QoS policy in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.298.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller_qos feature and qos_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.298.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.298.3 FortiOS Version Compatibility

6.298.4 Parameters

6.298.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.298.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch QoS policy.
    fortios_switch_controller_qos_qos_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_qos_qos_policy:
        default_cos: "3"
        name: "default_name_4"
        queue_policy: "<your_own_value> (source switch-controller.qos.queue-policy.
↪name)"
        trust_dot1p_map: "<your_own_value> (source switch-controller.qos.dot1p-map.
↪name)"
        trust_ip_dscp_map: "<your_own_value> (source switch-controller.qos.ip-dscp-
↪map.name)"
```

6.298.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.298.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.298.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.299 fortios_switch_controller_qos_queue_policy – Configure FortiSwitch QoS egress queue policy in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.299.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller_qos feature and queue_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.299.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.299.3 FortiOS Version Compatibility

6.299.4 Parameters

6.299.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.299.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch QoS egress queue policy.
    fortios_switch_controller_qos_queue_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_qos_queue_policy:
        cos_queue:
         -
            description: "<your_own_value>"
            drop_policy: "taildrop"
            ecn: "disable"
            max_rate: "7"
            max_rate_percent: "8"
            min_rate: "9"
            min_rate_percent: "10"
            name: "default_name_11"
            weight: "12"
        name: "default_name_13"
        rate_by: "kbps"
        schedule: "strict"
```

6.299.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.299.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.299.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.300 fortios_switch_controller_quarantine – Configure FortiSwitch quarantine support in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.300.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and quarantine category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.300.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.300.3 FortiOS Version Compatibility

6.300.4 Parameters

6.300.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.300.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch quarantine support.
    fortios_switch_controller_quarantine:
      vdom:  "{{ vdom }}"
      switch_controller_quarantine:
        quarantine: "enable"
        targets:
         -
            description: "<your_own_value>"
            entry_id: "6"
            mac: "<your_own_value>"
            tag:
             -
                tags: "<your_own_value>"
```

6.300.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.300.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.300.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.301 fortios_switch_controller_remote_log – Configure logging by FortiSwitch device to a remote syslog server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.301.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and remote_log category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.301.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.301.3 FortiOS Version Compatibility

6.301.4 Parameters

6.301.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.301.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure logging by FortiSwitch device to a remote syslog server.
    fortios_switch_controller_remote_log:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_remote_log:
        csv: "enable"
        facility: "kernel"
        name: "default_name_5"
        port: "6"
        server: "192.168.100.40"
        severity: "emergency"
        status: "enable"
```

6.301.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.301.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.301.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.302 fortios_switch_controller_security_policy_802_1x – Configure 802.1x MAC Authentication Bypass (MAB) policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.302.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller_security_policy feature and 802_1x category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.302.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.302.3 FortiOS Version Compatibility

6.302.4 Parameters

6.302.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.302.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure 802.1x MAC Authentication Bypass (MAB) policies.
    fortios_switch_controller_security_policy_802_1x:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_security_policy_802_1x:
        auth_fail_vlan: "disable"
        auth_fail_vlan_id: "<your_own_value> (source system.interface.name)"
        auth_fail_vlanid: "5"
        authserver_timeout_period: "6"
        authserver_timeout_vlan: "disable"
        authserver_timeout_vlanid: "<your_own_value> (source system.interface.name)"
        eap_auto_untagged_vlans: "disable"
        eap_passthru: "disable"
        framevid_apply: "disable"
        guest_auth_delay: "12"
        guest_vlan: "disable"
        guest_vlan_id: "<your_own_value> (source system.interface.name)"
        guest_vlanid: "15"
        mac_auth_bypass: "disable"
        name: "default_name_17"
        open_auth: "disable"
        policy_type: "802.1X"
        radius_timeout_overwrite: "disable"
        security_mode: "802.1X"
        user_group:
         -
            name: "default_name_23 (source user.group.name)"
```

6.302.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.302.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.302.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.303 fortios_switch_controller_security_policy_captive_portal – Names of VLANs that use captive portal authentication in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.303.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller_security_policy feature and captive_portal category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.303.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.303.3 FortiOS Version Compatibility

6.303.4 Parameters

6.303.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.303.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Names of VLANs that use captive portal authentication.
    fortios_switch_controller_security_policy_captive_portal:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_security_policy_captive_portal:
        name: "default_name_3"
        policy_type: "captive-portal"
        vlan: "<your_own_value> (source system.interface.name)"
```

6.303.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.303.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.303.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.304 fortios_switch_controller_security_policy_local_access – Configure allowaccess list for mgmt and internal interfaces on managed FortiSwitch in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.304.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller_security_policy feature and local_access category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.304.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.304.3 FortiOS Version Compatibility

6.304.4 Parameters

6.304.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.304.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure allowaccess list for mgmt and internal interfaces on managed␣
↪FortiSwitch.
    fortios_switch_controller_security_policy_local_access:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_security_policy_local_access:
        internal_allowaccess: "https"
        mgmt_allowaccess: "https"
        name: "default_name_5"
```

6.304.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.304.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.304.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.305 fortios_switch_controller_sflow – Configure FortiSwitch sFlow in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.305.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and sflow category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.305.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.305.3 FortiOS Version Compatibility

6.305.4 Parameters

6.305.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.305.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch sFlow.
    fortios_switch_controller_sflow:
      vdom:  "{{ vdom }}"
      switch_controller_sflow:
        collector_ip: "<your_own_value>"
        collector_port: "4"
```

6.305.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.305.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.305.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.306 fortios_switch_controller_snmp_community – Configure FortiSwitch SNMP v1/v2c communities globally in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.306.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and snmp_community category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.306.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.306.3 FortiOS Version Compatibility

6.306.4 Parameters

6.306.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.306.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure FortiSwitch SNMP v1/v2c communities globally.
  fortios_switch_controller_snmp_community:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    switch_controller_snmp_community:
      events: "cpu-high"
      hosts:
       -
          id:  "5"
          ip: "<your_own_value>"
      id:  "7"
      name: "default_name_8"
      query_v1_port: "9"
      query_v1_status: "disable"
      query_v2c_port: "11"
      query_v2c_status: "disable"
      status: "disable"
      trap_v1_lport: "14"
      trap_v1_rport: "15"
      trap_v1_status: "disable"
      trap_v2c_lport: "17"
      trap_v2c_rport: "18"
      trap_v2c_status: "disable"
```

6.306.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.306.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.306.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.307 fortios_switch_controller_snmp_sysinfo – Configure FortiSwitch SNMP system information globally in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.307.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and snmp_sysinfo category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.307.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.307.3 FortiOS Version Compatibility

6.307.4 Parameters

6.307.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.307.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch SNMP system information globally.
    fortios_switch_controller_snmp_sysinfo:
      vdom:  "{{ vdom }}"
      switch_controller_snmp_sysinfo:
        contact_info: "<your_own_value>"
        description: "<your_own_value>"
        engine_id: "<your_own_value>"
        location: "<your_own_value>"
        status: "disable"
```

6.307.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.307.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.307.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.308 fortios_switch_controller_snmp_trap_threshold – Configure FortiSwitch SNMP trap threshold values globally in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.308.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and snmp_trap_threshold category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.308.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.308.3 FortiOS Version Compatibility

6.308.4 Parameters

6.308.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.308.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch SNMP trap threshold values globally.
    fortios_switch_controller_snmp_trap_threshold:
      vdom:  "{{ vdom }}"
      switch_controller_snmp_trap_threshold:
        trap_high_cpu_threshold: "3"
        trap_log_full_threshold: "4"
        trap_low_memory_threshold: "5"
```

6.308.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.308.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.308.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.309 fortios_switch_controller_snmp_user – Configure FortiSwitch SNMP v3 users globally in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.309.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and snmp_user category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.309.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.309.3 FortiOS Version Compatibility

6.309.4 Parameters

6.309.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.309.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure FortiSwitch SNMP v3 users globally.
  fortios_switch_controller_snmp_user:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    switch_controller_snmp_user:
      auth_proto: "md5"
      auth_pwd: "<your_own_value>"
      name: "default_name_5"
      priv_proto: "aes"
      priv_pwd: "<your_own_value>"
      queries: "disable"
      query_port: "9"
      security_level: "no-auth-no-priv"
```

6.309.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.309.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.309.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.310 fortios_switch_controller_storm_control – Configure FortiSwitch storm control in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.310.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and storm_control category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.310.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.310.3 FortiOS Version Compatibility

6.310.4 Parameters

6.310.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.310.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure FortiSwitch storm control.
  fortios_switch_controller_storm_control:
    vdom:  "{{ vdom }}"
    switch_controller_storm_control:
      broadcast: "enable"
      rate: "4"
      unknown_multicast: "enable"
      unknown_unicast: "enable"
```

6.310.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.310.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.310.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.311 fortios_switch_controller_storm_control_policy – Configure FortiSwitch storm control policy to be applied on managed-switch ports in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.311.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and storm_control_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.311.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.311.3 FortiOS Version Compatibility

6.311.4 Parameters

6.311.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.311.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch storm control policy to be applied on managed-switch␣
↪ports.
    fortios_switch_controller_storm_control_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
    switch_controller_storm_control_policy:
      broadcast: "enable"
      description: "<your_own_value>"
      name: "default_name_5"
      rate: "6"
      storm_control_mode: "global"
      unknown_multicast: "enable"
      unknown_unicast: "enable"
```

6.311.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.311.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.311.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.312 fortios_switch_controller_stp_instance – Configure FortiSwitch multiple spanning tree protocol (MSTP) instances in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.312.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and stp_instance category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.312.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.312.3 FortiOS Version Compatibility

6.312.4 Parameters

6.312.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.312.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch multiple spanning tree protocol (MSTP) instances.
    fortios_switch_controller_stp_instance:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_stp_instance:
        id:  "3"
        vlan_range:
```

(continues on next page)

(continued from previous page)

```
        -
            vlan_name: "<your_own_value> (source system.interface.name)"
```

6.312.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.312.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.312.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.313 fortios_switch_controller_stp_settings – Configure FortiSwitch spanning tree protocol (STP) in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.313.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and stp_settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.313.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.313.3 FortiOS Version Compatibility

6.313.4 Parameters

6.313.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.313.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch spanning tree protocol (STP).
    fortios_switch_controller_stp_settings:
      vdom:  "{{ vdom }}"
      switch_controller_stp_settings:
        forward_time: "3"
        hello_time: "4"
        max_age: "5"
        max_hops: "6"
        name: "default_name_7"
        pending_timer: "8"
        revision: "9"
        status: "enable"
```

6.313.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.313.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.313.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.314 fortios_switch_controller_switch_group – Configure FortiSwitch switch groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.314.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and switch_group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.314.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.314.3 FortiOS Version Compatibility

6.314.4 Parameters

6.314.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.314.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch switch groups.
    fortios_switch_controller_switch_group:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_switch_group:
        description: "<your_own_value>"
        fortilink: "<your_own_value> (source system.interface.name)"
        members:
         -
            name: "default_name_6 (source switch-controller.managed-switch.switch-id)"
            switch_id: "<your_own_value> (source switch-controller.managed-switch.
↪switch-id)"
        name: "default_name_8"
```

6.314.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.314.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.314.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.315 fortios_switch_controller_switch_interface_tag – Configure switch object tags in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.315.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and switch_interface_tag category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.315.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.315.3 FortiOS Version Compatibility

6.315.4 Parameters

6.315.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.315.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure switch object tags.
    fortios_switch_controller_switch_interface_tag:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_switch_interface_tag:
        name: "default_name_3"
```

6.315.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.315.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.315.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.316 fortios_switch_controller_switch_log – Configure FortiSwitch logging (logs are transferred to and inserted into FortiGate event log) in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.316.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and switch_log category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.316.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.316.3 FortiOS Version Compatibility

6.316.4 Parameters

6.316.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.316.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch logging (logs are transferred to and inserted into␣
↪FortiGate event log).
    fortios_switch_controller_switch_log:
      vdom:  "{{ vdom }}"
      switch_controller_switch_log:
        severity: "emergency"
        status: "enable"
```

6.316.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.316.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.316.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.317 fortios_switch_controller_switch_profile – Configure FortiSwitch switch profile in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.317.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and switch_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.317.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.317.3 FortiOS Version Compatibility

6.317.4 Parameters

6.317.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.317.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSwitch switch profile.
    fortios_switch_controller_switch_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_switch_profile:
        login_passwd: "<your_own_value>"
        login_passwd_override: "enable"
        name: "default_name_5"
```

6.317.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.317.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.317.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.318 fortios_switch_controller_system – Configure system-wide switch controller settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.318.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and system category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.318.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.318.3 FortiOS Version Compatibility

6.318.4 Parameters

6.318.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.318.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure system-wide switch controller settings.
  fortios_switch_controller_system:
    vdom:  "{{ vdom }}"
    switch_controller_system:
      data_sync_interval: "3"
      dynamic_periodic_interval: "4"
      iot_holdoff: "5"
      iot_mac_idle: "6"
      iot_scan_interval: "7"
      iot_weight_threshold: "8"
      nac_periodic_interval: "9"
      parallel_process: "10"
      parallel_process_override: "disable"
      tunnel_mode: "compatible"
```

6.318.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.318.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.318.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.319 fortios_switch_controller_traffic_policy – Configure FortiSwitch traffic policy in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.319.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and traffic_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.319.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.319.3 FortiOS Version Compatibility

6.319.4 Parameters

6.319.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.319.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure FortiSwitch traffic policy.
  fortios_switch_controller_traffic_policy:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    switch_controller_traffic_policy:
      cos_queue: "3"
      description: "<your_own_value>"
      guaranteed_bandwidth: "5"
      guaranteed_burst: "6"
      id:  "7"
      maximum_burst: "8"
      name: "default_name_9"
      policer_status: "enable"
      type: "ingress"
```

6.319.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.319.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.319.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.320 fortios_switch_controller_traffic_sniffer – Configure FortiSwitch RSPAN/ERSPAN traffic sniffing parameters in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.320.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and traffic_sniffer category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.320.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.320.3 FortiOS Version Compatibility

6.320.4 Parameters

6.320.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.320.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
  tasks:
  - name: Configure FortiSwitch RSPAN/ERSPAN traffic sniffing parameters.
    fortios_switch_controller_traffic_sniffer:
      vdom:  "{{ vdom }}"
      switch_controller_traffic_sniffer:
        erspan_ip: "<your_own_value>"
        mode: "erspan-auto"
        target_ip:
         -
            description: "<your_own_value>"
            dst_entry_id: "7"
            ip: "<your_own_value>"
            src_entry_id: "9"
        target_mac:
         -
            description: "<your_own_value>"
            dst_entry_id: "12"
            mac: "<your_own_value>"
            src_entry_id: "14"
        target_port:
         -
            description: "<your_own_value>"
            in_ports:
             -
                name: "default_name_18"
            out_ports:
             -
                name: "default_name_20"
            switch_id: "<your_own_value> (source switch-controller.managed-switch.
↪switch-id)"
```

6.320.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.320.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.320.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.321 fortios_switch_controller_virtual_port_pool – Configure virtual pool in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.321.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and virtual_port_pool category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.321.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.321.3 FortiOS Version Compatibility

6.321.4 Parameters

6.321.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.321.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure virtual pool.
    fortios_switch_controller_virtual_port_pool:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_virtual_port_pool:
        description: "<your_own_value>"
        name: "default_name_4"
```

6.321.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.321.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.321.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.322 fortios_switch_controller_vlan – Configure VLANs for switch controller in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.322.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and vlan category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.322.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.322.3 FortiOS Version Compatibility

6.322.4 Parameters

6.322.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.322.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure VLANs for switch controller.
  fortios_switch_controller_vlan:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    switch_controller_vlan:
      auth: "radius"
      color: "4"
      comments: "<your_own_value>"
      name: "default_name_6"
      portal_message_override_group: "<your_own_value>"
      portal_message_overrides:
          auth_disclaimer_page: "<your_own_value>"
          auth_login_failed_page: "<your_own_value>"
          auth_login_page: "<your_own_value>"
          auth_reject_page: "<your_own_value>"
      radius_server: "<your_own_value> (source user.radius.name)"
      security: "open"
      selected_usergroups:
       -
          name: "default_name_16 (source user.group.name)"
      usergroup: "<your_own_value> (source user.group.name)"
      vdom: "<your_own_value>"
      vlanid: "19"
```

6.322.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.322.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.322.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.323 fortios_switch_controller_vlan_policy – Configure VLAN policy to be applied on the managed FortiSwitch ports through port-policy in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.323.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify switch_controller feature and vlan_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.323.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.323.3 FortiOS Version Compatibility

6.323.4 Parameters

6.323.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.323.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure VLAN policy to be applied on the managed FortiSwitch ports␣
↪through port-policy.
    fortios_switch_controller_vlan_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      switch_controller_vlan_policy:
        allowed_vlans:
         -
            vlan_name: "<your_own_value> (source system.interface.name)"
        allowed_vlans_all: "enable"
        description: "<your_own_value>"
        discard_mode: "none"
        fortilink: "<your_own_value> (source system.interface.name)"
        name: "default_name_9"
        untagged_vlans:
         -
            vlan_name: "<your_own_value> (source system.interface.name)"
        vlan: "<your_own_value> (source system.interface.name)"
```

6.323.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.323.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.323.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.324 fortios_system_3g_modem_custom – 3G MODEM custom in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.324.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_3g_modem feature and custom category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.324.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.324.3 FortiOS Version Compatibility

6.324.4 Parameters

6.324.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.324.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: 3G MODEM custom.
    fortios_system_3g_modem_custom:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_3g_modem_custom:
        class_id: "<your_own_value>"
        id:  "4"
        init_string: "<your_own_value>"
        model: "<your_own_value>"
        modeswitch_string: "<your_own_value>"
        product_id: "<your_own_value>"
        vendor: "<your_own_value>"
        vendor_id: "<your_own_value>"
```

6.324.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.324.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.324.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.325 fortios_system_accprofile – Configure access profiles for system administrators in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.325.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and accprofile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.325.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.325.3 FortiOS Version Compatibility

6.325.4 Parameters

6.325.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.325.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure access profiles for system administrators.
    fortios_system_accprofile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_accprofile:
        admintimeout: "3"
        admintimeout_override: "enable"
        authgrp: "none"
        comments: "<your_own_value>"
        ftviewgrp: "none"
        fwgrp: "none"
        fwgrp_permission:
            address: "none"
            policy: "none"
            schedule: "none"
            service: "none"
        loggrp: "none"
        loggrp_permission:
            config: "none"
            data_access: "none"
            report_access: "none"
            threat_weight: "none"
        name: "default_name_20"
        netgrp: "none"
        netgrp_permission:
            cfg: "none"
            packet_capture: "none"
            route_cfg: "none"
        scope: "vdom"
        secfabgrp: "none"
        sysgrp: "none"
        sysgrp_permission:
            admin: "none"
            cfg: "none"
            mnt: "none"
            upd: "none"
        system_diagnostics: "enable"
        utmgrp: "none"
        utmgrp_permission:
            antivirus: "none"
            application_control: "none"
            data_loss_prevention: "none"
            dnsfilter: "none"
            emailfilter: "none"
            endpoint_control: "none"
            file_filter: "none"
```

(continues on next page)

(continued from previous page)

```
            icap: "none"
            ips: "none"
            mmsgtp: "none"
            spamfilter: "none"
            voip: "none"
            waf: "none"
            webfilter: "none"
        vpngrp: "none"
        wanoptgrp: "none"
        wifi: "none"
```

6.325.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.325.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.325.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.326 fortios_system_acme – Configure ACME client in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.326.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and acme category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.326.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.326.3 FortiOS Version Compatibility

6.326.4 Parameters

6.326.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.326.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure ACME client.
    fortios_system_acme:
      vdom:  "{{ vdom }}"
      system_acme:
        accounts:
         -
```

(continues on next page)

(continued from previous page)

```
            ca_url: "<your_own_value>"
            email: "<your_own_value>"
            id:  "6"
            privatekey: "<your_own_value>"
            status: "<your_own_value>"
            url: "myurl.com"
        interface:
         -
            interface_name: "<your_own_value> (source system.interface.name)"
```

6.326.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.326.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.326.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.327 fortios_system_admin – Configure admin users in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.327.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and admin category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.327.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.327.3 FortiOS Version Compatibility

6.327.4 Parameters

6.327.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.327.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure admin users.
    fortios_system_admin:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_admin:
        accprofile: "<your_own_value> (source system.accprofile.name)"
        accprofile_override: "enable"
```

(continues on next page)

(continued from previous page)

```
        allow_remove_admin_session: "enable"
        comments: "<your_own_value>"
        email_to: "<your_own_value>"
        force_password_change: "enable"
        fortitoken: "<your_own_value>"
        guest_auth: "disable"
        guest_lang: "<your_own_value> (source system.custom-language.name)"
        guest_usergroups:
         -
            name: "default_name_13"
        gui_dashboard:
         -
            columns: "15"
            id:  "16"
            layout_type: "responsive"
            name: "default_name_18"
            permanent: "disable"
            scope: "global"
            vdom: "<your_own_value> (source system.vdom.name)"
            widget:
             -
                fabric_device: "<your_own_value>"
                fabric_device_widget_name: "<your_own_value>"
                fabric_device_widget_visualization_type: "<your_own_value>"
                fortiview_device: "<your_own_value>"
                fortiview_filters:
                 -
                    id:  "28"
                    key: "<your_own_value>"
                    value: "<your_own_value>"
                fortiview_sort_by: "<your_own_value>"
                fortiview_timeframe: "<your_own_value>"
                fortiview_type: "<your_own_value>"
                fortiview_visualization: "<your_own_value>"
                height: "35"
                id:  "36"
                industry: "default"
                interface: "<your_own_value> (source system.interface.name)"
                region: "default"
                title: "<your_own_value>"
                type: "sysinfo"
                width: "42"
                x_pos: "43"
                y_pos: "44"
        gui_global_menu_favorites:
         -
            id:  "46"
        gui_new_feature_acknowledge:
         -
            id:  "48"
        gui_vdom_menu_favorites:
         -
            id:  "50"
        hidden: "51"
        history0: "<your_own_value>"
        history1: "<your_own_value>"
        ip6_trusthost1: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        ip6_trusthost10: "<your_own_value>"
        ip6_trusthost2: "<your_own_value>"
        ip6_trusthost3: "<your_own_value>"
        ip6_trusthost4: "<your_own_value>"
        ip6_trusthost5: "<your_own_value>"
        ip6_trusthost6: "<your_own_value>"
        ip6_trusthost7: "<your_own_value>"
        ip6_trusthost8: "<your_own_value>"
        ip6_trusthost9: "<your_own_value>"
        login_time:
         -
            last_failed_login: "<your_own_value>"
            last_login: "<your_own_value>"
            usr_name: "<your_own_value>"
        name: "default_name_68"
        password: "<your_own_value>"
        password_expire: "<your_own_value>"
        peer_auth: "enable"
        peer_group: "<your_own_value>"
        radius_vdom_override: "enable"
        remote_auth: "enable"
        remote_group: "<your_own_value>"
        schedule: "<your_own_value>"
        sms_custom_server: "<your_own_value> (source system.sms-server.name)"
        sms_phone: "<your_own_value>"
        sms_server: "fortiguard"
        ssh_certificate: "<your_own_value> (source certificate.local.name)"
        ssh_public_key1: "<your_own_value>"
        ssh_public_key2: "<your_own_value>"
        ssh_public_key3: "<your_own_value>"
        trusthost1: "<your_own_value>"
        trusthost10: "<your_own_value>"
        trusthost2: "<your_own_value>"
        trusthost3: "<your_own_value>"
        trusthost4: "<your_own_value>"
        trusthost5: "<your_own_value>"
        trusthost6: "<your_own_value>"
        trusthost7: "<your_own_value>"
        trusthost8: "<your_own_value>"
        trusthost9: "<your_own_value>"
        two_factor: "disable"
        two_factor_authentication: "fortitoken"
        two_factor_notification: "email"
        vdom:
         -
            name: "default_name_98 (source system.vdom.name)"
        wildcard: "enable"
```

6.327.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.327.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.327.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.328 fortios_system_affinity_interrupt – Configure interrupt affinity in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.328.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and affinity_interrupt category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.328.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.328.3 FortiOS Version Compatibility

6.328.4 Parameters

6.328.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.328.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure interrupt affinity.
    fortios_system_affinity_interrupt:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_affinity_interrupt:
        affinity_cpumask: "<your_own_value>"
        id:  "4"
        interrupt: "<your_own_value>"
```

6.328.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.328.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.328.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.329 fortios_system_affinity_packet_redistribution – Configure packet redistribution in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.329.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and affinity_packet_redistribution category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.329.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.329.3 FortiOS Version Compatibility

6.329.4 Parameters

6.329.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.329.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure packet redistribution.
    fortios_system_affinity_packet_redistribution:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_affinity_packet_redistribution:
        affinity_cpumask: "<your_own_value>"
        id:  "4"
        interface: "<your_own_value> (source system.interface.name)"
        rxqid: "6"
```

6.329.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.329.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.329.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.330 fortios_system_alarm – Configure alarm in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.330.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and alarm category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.330.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.330.3 FortiOS Version Compatibility

6.330.4 Parameters

6.330.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.330.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure alarm.
    fortios_system_alarm:
      vdom:  "{{ vdom }}"
      system_alarm:
        audible: "enable"
        groups:
         -
            admin_auth_failure_threshold: "5"
            admin_auth_lockout_threshold: "6"
            decryption_failure_threshold: "7"
            encryption_failure_threshold: "8"
            fw_policy_id: "9"
            fw_policy_id_threshold: "10"
            fw_policy_violations:
             -
                dst_ip: "<your_own_value>"
                dst_port: "13"
                id:  "14"
                src_ip: "<your_own_value>"
                src_port: "16"
                threshold: "17"
            id:  "18"
            log_full_warning_threshold: "19"
            period: "20"
            replay_attempt_threshold: "21"
            self_test_failure_threshold: "22"
            user_auth_failure_threshold: "23"
            user_auth_lockout_threshold: "24"
        status: "enable"
```

6.330.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.330.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.330.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.331 fortios_system_alias – Configure alias command in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.331.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and alias category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.331.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.331.3 FortiOS Version Compatibility

6.331.4 Parameters

6.331.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.331.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure alias command.
    fortios_system_alias:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_alias:
        command: "<your_own_value>"
        name: "default_name_4"
```

6.331.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.331.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.331.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.332 fortios_system_api_user – Configure API users in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.332.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and api_user category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.332.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.332.3 FortiOS Version Compatibility

6.332.4 Parameters

6.332.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.332.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure API users.
    fortios_system_api_user:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_api_user:
        accprofile: "<your_own_value> (source system.accprofile.name)"
        api_key: "<your_own_value>"
        comments: "<your_own_value>"
        cors_allow_origin: "<your_own_value>"
        name: "default_name_7"
        peer_auth: "enable"
        peer_group: "<your_own_value>"
        schedule: "<your_own_value>"
        trusthost:
         -
            id:  "12"
            ipv4_trusthost: "<your_own_value>"
            ipv6_trusthost: "<your_own_value>"
            type: "ipv4-trusthost"
        vdom:
         -
            name: "default_name_17 (source system.vdom.name)"
```

6.332.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.332.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.332.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.333 fortios_system_arp_table – Configure ARP table in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.333.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and arp_table category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.333.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.333.3 FortiOS Version Compatibility

6.333.4 Parameters

6.333.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.333.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure ARP table.
    fortios_system_arp_table:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_arp_table:
        id:  "3"
        interface: "<your_own_value> (source system.interface.name)"
        ip: "<your_own_value>"
        mac: "<your_own_value>"
```

6.333.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.333.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.333.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.334 fortios_system_auto_install – Configure USB auto installation in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.334.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and auto_install category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.334.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.334.3 FortiOS Version Compatibility

6.334.4 Parameters

6.334.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.334.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure USB auto installation.
    fortios_system_auto_install:
      vdom:  "{{ vdom }}"
      system_auto_install:
        auto_install_config: "enable"
        auto_install_image: "enable"
        default_config_file: "<your_own_value>"
        default_image_file: "<your_own_value>"
```

6.334.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.334.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.334.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.335 fortios_system_auto_script – Configure auto script in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.335.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and auto_script category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.335.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.335.3 FortiOS Version Compatibility

6.335.4 Parameters

6.335.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.335.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure auto script.
  fortios_system_auto_script:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    system_auto_script:
      interval: "3"
      name: "default_name_4"
      output_size: "5"
      repeat: "6"
      script: "<your_own_value>"
      start: "manual"
      timeout: "9"
```

6.335.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.335.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.335.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.336 fortios_system_automation_action – Action for automation stitches in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.336.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and automation_action category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.336.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.336.3 FortiOS Version Compatibility

6.336.4 Parameters

6.336.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.336.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Action for automation stitches.
    fortios_system_automation_action:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    state: "present"
    access_token: "<your_own_value>"
    system_automation_action:
      accprofile: "<your_own_value> (source system.accprofile.name)"
      action_type: "email"
      alicloud_access_key_id: "<your_own_value>"
      alicloud_access_key_secret: "<your_own_value>"
      alicloud_account_id: "<your_own_value>"
      alicloud_function: "<your_own_value>"
      alicloud_function_authorization: "anonymous"
      alicloud_function_domain: "<your_own_value>"
      alicloud_region: "<your_own_value>"
      alicloud_service: "<your_own_value>"
      alicloud_version: "<your_own_value>"
      aws_api_id: "<your_own_value>"
      aws_api_key: "<your_own_value>"
      aws_api_path: "<your_own_value>"
      aws_api_stage: "<your_own_value>"
      aws_domain: "<your_own_value>"
      aws_region: "<your_own_value>"
      azure_api_key: "<your_own_value>"
      azure_app: "<your_own_value>"
      azure_domain: "<your_own_value>"
      azure_function: "<your_own_value>"
      azure_function_authorization: "anonymous"
      delay: "25"
      description: "<your_own_value>"
      email_body: "<your_own_value>"
      email_from: "<your_own_value>"
      email_subject: "<your_own_value>"
      email_to:
       -
          name: "default_name_31"
      gcp_function: "<your_own_value>"
      gcp_function_domain: "<your_own_value>"
      gcp_function_region: "<your_own_value>"
      gcp_project: "<your_own_value>"
      headers:
       -
          header: "<your_own_value>"
      http_body: "<your_own_value>"
      message: "<your_own_value>"
      message_type: "text"
      method: "post"
      minimum_interval: "42"
      name: "default_name_43"
      port: "44"
      protocol: "http"
      replacement_message: "enable"
      replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
      required: "enable"
      script: "<your_own_value>"
      sdn_connector:
       -
          name: "default_name_51 (source system.sdn-connector.name)"
      security_tag: "<your_own_value>"
      tls_certificate: "<your_own_value> (source certificate.local.name)"
```

(continues on next page)

(continued from previous page)

```
        uri: "<your_own_value>"
        verify_host_cert: "enable"
```

6.336.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.336.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.336.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.337 fortios_system_automation_destination – Automation destinations in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.337.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and automation_destination category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.337.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.337.3 FortiOS Version Compatibility

6.337.4 Parameters

6.337.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.337.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Automation destinations.
    fortios_system_automation_destination:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_automation_destination:
        destination:
         -
            name: "default_name_4"
        ha_group_id: "5"
        name: "default_name_6"
        type: "fortigate"
```

6.337.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.337.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.337.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.338 fortios_system_automation_stitch – Automation stitches in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.338.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and automation_stitch category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.338.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.338.3 FortiOS Version Compatibility

6.338.4 Parameters

6.338.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.338.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Automation stitches.
    fortios_system_automation_stitch:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_automation_stitch:
        action:
         -
            name: "default_name_4 (source system.automation-action.name)"
        description: "<your_own_value>"
        destination:
         -
            name: "default_name_7 (source system.automation-destination.name)"
        name: "default_name_8"
        status: "enable"
        trigger: "<your_own_value> (source system.automation-trigger.name)"
```

6.338.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.338.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.338.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.339 fortios_system_automation_trigger – Trigger for automation stitches in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.339.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and automation_trigger category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.339.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.339.3 FortiOS Version Compatibility

6.339.4 Parameters

6.339.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.339.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Trigger for automation stitches.
    fortios_system_automation_trigger:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_automation_trigger:
        description: "<your_own_value>"
        event_type: "ioc"
        fabric_event_name: "<your_own_value>"
        fabric_event_severity: "<your_own_value>"
        faz_event_name: "<your_own_value>"
        faz_event_severity: "<your_own_value>"
        faz_event_tags: "<your_own_value>"
        fields:
         -
            id:  "11"
            name: "default_name_12"
            value: "<your_own_value>"
        ioc_level: "medium"
        license_type: "forticare-support"
        logid: "16"
        name: "default_name_17"
        report_type: "PostureReport"
        serial: "<your_own_value>"
        trigger_day: "20"
        trigger_frequency: "hourly"
        trigger_hour: "22"
        trigger_minute: "23"
```

(continues on next page)

(continued from previous page)

```
        trigger_type: "event-based"
        trigger_weekday: "sunday"
```

6.339.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.339.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.339.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.340 fortios_system_autoupdate_push_update – Configure push updates in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.340.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_autoupdate feature and push_update category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.340.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.340.3 FortiOS Version Compatibility

6.340.4 Parameters

6.340.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.340.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure push updates.
    fortios_system_autoupdate_push_update:
      vdom:  "{{ vdom }}"
      system_autoupdate_push_update:
        address: "<your_own_value>"
        override: "enable"
        port: "5"
        status: "enable"
```

6.340.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.340.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.340.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.341 fortios_system_autoupdate_schedule – Configure update schedule in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.341.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_autoupdate feature and schedule category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.341.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.341.3 FortiOS Version Compatibility

6.341.4 Parameters

6.341.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.341.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure update schedule.
    fortios_system_autoupdate_schedule:
      vdom:  "{{ vdom }}"
      system_autoupdate_schedule:
        day: "Sunday"
        frequency: "every"
        status: "enable"
        time: "<your_own_value>"
```

6.341.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.341.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.341.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.342 fortios_system_autoupdate_tunneling – Configure web proxy tunnelling for the FDN in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.342.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_autoupdate feature and tunneling category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.342.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.342.3 FortiOS Version Compatibility

6.342.4 Parameters

6.342.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.342.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure web proxy tunnelling for the FDN.
    fortios_system_autoupdate_tunneling:
      vdom:  "{{ vdom }}"
      system_autoupdate_tunneling:
        address: "<your_own_value>"
        password: "<your_own_value>"
        port: "5"
        status: "enable"
        username: "<your_own_value>"
```

6.342.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.342.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.342.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.343 fortios_system_central_management – Configure central management in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.343.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and central_management category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.343.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.343.3 FortiOS Version Compatibility

6.343.4 Parameters

6.343.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.343.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure central management.
    fortios_system_central_management:
      vdom:  "{{ vdom }}"
      system_central_management:
        allow_monitor: "enable"
        allow_push_configuration: "enable"
        allow_push_firmware: "enable"
        allow_remote_firmware_upgrade: "enable"
        ca_cert: "<your_own_value>"
        enc_algorithm: "default"
        fmg: "<your_own_value>"
        fmg_source_ip: "<your_own_value>"
        fmg_source_ip6: "<your_own_value>"
        fmg_update_port: "8890"
        include_default_servers: "enable"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        local_cert: "<your_own_value>"
        mode: "normal"
        schedule_config_restore: "enable"
        schedule_script_restore: "enable"
        serial_number: "<your_own_value>"
        server_list:
         -
            addr_type: "ipv4"
            fqdn: "<your_own_value>"
            id:  "24"
            server_address: "<your_own_value>"
            server_address6: "<your_own_value>"
            server_type: "update"
        type: "fortimanager"
        vdom: "<your_own_value> (source system.vdom.name)"
```

6.343.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.343.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.343.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.344 fortios_system_cluster_sync – Configure FortiGate Session Life Support Protocol (FGSP) session synchronization in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.344.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and cluster_sync category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.344.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.344.3 FortiOS Version Compatibility

6.344.4 Parameters

6.344.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.344.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiGate Session Life Support Protocol (FGSP) session␣
↪synchronization.
    fortios_system_cluster_sync:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_cluster_sync:
        down_intfs_before_sess_sync:
         -
            name: "default_name_4 (source system.interface.name)"
        hb_interval: "5"
        hb_lost_threshold: "6"
        ike_heartbeat_interval: "7"
        ike_monitor: "enable"
        ike_monitor_interval: "9"
        ike_seqjump_speed: "10"
        ipsec_tunnel_sync: "enable"
        peerip: "<your_own_value>"
        peervd: "<your_own_value> (source system.vdom.name)"
        session_sync_filter:
            custom_service:
             -
                dst_port_range: "<your_own_value>"
                id:  "17"
                src_port_range: "<your_own_value>"
            dstaddr: "<your_own_value>"
            dstaddr6: "<your_own_value>"
            dstintf: "<your_own_value> (source system.interface.name)"
            srcaddr: "<your_own_value>"
            srcaddr6: "<your_own_value>"
            srcintf: "<your_own_value> (source system.interface.name)"
```

(continues on next page)

(continued from previous page)

```
        slave_add_ike_routes: "enable"
        sync_id: "26"
        syncvd:
         -
            name: "default_name_28 (source system.vdom.name)"
```

6.344.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.344.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.344.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.345 fortios_system_console – Configure console in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.345.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and console category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.345.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.345.3 FortiOS Version Compatibility

6.345.4 Parameters

6.345.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.345.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure console.
    fortios_system_console:
      vdom:  "{{ vdom }}"
      system_console:
        baudrate: "9600"
        fortiexplorer: "enable"
        login: "enable"
        mode: "batch"
        output: "standard"
```

6.345.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.345.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.345.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.346 fortios_system_csf – Add this FortiGate to a Security Fabric or set up a new Security Fabric on this FortiGate in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.346.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and csf category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.346.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.346.3 FortiOS Version Compatibility

6.346.4 Parameters

6.346.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.346.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Add this FortiGate to a Security Fabric or set up a new Security Fabric on␣
↪this FortiGate.
    fortios_system_csf:
      vdom:  "{{ vdom }}"
      system_csf:
        accept_auth_by_cert: "disable"
        authorization_request_type: "serial"
        certificate: "<your_own_value> (source certificate.local.name)"
        configuration_sync: "default"
        downstream_access: "enable"
        downstream_accprofile: "<your_own_value> (source system.accprofile.name)"
        fabric_connector:
         -
            accprofile: "<your_own_value> (source system.accprofile.name)"
            configuration_write_access: "enable"
            serial: "<your_own_value>"
        fabric_device:
```

(continues on next page)

(continued from previous page)

```
    -
        access_token: "<your_own_value>"
        device_ip: "<your_own_value>"
        device_type: "fortimail"
        https_port: "17"
        login: "<your_own_value>"
        name: "default_name_19"
        password: "<your_own_value>"
    fabric_object_unification: "default"
    fabric_workers: "22"
    fixed_key: "<your_own_value>"
    group_name: "<your_own_value>"
    group_password: "<your_own_value>"
    log_unification: "disable"
    management_ip: "<your_own_value>"
    management_port: "28"
    saml_configuration_sync: "default"
    status: "enable"
    trusted_list:
     -
        action: "accept"
        authorization_type: "serial"
        certificate: "<your_own_value>"
        downstream_authorization: "enable"
        ha_members: "<your_own_value>"
        name: "default_name_37"
        serial: "<your_own_value>"
    upstream_ip: "<your_own_value>"
    upstream_port: "40"
```

6.346.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.346.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.346.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.347 fortios_system_custom_language – Configure custom languages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.347.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and custom_language category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.347.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.347.3 FortiOS Version Compatibility

6.347.4 Parameters

6.347.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.347.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure custom languages.
    fortios_system_custom_language:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_custom_language:
        comments: "<your_own_value>"
        filename: "<your_own_value>"
        name: "default_name_5"
```

6.347.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.347.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.347.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.348 fortios_system_ddns – Configure DDNS in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.348.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and ddns category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.348.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.348.3 FortiOS Version Compatibility

6.348.4 Parameters

6.348.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.348.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
 tasks:
 - name: Configure DDNS.
   fortios_system_ddns:
     vdom:  "{{ vdom }}"
     state: "present"
     access_token: "<your_own_value>"
     system_ddns:
       addr_type: "ipv4"
       bound_ip: "<your_own_value>"
       clear_text: "disable"
       ddns_auth: "disable"
       ddns_domain: "<your_own_value>"
       ddns_key: "<your_own_value>"
       ddns_keyname: "<your_own_value>"
       ddns_password: "<your_own_value>"
       ddns_server: "dyndns.org"
       ddns_server_addr:
        -
           addr: "<your_own_value>"
       ddns_server_ip: "<your_own_value>"
       ddns_sn: "<your_own_value>"
       ddns_ttl: "16"
       ddns_username: "<your_own_value>"
       ddns_zone: "<your_own_value>"
       ddnsid: "19"
       monitor_interface:
        -
           interface_name: "<your_own_value> (source system.interface.name)"
       server_type: "ipv4"
       ssl_certificate: "<your_own_value> (source certificate.local.name)"
       update_interval: "24"
       use_public_ip: "disable"
```

6.348.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.348.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.348.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.349 fortios_system_dedicated_mgmt – Configure dedicated management in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.349.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and dedicated_mgmt category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.349.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.349.3 FortiOS Version Compatibility

6.349.4 Parameters

6.349.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.349.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure dedicated management.
    fortios_system_dedicated_mgmt:
      vdom:  "{{ vdom }}"
      system_dedicated_mgmt:
        default_gateway: "<your_own_value>"
        dhcp_end_ip: "<your_own_value>"
        dhcp_netmask: "<your_own_value>"
        dhcp_server: "enable"
        dhcp_start_ip: "<your_own_value>"
        interface: "<your_own_value> (source system.interface.name)"
        status: "enable"
```

6.349.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.349.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.349.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.350 fortios_system_dhcp6_server – Configure DHCPv6 servers in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.350.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_dhcp6 feature and server category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.350.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.350.3 FortiOS Version Compatibility

6.350.4 Parameters

6.350.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.350.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure DHCPv6 servers.
    fortios_system_dhcp6_server:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_dhcp6_server:
        dns_search_list: "delegated"
        dns_server1: "<your_own_value>"
        dns_server2: "<your_own_value>"
        dns_server3: "<your_own_value>"
        dns_server4: "<your_own_value>"
        dns_service: "delegated"
        domain: "<your_own_value>"
        id:  "10"
        interface: "<your_own_value> (source system.interface.name)"
        ip_mode: "range"
        ip_range:
         -
            end_ip: "<your_own_value>"
            id:  "15"
            start_ip: "<your_own_value>"
        lease_time: "17"
        option1: "<your_own_value>"
        option2: "<your_own_value>"
        option3: "<your_own_value>"
        prefix_mode: "dhcp6"
        prefix_range:
         -
            end_prefix: "<your_own_value>"
            id:  "24"
            prefix_length: "25"
            start_prefix: "<your_own_value>"
        rapid_commit: "disable"
        status: "disable"
        subnet: "<your_own_value>"
        upstream_interface: "<your_own_value> (source system.interface.name)"
```

6.350.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.350.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.350.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.351 fortios_system_dhcp_server – Configure DHCP servers in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.351.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_dhcp feature and server category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.351.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.351.3 FortiOS Version Compatibility

6.351.4 Parameters

6.351.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.351.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure DHCP servers.
    fortios_system_dhcp_server:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_dhcp_server:
        auto_configuration: "disable"
        auto_managed_status: "disable"
        conflicted_ip_timeout: "5"
        ddns_auth: "disable"
        ddns_key: "<your_own_value>"
        ddns_keyname: "<your_own_value>"
        ddns_server_ip: "<your_own_value>"
        ddns_ttl: "10"
        ddns_update: "disable"
        ddns_update_override: "disable"
        ddns_zone: "<your_own_value>"
        default_gateway: "<your_own_value>"
        dhcp_settings_from_fortiipam: "disable"
        dns_server1: "<your_own_value>"
        dns_server2: "<your_own_value>"
        dns_server3: "<your_own_value>"
        dns_server4: "<your_own_value>"
        dns_service: "local"
        domain: "<your_own_value>"
        exclude_range:
         -
            end_ip: "<your_own_value>"
            id:  "24"
            start_ip: "<your_own_value>"
        filename: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        forticlient_on_net_status: "disable"
        id:  "28"
        interface: "<your_own_value> (source system.interface.name)"
        ip_mode: "range"
        ip_range:
         -
            end_ip: "<your_own_value>"
            id:  "33"
            start_ip: "<your_own_value>"
        ipsec_lease_hold: "35"
        lease_time: "36"
        mac_acl_default_action: "assign"
        netmask: "<your_own_value>"
        next_server: "<your_own_value>"
        ntp_server1: "<your_own_value>"
        ntp_server2: "<your_own_value>"
        ntp_server3: "<your_own_value>"
        ntp_service: "local"
        options:
         -
            code: "45"
            id:  "46"
            ip: "<your_own_value>"
            type: "hex"
            value: "<your_own_value>"
        reserved_address:
         -
            action: "assign"
            circuit_id: "<your_own_value>"
            circuit_id_type: "hex"
            description: "<your_own_value>"
            id:  "55"
            ip: "<your_own_value>"
            mac: "<your_own_value>"
            remote_id: "<your_own_value>"
            remote_id_type: "hex"
            type: "mac"
        server_type: "regular"
        status: "disable"
        tftp_server:
         -
            tftp_server: "<your_own_value>"
        timezone: "01"
        timezone_option: "disable"
        vci_match: "disable"
        vci_string:
         -
            vci_string: "<your_own_value>"
        wifi_ac_service: "specify"
        wifi_ac1: "<your_own_value>"
        wifi_ac2: "<your_own_value>"
        wifi_ac3: "<your_own_value>"
        wins_server1: "<your_own_value>"
        wins_server2: "<your_own_value>"
```

6.351.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.351.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.351.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.352 fortios_system_dns – Configure DNS in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.352.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and dns category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.352.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.352.3 FortiOS Version Compatibility

6.352.4 Parameters

6.352.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.352.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure DNS.
    fortios_system_dns:
      vdom:  "{{ vdom }}"
      system_dns:
        cache_notfound_responses: "disable"
        dns_cache_limit: "4"
        dns_cache_ttl: "5"
        dns_over_tls: "disable"
        domain:
         -
            domain: "<your_own_value>"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        ip6_primary: "<your_own_value>"
        ip6_secondary: "<your_own_value>"
        primary: "<your_own_value>"
        protocol: "cleartext"
        retry: "15"
        secondary: "<your_own_value>"
        server_hostname:
         -
            hostname: "myhostname"
        source_ip: "84.230.14.43"
        ssl_certificate: "<your_own_value> (source certificate.local.name)"
        timeout: "21"
```

6.352.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.352.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.352.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.353 fortios_system_dns_database – Configure DNS databases in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.353.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and dns_database category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.353.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.353.3 FortiOS Version Compatibility

6.353.4 Parameters

6.353.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.353.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure DNS databases.
    fortios_system_dns_database:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_dns_database:
        allow_transfer: "<your_own_value>"
        authoritative: "enable"
        contact: "<your_own_value>"
        dns_entry:
         -
            canonical_name: "<your_own_value>"
            hostname: "myhostname"
            id:  "9"
            ip: "<your_own_value>"
            ipv6: "<your_own_value>"
            preference: "12"
            status: "enable"
            ttl: "14"
            type: "A"
        domain: "<your_own_value>"
        forwarder: "<your_own_value>"
        ip_master: "<your_own_value>"
        ip_primary: "<your_own_value>"
        name: "default_name_20"
```

(continues on next page)

(continued from previous page)

```
        primary_name: "<your_own_value>"
        rr_max: "22"
        source_ip: "84.230.14.43"
        status: "enable"
        ttl: "25"
        type: "master"
        view: "shadow"
```

6.353.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.353.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.353.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.354 fortios_system_dns_server – Configure DNS servers in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.354.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and dns_server category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.354.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.354.3 FortiOS Version Compatibility

6.354.4 Parameters

6.354.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.354.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure DNS servers.
    fortios_system_dns_server:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_dns_server:
        dnsfilter_profile: "<your_own_value> (source dnsfilter.profile.name)"
        doh: "enable"
        mode: "recursive"
        name: "default_name_6 (source system.interface.name)"
```

6.354.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.354.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.354.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.355 fortios_system_dscp_based_priority – Configure DSCP based priority table in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.355.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and dscp_based_priority category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.355.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.355.3 FortiOS Version Compatibility

6.355.4 Parameters

6.355.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.355.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure DSCP based priority table.
    fortios_system_dscp_based_priority:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_dscp_based_priority:
        ds: "3"
        id:  "4"
        priority: "low"
```

6.355.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.355.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.355.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.356 fortios_system_email_server – Configure the email server used by the FortiGate various things. For example, for sending email messages to users to support user authentication features in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.356.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and email_server category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.356.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.356.3 FortiOS Version Compatibility

6.356.4 Parameters

6.356.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.356.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure the email server used by the FortiGate various things. For␣
↪example, for sending email messages to users to support user authentication
     features.
    fortios_system_email_server:
      vdom:  "{{ vdom }}"
      system_email_server:
        authenticate: "enable"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        password: "<your_own_value>"
        port: "7"
        reply_to: "<your_own_value>"
        security: "none"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        source_ip6: "<your_own_value>"
        ssl_min_proto_version: "default"
        type: "custom"
        username: "<your_own_value>"
        validate_server: "enable"
```

6.356.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.356.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.356.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.357 fortios_system_external_resource – Configure external resource in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.357.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and external_resource category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.357.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.357.3 FortiOS Version Compatibility

6.357.4 Parameters

6.357.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.357.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure external resource.
    fortios_system_external_resource:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_external_resource:
        category: "3"
        comments: "<your_own_value>"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        name: "default_name_7"
        password: "<your_own_value>"
        refresh_rate: "9"
        resource: "<your_own_value>"
        source_ip: "84.230.14.43"
        status: "enable"
        type: "category"
        user_agent: "<your_own_value>"
        username: "<your_own_value>"
        uuid: "<your_own_value>"
```

6.357.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.357.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.357.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.358 fortios_system_federated_upgrade – Coordinate federated upgrades within the Security Fabric in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.358.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and federated_upgrade category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.358.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.358.3 FortiOS Version Compatibility

6.358.4 Parameters

6.358.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.358.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Coordinate federated upgrades within the Security Fabric.
    fortios_system_federated_upgrade:
      vdom:  "{{ vdom }}"
      system_federated_upgrade:
        node_list:
         -
            coordinating_fortigate: "<your_own_value>"
            device_type: "fortigate"
            serial: "<your_own_value>"
            setup_time: "<your_own_value>"
            time: "<your_own_value>"
            timing: "immediate"
            upgrade_path: "<your_own_value>"
        status: "disabled"
        upgrade_id: "12"
```

6.358.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.358.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.358.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.359 fortios_system_fips_cc – Configure FIPS-CC mode in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.359.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and fips_cc category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.359.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.359.3 FortiOS Version Compatibility

6.359.4 Parameters

6.359.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.359.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FIPS-CC mode.
    fortios_system_fips_cc:
      vdom:  "{{ vdom }}"
      system_fips_cc:
        entropy_token: "enable"
        key_generation_self_test: "enable"
        self_test_period: "5"
        status: "enable"
```

6.359.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.359.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.359.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.360 fortios_system_fm – Configure FM in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.360.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and fm category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.360.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.360.3 FortiOS Version Compatibility

6.360.4 Parameters

6.360.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.360.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FM.
    fortios_system_fm:
      vdom:  "{{ vdom }}"
      system_fm:
        auto_backup: "enable"
        id:  "4"
        ip: "<your_own_value>"
        ipsec: "enable"
        scheduled_config_restore: "enable"
        status: "enable"
        vdom: "<your_own_value> (source system.vdom.name)"
```

6.360.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.360.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.360.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.361 fortios_system_fortiguard – Configure FortiGuard services in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.361.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and fortiguard category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.361.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.361.3 FortiOS Version Compatibility

6.361.4 Parameters

6.361.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.361.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiGuard services.
    fortios_system_fortiguard:
      vdom:  "{{ vdom }}"
      system_fortiguard:
        antispam_cache: "enable"
        antispam_cache_mpercent: "4"
        antispam_cache_ttl: "5"
        antispam_expiration: "6"
        antispam_force_off: "enable"
        antispam_license: "8"
        antispam_timeout: "9"
        anycast_sdns_server_ip: "<your_own_value>"
        anycast_sdns_server_port: "11"
        auto_join_forticloud: "enable"
        ddns_server_ip: "<your_own_value>"
        ddns_server_port: "14"
        fortiguard_anycast: "enable"
        fortiguard_anycast_source: "fortinet"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        load_balance_servers: "19"
        outbreak_prevention_cache: "enable"
        outbreak_prevention_cache_mpercent: "21"
        outbreak_prevention_cache_ttl: "22"
        outbreak_prevention_expiration: "23"
        outbreak_prevention_force_off: "enable"
        outbreak_prevention_license: "25"
        outbreak_prevention_timeout: "26"
        persistent_connection: "enable"
        port: "8888"
        protocol: "udp"
        proxy_password: "<your_own_value>"
        proxy_server_ip: "<your_own_value>"
        proxy_server_port: "32"
        proxy_username: "<your_own_value>"
        sandbox_region: "<your_own_value>"
        sdns_options: "include-question-section"
        sdns_server_ip: "<your_own_value>"
        sdns_server_port: "37"
        service_account_id: "<your_own_value>"
        source_ip: "84.230.14.43"
        source_ip6: "<your_own_value>"
        update_build_proxy: "enable"
        update_extdb: "enable"
        update_ffdb: "enable"
        update_server_location: "usa"
        update_uwdb: "enable"
```

(continues on next page)

(continued from previous page)

```
        videofilter_expiration: "46"
        videofilter_license: "47"
        webfilter_cache: "enable"
        webfilter_cache_ttl: "49"
        webfilter_expiration: "50"
        webfilter_force_off: "enable"
        webfilter_license: "52"
        webfilter_timeout: "53"
```

6.361.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.361.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.361.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.362 fortios_system_fortimanager – Configure FortiManager in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.362.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and fortimanager category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.362.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.362.3 FortiOS Version Compatibility

6.362.4 Parameters

6.362.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.362.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiManager.
    fortios_system_fortimanager:
      vdom:  "{{ vdom }}"
      system_fortimanager:
        central_management: "enable"
        central_mgmt_auto_backup: "enable"
        central_mgmt_schedule_config_restore: "enable"
        central_mgmt_schedule_script_restore: "enable"
        ip: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        ipsec: "enable"
        vdom: "<your_own_value> (source system.vdom.name)"
```

6.362.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.362.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.362.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.363 fortios_system_fortisandbox – Configure FortiSandbox in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.363.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and fortisandbox category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.363.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.363.3 FortiOS Version Compatibility

6.363.4 Parameters

6.363.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.363.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiSandbox.
    fortios_system_fortisandbox:
      vdom:  "{{ vdom }}"
      system_fortisandbox:
        email: "<your_own_value>"
        enc_algorithm: "default"
        forticloud: "enable"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        ssl_min_proto_version: "default"
        status: "enable"
```

6.363.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.363.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.363.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.364 fortios_system_fsso_polling – Configure Fortinet Single Sign On (FSSO) server in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.364.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and fsso_polling category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.364.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.364.3 FortiOS Version Compatibility

6.364.4 Parameters

6.364.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.364.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Fortinet Single Sign On (FSSO) server.
    fortios_system_fsso_polling:
      vdom:  "{{ vdom }}"
      system_fsso_polling:
        auth_password: "<your_own_value>"
        authentication: "enable"
        listening_port: "5"
        status: "enable"
```

6.364.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.364.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.364.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.365 fortios_system_ftm_push – Configure FortiToken Mobile push services in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.365.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and ftm_push category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.365.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.365.3 FortiOS Version Compatibility

6.365.4 Parameters

6.365.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.365.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiToken Mobile push services.
    fortios_system_ftm_push:
      vdom:  "{{ vdom }}"
      system_ftm_push:
        server: "192.168.100.40"
        server_cert: "<your_own_value> (source certificate.local.name)"
        server_ip: "<your_own_value>"
        server_port: "6"
        status: "enable"
```

6.365.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.365.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.365.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.366 fortios_system_geneve – Configure GENEVE devices in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.366.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and geneve category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.366.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.366.3 FortiOS Version Compatibility

6.366.4 Parameters

6.366.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.366.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure GENEVE devices.
    fortios_system_geneve:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_geneve:
        dstport: "3"
        interface: "<your_own_value> (source system.interface.name)"
        ip_version: "ipv4-unicast"
        name: "default_name_6"
        remote_ip: "<your_own_value>"
        remote_ip6: "<your_own_value>"
        type: "ethernet"
        vni: "10"
```

6.366.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.366.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.366.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.367 fortios_system_geoip_country – Define geoip country name-ID table in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.367.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and geoip_country category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.367.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.367.3 FortiOS Version Compatibility

6.367.4 Parameters

6.367.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.367.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Define geoip country name-ID table.
    fortios_system_geoip_country:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_geoip_country:
        id:  "3"
        name: "default_name_4"
```

6.367.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.367.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.367.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.368 fortios_system_geoip_override – Configure geographical location mapping for IP address(es) to override mappings from FortiGuard in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.368.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and geoip_override category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.368.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.368.3 FortiOS Version Compatibility

6.368.4 Parameters

6.368.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.368.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
 tasks:
 - name: Configure geographical location mapping for IP address(es) to override␣
↪mappings from FortiGuard.
   fortios_system_geoip_override:
     vdom:  "{{ vdom }}"
     state: "present"
     access_token: "<your_own_value>"
     system_geoip_override:
       country_id: "<your_own_value>"
       description: "<your_own_value>"
       ip_range:
        -
           end_ip: "<your_own_value>"
           id:  "7"
           start_ip: "<your_own_value>"
       ip6_range:
        -
           end_ip: "<your_own_value>"
           id:  "11"
           start_ip: "<your_own_value>"
       name: "default_name_13"
```

6.368.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.368.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.368.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.369 fortios_system_gi_gk – Configure Gi Firewall Gatekeeper in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.369.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and gi_gk category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.369.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.369.3 FortiOS Version Compatibility

6.369.4 Parameters

6.369.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.369.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Gi Firewall Gatekeeper.
    fortios_system_gi_gk:
      vdom:  "{{ vdom }}"
      system_gi_gk:
        context: "3"
        port: "4"
```

6.369.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.369.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.369.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.370 fortios_system_global – Configure global attributes in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Synopsis*

6.370.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and global category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.370.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.370.3 FortiOS Version Compatibility

6.370.4 Parameters

6.370.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.370.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure global attributes.
```

(continues on next page)

(continued from previous page)

```
    fortios_system_global:
      vdom:  "{{ vdom }}"
      system_global:
        admin_concurrent: "enable"
        admin_console_timeout: "4"
        admin_forticloud_sso_login: "enable"
        admin_hsts_max_age: "6"
        admin_https_pki_required: "enable"
        admin_https_redirect: "enable"
        admin_https_ssl_versions: "tlsv1-0"
        admin_lockout_duration: "10"
        admin_lockout_threshold: "11"
        admin_login_max: "12"
        admin_maintainer: "enable"
        admin_port: "14"
        admin_restrict_local: "enable"
        admin_scp: "enable"
        admin_server_cert: "<your_own_value> (source certificate.local.name)"
        admin_sport: "18"
        admin_ssh_grace_time: "19"
        admin_ssh_password: "enable"
        admin_ssh_port: "21"
        admin_ssh_v1: "enable"
        admin_telnet: "enable"
        admin_telnet_port: "24"
        admintimeout: "25"
        alias: "<your_own_value>"
        allow_traffic_redirect: "enable"
        anti_replay: "disable"
        arp_max_entry: "29"
        asymroute: "enable"
        auth_cert: "<your_own_value> (source certificate.local.name)"
        auth_http_port: "32"
        auth_https_port: "33"
        auth_keepalive: "enable"
        auth_session_limit: "block-new"
        auto_auth_extension_device: "enable"
        autorun_log_fsck: "enable"
        av_affinity: "<your_own_value>"
        av_failopen: "pass"
        av_failopen_session: "enable"
        batch_cmdb: "enable"
        block_session_timer: "42"
        br_fdb_max_entry: "43"
        cert_chain_max: "44"
        cfg_revert_timeout: "45"
        cfg_save: "automatic"
        check_protocol_header: "loose"
        check_reset_range: "strict"
        cli_audit_log: "enable"
        cloud_communication: "enable"
        clt_cert_req: "enable"
        compliance_check: "enable"
        compliance_check_time: "<your_own_value>"
        cpu_use_threshold: "54"
        csr_ca_attribute: "enable"
        daily_restart: "enable"
```

(continues on next page)

(continued from previous page)

```
        default_service_source_port: "<your_own_value>"
        device_identification_active_scan_delay: "58"
        device_idle_timeout: "59"
        dh_params: "1024"
        dnsproxy_worker_count: "61"
        dst: "enable"
        edit_vdom_prompt: "enable"
        endpoint_control_fds_access: "enable"
        endpoint_control_portal_port: "65"
        failtime: "66"
        faz_disk_buffer_size: "67"
        fds_statistics: "enable"
        fds_statistics_period: "69"
        fec_port: "70"
        fgd_alert_subscription: "advisory"
        fortiextender: "enable"
        fortiextender_data_port: "73"
        fortiextender_vlan_mode: "enable"
        fortiipam_integration: "enable"
        fortiservice_port: "76"
        fortitoken_cloud: "enable"
        gui_allow_default_hostname: "enable"
        gui_certificates: "enable"
        gui_custom_language: "enable"
        gui_date_format: "yyyy/MM/dd"
        gui_date_time_source: "system"
        gui_device_latitude: "<your_own_value>"
        gui_device_longitude: "<your_own_value>"
        gui_display_hostname: "enable"
        gui_firmware_upgrade_warning: "enable"
        gui_forticare_registration_setup_warning: "enable"
        gui_fortigate_cloud_sandbox: "enable"
        gui_fortisandbox_cloud: "enable"
        gui_ipv6: "enable"
        gui_lines_per_page: "91"
        gui_local_out: "enable"
        gui_replacement_message_groups: "enable"
        gui_rest_api_cache: "enable"
        gui_theme: "green"
        gui_wireless_opensecurity: "enable"
        honor_df: "enable"
        hostname: "myhostname"
        igmp_state_limit: "99"
        interval: "100"
        ip_src_port_range: "<your_own_value>"
        ips_affinity: "<your_own_value>"
        ipsec_asic_offload: "enable"
        ipsec_ha_seqjump_rate: "104"
        ipsec_hmac_offload: "enable"
        ipsec_soft_dec_async: "enable"
        ipv6_accept_dad: "107"
        ipv6_allow_anycast_probe: "enable"
        ipv6_allow_traffic_redirect: "enable"
        irq_time_accounting: "auto"
        language: "english"
        ldapconntimeout: "112"
        lldp_reception: "enable"
```

(continues on next page)

(continued from previous page)

```
        lldp_transmission: "enable"
        log_ssl_connection: "enable"
        log_uuid: "disable"
        log_uuid_address: "enable"
        log_uuid_policy: "enable"
        login_timestamp: "enable"
        long_vdom_name: "enable"
        management_ip: "<your_own_value>"
        management_port: "122"
        management_vdom: "<your_own_value> (source system.vdom.name)"
        max_dlpstat_memory: "124"
        max_route_cache_size: "125"
        mc_ttl_notchange: "enable"
        memory_use_threshold_extreme: "127"
        memory_use_threshold_green: "128"
        memory_use_threshold_red: "129"
        miglog_affinity: "<your_own_value>"
        miglogd_children: "131"
        multi_factor_authentication: "optional"
        multicast_forward: "enable"
        ndp_max_entry: "134"
        per_user_bal: "enable"
        per_user_bwl: "enable"
        policy_auth_concurrent: "137"
        post_login_banner: "disable"
        pre_login_banner: "enable"
        private_data_encryption: "disable"
        proxy_auth_lifetime: "enable"
        proxy_auth_lifetime_timeout: "142"
        proxy_auth_timeout: "143"
        proxy_cipher_hardware_acceleration: "disable"
        proxy_hardware_acceleration: "disable"
        proxy_kxp_hardware_acceleration: "disable"
        proxy_re_authentication_mode: "session"
        proxy_resource_mode: "enable"
        proxy_worker_count: "149"
        radius_port: "150"
        reboot_upon_config_restore: "enable"
        refresh: "152"
        remoteauthtimeout: "153"
        reset_sessionless_tcp: "enable"
        restart_time: "<your_own_value>"
        revision_backup_on_logout: "enable"
        revision_image_auto_backup: "enable"
        scanunit_count: "158"
        security_rating_result_submission: "enable"
        security_rating_run_on_schedule: "enable"
        send_pmtu_icmp: "enable"
        snat_route_change: "enable"
        special_file_23_support: "disable"
        split_port: "<your_own_value>"
        ssd_trim_date: "165"
        ssd_trim_freq: "never"
        ssd_trim_hour: "167"
        ssd_trim_min: "168"
        ssd_trim_weekday: "sunday"
        ssh_cbc_cipher: "enable"
```

(continues on next page)

(continued from previous page)

```
        ssh_hmac_md5: "enable"
        ssh_kex_sha1: "enable"
        ssh_mac_weak: "enable"
        ssl_min_proto_version: "SSLv3"
        ssl_static_key_ciphers: "enable"
        sslvpn_cipher_hardware_acceleration: "enable"
        sslvpn_ems_sn_check: "enable"
        sslvpn_kxp_hardware_acceleration: "enable"
        sslvpn_max_worker_count: "179"
        sslvpn_plugin_version_check: "enable"
        strict_dirty_session_check: "enable"
        strong_crypto: "enable"
        switch_controller: "disable"
        switch_controller_reserved_network: "<your_own_value>"
        sys_perf_log_interval: "185"
        tcp_halfclose_timer: "186"
        tcp_halfopen_timer: "187"
        tcp_option: "enable"
        tcp_rst_timer: "189"
        tcp_timewait_timer: "190"
        tftp: "enable"
        timezone: "01"
        tp_mc_skip_policy: "enable"
        traffic_priority: "tos"
        traffic_priority_level: "low"
        two_factor_email_expiry: "196"
        two_factor_fac_expiry: "197"
        two_factor_ftk_expiry: "198"
        two_factor_ftm_expiry: "199"
        two_factor_sms_expiry: "200"
        udp_idle_timer: "201"
        url_filter_affinity: "<your_own_value>"
        url_filter_count: "203"
        user_device_store_max_devices: "204"
        user_device_store_max_users: "205"
        user_server_cert: "<your_own_value> (source certificate.local.name)"
        vdom_admin: "enable"
        vdom_mode: "no-vdom"
        vip_arp_range: "unlimited"
        virtual_server_count: "210"
        virtual_server_hardware_acceleration: "disable"
        wad_affinity: "<your_own_value>"
        wad_csvc_cs_count: "213"
        wad_csvc_db_count: "214"
        wad_memory_change_granularity: "215"
        wad_source_affinity: "disable"
        wad_worker_count: "217"
        wifi_ca_certificate: "<your_own_value> (source certificate.ca.name)"
        wifi_certificate: "<your_own_value> (source certificate.local.name)"
        wimax_4g_usb: "enable"
        wireless_controller: "enable"
        wireless_controller_port: "222"
```

6.370.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.370.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.370.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.371 fortios_system_gre_tunnel – Configure GRE tunnel in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.371.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and gre_tunnel category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.371.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.371.3 FortiOS Version Compatibility

6.371.4 Parameters

6.371.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.371.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure GRE tunnel.
    fortios_system_gre_tunnel:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_gre_tunnel:
        checksum_reception: "disable"
        checksum_transmission: "disable"
        diffservcode: "<your_own_value>"
        dscp_copying: "disable"
        interface: "<your_own_value> (source system.interface.name)"
        ip_version: "4"
        keepalive_failtimes: "9"
        keepalive_interval: "10"
        key_inbound: "11"
        key_outbound: "12"
        local_gw: "<your_own_value>"
        local_gw6: "<your_own_value>"
        name: "default_name_15"
        remote_gw: "<your_own_value>"
        remote_gw6: "<your_own_value>"
        sequence_number_reception: "disable"
        sequence_number_transmission: "disable"
        use_sdwan: "disable"
```

6.371.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.371.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.371.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.372 fortios_system_ha – Configure HA in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.372.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and ha category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.372.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.372.3 FortiOS Version Compatibility

6.372.4 Parameters

6.372.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.372.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure HA.
    fortios_system_ha:
      vdom:  "{{ vdom }}"
      system_ha:
        arps: "3"
        arps_interval: "4"
        authentication: "enable"
        cpu_threshold: "<your_own_value>"
        encryption: "enable"
        failover_hold_time: "8"
        ftp_proxy_threshold: "<your_own_value>"
        gratuitous_arps: "enable"
        group_id: "11"
        group_name: "<your_own_value>"
        ha_direct: "enable"
        ha_eth_type: "<your_own_value>"
        ha_mgmt_interfaces:
         -
            dst: "<your_own_value>"
            gateway: "<your_own_value>"
            gateway6: "<your_own_value>"
            id:  "19"
            interface: "<your_own_value> (source system.interface.name)"
        ha_mgmt_status: "enable"
        ha_uptime_diff_margin: "22"
```

(continues on next page)

(continued from previous page)

```
        hb_interval: "23"
        hb_interval_in_milliseconds: "100ms"
        hb_lost_threshold: "25"
        hbdev: "<your_own_value>"
        hc_eth_type: "<your_own_value>"
        hello_holddown: "28"
        http_proxy_threshold: "<your_own_value>"
        imap_proxy_threshold: "<your_own_value>"
        inter_cluster_session_sync: "enable"
        key: "<your_own_value>"
        l2ep_eth_type: "<your_own_value>"
        link_failed_signal: "enable"
        load_balance_all: "enable"
        logical_sn: "enable"
        memory_based_failover: "enable"
        memory_compatible_mode: "enable"
        memory_failover_flip_timeout: "39"
        memory_failover_monitor_period: "40"
        memory_failover_sample_rate: "41"
        memory_failover_threshold: "42"
        memory_threshold: "<your_own_value>"
        mode: "standalone"
        monitor: "<your_own_value> (source system.interface.name)"
        multicast_ttl: "46"
        nntp_proxy_threshold: "<your_own_value>"
        override: "enable"
        override_wait_time: "49"
        password: "<your_own_value>"
        pingserver_failover_threshold: "51"
        pingserver_flip_timeout: "52"
        pingserver_monitor_interface: "<your_own_value> (source system.interface.name)
↪"
        pingserver_secondary_force_reset: "enable"
        pingserver_slave_force_reset: "enable"
        pop3_proxy_threshold: "<your_own_value>"
        priority: "57"
        route_hold: "58"
        route_ttl: "59"
        route_wait: "60"
        schedule: "none"
        secondary_vcluster:
            monitor: "<your_own_value> (source system.interface.name)"
            override: "enable"
            override_wait_time: "65"
            pingserver_failover_threshold: "66"
            pingserver_monitor_interface: "<your_own_value> (source system.interface.
↪name)"
            pingserver_secondary_force_reset: "enable"
            pingserver_slave_force_reset: "enable"
            priority: "70"
            vcluster_id: "71"
            vdom: "<your_own_value>"
        session_pickup: "enable"
        session_pickup_connectionless: "enable"
        session_pickup_delay: "enable"
        session_pickup_expectation: "enable"
        session_pickup_nat: "enable"
```

(continues on next page)

(continued from previous page)

```
        session_sync_dev: "<your_own_value> (source system.interface.name)"
        smtp_proxy_threshold: "<your_own_value>"
        ssd_failover: "enable"
        standalone_config_sync: "enable"
        standalone_mgmt_vdom: "enable"
        sync_config: "enable"
        sync_packet_balance: "enable"
        unicast_gateway: "<your_own_value>"
        unicast_hb: "enable"
        unicast_hb_netmask: "<your_own_value>"
        unicast_hb_peerip: "<your_own_value>"
        unicast_peers:
         -
            id:  "90"
            peer_ip: "<your_own_value>"
        unicast_status: "enable"
        uninterruptible_upgrade: "enable"
        vcluster_id: "94"
        vcluster2: "enable"
        vdom: "<your_own_value>"
        weight: "<your_own_value>"
```

6.372.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.372.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.372.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.373 fortios_system_ha_monitor – Configure HA monitor in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.373.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and ha_monitor category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.373.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.373.3 FortiOS Version Compatibility

6.373.4 Parameters

6.373.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.373.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure HA monitor.
    fortios_system_ha_monitor:
      vdom:  "{{ vdom }}"
      system_ha_monitor:
        monitor_vlan: "enable"
        vlan_hb_interval: "4"
        vlan_hb_lost_threshold: "5"
```

6.373.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.373.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.373.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.374 fortios_system_ike – Configure IKE global attributes in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.374.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and ike category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.374.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.374.3 FortiOS Version Compatibility

6.374.4 Parameters

6.374.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.374.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure IKE global attributes.
  fortios_system_ike:
    vdom:  "{{ vdom }}"
    system_ike:
      dh_group_1:
          keypair_cache: "global"
          keypair_count: "5"
          mode: "software"
      dh_group_14:
          keypair_cache: "global"
          keypair_count: "9"
          mode: "software"
      dh_group_15:
          keypair_cache: "global"
          keypair_count: "13"
          mode: "software"
      dh_group_16:
          keypair_cache: "global"
          keypair_count: "17"
          mode: "software"
      dh_group_17:
          keypair_cache: "global"
          keypair_count: "21"
          mode: "software"
      dh_group_18:
          keypair_cache: "global"
          keypair_count: "25"
          mode: "software"
      dh_group_19:
          keypair_cache: "global"
          keypair_count: "29"
          mode: "software"
      dh_group_2:
          keypair_cache: "global"
          keypair_count: "33"
          mode: "software"
      dh_group_20:
          keypair_cache: "global"
          keypair_count: "37"
          mode: "software"
      dh_group_21:
          keypair_cache: "global"
          keypair_count: "41"
          mode: "software"
      dh_group_27:
          keypair_cache: "global"
          keypair_count: "45"
          mode: "software"
      dh_group_28:
          keypair_cache: "global"
          keypair_count: "49"
          mode: "software"
      dh_group_29:
          keypair_cache: "global"
          keypair_count: "53"
          mode: "software"
```

(continues on next page)

(continued from previous page)

```
        dh_group_30:
            keypair_cache: "global"
            keypair_count: "57"
            mode: "software"
        dh_group_31:
            keypair_cache: "global"
            keypair_count: "61"
            mode: "software"
        dh_group_32:
            keypair_cache: "global"
            keypair_count: "65"
            mode: "software"
        dh_group_5:
            keypair_cache: "global"
            keypair_count: "69"
            mode: "software"
        dh_keypair_cache: "enable"
        dh_keypair_count: "72"
        dh_keypair_throttle: "enable"
        dh_mode: "software"
        dh_multiprocess: "enable"
        dh_worker_count: "76"
        embryonic_limit: "77"
```

6.374.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.374.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.374.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.375 fortios_system_interface – Configure interfaces in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.375.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and interface category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.375.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.375.3 FortiOS Version Compatibility

6.375.4 Parameters

6.375.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.375.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure interfaces.
    fortios_system_interface:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_interface:
        ac_name: "<your_own_value>"
        aggregate: "<your_own_value>"
        algorithm: "L2"
        alias: "<your_own_value>"
        allowaccess: "ping"
        ap_discover: "enable"
        arpforward: "enable"
        auth_type: "auto"
        auto_auth_extension_device: "enable"
        bandwidth_measure_time: "12"
        bfd: "global"
        bfd_desired_min_tx: "14"
        bfd_detect_mult: "15"
        bfd_required_min_rx: "16"
        broadcast_forticlient_discovery: "enable"
        broadcast_forward: "enable"
        captive_portal: "19"
        cli_conn_status: "20"
        client_options:
         -
            code: "22"
            id:  "23"
            ip: "<your_own_value>"
            type: "hex"
            value: "<your_own_value>"
        color: "27"
        dedicated_to: "none"
        defaultgw: "enable"
        description: "<your_own_value>"
        detected_peer_mtu: "31"
        detectprotocol: "ping"
        detectserver: "<your_own_value>"
        device_access_list: "<your_own_value>"
        device_identification: "enable"
        device_identification_active_scan: "enable"
        device_netscan: "disable"
        device_user_identification: "enable"
        devindex: "39"
        dhcp_client_identifier:  "myId_40"
        dhcp_relay_agent_option: "enable"
        dhcp_relay_interface: "<your_own_value> (source system.interface.name)"
```

(continues on next page)

(continued from previous page)

```
        dhcp_relay_interface_select_method: "auto"
        dhcp_relay_ip: "<your_own_value>"
        dhcp_relay_request_all_server: "disable"
        dhcp_relay_service: "disable"
        dhcp_relay_type: "regular"
        dhcp_renew_time: "48"
        disc_retry_timeout: "49"
        disconnect_threshold: "50"
        distance: "51"
        dns_server_override: "enable"
        drop_fragment: "enable"
        drop_overlapped_fragment: "enable"
        egress_cos: "disable"
        egress_queues:
            cos0: "<your_own_value> (source system.isf-queue-profile.name)"
            cos1: "<your_own_value> (source system.isf-queue-profile.name)"
            cos2: "<your_own_value> (source system.isf-queue-profile.name)"
            cos3: "<your_own_value> (source system.isf-queue-profile.name)"
            cos4: "<your_own_value> (source system.isf-queue-profile.name)"
            cos5: "<your_own_value> (source system.isf-queue-profile.name)"
            cos6: "<your_own_value> (source system.isf-queue-profile.name)"
            cos7: "<your_own_value> (source system.isf-queue-profile.name)"
        egress_shaping_profile: "<your_own_value> (source firewall.shaping-profile.
↪profile-name)"
        endpoint_compliance: "enable"
        estimated_downstream_bandwidth: "67"
        estimated_upstream_bandwidth: "68"
        explicit_ftp_proxy: "enable"
        explicit_web_proxy: "enable"
        external: "enable"
        fail_action_on_extender: "soft-restart"
        fail_alert_interfaces:
         -
            name: "default_name_74 (source system.interface.name)"
        fail_alert_method: "link-failed-signal"
        fail_detect: "enable"
        fail_detect_option: "detectserver"
        fortiheartbeat: "enable"
        fortilink: "enable"
        fortilink_backup_link: "80"
        fortilink_neighbor_detect: "lldp"
        fortilink_split_interface: "enable"
        fortilink_stacking: "enable"
        forward_domain: "84"
        gi_gk: "enable"
        gwdetect: "enable"
        ha_priority: "87"
        icmp_accept_redirect: "enable"
        icmp_send_redirect: "enable"
        ident_accept: "enable"
        idle_timeout: "91"
        inbandwidth: "92"
        ingress_cos: "disable"
        ingress_shaping_profile: "<your_own_value> (source firewall.shaping-profile.
↪profile-name)"
        ingress_spillover_threshold: "95"
        interface: "<your_own_value> (source system.interface.name)"
```

(continues on next page)

(continued from previous page)

```
        internal: "97"
        ip: "<your_own_value>"
        ip_managed_by_fortiipam: "enable"
        ipmac: "enable"
        ips_sniffer_mode: "enable"
        ipunnumbered: "<your_own_value>"
        ipv6:
            autoconf: "enable"
            cli_conn6_status: "105"
            dhcp6_client_options: "rapid"
            dhcp6_information_request: "enable"
            dhcp6_prefix_delegation: "enable"
            dhcp6_prefix_hint: "<your_own_value>"
            dhcp6_prefix_hint_plt: "110"
            dhcp6_prefix_hint_vlt: "111"
            dhcp6_relay_ip: "<your_own_value>"
            dhcp6_relay_service: "disable"
            dhcp6_relay_type: "regular"
            icmp6_send_redirect: "enable"
            interface_identifier: "<your_own_value>"
            ip6_address: "<your_own_value>"
            ip6_allowaccess: "ping"
            ip6_default_life: "119"
            ip6_delegated_prefix_list:
             -
                autonomous_flag: "enable"
                onlink_flag: "enable"
                prefix_id: "123"
                rdnss: "<your_own_value>"
                rdnss_service: "delegated"
                subnet: "<your_own_value>"
                upstream_interface: "<your_own_value> (source system.interface.name)"
            ip6_dns_server_override: "enable"
            ip6_extra_addr:
             -
                prefix: "<your_own_value>"
            ip6_hop_limit: "131"
            ip6_link_mtu: "132"
            ip6_manage_flag: "enable"
            ip6_max_interval: "134"
            ip6_min_interval: "135"
            ip6_mode: "static"
            ip6_other_flag: "enable"
            ip6_prefix_list:
             -
                autonomous_flag: "enable"
                dnssl:
                 -
                    domain: "<your_own_value>"
                onlink_flag: "enable"
                preferred_life_time: "143"
                prefix: "<your_own_value>"
                rdnss: "<your_own_value>"
                valid_life_time: "146"
            ip6_prefix_mode: "dhcp6"
            ip6_reachable_time: "148"
            ip6_retrans_time: "149"
```

(continues on next page)

(continued from previous page)

```
            ip6_send_adv: "enable"
            ip6_subnet: "<your_own_value>"
            ip6_upstream_interface: "<your_own_value> (source system.interface.name)"
            nd_cert: "<your_own_value> (source certificate.local.name)"
            nd_cga_modifier: "<your_own_value>"
            nd_mode: "basic"
            nd_security_level: "156"
            nd_timestamp_delta: "157"
            nd_timestamp_fuzz: "158"
            ra_send_mtu: "enable"
            unique_autoconf_addr: "enable"
            vrip6_link_local: "<your_own_value>"
            vrrp_virtual_mac6: "enable"
            vrrp6:
             -
                accept_mode: "enable"
                adv_interval: "165"
                preempt: "enable"
                priority: "167"
                start_time: "168"
                status: "enable"
                vrdst6: "<your_own_value>"
                vrgrp: "171"
                vrid: "172"
                vrip6: "<your_own_value>"
        l2forward: "enable"
        lacp_ha_slave: "enable"
        lacp_mode: "static"
        lacp_speed: "slow"
        lcp_echo_interval: "178"
        lcp_max_echo_fails: "179"
        link_up_delay: "180"
        lldp_network_policy: "<your_own_value> (source system.lldp.network-policy.
↪name)"
        lldp_reception: "enable"
        lldp_transmission: "enable"
        macaddr: "<your_own_value>"
        managed_device:
         -
            name: "default_name_186"
        managed_subnetwork_size: "256"
        management_ip: "<your_own_value>"
        measured_downstream_bandwidth: "189"
        measured_upstream_bandwidth: "190"
        mediatype: "cfp2-sr10"
        member:
         -
            interface_name: "<your_own_value> (source system.interface.name)"
        min_links: "194"
        min_links_down: "operational"
        mode: "static"
        monitor_bandwidth: "enable"
        mtu: "198"
        mtu_override: "enable"
        name: "default_name_200"
        ndiscforward: "enable"
        netbios_forward: "disable"
```

(continues on next page)

(continued from previous page)

```
        netflow_sampler: "disable"
        outbandwidth: "204"
        padt_retry_timeout: "205"
        password: "<your_own_value>"
        ping_serv_status: "207"
        polling_interval: "208"
        pppoe_unnumbered_negotiate: "enable"
        pptp_auth_type: "auto"
        pptp_client: "enable"
        pptp_password: "<your_own_value>"
        pptp_server_ip: "<your_own_value>"
        pptp_timeout: "214"
        pptp_user: "<your_own_value>"
        preserve_session_route: "enable"
        priority: "217"
        priority_override: "enable"
        proxy_captive_portal: "enable"
        redundant_interface: "<your_own_value>"
        remote_ip: "<your_own_value>"
        replacemsg_override_group: "<your_own_value>"
        ring_rx: "223"
        ring_tx: "224"
        role: "lan"
        sample_direction: "tx"
        sample_rate: "227"
        scan_botnet_connections: "disable"
        secondary_IP: "enable"
        secondaryip:
         -
            allowaccess: "ping"
            detectprotocol: "ping"
            detectserver: "<your_own_value>"
            gwdetect: "enable"
            ha_priority: "235"
            id:  "236"
            ip: "<your_own_value>"
            ping_serv_status: "238"
        security_exempt_list: "<your_own_value>"
        security_external_logout: "<your_own_value>"
        security_external_web: "<your_own_value>"
        security_groups:
         -
            name: "default_name_243 (source user.group.name)"
        security_mac_auth_bypass: "enable"
        security_mode: "none"
        security_redirect_url: "<your_own_value>"
        service_name: "<your_own_value>"
        sflow_sampler: "enable"
        snmp_index: "249"
        speed: "auto"
        spillover_threshold: "251"
        src_check: "enable"
        status: "up"
        stp: "disable"
        stp_ha_secondary: "disable"
        stp_ha_slave: "disable"
        stpforward: "enable"
```

(continues on next page)

(continued from previous page)

```
        stpforward_mode: "rpl-all-ext-id"
        subst: "enable"
        substitute_dst_mac: "<your_own_value>"
        swc_first_create: "261"
        swc_vlan: "262"
        switch: "<your_own_value>"
        switch_controller_access_vlan: "enable"
        switch_controller_arp_inspection: "enable"
        switch_controller_dhcp_snooping: "enable"
        switch_controller_dhcp_snooping_option82: "enable"
        switch_controller_dhcp_snooping_verify_mac: "enable"
        switch_controller_dynamic: "<your_own_value> (source switch-controller.
↪fortilink-settings.name)"
        switch_controller_feature: "none"
        switch_controller_igmp_snooping: "enable"
        switch_controller_igmp_snooping_fast_leave: "enable"
        switch_controller_igmp_snooping_proxy: "enable"
        switch_controller_iot_scanning: "enable"
        switch_controller_learning_limit: "275"
        switch_controller_mgmt_vlan: "276"
        switch_controller_nac: "<your_own_value> (source switch-controller.nac-
↪settings.name)"
        switch_controller_rspan_mode: "disable"
        switch_controller_source_ip: "outbound"
        switch_controller_traffic_policy: "<your_own_value> (source switch-controller.
↪traffic-policy.name)"
        tagging:
         -
            category: "<your_own_value> (source system.object-tagging.category)"
            name: "default_name_283"
            tags:
             -
                name: "default_name_285 (source system.object-tagging.tags.name)"
        tcp_mss: "286"
        trust_ip_1: "<your_own_value>"
        trust_ip_2: "<your_own_value>"
        trust_ip_3: "<your_own_value>"
        trust_ip6_1: "<your_own_value>"
        trust_ip6_2: "<your_own_value>"
        trust_ip6_3: "<your_own_value>"
        type: "physical"
        username: "<your_own_value>"
        vdom: "<your_own_value> (source system.vdom.name)"
        vindex: "296"
        vlan_protocol: "8021q"
        vlanforward: "enable"
        vlanid: "299"
        vrf: "300"
        vrrp:
         -
            accept_mode: "enable"
            adv_interval: "303"
            ignore_default_route: "enable"
            preempt: "enable"
            priority: "306"
            proxy_arp:
             -
```

(continues on next page)

(continued from previous page)

```
            id:  "308"
            ip: "<your_own_value>"
        start_time: "310"
        status: "enable"
        version: "2"
        vrdst: "<your_own_value>"
        vrdst_priority: "314"
        vrgrp: "315"
        vrid: "316"
        vrip: "<your_own_value>"
    vrrp_virtual_mac: "enable"
    wccp: "enable"
    weight: "320"
    wins_ip: "<your_own_value>"
```

6.375.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.375.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.375.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.376 fortios_system_ipip_tunnel – Configure IP in IP Tunneling in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.376.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and ipip_tunnel category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.376.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.376.3 FortiOS Version Compatibility

6.376.4 Parameters

6.376.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.376.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IP in IP Tunneling.
    fortios_system_ipip_tunnel:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    state: "present"
    access_token: "<your_own_value>"
    system_ipip_tunnel:
      auto_asic_offload: "enable"
      interface: "<your_own_value> (source system.interface.name)"
      local_gw: "<your_own_value>"
      name: "default_name_6"
      remote_gw: "<your_own_value>"
      use_sdwan: "disable"
```

6.376.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.376.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.376.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.377 fortios_system_ips – Configure IPS system settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.377.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and ips category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.377.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.377.3 FortiOS Version Compatibility

6.377.4 Parameters

6.377.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.377.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPS system settings.
    fortios_system_ips:
      vdom:  "{{ vdom }}"
      system_ips:
        override_signature_hold_by_id: "enable"
        signature_hold_time: "<your_own_value>"
```

6.377.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.377.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.377.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.378 fortios_system_ips_urlfilter_dns – Configure IPS URL filter DNS servers in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.378.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and ips_urlfilter_dns category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.378.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.378.3 FortiOS Version Compatibility

6.378.4 Parameters

6.378.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.378.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPS URL filter DNS servers.
    fortios_system_ips_urlfilter_dns:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_ips_urlfilter_dns:
        address: "<your_own_value>"
        ipv6_capability: "enable"
        status: "enable"
```

6.378.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.378.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.378.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.379 fortios_system_ips_urlfilter_dns6 – Configure IPS URL filter IPv6 DNS servers in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.379.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and ips_urlfilter_dns6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.379.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.379.3 FortiOS Version Compatibility

6.379.4 Parameters

6.379.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.379.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPS URL filter IPv6 DNS servers.
    fortios_system_ips_urlfilter_dns6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_ips_urlfilter_dns6:
        address6: "<your_own_value>"
        status: "enable"
```

6.379.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.379.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.379.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.380 fortios_system_ipsec_aggregate – Configure an aggregate of IPsec tunnels in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.380.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and ipsec_aggregate category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.380.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.380.3 FortiOS Version Compatibility

6.380.4 Parameters

6.380.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.380.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure an aggregate of IPsec tunnels.
    fortios_system_ipsec_aggregate:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_ipsec_aggregate:
        algorithm: "L3"
        member:
         -
            tunnel_name: "<your_own_value> (source vpn.ipsec.phase1-interface.name)"
        name: "default_name_6"
```

6.380.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.380.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.380.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.381 fortios_system_ipv6_neighbor_cache – Configure IPv6 neighbor cache table in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.381.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and ipv6_neighbor_cache category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.381.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.381.3 FortiOS Version Compatibility

6.381.4 Parameters

6.381.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.381.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 neighbor cache table.
    fortios_system_ipv6_neighbor_cache:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_ipv6_neighbor_cache:
        id:  "3"
        interface: "<your_own_value> (source system.interface.name)"
        ipv6: "<your_own_value>"
        mac: "<your_own_value>"
```

6.381.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.381.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.381.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.382 fortios_system_ipv6_tunnel – Configure IPv6/IPv4 in IPv6 tunnel in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.382.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and ipv6_tunnel category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.382.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.382.3 FortiOS Version Compatibility

6.382.4 Parameters

6.382.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.382.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure IPv6/IPv4 in IPv6 tunnel.
  fortios_system_ipv6_tunnel:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    system_ipv6_tunnel:
      auto_asic_offload: "enable"
      destination: "<your_own_value>"
      interface: "<your_own_value> (source system.interface.name)"
      name: "default_name_6"
      source: "<your_own_value>"
      use_sdwan: "disable"
```

6.382.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.382.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.382.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.383 fortios_system_isf_queue_profile – Create a queue profile of switch in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.383.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and isf_queue_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.383.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.383.3 FortiOS Version Compatibility

6.383.4 Parameters

6.383.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.383.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Create a queue profile of switch.
    fortios_system_isf_queue_profile:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    state: "present"
    access_token: "<your_own_value>"
    system_isf_queue_profile:
      bandwidth_unit: "kbps"
      burst_control: "disable"
      guaranteed_bandwidth: "5"
      maximum_bandwidth: "6"
      name: "default_name_7"
```

6.383.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.383.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.383.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.384 fortios_system_link_monitor – Configure Link Health Monitor in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.384.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and link_monitor category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.384.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.384.3 FortiOS Version Compatibility

6.384.4 Parameters

6.384.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.384.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Link Health Monitor.
    fortios_system_link_monitor:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_link_monitor:
        addr_mode: "ipv4"
        class_id: "4 (source firewall.traffic-class.class-id)"
        diffservcode: "<your_own_value>"
        failtime: "6"
```

(continues on next page)

(continued from previous page)

```
        gateway_ip: "<your_own_value>"
        gateway_ip6: "<your_own_value>"
        ha_priority: "9"
        http_agent: "<your_own_value>"
        http_get: "<your_own_value>"
        http_match: "<your_own_value>"
        interval: "13"
        name: "default_name_14"
        packet_size: "15"
        password: "<your_own_value>"
        port: "17"
        probe_count: "18"
        probe_timeout: "19"
        protocol: "ping"
        recoverytime: "21"
        route:
         -
            subnet: "<your_own_value>"
        security_mode: "none"
        server:
         -
            address: "<your_own_value>"
        service_detection: "enable"
        source_ip: "84.230.14.43"
        source_ip6: "<your_own_value>"
        srcintf: "<your_own_value> (source system.interface.name)"
        status: "enable"
        update_cascade_interface: "enable"
        update_static_route: "enable"
```

6.384.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.384.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.384.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.385 fortios_system_lldp_network_policy – Configure LLDP network policy in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.385.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_lldp feature and network_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.385.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.385.3 FortiOS Version Compatibility

6.385.4 Parameters

6.385.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.385.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure LLDP network policy.
    fortios_system_lldp_network_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_lldp_network_policy:
        comment: "Comment."
        guest:
            dscp: "5"
            priority: "6"
            status: "disable"
            tag: "none"
            vlan: "9"
        guest_voice_signaling:
            dscp: "11"
            priority: "12"
            status: "disable"
            tag: "none"
            vlan: "15"
        name: "default_name_16"
        softphone:
            dscp: "18"
            priority: "19"
            status: "disable"
            tag: "none"
            vlan: "22"
        streaming_video:
            dscp: "24"
            priority: "25"
            status: "disable"
            tag: "none"
            vlan: "28"
        video_conferencing:
            dscp: "30"
            priority: "31"
            status: "disable"
            tag: "none"
            vlan: "34"
        video_signaling:
            dscp: "36"
            priority: "37"
            status: "disable"
            tag: "none"
            vlan: "40"
        voice:
```

(continues on next page)

(continued from previous page)

```
            dscp: "42"
            priority: "43"
            status: "disable"
            tag: "none"
            vlan: "46"
        voice_signaling:
            dscp: "48"
            priority: "49"
            status: "disable"
            tag: "none"
            vlan: "52"
```

6.385.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.385.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.385.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.386 fortios_system_lte_modem – Configure USB LTE/WIMAX devices in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.386.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and lte_modem category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.386.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.386.3 FortiOS Version Compatibility

6.386.4 Parameters

6.386.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.386.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure USB LTE/WIMAX devices.
    fortios_system_lte_modem:
      vdom:  "{{ vdom }}"
      system_lte_modem:
        apn: "<your_own_value>"
        authtype: "none"
```

(continues on next page)

(continued from previous page)

```
        extra_init: "<your_own_value>"
        holddown_timer: "6"
        interface: "<your_own_value> (source system.interface.name)"
        mode: "standalone"
        modem_port: "9"
        passwd: "<your_own_value>"
        status: "enable"
        username: "<your_own_value>"
```

6.386.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.386.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.386.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.387 fortios_system_mac_address_table – Configure MAC address tables in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.387.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and mac_address_table category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.387.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.387.3 FortiOS Version Compatibility

6.387.4 Parameters

6.387.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.387.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure MAC address tables.
    fortios_system_mac_address_table:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_mac_address_table:
        interface: "<your_own_value> (source system.interface.name)"
        mac: "<your_own_value>"
        reply_substitute: "<your_own_value>"
```

6.387.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.387.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.387.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.388 fortios_system_management_tunnel – Management tunnel configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.388.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and management_tunnel category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.388.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.388.3 FortiOS Version Compatibility

6.388.4 Parameters

6.388.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.388.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Management tunnel configuration.
    fortios_system_management_tunnel:
      vdom:  "{{ vdom }}"
      system_management_tunnel:
        allow_collect_statistics: "enable"
        allow_config_restore: "enable"
        allow_push_configuration: "enable"
        allow_push_firmware: "enable"
        authorized_manager_only: "enable"
        serial_number: "<your_own_value>"
        status: "enable"
```

6.388.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.388.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.388.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.389 fortios_system_mem_mgr – Configure memory manager in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.389.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and mem_mgr category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.389.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.389.3 FortiOS Version Compatibility

6.389.4 Parameters

6.389.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.389.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure memory manager.
    fortios_system_mem_mgr:
      vdom:  "{{ vdom }}"
      system_mem_mgr:
        mass_mmsd: "3"
```

6.389.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.389.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.389.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.390 fortios_system_mobile_tunnel – Configure Mobile tunnels, an implementation of Network Mobility (NEMO) extensions for Mobile IPv4 RFC5177 in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.390.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and mobile_tunnel category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.390.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.390.3 FortiOS Version Compatibility

6.390.4 Parameters

6.390.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.390.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Mobile tunnels, an implementation of Network Mobility (NEMO)␣
↪extensions for Mobile IPv4 RFC5177.
    fortios_system_mobile_tunnel:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_mobile_tunnel:
        hash_algorithm: "hmac-md5"
        home_address: "<your_own_value>"
        home_agent: "<your_own_value>"
        lifetime: "6"
        n_mhae_key: "<your_own_value>"
        n_mhae_key_type: "ascii"
        n_mhae_spi: "9"
        name: "default_name_10"
        network:
         -
            id:  "12"
            interface: "<your_own_value> (source system.interface.name)"
            prefix: "<your_own_value>"
        reg_interval: "15"
        reg_retry: "16"
        renew_interval: "17"
        roaming_interface: "<your_own_value> (source system.interface.name)"
        status: "disable"
        tunnel_mode: "gre"
```

6.390.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.390.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.390.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.391 fortios_system_modem – Configure MODEM in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.391.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and modem category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.391.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.391.3 FortiOS Version Compatibility

6.391.4 Parameters

6.391.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.391.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure MODEM.
    fortios_system_modem:
      vdom:  "{{ vdom }}"
      system_modem:
        action: "dial"
        altmode: "enable"
        authtype1: "pap"
        authtype2: "pap"
        authtype3: "pap"
        auto_dial: "enable"
        connect_timeout: "9"
        dial_cmd1: "<your_own_value>"
        dial_cmd2: "<your_own_value>"
        dial_cmd3: "<your_own_value>"
        dial_on_demand: "enable"
        distance: "14"
        dont_send_CR1: "enable"
        dont_send_CR2: "enable"
        dont_send_CR3: "enable"
        extra_init1: "<your_own_value>"
        extra_init2: "<your_own_value>"
        extra_init3: "<your_own_value>"
        holddown_timer: "21"
        idle_timer: "22"
        interface: "<your_own_value> (source system.interface.name)"
        lockdown_lac: "<your_own_value>"
        mode: "standalone"
        network_init: "<your_own_value>"
        passwd1: "<your_own_value>"
        passwd2: "<your_own_value>"
        passwd3: "<your_own_value>"
        peer_modem1: "generic"
        peer_modem2: "generic"
        peer_modem3: "generic"
        phone1: "<your_own_value>"
        phone2: "<your_own_value>"
        phone3: "<your_own_value>"
        pin_init: "<your_own_value>"
        ppp_echo_request1: "enable"
        ppp_echo_request2: "enable"
        ppp_echo_request3: "enable"
```

(continues on next page)

(continued from previous page)

```
        priority: "40"
        redial: "none"
        reset: "42"
        status: "enable"
        traffic_check: "enable"
        username1: "<your_own_value>"
        username2: "<your_own_value>"
        username3: "<your_own_value>"
        wireless_port: "48"
```

6.391.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.391.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.391.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.392 fortios_system_nat64 – Configure NAT64 in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.392.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and nat64 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.392.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.392.3 FortiOS Version Compatibility

6.392.4 Parameters

6.392.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.392.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure NAT64.
    fortios_system_nat64:
      vdom:  "{{ vdom }}"
      system_nat64:
        always_synthesize_aaaa_record: "enable"
        generate_ipv6_fragment_header: "enable"
        nat46_force_ipv4_packet_forwarding: "enable"
        nat64_prefix: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        secondary_prefix:
         -
            name: "default_name_8"
            nat64_prefix: "<your_own_value>"
        secondary_prefix_status: "enable"
        status: "enable"
```

6.392.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.392.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.392.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.393 fortios_system_nd_proxy – Configure IPv6 neighbor discovery proxy (RFC4389) in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.393.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and nd_proxy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.393.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.393.3 FortiOS Version Compatibility

6.393.4 Parameters

6.393.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.393.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 neighbor discovery proxy (RFC4389).
    fortios_system_nd_proxy:
      vdom:  "{{ vdom }}"
      system_nd_proxy:
        member:
         -
            interface_name: "<your_own_value> (source system.interface.name)"
        status: "enable"
```

6.393.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.393.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.393.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.394 fortios_system_netflow – Configure NetFlow in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.394.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and netflow category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.394.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.394.3 FortiOS Version Compatibility

6.394.4 Parameters

6.394.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.394.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure NetFlow.
    fortios_system_netflow:
      vdom:  "{{ vdom }}"
      system_netflow:
        active_flow_timeout: "3"
        collector_ip: "<your_own_value>"
        collector_port: "5"
        inactive_flow_timeout: "6"
        source_ip: "84.230.14.43"
        template_tx_counter: "8"
        template_tx_timeout: "9"
```

6.394.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.394.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.394.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.395 fortios_system_network_visibility – Configure network visibility settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.395.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and network_visibility category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.395.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.395.3 FortiOS Version Compatibility

6.395.4 Parameters

6.395.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.395.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure network visibility settings.
    fortios_system_network_visibility:
      vdom:  "{{ vdom }}"
      system_network_visibility:
        destination_hostname_visibility: "disable"
        destination_location: "disable"
        destination_visibility: "disable"
        hostname_limit: "6"
        hostname_ttl: "7"
        source_location: "disable"
```

6.395.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.395.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.395.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.396 fortios_system_np6 – Configure NP6 attributes in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.396.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and np6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.396.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.396.3 FortiOS Version Compatibility

6.396.4 Parameters

6.396.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.396.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure NP6 attributes.
    fortios_system_np6:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_np6:
        fastpath: "disable"
        fp_anomaly:
            icmp_csum_err: "drop"
            icmp_frag: "allow"
            icmp_land: "allow"
            ipv4_csum_err: "drop"
            ipv4_land: "allow"
            ipv4_optlsrr: "allow"
            ipv4_optrr: "allow"
            ipv4_optsecurity: "allow"
            ipv4_optssrr: "allow"
            ipv4_optstream: "allow"
            ipv4_opttimestamp: "allow"
            ipv4_proto_err: "allow"
            ipv4_unknopt: "allow"
            ipv6_daddr_err: "allow"
            ipv6_land: "allow"
            ipv6_optendpid: "allow"
            ipv6_opthomeaddr: "allow"
            ipv6_optinvld: "allow"
            ipv6_optjumbo: "allow"
            ipv6_optnsap: "allow"
            ipv6_optralert: "allow"
            ipv6_opttunnel: "allow"
            ipv6_proto_err: "allow"
            ipv6_saddr_err: "allow"
            ipv6_unknopt: "allow"
            tcp_csum_err: "drop"
            tcp_fin_noack: "allow"
            tcp_fin_only: "allow"
            tcp_land: "allow"
            tcp_no_flag: "allow"
            tcp_syn_data: "allow"
            tcp_syn_fin: "allow"
            tcp_winnuke: "allow"
            udp_csum_err: "drop"
```

(continues on next page)

(continued from previous page)

```
        udp_land: "allow"
    garbage_session_collector: "disable"
    hpe:
        arp_max: "42"
        enable_shaper: "disable"
        esp_max: "44"
        icmp_max: "45"
        ip_frag_max: "46"
        ip_others_max: "47"
        l2_others_max: "48"
        pri_type_max: "49"
        sctp_max: "50"
        tcp_max: "51"
        tcpfin_rst_max: "52"
        tcpsyn_ack_max: "53"
        tcpsyn_max: "54"
        udp_max: "55"
    ipsec_ob_hash_function: "global-hash"
    ipsec_outbound_hash: "disable"
    low_latency_mode: "disable"
    name: "default_name_59"
    per_session_accounting: "disable"
    session_collector_interval: "61"
    session_timeout_fixed: "disable"
    session_timeout_interval: "63"
    session_timeout_random_range: "64"
```

6.396.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.396.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.396.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.397 fortios_system_npu – Configure NPU attributes in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.397.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and npu category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.397.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.397.3 FortiOS Version Compatibility

6.397.4 Parameters

6.397.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.397.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure NPU attributes.
    fortios_system_npu:
      vdom:  "{{ vdom }}"
      system_npu:
        capwap_offload: "enable"
        dedicated_management_cpu: "enable"
        fastpath: "disable"
        gtp_enhanced_cpu_range: "0"
        gtp_enhanced_mode: "enable"
        intf_shaping_offload: "enable"
        ipsec_dec_subengine_mask: "<your_own_value>"
        ipsec_enc_subengine_mask: "<your_own_value>"
        ipsec_inbound_cache: "enable"
        ipsec_mtu_override: "disable"
        ipsec_over_vlink: "enable"
        isf_np_queues:
            cos0: "<your_own_value> (source system.isf-queue-profile.name)"
            cos1: "<your_own_value> (source system.isf-queue-profile.name)"
            cos2: "<your_own_value> (source system.isf-queue-profile.name)"
            cos3: "<your_own_value> (source system.isf-queue-profile.name)"
            cos4: "<your_own_value> (source system.isf-queue-profile.name)"
            cos5: "<your_own_value> (source system.isf-queue-profile.name)"
            cos6: "<your_own_value> (source system.isf-queue-profile.name)"
            cos7: "<your_own_value> (source system.isf-queue-profile.name)"
        lag_out_port_select: "disable"
        mcast_session_accounting: "tpe-based"
        port_cpu_map:
         -
            cpu_core: "<your_own_value>"
            interface: "<your_own_value>"
        port_npu_map:
         -
            interface: "<your_own_value>"
            npu_group_index: "30"
        priority_protocol:
            bfd: "enable"
            bgp: "enable"
            slbc: "enable"
        qos_mode: "disable"
        rdp_offload: "enable"
        session_denied_offload: "disable"
        sse_backpressure: "enable"
        strip_clear_text_padding: "enable"
        strip_esp_padding: "enable"
        sw_np_bandwidth: "0G"
        uesp_offload: "enable"
```

6.397.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.397.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.397.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.398 fortios_system_ntp – Configure system NTP information in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.398.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and ntp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.398.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.398.3 FortiOS Version Compatibility

6.398.4 Parameters

6.398.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.398.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure system NTP information.
    fortios_system_ntp:
      vdom:  "{{ vdom }}"
      system_ntp:
        authentication: "enable"
        interface:
         -
            interface_name: "<your_own_value> (source system.interface.name)"
        key: "<your_own_value>"
        key_id: "7"
        key_type: "MD5"
        ntpserver:
         -
            authentication: "enable"
            id:  "11"
            interface: "<your_own_value> (source system.interface.name)"
            interface_select_method: "auto"
            key: "<your_own_value>"
            key_id: "15"
            ntpv3: "enable"
            server: "192.168.100.40"
        ntpsync: "enable"
        server_mode: "enable"
        source_ip: "84.230.14.43"
        source_ip6: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        syncinterval: "22"
        type: "fortiguard"
```

6.398.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.398.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.398.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.399 fortios_system_object_tagging – Configure object tagging in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.399.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and object_tagging category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.399.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.399.3 FortiOS Version Compatibility

6.399.4 Parameters

6.399.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.399.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure object tagging.
    fortios_system_object_tagging:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_object_tagging:
        address: "disable"
        category: "<your_own_value>"
        color: "5"
        device: "disable"
        interface: "disable"
        multiple: "enable"
        tags:
         -
            name: "default_name_10"
```

6.399.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.399.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.399.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.400 fortios_system_password_policy – Configure password policy for locally defined administrator passwords and IPsec VPN pre-shared keys in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.400.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and password_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.400.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.400.3 FortiOS Version Compatibility

6.400.4 Parameters

6.400.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.400.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure password policy for locally defined administrator passwords and␣
↪IPsec VPN pre-shared keys.
    fortios_system_password_policy:
      vdom:  "{{ vdom }}"
      system_password_policy:
        apply_to: "admin-password"
        change_4_characters: "enable"
        expire_day: "5"
        expire_status: "enable"
        min_change_characters: "7"
        min_lower_case_letter: "8"
        min_non_alphanumeric: "9"
        min_number: "10"
        min_upper_case_letter: "11"
        minimum_length: "12"
        reuse_password: "enable"
        status: "enable"
```

6.400.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.400.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.400.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.401 fortios_system_password_policy_guest_admin – Configure the password policy for guest administrators in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.401.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and password_policy_guest_admin category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.401.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.401.3 FortiOS Version Compatibility

6.401.4 Parameters

6.401.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.401.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure the password policy for guest administrators.
    fortios_system_password_policy_guest_admin:
      vdom:  "{{ vdom }}"
      system_password_policy_guest_admin:
        apply_to: "guest-admin-password"
        change_4_characters: "enable"
        expire_day: "5"
        expire_status: "enable"
        min_change_characters: "7"
        min_lower_case_letter: "8"
        min_non_alphanumeric: "9"
        min_number: "10"
        min_upper_case_letter: "11"
        minimum_length: "12"
        reuse_password: "enable"
        status: "enable"
```

6.401.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.401.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.401.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.402 fortios_system_performance_top – Display information about the top CPU processes in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.402.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_performance feature and top category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.402.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.402.3 FortiOS Version Compatibility

6.402.4 Parameters

6.402.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.402.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Display information about the top CPU processes.
    fortios_system_performance_top:
      vdom:  "{{ vdom }}"
      system_performance_top:
        <delay>: "<your_own_value>"
```

6.402.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.402.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.402.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.403 fortios_system_physical_switch – Configure physical switches in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.403.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and physical_switch category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.403.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.403.3 FortiOS Version Compatibility

6.403.4 Parameters

6.403.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.403.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure physical switches.
    fortios_system_physical_switch:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_physical_switch:
        age_enable: "enable"
        age_val: "4"
        name: "default_name_5"
        port:
         -
            name: "default_name_7"
            speed: "auto"
            status: "up"
```

6.403.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.403.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.403.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.404 fortios_system_pppoe_interface – Configure the PPPoE interfaces in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.404.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and pppoe_interface category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.404.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.404.3 FortiOS Version Compatibility

6.404.4 Parameters

6.404.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.404.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure the PPPoE interfaces.
    fortios_system_pppoe_interface:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_pppoe_interface:
        ac_name: "<your_own_value>"
        auth_type: "auto"
        device: "<your_own_value> (source system.interface.name)"
        dial_on_demand: "enable"
        disc_retry_timeout: "7"
        idle_timeout: "8"
        ipunnumbered: "<your_own_value>"
        ipv6: "enable"
        lcp_echo_interval: "11"
        lcp_max_echo_fails: "12"
        name: "default_name_13"
        padt_retry_timeout: "14"
        password: "<your_own_value>"
        pppoe_unnumbered_negotiate: "enable"
        service_name: "<your_own_value>"
        username: "<your_own_value>"
```

6.404.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.404.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.404.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.405 fortios_system_probe_response – Configure system probe response in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.405.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and probe_response category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.405.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.405.3 FortiOS Version Compatibility

6.405.4 Parameters

6.405.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.405.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure system probe response.
    fortios_system_probe_response:
      vdom:  "{{ vdom }}"
      system_probe_response:
        http_probe_value: "<your_own_value>"
        mode: "none"
        password: "<your_own_value>"
        port: "6"
        security_mode: "none"
        timeout: "8"
        ttl_mode: "reinit"
```

6.405.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.405.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.405.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.406 fortios_system_proxy_arp – Configure proxy-ARP in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.406.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and proxy_arp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.406.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.406.3 FortiOS Version Compatibility

6.406.4 Parameters

6.406.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.406.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure proxy-ARP.
    fortios_system_proxy_arp:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_proxy_arp:
        end_ip: "<your_own_value>"
        id:  "4"
        interface: "<your_own_value> (source system.interface.name)"
        ip: "<your_own_value>"
```

6.406.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.406.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.406.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.407 fortios_system_ptp – Configure system PTP information in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.407.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and ptp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.407.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.407.3 FortiOS Version Compatibility

6.407.4 Parameters

6.407.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.407.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure system PTP information.
  fortios_system_ptp:
    vdom:  "{{ vdom }}"
    system_ptp:
      delay_mechanism: "E2E"
      interface: "<your_own_value> (source system.interface.name)"
      mode: "multicast"
      request_interval: "6"
      status: "enable"
```

6.407.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.407.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.407.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.408 fortios_system_replacemsg_admin – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.408.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and admin category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.408.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.408.3 FortiOS Version Compatibility

6.408.4 Parameters

6.408.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.408.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_admin:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_admin:
```

(continues on next page)

(continued from previous page)

```
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

6.408.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.408.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.408.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.409 fortios_system_replacemsg_alertmail – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.409.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and alertmail category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.409.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.409.3 FortiOS Version Compatibility

6.409.4 Parameters

6.409.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.409.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_alertmail:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_alertmail:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

6.409.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.409.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.409.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.410 fortios_system_replacemsg_auth – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.410.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and auth category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.410.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.410.3 FortiOS Version Compatibility

6.410.4 Parameters

6.410.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.410.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_auth:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_auth:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

6.410.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.410.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.410.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.411 fortios_system_replacemsg_automation – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.411.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and automation category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.411.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.411.3 FortiOS Version Compatibility

6.411.4 Parameters

6.411.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.411.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_automation:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_automation:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

6.411.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.411.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.411.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.412 fortios_system_replacemsg_device_detection_portal – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.412.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and device_detection_portal category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.412.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.412.3 FortiOS Version Compatibility

6.412.4 Parameters

6.412.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.412.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_device_detection_portal:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_device_detection_portal:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

6.412.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.412.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.412.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.413 fortios_system_replacemsg_ec – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.413.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and ec category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.413.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.413.3 FortiOS Version Compatibility

6.413.4 Parameters

6.413.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.413.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_ec:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_ec:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

6.413.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.413.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.413.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.414 fortios_system_replacemsg_fortiguard_wf – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.414.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and fortiguard_wf category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.414.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.414.3 FortiOS Version Compatibility

6.414.4 Parameters

6.414.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.414.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Replacement messages.
  fortios_system_replacemsg_fortiguard_wf:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    system_replacemsg_fortiguard_wf:
      buffer: "<your_own_value>"
      format: "none"
      header: "none"
      msg_type: "<your_own_value>"
```

6.414.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.414.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.414.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.415 fortios_system_replacemsg_ftp – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.415.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and ftp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.415.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.415.3 FortiOS Version Compatibility

6.415.4 Parameters

6.415.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.415.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_ftp:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
    system_replacemsg_ftp:
      buffer: "<your_own_value>"
      format: "none"
      header: "none"
      msg_type: "<your_own_value>"
```

6.415.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.415.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.415.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.416 fortios_system_replacemsg_group – Configure replacement message groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.416.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and replacemsg_group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.416.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.416.3 FortiOS Version Compatibility

6.416.4 Parameters

6.416.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.416.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure replacement message groups.
    fortios_system_replacemsg_group:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_group:
        admin:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        alertmail:
```

(continues on next page)

(continued from previous page)

```
        -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        auth:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        automation:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        comment: "Comment."
        custom_message:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        device_detection_portal:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        ec:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        fortiguard_wf:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        ftp:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        group_type: "default"
        http:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        icap:
         -
```

(continues on next page)

(continued from previous page)

```
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        mail:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        mm1:
         -
            add_smil: "enable"
            charset: "utf-8"
            class: "not-included"
            format: "none"
            from: "<your_own_value>"
            from_sender: "enable"
            header: "none"
            image: "<your_own_value> (source system.replacemsg-image.name)"
            message: "<your_own_value>"
            msg_type: "<your_own_value>"
            priority: "not-included"
            rsp_status: "ok"
            rsp_text: "<your_own_value>"
            sender_visibility: "not-specified"
            smil_part: "<your_own_value>"
            subject: "<your_own_value>"
        mm3:
         -
            add_html: "enable"
            charset: "utf-8"
            format: "none"
            from: "<your_own_value>"
            from_sender: "enable"
            header: "none"
            html_part: "<your_own_value>"
            image: "<your_own_value> (source system.replacemsg-image.name)"
            message: "<your_own_value>"
            msg_type: "<your_own_value>"
            priority: "not-included"
            subject: "<your_own_value>"
        mm4:
         -
            add_smil: "enable"
            charset: "utf-8"
            class: "not-included"
            domain: "<your_own_value>"
            format: "none"
            from: "<your_own_value>"
            from_sender: "enable"
            header: "none"
            image: "<your_own_value> (source system.replacemsg-image.name)"
            message: "<your_own_value>"
            msg_type: "<your_own_value>"
            priority: "not-included"
            rsp_status: "ok"
```

(continues on next page)

(continued from previous page)

```
            smil_part: "<your_own_value>"
            subject: "<your_own_value>"
        mm7:
         -
            add_smil: "enable"
            addr_type: "rfc2822-addr"
            allow_content_adaptation: "enable"
            charset: "utf-8"
            class: "not-included"
            format: "none"
            from: "<your_own_value>"
            from_sender: "enable"
            header: "none"
            image: "<your_own_value> (source system.replacemsg-image.name)"
            message: "<your_own_value>"
            msg_type: "<your_own_value>"
            priority: "not-included"
            rsp_status: "success"
            smil_part: "<your_own_value>"
            subject: "<your_own_value>"
        mms:
         -
            buffer: "<your_own_value>"
            charset: "utf-8"
            format: "none"
            header: "none"
            image: "<your_own_value> (source system.replacemsg-image.name)"
            msg_type: "<your_own_value>"
        nac_quar:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        name: "default_name_140"
        nntp:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        spam:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        sslvpn:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        traffic_quota:
         -
            buffer: "<your_own_value>"
            format: "none"
```

(continues on next page)

(continued from previous page)

```
            header: "none"
            msg_type: "<your_own_value>"
        utm:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        webproxy:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
```

6.416.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.416.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.416.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.417 fortios_system_replacemsg_http – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.417.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and http category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.417.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.417.3 FortiOS Version Compatibility

6.417.4 Parameters

6.417.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.417.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_http:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    state: "present"
    access_token: "<your_own_value>"
    system_replacemsg_http:
      buffer: "<your_own_value>"
      format: "none"
      header: "none"
      msg_type: "<your_own_value>"
```

6.417.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.417.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.417.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.418 fortios_system_replacemsg_icap – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.418.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and icap category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.418.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.418.3 FortiOS Version Compatibility

6.418.4 Parameters

6.418.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.418.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_icap:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_icap:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

6.418.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.418.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.418.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.419 fortios_system_replacemsg_image – Configure replacement message images in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.419.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and replacemsg_image category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.419.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.419.3 FortiOS Version Compatibility

6.419.4 Parameters

6.419.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.419.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure replacement message images.
    fortios_system_replacemsg_image:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_image:
        image_base64: "<your_own_value>"
        image_type: "gif"
        name: "default_name_5"
```

6.419.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.419.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.419.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.420 fortios_system_replacemsg_mail – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.420.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and mail category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.420.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.420.3 FortiOS Version Compatibility

6.420.4 Parameters

6.420.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.420.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_mail:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_mail:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

6.420.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.420.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.420.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.421 fortios_system_replacemsg_mm1 – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.421.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and mm1 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.421.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.421.3 FortiOS Version Compatibility

6.421.4 Parameters

6.421.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.421.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_mm1:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_mm1:
        add_smil: "enable"
        charset: "utf-8"
        class: "not-included"
        format: "none"
        from: "<your_own_value>"
        from_sender: "enable"
        header: "none"
        image: "<your_own_value> (source system.replacemsg-image.name)"
        message: "<your_own_value>"
        msg_type: "<your_own_value>"
        priority: "not-included"
        rsp_status: "ok"
        rsp_text: "<your_own_value>"
        sender_visibility: "not-specified"
        smil_part: "<your_own_value>"
        subject: "<your_own_value>"
```

6.421.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.421.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.421.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.422 fortios_system_replacemsg_mm3 – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.422.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and mm3 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.422.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.422.3 FortiOS Version Compatibility

6.422.4 Parameters

6.422.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.422.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_mm3:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_mm3:
        add_html: "enable"
        charset: "utf-8"
        format: "none"
        from: "<your_own_value>"
        from_sender: "enable"
        header: "none"
        html_part: "<your_own_value>"
        image: "<your_own_value> (source system.replacemsg-image.name)"
        message: "<your_own_value>"
        msg_type: "<your_own_value>"
        priority: "not-included"
        subject: "<your_own_value>"
```

6.422.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.422.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.422.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.423 fortios_system_replacemsg_mm4 – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.423.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and mm4 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.423.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.423.3 FortiOS Version Compatibility

6.423.4 Parameters

6.423.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.423.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_mm4:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_mm4:
        add_smil: "enable"
        charset: "utf-8"
        class: "not-included"
        domain: "<your_own_value>"
        format: "none"
        from: "<your_own_value>"
        from_sender: "enable"
        header: "none"
        image: "<your_own_value> (source system.replacemsg-image.name)"
        message: "<your_own_value>"
        msg_type: "<your_own_value>"
        priority: "not-included"
        rsp_status: "ok"
        smil_part: "<your_own_value>"
        subject: "<your_own_value>"
```

6.423.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.423.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.423.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.424 fortios_system_replacemsg_mm7 – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.424.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and mm7 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.424.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.424.3 FortiOS Version Compatibility

6.424.4 Parameters

6.424.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.424.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_mm7:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_mm7:
        add_smil: "enable"
        addr_type: "rfc2822-addr"
        allow_content_adaptation: "enable"
        charset: "utf-8"
        class: "not-included"
        format: "none"
        from: "<your_own_value>"
        from_sender: "enable"
        header: "none"
        image: "<your_own_value> (source system.replacemsg-image.name)"
        message: "<your_own_value>"
        msg_type: "<your_own_value>"
        priority: "not-included"
        rsp_status: "success"
        smil_part: "<your_own_value>"
        subject: "<your_own_value>"
```

6.424.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.424.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.424.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.425 fortios_system_replacemsg_mms – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.425.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and mms category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.425.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.425.3 FortiOS Version Compatibility

6.425.4 Parameters

6.425.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.425.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_mms:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_mms:
        buffer: "<your_own_value>"
        charset: "utf-8"
        format: "none"
        header: "none"
        image: "<your_own_value> (source system.replacemsg-image.name)"
        msg_type: "<your_own_value>"
```

6.425.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.425.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.425.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.426 fortios_system_replacemsg_nac_quar – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.426.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and nac_quar category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.426.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.426.3 FortiOS Version Compatibility

6.426.4 Parameters

6.426.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.426.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_nac_quar:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_nac_quar:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

6.426.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.426.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.426.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.427 fortios_system_replacemsg_nntp – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.427.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and nntp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.427.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.427.3 FortiOS Version Compatibility

6.427.4 Parameters

6.427.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.427.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
 tasks:
 - name: Replacement messages.
   fortios_system_replacemsg_nntp:
     vdom:  "{{ vdom }}"
     state: "present"
     access_token: "<your_own_value>"
     system_replacemsg_nntp:
       buffer: "<your_own_value>"
       format: "none"
       header: "none"
       msg_type: "<your_own_value>"
```

6.427.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.427.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.427.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.428 fortios_system_replacemsg_spam – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.428.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and spam category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.428.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.428.3 FortiOS Version Compatibility

6.428.4 Parameters

6.428.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.428.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_spam:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
    system_replacemsg_spam:
      buffer: "<your_own_value>"
      format: "none"
      header: "none"
      msg_type: "<your_own_value>"
```

6.428.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.428.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.428.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.429 fortios_system_replacemsg_sslvpn – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.429.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and sslvpn category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.429.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.429.3 FortiOS Version Compatibility

6.429.4 Parameters

6.429.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.429.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_sslvpn:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_sslvpn:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

6.429.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.429.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.429.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.430 fortios_system_replacemsg_traffic_quota – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.430.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and traffic_quota category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.430.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.430.3 FortiOS Version Compatibility

6.430.4 Parameters

6.430.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.430.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_traffic_quota:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_traffic_quota:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

6.430.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.430.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.430.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.431 fortios_system_replacemsg_utm – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.431.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and utm category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.431.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.431.3 FortiOS Version Compatibility

6.431.4 Parameters

6.431.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.431.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_utm:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_utm:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

6.431.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.431.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.431.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.432 fortios_system_replacemsg_webproxy – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.432.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_replacemsg feature and webproxy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.432.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.432.3 FortiOS Version Compatibility

6.432.4 Parameters

6.432.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.432.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Replacement messages.
    fortios_system_replacemsg_webproxy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_webproxy:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

6.432.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.432.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.432.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.433 fortios_system_resource_limits – Configure resource limits in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.433.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and resource_limits category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.433.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.433.3 FortiOS Version Compatibility

6.433.4 Parameters

6.433.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.433.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure resource limits.
    fortios_system_resource_limits:
      vdom:  "{{ vdom }}"
      system_resource_limits:
        custom_service: "3"
        dialup_tunnel: "4"
        firewall_address: "5"
        firewall_addrgrp: "6"
        firewall_policy: "7"
        ipsec_phase1: "8"
        ipsec_phase1_interface: "9"
        ipsec_phase2: "10"
        ipsec_phase2_interface: "11"
        log_disk_quota: "12"
        onetime_schedule: "13"
        proxy: "14"
        recurring_schedule: "15"
        service_group: "16"
        session: "17"
        sslvpn: "18"
        user: "19"
        user_group: "20"
```

6.433.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.433.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.433.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.434 fortios_system_saml – Global settings for SAML authentication in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.434.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and saml category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.434.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.434.3 FortiOS Version Compatibility

6.434.4 Parameters

6.434.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.434.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Global settings for SAML authentication.
    fortios_system_saml:
      vdom:  "{{ vdom }}"
      system_saml:
        artifact_resolution_url: "<your_own_value>"
        binding_protocol: "post"
        cert: "<your_own_value> (source certificate.local.name)"
        default_login_page: "normal"
        default_profile: "<your_own_value> (source system.accprofile.name)"
        entity_id: "<your_own_value>"
        idp_artifact_resolution_url: "<your_own_value>"
        idp_cert: "<your_own_value> (source certificate.remote.name)"
        idp_entity_id: "<your_own_value>"
        idp_single_logout_url: "<your_own_value>"
        idp_single_sign_on_url: "<your_own_value>"
        life: "14"
        portal_url: "<your_own_value>"
        role: "identity-provider"
        server_address: "<your_own_value>"
        service_providers:
         -
            assertion_attributes:
             -
                name: "default_name_20"
                type: "username"
            idp_artifact_resolution_url: "<your_own_value>"
            idp_entity_id: "<your_own_value>"
            idp_single_logout_url: "<your_own_value>"
            idp_single_sign_on_url: "<your_own_value>"
            name: "default_name_26"
            prefix: "<your_own_value>"
            sp_artifact_resolution_url: "<your_own_value>"
            sp_binding_protocol: "post"
            sp_cert: "<your_own_value> (source certificate.remote.name)"
            sp_entity_id: "<your_own_value>"
            sp_portal_url: "<your_own_value>"
            sp_single_logout_url: "<your_own_value>"
            sp_single_sign_on_url: "<your_own_value>"
        single_logout_url: "<your_own_value>"
        single_sign_on_url: "<your_own_value>"
        status: "enable"
        tolerance: "38"
```

6.434.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.434.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.434.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.435 fortios_system_sdn_connector – Configure connection to SDN Connector in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.435.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and sdn_connector category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.435.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.435.3 FortiOS Version Compatibility

6.435.4 Parameters

6.435.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.435.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure connection to SDN Connector.
    fortios_system_sdn_connector:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_sdn_connector:
        access_key: "<your_own_value>"
        api_key: "<your_own_value>"
        azure_region: "global"
        client_id: "<your_own_value>"
        client_secret: "<your_own_value>"
        compartment_id: "<your_own_value>"
        compute_generation: "9"
        domain: "<your_own_value>"
        external_ip:
         -
            name: "default_name_12"
        gcp_project: "<your_own_value>"
        group_name: "<your_own_value>"
        ha_status: "disable"
        ibm_region: "us-south"
        ibm_region_gen1: "us-south"
        ibm_region_gen2: "us-south"
        key_passwd: "<your_own_value>"
        login_endpoint: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        name: "default_name_21"
        nic:
         -
            ip:
             -
                name: "default_name_24"
                public_ip: "<your_own_value>"
                resource_group: "<your_own_value>"
            name: "default_name_27"
        oci_cert: "<your_own_value> (source certificate.local.name)"
        oci_fingerprint: "<your_own_value>"
        oci_region: "phoenix"
        oci_region_type: "commercial"
        password: "<your_own_value>"
        private_key: "<your_own_value>"
        region: "<your_own_value>"
        resource_group: "<your_own_value>"
        resource_url: "<your_own_value>"
        route:
         -
            name: "default_name_38"
        route_table:
         -
            name: "default_name_40"
            resource_group: "<your_own_value>"
            route:
             -
                name: "default_name_43"
                next_hop: "<your_own_value>"
            subscription_id: "<your_own_value>"
        secret_key: "<your_own_value>"
        secret_token: "<your_own_value>"
        server: "192.168.100.40"
        server_list:
         -
            ip: "<your_own_value>"
        server_port: "51"
        service_account: "<your_own_value>"
        status: "disable"
        subscription_id: "<your_own_value>"
        tenant_id: "<your_own_value>"
        type: "aci"
        update_interval: "57"
        use_metadata_iam: "disable"
        user_id: "<your_own_value>"
        username: "<your_own_value>"
        vcenter_password: "<your_own_value>"
        vcenter_server: "<your_own_value>"
        vcenter_username: "<your_own_value>"
        vpc_id: "<your_own_value>"
```

6.435.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.435.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.435.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.436 fortios_system_sdwan – Configure redundant internet connections using SD-WAN (formerly virtual WAN link) in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.436.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and sdwan category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.436.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.436.3 FortiOS Version Compatibility

6.436.4 Parameters

6.436.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.436.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure redundant internet connections using SD-WAN (formerly virtual WAN␣
↪link).
    fortios_system_sdwan:
      vdom:  "{{ vdom }}"
      system_sdwan:
        duplication:
         -
            dstaddr:
             -
                name: "default_name_5 (source firewall.address.name firewall.addrgrp.
↪name)"
            dstaddr6:
             -
                name: "default_name_7 (source firewall.address6.name firewall.
↪addrgrp6.name)"
            dstintf:
             -
                name: "default_name_9 (source system.interface.name system.zone.name␣
↪system.sdwan.zone.name)"
            id:  "10"
            packet_de_duplication: "enable"
            packet_duplication: "disable"
            service:
             -
                name: "default_name_14 (source firewall.service.custom.name firewall.
↪service.group.name)"
```

(continues on next page)

(continued from previous page)

```
            service_id:
             -
                id:  "16 (source system.sdwan.service.id)"
            srcaddr:
             -
                name: "default_name_18 (source firewall.address.name firewall.addrgrp.
↪name)"
            srcaddr6:
             -
                name: "default_name_20 (source firewall.address6.name firewall.
↪addrgrp6.name)"
            srcintf:
             -
                name: "default_name_22 (source system.interface.name system.zone.name␣
↪system.sdwan.zone.name)"
        duplication_max_num: "23"
        fail_alert_interfaces:
         -
            name: "default_name_25 (source system.interface.name)"
        fail_detect: "enable"
        health_check:
         -
            addr_mode: "ipv4"
            detect_mode: "active"
            diffservcode: "<your_own_value>"
            dns_match_ip: "<your_own_value>"
            dns_request_domain: "<your_own_value>"
            failtime: "33"
            ftp_file: "<your_own_value>"
            ftp_mode: "passive"
            ha_priority: "36"
            http_agent: "<your_own_value>"
            http_get: "<your_own_value>"
            http_match: "<your_own_value>"
            interval: "40"
            members:
             -
                seq_num: "42 (source system.sdwan.members.seq-num)"
            name: "default_name_43"
            packet_size: "44"
            password: "<your_own_value>"
            port: "46"
            probe_count: "47"
            probe_packets: "disable"
            probe_timeout: "49"
            protocol: "ping"
            quality_measured_method: "half-open"
            recoverytime: "52"
            security_mode: "none"
            server: "192.168.100.40"
            sla:
             -
                id:  "56"
                jitter_threshold: "57"
                latency_threshold: "58"
                link_cost_factor: "latency"
                packetloss_threshold: "60"
```

(continues on next page)

(continued from previous page)

```
            sla_fail_log_period: "61"
            sla_pass_log_period: "62"
            system_dns: "disable"
            threshold_alert_jitter: "64"
            threshold_alert_latency: "65"
            threshold_alert_packetloss: "66"
            threshold_warning_jitter: "67"
            threshold_warning_latency: "68"
            threshold_warning_packetloss: "69"
            update_cascade_interface: "enable"
            update_static_route: "enable"
            user: "<your_own_value>"
        load_balance_mode: "source-ip-based"
        members:
         -
            comment: "Comments."
            cost: "76"
            gateway: "<your_own_value>"
            gateway6: "<your_own_value>"
            ingress_spillover_threshold: "79"
            interface: "<your_own_value> (source system.interface.name)"
            priority: "81"
            priority6: "82"
            seq_num: "83"
            source: "<your_own_value>"
            source6: "<your_own_value>"
            spillover_threshold: "86"
            status: "disable"
            volume_ratio: "88"
            weight: "89"
            zone: "<your_own_value> (source system.sdwan.zone.name)"
        neighbor:
         -
            health_check: "<your_own_value> (source system.sdwan.health-check.name)"
            ip: "<your_own_value> (source router.bgp.neighbor.ip)"
            member: "94 (source system.sdwan.members.seq-num)"
            role: "standalone"
            sla_id: "96"
        neighbor_hold_boot_time: "97"
        neighbor_hold_down: "enable"
        neighbor_hold_down_time: "99"
        service:
         -
            addr_mode: "ipv4"
            bandwidth_weight: "102"
            default: "enable"
            dscp_forward: "enable"
            dscp_forward_tag: "<your_own_value>"
            dscp_reverse: "enable"
            dscp_reverse_tag: "<your_own_value>"
            dst:
             -
                name: "default_name_109 (source firewall.address.name firewall.
↪addrgrp.name)"
            dst_negate: "enable"
            dst6:
             -
```

(continues on next page)

(continued from previous page)

```
                name: "default_name_112 (source firewall.address6.name firewall.
↪addrgrp6.name)"
            end_port: "113"
            gateway: "enable"
            groups:
             -
                name: "default_name_116 (source user.group.name)"
            hash_mode: "round-robin"
            health_check:
             -
                name: "default_name_119 (source system.sdwan.health-check.name)"
            hold_down_time: "120"
            id:  "121"
            input_device:
             -
                name: "default_name_123 (source system.interface.name)"
            input_device_negate: "enable"
            internet_service: "enable"
            internet_service_app_ctrl:
             -
                id:  "127"
            internet_service_app_ctrl_group:
             -
                name: "default_name_129 (source application.group.name)"
            internet_service_custom:
             -
                name: "default_name_131 (source firewall.internet-service-custom.name)
↪"
            internet_service_custom_group:
             -
                name: "default_name_133 (source firewall.internet-service-custom-
↪group.name)"
            internet_service_group:
             -
                name: "default_name_135 (source firewall.internet-service-group.name)"
            internet_service_name:
             -
                name: "default_name_137 (source firewall.internet-service-name.name)"
            jitter_weight: "138"
            latency_weight: "139"
            link_cost_factor: "latency"
            link_cost_threshold: "141"
            minimum_sla_meet_members: "142"
            mode: "auto"
            name: "default_name_144"
            packet_loss_weight: "145"
            priority_members:
             -
                seq_num: "147 (source system.sdwan.members.seq-num)"
            protocol: "148"
            quality_link: "149"
            role: "standalone"
            route_tag: "151"
            sla:
             -
                health_check: "<your_own_value> (source system.sdwan.health-check.
↪name)"
```

(continues on next page)

(continued from previous page)

```
                id:  "154"
            sla_compare_method: "order"
            src:
             -
                name: "default_name_157 (source firewall.address.name firewall.
↪addrgrp.name)"
            src_negate: "enable"
            src6:
             -
                name: "default_name_160 (source firewall.address6.name firewall.
↪addrgrp6.name)"
            standalone_action: "enable"
            start_port: "162"
            status: "enable"
            tie_break: "zone"
            tos: "<your_own_value>"
            tos_mask: "<your_own_value>"
            use_shortcut_sla: "enable"
            users:
             -
                name: "default_name_169 (source user.local.name)"
        status: "disable"
        zone:
         -
            name: "default_name_172"
            service_sla_tie_break: "cfg-order"
```

6.436.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.436.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.436.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.437 fortios_system_session_helper – Configure session helper in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.437.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and session_helper category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.437.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.437.3 FortiOS Version Compatibility

6.437.4 Parameters

6.437.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.437.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure session helper.
    fortios_system_session_helper:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_session_helper:
        id:  "3"
        name: "default_name_4"
        port: "5"
        protocol: "6"
```

6.437.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.437.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.437.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.438 fortios_system_session_ttl – Configure global session TTL timers for this FortiGate in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.438.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and session_ttl category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.438.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.438.3 FortiOS Version Compatibility

6.438.4 Parameters

6.438.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.438.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure global session TTL timers for this FortiGate.
  fortios_system_session_ttl:
    vdom:  "{{ vdom }}"
    system_session_ttl:
      default: "<your_own_value>"
      port:
       -
          end_port: "5"
          id:  "6"
          protocol: "7"
          start_port: "8"
          timeout: "<your_own_value>"
```

6.438.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.438.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.438.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.439 fortios_system_settings – Configure VDOM settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.439.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.439.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.439.3 FortiOS Version Compatibility

6.439.4 Parameters

6.439.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.439.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure VDOM settings.
    fortios_system_settings:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    system_settings:
      allow_linkdown_path: "enable"
      allow_subnet_overlap: "enable"
      application_bandwidth_tracking: "disable"
      asymroute: "enable"
      asymroute_icmp: "enable"
      asymroute6: "enable"
      asymroute6_icmp: "enable"
      auxiliary_session: "enable"
      bfd: "enable"
      bfd_desired_min_tx: "12"
      bfd_detect_mult: "13"
      bfd_dont_enforce_src_port: "enable"
      bfd_required_min_rx: "15"
      block_land_attack: "disable"
      central_nat: "enable"
      comments: "<your_own_value>"
      compliance_check: "enable"
      consolidated_firewall_mode: "enable"
      default_voip_alg_mode: "proxy-based"
      deny_tcp_with_icmp: "enable"
      device: "<your_own_value> (source system.interface.name)"
      dhcp_proxy: "enable"
      dhcp_proxy_interface: "<your_own_value> (source system.interface.name)"
      dhcp_proxy_interface_select_method: "auto"
      dhcp_server_ip: "<your_own_value>"
      dhcp6_server_ip: "<your_own_value>"
      discovered_device_timeout: "29"
      ecmp_max_paths: "30"
      email_portal_check_dns: "disable"
      firewall_session_dirty: "check-all"
      fw_session_hairpin: "enable"
      gateway: "<your_own_value>"
      gateway6: "<your_own_value>"
      gtp_asym_fgsp: "disable"
      gtp_monitor_mode: "enable"
      gui_advanced_policy: "enable"
      gui_allow_unnamed_policy: "enable"
      gui_antivirus: "enable"
      gui_ap_profile: "enable"
      gui_application_control: "enable"
      gui_default_policy_columns:
        -
          name: "default_name_44"
      gui_dhcp_advanced: "enable"
      gui_dlp: "enable"
      gui_dns_database: "enable"
      gui_dnsfilter: "enable"
      gui_domain_ip_reputation: "enable"
      gui_dos_policy: "enable"
      gui_dynamic_profile_display: "enable"
      gui_dynamic_routing: "enable"
      gui_email_collection: "enable"
      gui_endpoint_control: "enable"
      gui_endpoint_control_advanced: "enable"
      gui_explicit_proxy: "enable"
      gui_file_filter: "enable"
```

(continues on next page)

(continued from previous page)

```
        gui_fortiap_split_tunneling: "enable"
        gui_fortiextender_controller: "enable"
        gui_icap: "enable"
        gui_implicit_policy: "enable"
        gui_ips: "enable"
        gui_load_balance: "enable"
        gui_local_in_policy: "enable"
        gui_local_reports: "enable"
        gui_multicast_policy: "enable"
        gui_multiple_interface_policy: "enable"
        gui_multiple_utm_profiles: "enable"
        gui_nat46_64: "enable"
        gui_object_colors: "enable"
        gui_per_policy_disclaimer: "enable"
        gui_policy_based_ipsec: "enable"
        gui_policy_disclaimer: "enable"
        gui_policy_learning: "enable"
        gui_replacement_message_groups: "enable"
        gui_security_profile_group: "enable"
        gui_spamfilter: "enable"
        gui_sslvpn_personal_bookmarks: "enable"
        gui_sslvpn_realms: "enable"
        gui_switch_controller: "enable"
        gui_threat_weight: "enable"
        gui_traffic_shaping: "enable"
        gui_videofilter: "enable"
        gui_voip_profile: "enable"
        gui_vpn: "enable"
        gui_waf_profile: "enable"
        gui_wan_load_balancing: "enable"
        gui_wanopt_cache: "enable"
        gui_webfilter: "enable"
        gui_webfilter_advanced: "enable"
        gui_wireless_controller: "enable"
        gui_ztna: "enable"
        http_external_dest: "fortiweb"
        ike_dn_format: "with-space"
        ike_port: "95"
        ike_quick_crash_detect: "enable"
        ike_session_resume: "enable"
        implicit_allow_dns: "enable"
        inspection_mode: "proxy"
        ip: "<your_own_value>"
        ip6: "<your_own_value>"
        link_down_access: "enable"
        lldp_reception: "enable"
        lldp_transmission: "enable"
        location_id: "<your_own_value>"
        mac_ttl: "106"
        manageip: "<your_own_value>"
        manageip6: "<your_own_value>"
        multicast_forward: "enable"
        multicast_skip_policy: "enable"
        multicast_ttl_notchange: "enable"
        ngfw_mode: "profile-based"
        opmode: "nat"
        prp_trailer_action: "enable"
```

(continues on next page)

(continued from previous page)

```
        sccp_port: "115"
        sctp_session_without_init: "enable"
        ses_denied_traffic: "enable"
        sip_expectation: "enable"
        sip_helper: "enable"
        sip_nat_trace: "enable"
        sip_ssl_port: "121"
        sip_tcp_port: "122"
        sip_udp_port: "123"
        snat_hairpin_traffic: "enable"
        ssl_ssh_profile: "<your_own_value> (source firewall.ssl-ssh-profile.name)"
        status: "enable"
        strict_src_check: "enable"
        tcp_session_without_syn: "enable"
        utf8_spam_tagging: "enable"
        v4_ecmp_mode: "source-ip-based"
        vpn_stats_log: "ipsec"
        vpn_stats_period: "132"
        wccp_cache_engine: "enable"
```

6.439.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.439.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.439.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.440 fortios_system_sflow – Configure sFlow in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.440.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and sflow category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.440.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.440.3 FortiOS Version Compatibility

6.440.4 Parameters

6.440.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.440.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure sFlow.
  fortios_system_sflow:
    vdom:  "{{ vdom }}"
    system_sflow:
      collector_ip: "<your_own_value>"
      collector_port: "4"
      source_ip: "84.230.14.43"
```

6.440.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.440.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.440.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.441 fortios_system_sit_tunnel – Configure IPv6 tunnel over IPv4 in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.441.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and sit_tunnel category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.441.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.441.3 FortiOS Version Compatibility

6.441.4 Parameters

6.441.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.441.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPv6 tunnel over IPv4.
    fortios_system_sit_tunnel:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_sit_tunnel:
        auto_asic_offload: "enable"
        destination: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        interface: "<your_own_value> (source system.interface.name)"
        ip6: "<your_own_value>"
        name: "default_name_7"
        source: "<your_own_value>"
        use_sdwan: "disable"
```

6.441.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.441.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.441.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.442 fortios_system_smc_ntp – Configure SMC NTP information in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.442.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and smc_ntp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.442.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.442.3 FortiOS Version Compatibility

6.442.4 Parameters

6.442.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.442.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure SMC NTP information.
    fortios_system_smc_ntp:
      vdom:  "{{ vdom }}"
      system_smc_ntp:
        channel: "3"
        ntpserver:
         -
            id:  "5"
            server: "192.168.100.40"
        ntpsync: "enable"
        syncinterval: "8"
```

6.442.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.442.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.442.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.443 fortios_system_sms_server – Configure SMS server for sending SMS messages to support user authentication in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.443.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and sms_server category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.443.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.443.3 FortiOS Version Compatibility

6.443.4 Parameters

6.443.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.443.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure SMS server for sending SMS messages to support user␣
↪authentication.
    fortios_system_sms_server:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_sms_server:
        mail_server: "<your_own_value>"
        name: "default_name_4"
```

6.443.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.443.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.443.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.444 fortios_system_snmp_community – SNMP community configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.444.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_snmp feature and community category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.444.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.444.3 FortiOS Version Compatibility

6.444.4 Parameters

6.444.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.444.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: SNMP community configuration.
    fortios_system_snmp_community:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_snmp_community:
        events: "cpu-high"
        hosts:
         -
            ha_direct: "enable"
            host_type: "any"
            id:  "7"
            ip: "<your_own_value>"
            source_ip: "84.230.14.43"
        hosts6:
         -
            ha_direct: "enable"
            host_type: "any"
            id:  "13"
            ipv6: "<your_own_value>"
            source_ipv6: "<your_own_value>"
        id:  "16"
        name: "default_name_17"
        query_v1_port: "18"
        query_v1_status: "enable"
        query_v2c_port: "20"
        query_v2c_status: "enable"
        status: "enable"
```

(continues on next page)

(continued from previous page)

```
        trap_v1_lport: "23"
        trap_v1_rport: "24"
        trap_v1_status: "enable"
        trap_v2c_lport: "26"
        trap_v2c_rport: "27"
        trap_v2c_status: "enable"
```

6.444.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.444.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.444.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.445 fortios_system_snmp_sysinfo – SNMP system info configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.445.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_snmp feature and sysinfo category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.445.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.445.3 FortiOS Version Compatibility

6.445.4 Parameters

6.445.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.445.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: SNMP system info configuration.
    fortios_system_snmp_sysinfo:
      vdom:  "{{ vdom }}"
      system_snmp_sysinfo:
        contact_info: "<your_own_value>"
        description: "<your_own_value>"
        engine_id: "<your_own_value>"
        location: "<your_own_value>"
        status: "enable"
        trap_high_cpu_threshold: "8"
        trap_log_full_threshold: "9"
        trap_low_memory_threshold: "10"
```

6.445.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.445.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.445.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.446 fortios_system_snmp_user – SNMP user configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.446.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system_snmp feature and user category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.446.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.446.3 FortiOS Version Compatibility

6.446.4 Parameters

6.446.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.446.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: SNMP user configuration.
    fortios_system_snmp_user:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_snmp_user:
        auth_proto: "md5"
        auth_pwd: "<your_own_value>"
        events: "cpu-high"
        ha_direct: "enable"
        name: "default_name_7"
        notify_hosts: "<your_own_value>"
        notify_hosts6: "<your_own_value>"
        priv_proto: "aes"
        priv_pwd: "<your_own_value>"
        queries: "enable"
        query_port: "13"
        security_level: "no-auth-no-priv"
        source_ip: "84.230.14.43"
        source_ipv6: "<your_own_value>"
        status: "enable"
        trap_lport: "18"
        trap_rport: "19"
        trap_status: "enable"
```

6.446.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.446.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.446.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.447 fortios_system_speed_test_schedule – Speed test schedule for each interface in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.447.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and speed_test_schedule category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.447.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.447.3 FortiOS Version Compatibility

6.447.4 Parameters

6.447.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.447.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Speed test schedule for each interface.
    fortios_system_speed_test_schedule:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_speed_test_schedule:
        diffserv: "<your_own_value>"
        interface: "<your_own_value> (source system.interface.name)"
        schedules:
         -
            name: "default_name_6 (source firewall.schedule.recurring.name)"
        server_name: "<your_own_value>"
        status: "disable"
        update_inbandwidth: "disable"
        update_inbandwidth_maximum: "10"
        update_inbandwidth_minimum: "11"
        update_outbandwidth: "disable"
        update_outbandwidth_maximum: "13"
        update_outbandwidth_minimum: "14"
```

6.447.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.447.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.447.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.448 fortios_system_speed_test_server – Configure speed test server list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.448.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and speed_test_server category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.448.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.448.3 FortiOS Version Compatibility

6.448.4 Parameters

6.448.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.448.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure speed test server list.
    fortios_system_speed_test_server:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_speed_test_server:
        host:
         -
            id:  "4"
            ip: "<your_own_value>"
            password: "<your_own_value>"
            port: "7"
            user: "<your_own_value>"
        name: "default_name_9"
        timestamp: "10"
```

6.448.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.448.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.448.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.449 fortios_system_sso_admin – Configure SSO admin users in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.449.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and sso_admin category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.449.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.449.3 FortiOS Version Compatibility

6.449.4 Parameters

6.449.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.449.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure SSO admin users.
    fortios_system_sso_admin:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_sso_admin:
        accprofile: "<your_own_value> (source system.accprofile.name)"
        gui_dashboard:
         -
            columns: "5"
            id:  "6"
            layout_type: "responsive"
            name: "default_name_8"
            permanent: "disable"
            vdom: "<your_own_value> (source system.vdom.name)"
            widget:
             -
                fabric_device: "<your_own_value>"
                fabric_device_widget_name: "<your_own_value>"
                fabric_device_widget_visualization_type: "<your_own_value>"
                fortiview_device: "<your_own_value>"
                fortiview_filters:
                 -
                    id:  "17"
                    key: "<your_own_value>"
                    value: "<your_own_value>"
                fortiview_sort_by: "<your_own_value>"
                fortiview_timeframe: "<your_own_value>"
                fortiview_type: "<your_own_value>"
                fortiview_visualization: "<your_own_value>"
                height: "24"
```

(continues on next page)

(continued from previous page)

```
            id:  "25"
            industry: "default"
            interface: "<your_own_value> (source system.interface.name)"
            region: "default"
            title: "<your_own_value>"
            type: "sysinfo"
            width: "31"
            x_pos: "32"
            y_pos: "33"
        gui_global_menu_favorites:
         -
            id:  "35"
        gui_ignore_release_overview_version: "<your_own_value>"
        gui_new_feature_acknowledge:
         -
            id:  "38"
        gui_vdom_menu_favorites:
         -
            id:  "40"
        name: "default_name_41"
        vdom:
         -
            name: "default_name_43 (source system.vdom.name)"
```

6.449.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.449.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.449.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.450 fortios_system_sso_forticloud_admin – Configure FortiCloud SSO admin users in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.450.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and sso_forticloud_admin category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.450.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.450.3 FortiOS Version Compatibility

6.450.4 Parameters

6.450.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.450.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiCloud SSO admin users.
    fortios_system_sso_forticloud_admin:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_sso_forticloud_admin:
        name: "default_name_3"
        vdom:
         -
            name: "default_name_5 (source system.vdom.name)"
```

6.450.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.450.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.450.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.451 fortios_system_standalone_cluster – Configure FortiGate Session Life Support Protocol (FGSP) cluster attributes in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.451.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and standalone_cluster category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.451.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.451.3 FortiOS Version Compatibility

6.451.4 Parameters

6.451.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.451.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiGate Session Life Support Protocol (FGSP) cluster attributes.
    fortios_system_standalone_cluster:
      vdom:  "{{ vdom }}"
      system_standalone_cluster:
        encryption: "enable"
        group_member_id: "4"
        layer2_connection: "available"
        psksecret: "<your_own_value>"
        session_sync_dev: "<your_own_value> (source system.interface.name)"
        standalone_group_id: "8"
```

6.451.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.451.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.451.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.452 fortios_system_storage – Configure logical storage in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.452.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and storage category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.452.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.452.3 FortiOS Version Compatibility

6.452.4 Parameters

6.452.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.452.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure logical storage.
    fortios_system_storage:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_storage:
        device: "<your_own_value>"
        media_status: "enable"
        name: "default_name_5"
        order: "6"
        partition: "<your_own_value>"
        size: "8"
        status: "enable"
        usage: "log"
        wanopt_mode: "mix"
```

6.452.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.452.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.452.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.453 fortios_system_stp – Configure Spanning Tree Protocol (STP) in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.453.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and stp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.453.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.453.3 FortiOS Version Compatibility

6.453.4 Parameters

6.453.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.453.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Spanning Tree Protocol (STP).
    fortios_system_stp:
      vdom:  "{{ vdom }}"
      system_stp:
        config_revision: "3"
        forward_delay: "4"
        hello_time: "5"
        max_age: "6"
        max_hops: "7"
        region_name: "<your_own_value>"
        status: "<your_own_value>"
        switch_priority: "0"
```

6.453.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.453.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.453.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.454 fortios_system_switch_interface – Configure software switch interfaces by grouping physical and WiFi interfaces in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.454.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and switch_interface category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.454.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.454.3 FortiOS Version Compatibility

6.454.4 Parameters

6.454.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.454.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure software switch interfaces by grouping physical and WiFi␣
↪interfaces.
    fortios_system_switch_interface:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_switch_interface:
        intra_switch_policy: "implicit"
        mac_ttl: "4"
        member:
         -
            interface_name: "<your_own_value> (source system.interface.name)"
        name: "default_name_7"
        span: "disable"
        span_dest_port: "<your_own_value> (source system.interface.name)"
        span_direction: "rx"
        span_source_port:
         -
            interface_name: "<your_own_value> (source system.interface.name)"
        type: "switch"
        vdom: "<your_own_value> (source system.vdom.name)"
```

6.454.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.454.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.454.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.455 fortios_system_tos_based_priority – Configure Type of Service (ToS) based priority table to set network traffic priorities in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.455.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and tos_based_priority category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.455.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.455.3 FortiOS Version Compatibility

6.455.4 Parameters

6.455.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.455.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Type of Service (ToS) based priority table to set network traffic␣
↪priorities.
    fortios_system_tos_based_priority:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_tos_based_priority:
        id:  "3"
        priority: "low"
        tos: "5"
```

6.455.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.455.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.455.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.456 fortios_system_vdom – Configure virtual domain in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.456.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and vdom category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.456.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.456.3 FortiOS Version Compatibility

6.456.4 Parameters

6.456.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.456.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure virtual domain.
    fortios_system_vdom:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_vdom:
        flag: "3"
        name: "default_name_4"
        short_name: "<your_own_value>"
        temporary: "6"
        vcluster_id: "7"
```

6.456.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.456.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.456.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.457 fortios_system_vdom_dns – Configure DNS servers for a non-management VDOM in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.457.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and vdom_dns category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.457.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.457.3 FortiOS Version Compatibility

6.457.4 Parameters

6.457.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.457.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure DNS servers for a non-management VDOM.
  fortios_system_vdom_dns:
    vdom:  "{{ vdom }}"
    system_vdom_dns:
      dns_over_tls: "disable"
      interface: "<your_own_value> (source system.interface.name)"
      interface_select_method: "auto"
      ip6_primary: "<your_own_value>"
      ip6_secondary: "<your_own_value>"
      primary: "<your_own_value>"
      protocol: "cleartext"
      secondary: "<your_own_value>"
      server_hostname:
       -
          hostname: "myhostname"
      source_ip: "84.230.14.43"
      ssl_certificate: "<your_own_value> (source certificate.local.name)"
      vdom_dns: "enable"
```

6.457.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.457.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.457.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.458 fortios_system_vdom_exception – Global configuration objects that can be configured independently for all VDOMs or for the defined VDOM scope in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.458.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and vdom_exception category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.458.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.458.3 FortiOS Version Compatibility

6.458.4 Parameters

6.458.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.458.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Global configuration objects that can be configured independently for all␣
↪VDOMs or for the defined VDOM scope.
    fortios_system_vdom_exception:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_vdom_exception:
        id:  "3"
        object: "log.fortianalyzer.setting"
        oid: "5"
        scope: "all"
        vdom:
         -
            name: "default_name_8 (source system.vdom.name)"
```

6.458.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.458.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.458.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.459 fortios_system_vdom_link – Configure VDOM links in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.459.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and vdom_link category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.459.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.459.3 FortiOS Version Compatibility

6.459.4 Parameters

6.459.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.459.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure VDOM links.
    fortios_system_vdom_link:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_vdom_link:
        name: "default_name_3"
        type: "ppp"
        vcluster: "vcluster1"
```

6.459.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.459.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.459.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.460 fortios_system_vdom_netflow – Configure NetFlow per VDOM in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.460.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and vdom_netflow category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.460.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.460.3 FortiOS Version Compatibility

6.460.4 Parameters

6.460.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.460.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure NetFlow per VDOM.
  fortios_system_vdom_netflow:
    vdom:  "{{ vdom }}"
    system_vdom_netflow:
      collector_ip: "<your_own_value>"
      collector_port: "4"
      source_ip: "84.230.14.43"
      vdom_netflow: "enable"
```

6.460.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.460.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.460.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.461 fortios_system_vdom_property – Configure VDOM property in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.461.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and vdom_property category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.461.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.461.3 FortiOS Version Compatibility

6.461.4 Parameters

6.461.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.461.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure VDOM property.
    fortios_system_vdom_property:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_vdom_property:
```

(continues on next page)

(continued from previous page)

```
        custom_service: "<your_own_value>"
        description: "<your_own_value>"
        dialup_tunnel: "<your_own_value>"
        firewall_address: "<your_own_value>"
        firewall_addrgrp: "<your_own_value>"
        firewall_policy: "<your_own_value>"
        ipsec_phase1: "<your_own_value>"
        ipsec_phase1_interface: "<your_own_value>"
        ipsec_phase2: "<your_own_value>"
        ipsec_phase2_interface: "<your_own_value>"
        log_disk_quota: "<your_own_value>"
        name: "default_name_14 (source system.vdom.name)"
        onetime_schedule: "<your_own_value>"
        proxy: "<your_own_value>"
        recurring_schedule: "<your_own_value>"
        service_group: "<your_own_value>"
        session: "<your_own_value>"
        snmp_index: "20"
        sslvpn: "<your_own_value>"
        user: "<your_own_value>"
        user_group: "<your_own_value>"
```

6.461.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.461.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.461.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.462 fortios_system_vdom_radius_server – Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server for this VDOM in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.462.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and vdom_radius_server category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.462.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.462.3 FortiOS Version Compatibility

6.462.4 Parameters

6.462.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.462.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure a RADIUS server to use as a RADIUS Single Sign On (RSSO) server␣
↪for this VDOM.
    fortios_system_vdom_radius_server:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_vdom_radius_server:
        name: "default_name_3 (source system.vdom.name)"
        radius_server_vdom: "<your_own_value> (source system.vdom.name)"
        status: "enable"
```

6.462.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.462.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.462.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.463 fortios_system_vdom_sflow – Configure sFlow per VDOM to add or change the IP address and UDP port that FortiGate sFlow agents in this VDOM use to send sFlow datagrams to an sFlow collector in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.463.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and vdom_sflow category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.463.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.463.3 FortiOS Version Compatibility

6.463.4 Parameters

6.463.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.463.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure sFlow per VDOM to add or change the IP address and UDP port that␣
↪FortiGate sFlow agents in this VDOM use to send sFlow datagrams to an
     sFlow collector.
    fortios_system_vdom_sflow:
      vdom:  "{{ vdom }}"
      system_vdom_sflow:
        collector_ip: "<your_own_value>"
        collector_port: "4"
        source_ip: "84.230.14.43"
        vdom_sflow: "enable"
```

6.463.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.463.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.463.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.464 fortios_system_virtual_switch – Configure virtual hardware switch interfaces in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.464.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and virtual_switch category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.464.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.464.3 FortiOS Version Compatibility

6.464.4 Parameters

6.464.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.464.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure virtual hardware switch interfaces.
    fortios_system_virtual_switch:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_virtual_switch:
        name: "default_name_3"
        physical_switch: "<your_own_value> (source system.physical-switch.name)"
        port:
         -
            alias: "<your_own_value>"
            mediatype: "cfp2-sr10"
            name: "default_name_8"
            speed: "auto"
            status: "up"
        span: "disable"
        span_dest_port: "<your_own_value>"
        span_direction: "rx"
        span_source_port: "<your_own_value>"
```

6.464.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.464.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.464.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.465 fortios_system_virtual_wan_link – Configure redundant internet connections using SD-WAN (formerly virtual WAN link) in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.465.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and virtual_wan_link category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.465.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.465.3 FortiOS Version Compatibility

6.465.4 Parameters

6.465.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.465.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure redundant internet connections using SD-WAN (formerly virtual WAN␣
↪link).
    fortios_system_virtual_wan_link:
      vdom:  "{{ vdom }}"
      system_virtual_wan_link:
        fail_alert_interfaces:
         -
            name: "default_name_4 (source system.interface.name)"
        fail_detect: "enable"
        health_check:
         -
            addr_mode: "ipv4"
            diffservcode: "<your_own_value>"
            failtime: "9"
            ha_priority: "10"
            http_agent: "<your_own_value>"
            http_get: "<your_own_value>"
            http_match: "<your_own_value>"
            interval: "14"
            members:
             -
                seq_num: "16 (source system.virtual-wan-link.members.seq-num)"
            name: "default_name_17"
            packet_size: "18"
            password: "<your_own_value>"
            port: "20"
            probe_packets: "disable"
            probe_timeout: "22"
            protocol: "ping"
            recoverytime: "24"
            security_mode: "none"
            server: "192.168.100.40"
            sla:
             -
                id:  "28"
                jitter_threshold: "29"
                latency_threshold: "30"
                link_cost_factor: "latency"
                packetloss_threshold: "32"
            sla_fail_log_period: "33"
            sla_pass_log_period: "34"
            threshold_alert_jitter: "35"
            threshold_alert_latency: "36"
            threshold_alert_packetloss: "37"
            threshold_warning_jitter: "38"
```

(continues on next page)

(continued from previous page)

```
            threshold_warning_latency: "39"
            threshold_warning_packetloss: "40"
            update_cascade_interface: "enable"
            update_static_route: "enable"
        load_balance_mode: "source-ip-based"
        members:
         -
            comment: "Comments."
            cost: "46"
            gateway: "<your_own_value>"
            gateway6: "<your_own_value>"
            ingress_spillover_threshold: "49"
            interface: "<your_own_value> (source system.interface.name)"
            priority: "51"
            seq_num: "52"
            source: "<your_own_value>"
            source6: "<your_own_value>"
            spillover_threshold: "55"
            status: "disable"
            volume_ratio: "57"
            weight: "58"
        neighbor:
         -
            health_check: "<your_own_value> (source system.virtual-wan-link.health-
↪check.name)"
            ip: "<your_own_value> (source router.bgp.neighbor.ip)"
            member: "62 (source system.virtual-wan-link.members.seq-num)"
            role: "standalone"
            sla_id: "64"
        neighbor_hold_boot_time: "65"
        neighbor_hold_down: "enable"
        neighbor_hold_down_time: "67"
        service:
         -
            addr_mode: "ipv4"
            bandwidth_weight: "70"
            default: "enable"
            dscp_forward: "enable"
            dscp_forward_tag: "<your_own_value>"
            dscp_reverse: "enable"
            dscp_reverse_tag: "<your_own_value>"
            dst:
             -
                name: "default_name_77 (source firewall.address.name firewall.addrgrp.
↪name)"
            dst_negate: "enable"
            dst6:
             -
                name: "default_name_80 (source firewall.address6.name firewall.
↪addrgrp6.name)"
            end_port: "81"
            gateway: "enable"
            groups:
             -
                name: "default_name_84 (source user.group.name)"
            health_check: "<your_own_value> (source system.virtual-wan-link.health-
↪check.name)"
```

(continues on next page)

(continued from previous page)

```
            hold_down_time: "86"
            id:  "87"
            input_device:
             -
                name: "default_name_89 (source system.interface.name)"
            input_device_negate: "enable"
            internet_service: "enable"
            internet_service_app_ctrl:
             -
                id:  "93"
            internet_service_app_ctrl_group:
             -
                name: "default_name_95 (source application.group.name)"
            internet_service_ctrl:
             -
                id:  "97"
            internet_service_ctrl_group:
             -
                name: "default_name_99 (source application.group.name)"
            internet_service_custom:
             -
                name: "default_name_101 (source firewall.internet-service-custom.name)
↪"
            internet_service_custom_group:
             -
                name: "default_name_103 (source firewall.internet-service-custom-
↪group.name)"
            internet_service_group:
             -
                name: "default_name_105 (source firewall.internet-service-group.name)"
            internet_service_id:
             -
                id:  "107 (source firewall.internet-service.id)"
            jitter_weight: "108"
            latency_weight: "109"
            link_cost_factor: "latency"
            link_cost_threshold: "111"
            member: "112 (source system.virtual-wan-link.members.seq-num)"
            mode: "auto"
            name: "default_name_114"
            packet_loss_weight: "115"
            priority_members:
             -
                seq_num: "117 (source system.virtual-wan-link.members.seq-num)"
            protocol: "118"
            quality_link: "119"
            role: "standalone"
            route_tag: "121"
            sla:
             -
                health_check: "<your_own_value> (source system.virtual-wan-link.
↪health-check.name)"
                id:  "124"
            sla_compare_method: "order"
            src:
             -
                name: "default_name_127 (source firewall.address.name firewall.
↪addrgrp.name)"
```

(continues on next page)

(continued from previous page)

```
            src_negate: "enable"
            src6:
             -
                name: "default_name_130 (source firewall.address6.name firewall.
↪addrgrp6.name)"
            standalone_action: "enable"
            start_port: "132"
            status: "enable"
            tos: "<your_own_value>"
            tos_mask: "<your_own_value>"
            users:
             -
                name: "default_name_137 (source user.local.name)"
        status: "disable"
        zone:
         -
            name: "default_name_140"
```

6.465.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.465.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.465.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.466 fortios_system_virtual_wire_pair – Configure virtual wire pairs in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.466.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and virtual_wire_pair category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.466.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.466.3 FortiOS Version Compatibility

6.466.4 Parameters

6.466.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.466.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure virtual wire pairs.
  fortios_system_virtual_wire_pair:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    system_virtual_wire_pair:
      member:
       -
          interface_name: "<your_own_value> (source system.interface.name)"
      name: "default_name_5"
      vlan_filter: "<your_own_value>"
      wildcard_vlan: "enable"
```

6.466.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.466.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.466.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.467 fortios_system_vne_tunnel – Configure virtual network enabler tunnel in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.467.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and vne_tunnel category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.467.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.467.3 FortiOS Version Compatibility

6.467.4 Parameters

6.467.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.467.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure virtual network enabler tunnel.
    fortios_system_vne_tunnel:
      vdom:  "{{ vdom }}"
      system_vne_tunnel:
        auto_asic_offload: "enable"
```

(continues on next page)

(continued from previous page)

```
        bmr_hostname: "<your_own_value>"
        br: "<your_own_value>"
        interface: "<your_own_value> (source system.interface.name)"
        ipv4_address: "<your_own_value>"
        mode: "map-e"
        ssl_certificate: "<your_own_value> (source certificate.local.name)"
        status: "enable"
        update_url: "<your_own_value>"
```

6.467.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.467.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.467.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.468 fortios_system_vxlan – Configure VXLAN devices in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.468.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and vxlan category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.468.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.468.3 FortiOS Version Compatibility

6.468.4 Parameters

6.468.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.468.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure VXLAN devices.
    fortios_system_vxlan:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_vxlan:
        dstport: "3"
        interface: "<your_own_value> (source system.interface.name)"
        ip_version: "ipv4-unicast"
        multicast_ttl: "6"
```

(continues on next page)

(continued from previous page)

```
        name: "default_name_7"
        remote_ip:
         -
            ip: "<your_own_value>"
        remote_ip6:
         -
            ip6: "<your_own_value>"
        vni: "12"
```

6.468.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.468.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.468.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.469 fortios_system_wccp – Configure WCCP in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.469.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and wccp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.469.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.469.3 FortiOS Version Compatibility

6.469.4 Parameters

6.469.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.469.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure WCCP.
    fortios_system_wccp:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_wccp:
        assignment_bucket_format: "wccp-v2"
        assignment_dstaddr_mask: "<your_own_value>"
        assignment_method: "HASH"
        assignment_srcaddr_mask: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        assignment_weight: "7"
        authentication: "enable"
        cache_engine_method: "GRE"
        cache_id: "<your_own_value>"
        forward_method: "GRE"
        group_address: "<your_own_value>"
        password: "<your_own_value>"
        ports: "<your_own_value>"
        ports_defined: "source"
        primary_hash: "src-ip"
        priority: "17"
        protocol: "18"
        return_method: "GRE"
        router_id: "<your_own_value>"
        router_list: "<your_own_value>"
        server_list: "<your_own_value>"
        server_type: "forward"
        service_id: "<your_own_value>"
        service_type: "auto"
```

6.469.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.469.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.469.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.470 fortios_system_zone – Configure zones to group two or more interfaces. When a zone is created you can configure policies for the zone instead of individual interfaces in the zone in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.470.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and zone category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.470.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.470.3 FortiOS Version Compatibility

6.470.4 Parameters

6.470.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.470.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure zones to group two or more interfaces. When a zone is created you␣
↪can configure policies for the zone instead of individual interfaces in
     the zone.
    fortios_system_zone:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_zone:
        description: "<your_own_value>"
        interface:
         -
            interface_name: "<your_own_value> (source system.interface.name)"
        intrazone: "allow"
        name: "default_name_7"
        tagging:
         -
            category: "<your_own_value> (source system.object-tagging.category)"
            name: "default_name_10"
            tags:
             -
                name: "default_name_12 (source system.object-tagging.tags.name)"
```

6.470.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.470.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.470.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.471 fortios_user_adgrp – Configure FSSO groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.471.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and adgrp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.471.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.471.3 FortiOS Version Compatibility

6.471.4 Parameters

6.471.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.471.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FSSO groups.
    fortios_user_adgrp:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_adgrp:
        connector_source: "<your_own_value>"
        id:  "4"
        name: "default_name_5"
        server_name: "<your_own_value> (source user.fsso.name)"
```

6.471.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.471.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.471.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.472 fortios_user_device – Configure devices in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.472.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and device category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.472.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.472.3 FortiOS Version Compatibility

6.472.4 Parameters

6.472.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.472.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure devices.
    fortios_user_device:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_device:
        alias: "<your_own_value>"
        avatar: "<your_own_value>"
        category: "none"
        comment: "Comment."
        mac: "<your_own_value>"
        master_device: "<your_own_value> (source user.device.alias)"
        tagging:
         -
            category: "<your_own_value> (source system.object-tagging.category)"
            name: "default_name_11"
            tags:
             -
                name: "default_name_13 (source system.object-tagging.tags.name)"
        type: "unknown"
        user: "<your_own_value>"
```

6.472.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.472.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.472.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.473 fortios_user_device_access_list – Configure device access control lists in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.473.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and device_access_list category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.473.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.473.3 FortiOS Version Compatibility

6.473.4 Parameters

6.473.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.473.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure device access control lists.
    fortios_user_device_access_list:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_device_access_list:
        default_action: "accept"
        device_list:
         -
            action: "accept"
            device: "<your_own_value> (source user.device.alias user.device-group.
↪name user.device-category.name)"
            id:  "7"
        name: "default_name_8"
```

6.473.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.473.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.473.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.474 fortios_user_device_category – Configure device categories in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.474.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and device_category category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.474.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.474.3 FortiOS Version Compatibility

6.474.4 Parameters

6.474.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.474.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure device categories.
    fortios_user_device_category:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_device_category:
        comment: "Comment."
        desc: "<your_own_value>"
        name: "default_name_5"
```

6.474.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.474.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.474.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.475 fortios_user_device_group – Configure device groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.475.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and device_group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.475.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.475.3 FortiOS Version Compatibility

6.475.4 Parameters

6.475.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.475.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
 tasks:
 - name: Configure device groups.
   fortios_user_device_group:
     vdom:  "{{ vdom }}"
     state: "present"
     access_token: "<your_own_value>"
     user_device_group:
       comment: "Comment."
       member:
        -
           name: "default_name_5 (source user.device.alias user.device-category.name)
↪"
       name: "default_name_6"
       tagging:
        -
           category: "<your_own_value> (source system.object-tagging.category)"
           name: "default_name_9"
           tags:
            -
               name: "default_name_11 (source system.object-tagging.tags.name)"
```

6.475.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.475.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.475.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.476 fortios_user_domain_controller – Configure domain controller entries in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.476.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and domain_controller category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.476.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.476.3 FortiOS Version Compatibility

6.476.4 Parameters

6.476.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.476.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure domain controller entries.
    fortios_user_domain_controller:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_domain_controller:
        ad_mode: "none"
        adlds_dn: "<your_own_value>"
        adlds_ip_address: "<your_own_value>"
        adlds_ip6: "<your_own_value>"
        adlds_port: "7"
        dns_srv_lookup: "enable"
        domain_name: "<your_own_value>"
        extra_server:
         -
            id:  "11"
            ip_address: "<your_own_value>"
            port: "13"
            source_ip_address: "<your_own_value>"
            source_port: "15"
        hostname: "myhostname"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        ip_address: "<your_own_value>"
        ip6: "<your_own_value>"
        ldap_server: "<your_own_value> (source user.ldap.name)"
        name: "default_name_22"
        password: "<your_own_value>"
        port: "24"
        replication_port: "25"
        source_ip_address: "<your_own_value>"
        source_ip6: "<your_own_value>"
        source_port: "28"
        username: "<your_own_value>"
```

6.476.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.476.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.476.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.477 fortios_user_exchange – Configure MS Exchange server entries in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.477.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and exchange category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.477.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.477.3 FortiOS Version Compatibility

6.477.4 Parameters

6.477.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.477.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure MS Exchange server entries.
    fortios_user_exchange:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_exchange:
        auth_level: "connect"
        auth_type: "spnego"
        auto_discover_kdc: "enable"
        connect_protocol: "rpc-over-tcp"
        domain_name: "<your_own_value>"
        http_auth_type: "basic"
        ip: "<your_own_value>"
        kdc_ip:
         -
            ipv4: "<your_own_value>"
        name: "default_name_12"
        password: "<your_own_value>"
        server_name: "<your_own_value>"
        ssl_min_proto_version: "default"
        username: "<your_own_value>"
```

6.477.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.477.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.477.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.478 fortios_user_fortitoken – Configure FortiToken in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.478.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and fortitoken category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.478.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.478.3 FortiOS Version Compatibility

6.478.4 Parameters

6.478.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.478.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiToken.
    fortios_user_fortitoken:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_fortitoken:
        activation_code: "<your_own_value>"
        activation_expire: "4"
        comments: "<your_own_value>"
        license: "<your_own_value>"
        os_ver: "<your_own_value>"
        reg_id: "<your_own_value>"
        seed: "<your_own_value>"
        serial_number: "<your_own_value>"
        status: "active"
```

6.478.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.478.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.478.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.479 fortios_user_fsso – Configure Fortinet Single Sign On (FSSO) agents in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.479.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and fsso category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.479.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.479.3 FortiOS Version Compatibility

6.479.4 Parameters

6.479.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.479.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Fortinet Single Sign On (FSSO) agents.
    fortios_user_fsso:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_fsso:
        group_poll_interval: "3"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        ldap_poll: "enable"
        ldap_poll_filter: "<your_own_value>"
        ldap_poll_interval: "8"
        ldap_server: "<your_own_value> (source user.ldap.name)"
        name: "default_name_10"
        password: "<your_own_value>"
        password2: "<your_own_value>"
        password3: "<your_own_value>"
        password4: "<your_own_value>"
        password5: "<your_own_value>"
        port: "16"
        port2: "17"
        port3: "18"
        port4: "19"
        port5: "20"
        server: "192.168.100.40"
        server2: "<your_own_value>"
        server3: "<your_own_value>"
        server4: "<your_own_value>"
        server5: "<your_own_value>"
        source_ip: "84.230.14.43"
        source_ip6: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        ssl: "enable"
        ssl_trusted_cert: "<your_own_value> (source vpn.certificate.remote.name vpn.
↪certificate.ca.name)"
        type: "default"
        user_info_server: "<your_own_value> (source user.ldap.name)"
```

6.479.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.479.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.479.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.480 fortios_user_fsso_polling – Configure FSSO active directory servers for polling mode in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.480.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and fsso_polling category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.480.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.480.3 FortiOS Version Compatibility

6.480.4 Parameters

6.480.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.480.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FSSO active directory servers for polling mode.
    fortios_user_fsso_polling:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_fsso_polling:
        adgrp:
         -
            name: "default_name_4"
        default_domain: "<your_own_value>"
        id:  "6"
        ldap_server: "<your_own_value> (source user.ldap.name)"
        logon_history: "8"
```

(continues on next page)

(continued from previous page)

```
        password: "<your_own_value>"
        polling_frequency: "10"
        port: "11"
        server: "192.168.100.40"
        smb_ntlmv1_auth: "enable"
        smbv1: "enable"
        status: "enable"
        user: "<your_own_value>"
```

6.480.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.480.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.480.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.481 fortios_user_group – Configure user groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.481.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.481.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.481.3 FortiOS Version Compatibility

6.481.4 Parameters

6.481.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.481.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure user groups.
    fortios_user_group:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_group:
        auth_concurrent_override: "enable"
        auth_concurrent_value: "4"
        authtimeout: "5"
        company: "optional"
```

(continues on next page)

(continued from previous page)

```
        email: "disable"
        expire: "8"
        expire_type: "immediately"
        group_type: "firewall"
        guest:
         -
            comment: "Comment."
            company: "<your_own_value>"
            email: "<your_own_value>"
            expiration: "<your_own_value>"
            id:  "16"
            mobile_phone: "<your_own_value>"
            name: "default_name_18"
            password: "<your_own_value>"
            sponsor: "<your_own_value>"
            user_id: "<your_own_value>"
        http_digest_realm: "<your_own_value>"
        id:  "23"
        match:
         -
            group_name: "<your_own_value>"
            id:  "26"
            server_name: "<your_own_value> (source user.radius.name user.ldap.name␣
↪user.tacacs+.name)"
        max_accounts: "28"
        member:
         -
            name: "default_name_30 (source user.peer.name user.local.name user.radius.
↪name user.tacacs+.name user.ldap.name user.adgrp.name user.pop3.name)"
        mobile_phone: "disable"
        multiple_guest_add: "disable"
        name: "default_name_33"
        password: "auto-generate"
        sms_custom_server: "<your_own_value> (source system.sms-server.name)"
        sms_server: "fortiguard"
        sponsor: "optional"
        sso_attribute_value: "<your_own_value>"
        user_id: "email"
        user_name: "disable"
```

6.481.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.481.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.481.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.482 fortios_user_krb_keytab – Configure Kerberos keytab entries in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.482.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and krb_keytab category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.482.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.482.3 FortiOS Version Compatibility

6.482.4 Parameters

6.482.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.482.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Kerberos keytab entries.
    fortios_user_krb_keytab:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_krb_keytab:
        keytab: "<your_own_value>"
        ldap_server: "<your_own_value> (source user.ldap.name)"
        name: "default_name_5"
        pac_data: "enable"
        password: "<your_own_value>"
        principal: "<your_own_value>"
```

6.482.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.482.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.482.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.483 fortios_user_ldap – Configure LDAP server entries in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.483.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and ldap category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.483.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.483.3 FortiOS Version Compatibility

6.483.4 Parameters

6.483.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.483.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure LDAP server entries.
    fortios_user_ldap:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_ldap:
        account_key_filter: "<your_own_value>"
        account_key_processing: "same"
        antiphish: "enable"
        ca_cert: "<your_own_value> (source vpn.certificate.ca.name)"
        cnid: "<your_own_value>"
        dn: "<your_own_value>"
        group_filter: "<your_own_value>"
        group_member_check: "user-attr"
        group_object_filter: "<your_own_value>"
        group_search_base: "<your_own_value>"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        member_attr: "<your_own_value>"
        name: "default_name_16"
        obtain_user_info: "enable"
        password: "<your_own_value>"
        password_attr: "<your_own_value>"
        password_expiry_warning: "enable"
        password_renewal: "enable"
        port: "22"
        search_type: "recursive"
        secondary_server: "<your_own_value>"
        secure: "disable"
        server: "192.168.100.40"
        server_identity_check: "enable"
        source_ip: "84.230.14.43"
        source_port: "29"
        ssl_min_proto_version: "default"
        tertiary_server: "<your_own_value>"
        two_factor: "disable"
        two_factor_authentication: "fortitoken"
        two_factor_notification: "email"
        type: "simple"
        user_info_exchange_server: "<your_own_value> (source user.exchange.name)"
        username: "<your_own_value>"
```

6.483.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.483.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.483.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.484 fortios_user_local – Configure local users in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.484.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and local category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.484.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.484.3 FortiOS Version Compatibility

6.484.4 Parameters

6.484.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.484.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure local users.
    fortios_user_local:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_local:
        auth_concurrent_override: "enable"
        auth_concurrent_value: "4"
        authtimeout: "5"
        email_to: "<your_own_value>"
        fortitoken: "<your_own_value> (source user.fortitoken.serial-number)"
        id:  "8"
        ldap_server: "<your_own_value> (source user.ldap.name)"
        name: "default_name_10"
        passwd: "<your_own_value>"
        passwd_policy: "<your_own_value> (source user.password-policy.name)"
        passwd_time: "<your_own_value>"
        ppk_identity: "<your_own_value>"
        ppk_secret: "<your_own_value>"
        radius_server: "<your_own_value> (source user.radius.name)"
        sms_custom_server: "<your_own_value> (source system.sms-server.name)"
        sms_phone: "<your_own_value>"
        sms_server: "fortiguard"
        status: "enable"
        tacacs+_server: "<your_own_value> (source user.tacacs+.name)"
```

(continues on next page)

(continued from previous page)

```
        two_factor: "disable"
        two_factor_authentication: "fortitoken"
        two_factor_notification: "email"
        type: "password"
        username_case_sensitivity: "disable"
        workstation: "<your_own_value>"
```

6.484.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.484.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.484.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.485 fortios_user_nac_policy – Configure NAC policy matching pattern to identify matching NAC devices in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.485.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and nac_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.485.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.485.3 FortiOS Version Compatibility

6.485.4 Parameters

6.485.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.485.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure NAC policy matching pattern to identify matching NAC devices.
    fortios_user_nac_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_nac_policy:
        category: "device"
        description: "<your_own_value>"
        ems_tag: "<your_own_value> (source firewall.address.name)"
        family: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        host: "myhostname"
        hw_vendor: "<your_own_value>"
        hw_version: "<your_own_value>"
        mac: "<your_own_value>"
        name: "default_name_11"
        os: "<your_own_value>"
        src: "<your_own_value>"
        ssid_policy: "<your_own_value> (source wireless-controller.ssid-policy.name)"
        status: "enable"
        sw_version: "<your_own_value>"
        switch_auto_auth: "global"
        switch_fortilink: "<your_own_value> (source system.interface.name)"
        switch_mac_policy: "<your_own_value> (source switch-controller.mac-policy.
↪name)"
        switch_port_policy: "<your_own_value> (source switch-controller.port-policy.
↪name)"
        switch_scope:
         -
            switch_id: "<your_own_value> (source switch-controller.managed-switch.
↪switch-id)"
        type: "<your_own_value>"
        user: "<your_own_value>"
        user_group: "<your_own_value> (source user.group.name)"
```

6.485.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.485.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.485.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.486 fortios_user_password_policy – Configure user password policy in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.486.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and password_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.486.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.486.3 FortiOS Version Compatibility

6.486.4 Parameters

6.486.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.486.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure user password policy.
    fortios_user_password_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_password_policy:
        expire_days: "3"
        expired_password_renewal: "enable"
        name: "default_name_5"
        warn_days: "6"
```

6.486.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.486.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.486.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.487 fortios_user_peer – Configure peer users in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.487.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and peer category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.487.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.487.3 FortiOS Version Compatibility

6.487.4 Parameters

6.487.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.487.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
    ansible_httpapi_port: 443
  tasks:
  - name: Configure peer users.
    fortios_user_peer:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_peer:
        ca: "<your_own_value> (source vpn.certificate.ca.name)"
        cn: "<your_own_value>"
        cn_type: "string"
        ldap_mode: "password"
        ldap_password: "<your_own_value>"
        ldap_server: "<your_own_value> (source user.ldap.name)"
        ldap_username: "<your_own_value>"
        mandatory_ca_verify: "enable"
        name: "default_name_11"
        ocsp_override_server: "<your_own_value> (source vpn.certificate.ocsp-server.
↪name)"
        passwd: "<your_own_value>"
        subject: "<your_own_value>"
        two_factor: "enable"
```

6.487.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.487.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.487.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.488 fortios_user_peergrp – Configure peer groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.488.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and peergrp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.488.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.488.3 FortiOS Version Compatibility

6.488.4 Parameters

6.488.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.488.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure peer groups.
    fortios_user_peergrp:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_peergrp:
        member:
         -
            name: "default_name_4 (source user.peer.name)"
        name: "default_name_5"
```

6.488.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.488.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.488.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.489 fortios_user_pop3 – POP3 server entry configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.489.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and pop3 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.489.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.489.3 FortiOS Version Compatibility

6.489.4 Parameters

6.489.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.489.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: POP3 server entry configuration.
  fortios_user_pop3:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    user_pop3:
      name: "default_name_3"
      port: "4"
      secure: "none"
      server: "192.168.100.40"
      ssl_min_proto_version: "default"
```

6.489.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.489.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.489.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.490 fortios_user_quarantine – Configure quarantine support in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.490.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and quarantine category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.490.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.490.3 FortiOS Version Compatibility

6.490.4 Parameters

6.490.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.490.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure quarantine support.
    fortios_user_quarantine:
      vdom:  "{{ vdom }}"
      user_quarantine:
        firewall_groups: "<your_own_value> (source firewall.addrgrp.name)"
```

(continues on next page)

(continued from previous page)

```
        quarantine: "enable"
        targets:
         -
            description: "<your_own_value>"
            entry: "<your_own_value>"
            macs:
             -
                description: "<your_own_value>"
                drop: "disable"
                entry_id: "11"
                mac: "<your_own_value>"
                parent: "<your_own_value>"
        traffic_policy: "<your_own_value> (source switch-controller.traffic-policy.
↪name)"
```

6.490.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.490.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.490.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.491 fortios_user_radius – Configure RADIUS server entries in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.491.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and radius category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.491.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.491.3 FortiOS Version Compatibility

6.491.4 Parameters

6.491.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.491.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure RADIUS server entries.
    fortios_user_radius:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    state: "present"
    access_token: "<your_own_value>"
    user_radius:
      accounting_server:
       -
          id:  "4"
          interface: "<your_own_value> (source system.interface.name)"
          interface_select_method: "auto"
          port: "7"
          secret: "<your_own_value>"
          server: "192.168.100.40"
          source_ip: "84.230.14.43"
          status: "enable"
      acct_all_servers: "enable"
      acct_interim_interval: "13"
      all_usergroup: "disable"
      auth_type: "auto"
      class:
       -
          name: "default_name_17"
      group_override_attr_type: "filter-Id"
      h3c_compatibility: "enable"
      interface: "<your_own_value> (source system.interface.name)"
      interface_select_method: "auto"
      name: "default_name_22"
      nas_ip: "<your_own_value>"
      password_encoding: "auto"
      password_renewal: "enable"
      radius_coa: "enable"
      radius_port: "27"
      rsso: "enable"
      rsso_context_timeout: "29"
      rsso_endpoint_attribute: "User-Name"
      rsso_endpoint_block_attribute: "User-Name"
      rsso_ep_one_ip_only: "enable"
      rsso_flush_ip_session: "enable"
      rsso_log_flags: "protocol-error"
      rsso_log_period: "35"
      rsso_radius_response: "enable"
      rsso_radius_server_port: "37"
      rsso_secret: "<your_own_value>"
      rsso_validate_request_secret: "enable"
      secondary_secret: "<your_own_value>"
      secondary_server: "<your_own_value>"
      secret: "<your_own_value>"
      server: "192.168.100.40"
      source_ip: "84.230.14.43"
      sso_attribute: "User-Name"
      sso_attribute_key: "<your_own_value>"
      sso_attribute_value_override: "enable"
      switch_controller_acct_fast_framedip_detect: "48"
      switch_controller_service_type: "login"
      tertiary_secret: "<your_own_value>"
      tertiary_server: "<your_own_value>"
      timeout: "52"
      use_management_vdom: "enable"
      username_case_sensitive: "enable"
```

6.491.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.491.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.491.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.492 fortios_user_saml – SAML server entry configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.492.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and saml category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.492.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.492.3 FortiOS Version Compatibility

6.492.4 Parameters

6.492.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.492.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: SAML server entry configuration.
    fortios_user_saml:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_saml:
        adfs_claim: "enable"
        cert: "<your_own_value> (source vpn.certificate.local.name)"
        digest_method: "sha1"
        entity_id: "<your_own_value>"
        group_claim_type: "email"
        group_name: "<your_own_value>"
        idp_cert: "<your_own_value> (source vpn.certificate.remote.name)"
        idp_entity_id: "<your_own_value>"
        idp_single_logout_url: "<your_own_value>"
        idp_single_sign_on_url: "<your_own_value>"
        limit_relaystate: "enable"
        name: "default_name_14"
        single_logout_url: "<your_own_value>"
        single_sign_on_url: "<your_own_value>"
        user_claim_type: "email"
        user_name: "<your_own_value>"
```

6.492.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.492.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.492.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.493 fortios_user_security_exempt_list – Configure security exemption list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.493.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and security_exempt_list category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.493.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.493.3 FortiOS Version Compatibility

6.493.4 Parameters

6.493.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.493.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure security exemption list.
    fortios_user_security_exempt_list:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_security_exempt_list:
        description: "<your_own_value>"
        name: "default_name_4"
        rule:
         -
            devices:
             -
                name: "default_name_7 (source user.device.alias user.device-group.
↪name user.device-category.name)"
            dstaddr:
             -
                name: "default_name_9 (source firewall.address.name firewall.addrgrp.
↪name)"
            id:  "10"
            service:
             -
                name: "default_name_12 (source firewall.service.custom.name firewall.
↪service.group.name)"
            srcaddr:
```

(continues on next page)

(continued from previous page)

```
            -
                name: "default_name_14 (source firewall.address.name firewall.addrgrp.
↪name)"
```

6.493.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.493.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.493.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.494 fortios_user_setting – Configure user authentication setting in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.494.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.494.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.494.3 FortiOS Version Compatibility

6.494.4 Parameters

6.494.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.494.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure user authentication setting.
    fortios_user_setting:
      vdom:  "{{ vdom }}"
      user_setting:
        auth_blackout_time: "3"
        auth_ca_cert: "<your_own_value> (source vpn.certificate.local.name)"
        auth_cert: "<your_own_value> (source vpn.certificate.local.name)"
        auth_http_basic: "enable"
        auth_invalid_max: "7"
        auth_lockout_duration: "8"
        auth_lockout_threshold: "9"
        auth_on_demand: "always"
        auth_portal_timeout: "11"
        auth_ports:
         -
            id:  "13"
            port: "14"
```

(continues on next page)

(continued from previous page)

```
        type: "http"
    auth_secure_http: "enable"
    auth_src_mac: "enable"
    auth_ssl_allow_renegotiation: "enable"
    auth_ssl_min_proto_version: "default"
    auth_timeout: "20"
    auth_timeout_type: "idle-timeout"
    auth_type: "http"
    per_policy_disclaimer: "enable"
    radius_ses_timeout_act: "hard-timeout"
```

6.494.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.494.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.494.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.495 fortios_user_tacacsplus – Configure TACACS+ server entries in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.495.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify user feature and tacacsplus category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.495.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.495.3 FortiOS Version Compatibility

6.495.4 Parameters

6.495.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.495.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure TACACS+ server entries.
    fortios_user_tacacsplus:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      user_tacacsplus:
```

(continues on next page)

(continued from previous page)

```
        authen_type: "mschap"
        authorization: "enable"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        key: "<your_own_value>"
        name: "default_name_8"
        port: "9"
        secondary_key: "<your_own_value>"
        secondary_server: "<your_own_value>"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        tertiary_key: "<your_own_value>"
        tertiary_server: "<your_own_value>"
```

6.495.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.495.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.495.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.496 fortios_videofilter_profile – Configure VideoFilter profile in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.496.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify videofilter feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.496.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.496.3 FortiOS Version Compatibility

6.496.4 Parameters

6.496.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.496.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure VideoFilter profile.
    fortios_videofilter_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
    videofilter_profile:
      comment: "Comment."
      dailymotion: "enable"
      fortiguard_category:
          filters:
           -
              action: "bypass"
              category_id: "8"
              id:  "9"
              log: "enable"
      name: "default_name_11"
      vimeo: "enable"
      vimeo_restrict: "<your_own_value>"
      youtube: "enable"
      youtube_channel_filter: "15 (source videofilter.youtube-channel-filter.id)"
      youtube_restrict: "none"
```

6.496.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.496.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.496.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.497 fortios_videofilter_youtube_channel_filter – Configure YouTube channel filter in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.497.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify videofilter feature and youtube_channel_filter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.497.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.497.3 FortiOS Version Compatibility

6.497.4 Parameters

6.497.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.497.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure YouTube channel filter.
  fortios_videofilter_youtube_channel_filter:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    videofilter_youtube_channel_filter:
      comment: "Comment."
      entries:
       -
          action: "bypass"
          channel_id: "<your_own_value>"
          comment: "Comment."
          id:  "8"
      id:  "9"
      name: "default_name_10"
```

6.497.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.497.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.497.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.498 fortios_videofilter_youtube_key – Configure YouTube API keys in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.498.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify videofilter feature and youtube_key category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.498.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.498.3 FortiOS Version Compatibility

6.498.4 Parameters

6.498.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.498.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Configure YouTube API keys.
  fortios_videofilter_youtube_key:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    videofilter_youtube_key:
      id:  "3"
      key: "<your_own_value>"
      status: "enable"
```

6.498.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.498.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.498.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.499 fortios_voip_profile – Configure VoIP profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.499.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify voip feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.499.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.499.3 FortiOS Version Compatibility

6.499.4 Parameters

6.499.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.499.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure VoIP profiles.
    fortios_voip_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      voip_profile:
```

(continues on next page)

(continued from previous page)

```
        comment: "Comment."
        feature_set: "flow"
        name: "default_name_5"
        sccp:
            block_mcast: "disable"
            log_call_summary: "disable"
            log_violations: "disable"
            max_calls: "10"
            status: "disable"
            verify_header: "disable"
        sip:
            ack_rate: "14"
            ack_rate_track: "none"
            block_ack: "disable"
            block_bye: "disable"
            block_cancel: "disable"
            block_geo_red_options: "disable"
            block_info: "disable"
            block_invite: "disable"
            block_long_lines: "disable"
            block_message: "disable"
            block_notify: "disable"
            block_options: "disable"
            block_prack: "disable"
            block_publish: "disable"
            block_refer: "disable"
            block_register: "disable"
            block_subscribe: "disable"
            block_unknown: "disable"
            block_update: "disable"
            bye_rate: "33"
            bye_rate_track: "none"
            call_keepalive: "35"
            cancel_rate: "36"
            cancel_rate_track: "none"
            contact_fixup: "disable"
            hnt_restrict_source_ip: "disable"
            hosted_nat_traversal: "disable"
            info_rate: "41"
            info_rate_track: "none"
            invite_rate: "43"
            invite_rate_track: "none"
            ips_rtp: "disable"
            log_call_summary: "disable"
            log_violations: "disable"
            malformed_header_allow: "discard"
            malformed_header_call_id: "discard"
            malformed_header_contact: "discard"
            malformed_header_content_length: "discard"
            malformed_header_content_type: "discard"
            malformed_header_cseq: "discard"
            malformed_header_expires: "discard"
            malformed_header_from: "discard"
            malformed_header_max_forwards: "discard"
            malformed_header_no_proxy_require: "discard"
            malformed_header_no_require: "discard"
            malformed_header_p_asserted_identity: "discard"
```

(continues on next page)

(continued from previous page)

```
            malformed_header_rack: "discard"
            malformed_header_record_route: "discard"
            malformed_header_route: "discard"
            malformed_header_rseq: "discard"
            malformed_header_sdp_a: "discard"
            malformed_header_sdp_b: "discard"
            malformed_header_sdp_c: "discard"
            malformed_header_sdp_i: "discard"
            malformed_header_sdp_k: "discard"
            malformed_header_sdp_m: "discard"
            malformed_header_sdp_o: "discard"
            malformed_header_sdp_r: "discard"
            malformed_header_sdp_s: "discard"
            malformed_header_sdp_t: "discard"
            malformed_header_sdp_v: "discard"
            malformed_header_sdp_z: "discard"
            malformed_header_to: "discard"
            malformed_header_via: "discard"
            malformed_request_line: "discard"
            max_body_length: "79"
            max_dialogs: "80"
            max_idle_dialogs: "81"
            max_line_length: "82"
            message_rate: "83"
            message_rate_track: "none"
            nat_port_range: "<your_own_value>"
            nat_trace: "disable"
            no_sdp_fixup: "disable"
            notify_rate: "88"
            notify_rate_track: "none"
            open_contact_pinhole: "disable"
            open_record_route_pinhole: "disable"
            open_register_pinhole: "disable"
            open_via_pinhole: "disable"
            options_rate: "94"
            options_rate_track: "none"
            prack_rate: "96"
            prack_rate_track: "none"
            preserve_override: "disable"
            provisional_invite_expiry_time: "99"
            publish_rate: "100"
            publish_rate_track: "none"
            refer_rate: "102"
            refer_rate_track: "none"
            register_contact_trace: "disable"
            register_rate: "105"
            register_rate_track: "none"
            rfc2543_branch: "disable"
            rtp: "disable"
            ssl_algorithm: "high"
            ssl_auth_client: "<your_own_value> (source user.peer.name user.peergrp.
↪name)"
            ssl_auth_server: "<your_own_value> (source user.peer.name user.peergrp.
↪name)"
            ssl_client_certificate: "<your_own_value> (source vpn.certificate.local.
↪name)"
            ssl_client_renegotiation: "allow"
```

(continues on next page)

(continued from previous page)

```
            ssl_max_version: "ssl-3.0"
            ssl_min_version: "ssl-3.0"
            ssl_mode: "off"
            ssl_pfs: "require"
            ssl_send_empty_frags: "enable"
            ssl_server_certificate: "<your_own_value> (source vpn.certificate.local.
↪name)"
            status: "disable"
            strict_register: "disable"
            subscribe_rate: "122"
            subscribe_rate_track: "none"
            unknown_header: "discard"
            update_rate: "125"
            update_rate_track: "none"
```

6.499.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.499.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.499.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.500 fortios_vpn_certificate_ca – CA certificate in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.500.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_certificate feature and ca category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.500.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.500.3 FortiOS Version Compatibility

6.500.4 Parameters

6.500.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.500.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: CA certificate.
    fortios_vpn_certificate_ca:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    state: "present"
    access_token: "<your_own_value>"
    vpn_certificate_ca:
      auto_update_days: "3"
      auto_update_days_warning: "4"
      ca: "<your_own_value>"
      last_updated: "6"
      name: "default_name_7"
      range: "global"
      scep_url: "<your_own_value>"
      source: "factory"
      source_ip: "84.230.14.43"
      ssl_inspection_trusted: "enable"
      trusted: "enable"
```

6.500.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.500.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.500.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.501 fortios_vpn_certificate_crl – Certificate Revocation List as a PEM file in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.501.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_certificate feature and crl category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.501.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.501.3 FortiOS Version Compatibility

6.501.4 Parameters

6.501.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.501.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Certificate Revocation List as a PEM file.
    fortios_vpn_certificate_crl:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    state: "present"
    access_token: "<your_own_value>"
    vpn_certificate_crl:
      crl: "<your_own_value>"
      http_url: "<your_own_value>"
      last_updated: "5"
      ldap_password: "<your_own_value>"
      ldap_server: "<your_own_value>"
      ldap_username: "<your_own_value>"
      name: "default_name_9"
      range: "global"
      scep_cert: "<your_own_value> (source vpn.certificate.local.name)"
      scep_url: "<your_own_value>"
      source: "factory"
      source_ip: "84.230.14.43"
      update_interval: "15"
      update_vdom: "<your_own_value> (source system.vdom.name)"
```

6.501.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.501.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.501.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.502 fortios_vpn_certificate_local – Local keys and certificates in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.502.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_certificate feature and local category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.502.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.502.3 FortiOS Version Compatibility

6.502.4 Parameters

6.502.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.502.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
tasks:
- name: Local keys and certificates.
  fortios_vpn_certificate_local:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    vpn_certificate_local:
      acme_ca_url: "<your_own_value>"
      acme_domain: "<your_own_value>"
      acme_email: "<your_own_value>"
      acme_renew_window: "6"
      acme_rsa_key_size: "7"
      auto_regenerate_days: "8"
      auto_regenerate_days_warning: "9"
      ca_identifier:  "myId_10"
      certificate: "<your_own_value>"
      cmp_path: "<your_own_value>"
      cmp_regeneration_method: "keyupate"
      cmp_server: "<your_own_value>"
      cmp_server_cert: "<your_own_value> (source vpn.certificate.ca.name)"
      comments: "<your_own_value>"
      csr: "<your_own_value>"
      enroll_protocol: "none"
      ike_localid: "<your_own_value>"
      ike_localid_type: "asn1dn"
      last_updated: "21"
      name: "default_name_22"
      name_encoding: "printable"
      password: "<your_own_value>"
      private_key: "<your_own_value>"
      range: "global"
      scep_password: "<your_own_value>"
      scep_url: "<your_own_value>"
      source: "factory"
      source_ip: "84.230.14.43"
      state: "<your_own_value>"
```

6.502.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.502.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.502.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.503 fortios_vpn_certificate_ocsp_server – OCSP server configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.503.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_certificate feature and ocsp_server category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.503.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.503.3 FortiOS Version Compatibility

6.503.4 Parameters

6.503.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.503.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: OCSP server configuration.
    fortios_vpn_certificate_ocsp_server:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_certificate_ocsp_server:
        cert: "<your_own_value> (source vpn.certificate.remote.name vpn.certificate.
↪ca.name)"
        name: "default_name_4"
        secondary_cert: "<your_own_value> (source vpn.certificate.remote.name vpn.
↪certificate.ca.name)"
        secondary_url: "<your_own_value>"
        source_ip: "84.230.14.43"
        unavail_action: "revoke"
        url: "myurl.com"
```

6.503.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.503.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.503.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.504 fortios_vpn_certificate_remote – Remote certificate as a PEM file in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.504.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_certificate feature and remote category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.504.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.504.3 FortiOS Version Compatibility

6.504.4 Parameters

6.504.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.504.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Remote certificate as a PEM file.
    fortios_vpn_certificate_remote:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_certificate_remote:
        name: "default_name_3"
        range: "global"
        remote: "<your_own_value>"
        source: "factory"
```

6.504.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.504.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.504.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.505 fortios_vpn_certificate_setting – VPN certificate setting in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.505.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_certificate feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.505.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.505.3 FortiOS Version Compatibility

6.505.4 Parameters

6.505.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.505.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: VPN certificate setting.
    fortios_vpn_certificate_setting:
      vdom:  "{{ vdom }}"
      vpn_certificate_setting:
        certname_dsa1024: "<your_own_value> (source vpn.certificate.local.name)"
        certname_dsa2048: "<your_own_value> (source vpn.certificate.local.name)"
        certname_ecdsa256: "<your_own_value> (source vpn.certificate.local.name)"
        certname_ecdsa384: "<your_own_value> (source vpn.certificate.local.name)"
        certname_ecdsa521: "<your_own_value> (source vpn.certificate.local.name)"
        certname_ed25519: "<your_own_value> (source vpn.certificate.local.name)"
        certname_ed448: "<your_own_value> (source vpn.certificate.local.name)"
        certname_rsa1024: "<your_own_value> (source vpn.certificate.local.name)"
        certname_rsa2048: "<your_own_value> (source vpn.certificate.local.name)"
        certname_rsa4096: "<your_own_value> (source vpn.certificate.local.name)"
        check_ca_cert: "enable"
        check_ca_chain: "enable"
        cmp_key_usage_checking: "enable"
        cmp_save_extra_certs: "enable"
        cn_match: "substring"
        interface: "<your_own_value> (source system.interface.name)"
        interface_select_method: "auto"
        ocsp_default_server: "<your_own_value> (source vpn.certificate.ocsp-server.
↪name)"
        ocsp_option: "certificate"
        ocsp_status: "enable"
        ssl_min_proto_version: "default"
        ssl_ocsp_option: "certificate"
        ssl_ocsp_source_ip: "<your_own_value>"
        ssl_ocsp_status: "enable"
        strict_crl_check: "enable"
        strict_ocsp_check: "enable"
        subject_match: "substring"
```

6.505.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.505.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.505.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.506 fortios_vpn_ike_gateway – List gateways in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.506.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ike feature and gateway category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.506.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.506.3 FortiOS Version Compatibility

6.506.4 Parameters

6.506.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.506.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: List gateways.
    fortios_vpn_ike_gateway:
      vdom:  "{{ vdom }}"
      vpn_ike_gateway:
        <name>: "<your_own_value>"
```

6.506.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.506.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.506.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.507 fortios_vpn_ipsec_concentrator – Concentrator configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.507.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ipsec feature and concentrator category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.507.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.507.3 FortiOS Version Compatibility

6.507.4 Parameters

6.507.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.507.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Concentrator configuration.
    fortios_vpn_ipsec_concentrator:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_ipsec_concentrator:
        member:
         -
            name: "default_name_4 (source vpn.ipsec.manualkey.name vpn.ipsec.phase1.
↪name)"
        name: "default_name_5"
        src_check: "disable"
```

6.507.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.507.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.507.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.508 fortios_vpn_ipsec_forticlient – Configure FortiClient policy realm in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.508.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ipsec feature and forticlient category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.508.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.508.3 FortiOS Version Compatibility

6.508.4 Parameters

6.508.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.508.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiClient policy realm.
    fortios_vpn_ipsec_forticlient:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_ipsec_forticlient:
        phase2name: "<your_own_value> (source vpn.ipsec.phase2.name vpn.ipsec.phase2-
↪interface.name)"
        realm: "<your_own_value>"
        status: "enable"
        usergroupname: "<your_own_value> (source user.group.name)"
```

6.508.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.508.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.508.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.509 fortios_vpn_ipsec_manualkey – Configure IPsec manual keys in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.509.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ipsec feature and manualkey category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.509.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.509.3 FortiOS Version Compatibility

6.509.4 Parameters

6.509.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.509.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure IPsec manual keys.
  fortios_vpn_ipsec_manualkey:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    vpn_ipsec_manualkey:
      authentication: "null"
      authkey: "<your_own_value>"
      enckey: "<your_own_value>"
      encryption: "null"
      interface: "<your_own_value> (source system.interface.name)"
      local_gw: "<your_own_value>"
      localspi: "<your_own_value>"
      name: "default_name_10"
      npu_offload: "enable"
      remote_gw: "<your_own_value>"
      remotespi: "<your_own_value>"
```

6.509.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.509.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.509.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.510 fortios_vpn_ipsec_manualkey_interface – Configure IPsec manual keys in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.510.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ipsec feature and manualkey_interface category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.510.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.510.3 FortiOS Version Compatibility

6.510.4 Parameters

6.510.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.510.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure IPsec manual keys.
  fortios_vpn_ipsec_manualkey_interface:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    vpn_ipsec_manualkey_interface:
      addr_type: "4"
      auth_alg: "null"
      auth_key: "<your_own_value>"
      enc_alg: "null"
      enc_key: "<your_own_value>"
      interface: "<your_own_value> (source system.interface.name)"
      ip_version: "4"
      local_gw: "<your_own_value>"
      local_gw6: "<your_own_value>"
      local_spi: "<your_own_value>"
      name: "default_name_13"
      npu_offload: "enable"
      remote_gw: "<your_own_value>"
      remote_gw6: "<your_own_value>"
      remote_spi: "<your_own_value>"
```

6.510.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.510.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.510.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.511 fortios_vpn_ipsec_phase1 – Configure VPN remote gateway in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.511.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ipsec feature and phase1 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.511.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.511.3 FortiOS Version Compatibility

6.511.4 Parameters

6.511.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.511.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure VPN remote gateway.
    fortios_vpn_ipsec_phase1:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_ipsec_phase1:
        acct_verify: "enable"
        add_gw_route: "enable"
        add_route: "disable"
        assign_ip: "disable"
        assign_ip_from: "range"
        authmethod: "psk"
        authmethod_remote: "psk"
        authpasswd: "<your_own_value>"
        authusr: "<your_own_value>"
        authusrgrp: "<your_own_value> (source user.group.name)"
        auto_negotiate: "enable"
        backup_gateway:
         -
            address: "<your_own_value>"
        banner: "<your_own_value>"
        cert_id_validation: "enable"
        certificate:
         -
            name: "default_name_19 (source vpn.certificate.local.name)"
        childless_ike: "enable"
        client_auto_negotiate: "disable"
        client_keep_alive: "disable"
        comments: "<your_own_value>"
        dhcp_ra_giaddr: "<your_own_value>"
        dhcp6_ra_linkaddr: "<your_own_value>"
        dhgrp: "1"
        digital_signature_auth: "enable"
        distance: "28"
        dns_mode: "manual"
        domain: "<your_own_value>"
        dpd: "disable"
        dpd_retrycount: "32"
        dpd_retryinterval: "<your_own_value>"
        eap: "enable"
        eap_exclude_peergrp: "<your_own_value> (source user.peergrp.name)"
        eap_identity: "use-id-payload"
        enforce_unique_id: "disable"
        esn: "require"
        fec_base: "39"
        fec_codec: "40"
        fec_egress: "enable"
```

(continues on next page)

(continued from previous page)

```
        fec_ingress: "enable"
        fec_receive_timeout: "43"
        fec_redundant: "44"
        fec_send_timeout: "45"
        forticlient_enforcement: "enable"
        fragmentation: "enable"
        fragmentation_mtu: "48"
        group_authentication: "enable"
        group_authentication_secret: "<your_own_value>"
        ha_sync_esp_seqno: "enable"
        idle_timeout: "enable"
        idle_timeoutinterval: "53"
        ike_version: "1"
        include_local_lan: "disable"
        interface: "<your_own_value> (source system.interface.name)"
        ipv4_dns_server1: "<your_own_value>"
        ipv4_dns_server2: "<your_own_value>"
        ipv4_dns_server3: "<your_own_value>"
        ipv4_end_ip: "<your_own_value>"
        ipv4_exclude_range:
         -
            end_ip: "<your_own_value>"
            id:  "63"
            start_ip: "<your_own_value>"
        ipv4_name: "<your_own_value> (source firewall.address.name firewall.addrgrp.
↪name)"
        ipv4_netmask: "<your_own_value>"
        ipv4_split_exclude: "<your_own_value> (source firewall.address.name firewall.
↪addrgrp.name)"
        ipv4_split_include: "<your_own_value> (source firewall.address.name firewall.
↪addrgrp.name)"
        ipv4_start_ip: "<your_own_value>"
        ipv4_wins_server1: "<your_own_value>"
        ipv4_wins_server2: "<your_own_value>"
        ipv6_dns_server1: "<your_own_value>"
        ipv6_dns_server2: "<your_own_value>"
        ipv6_dns_server3: "<your_own_value>"
        ipv6_end_ip: "<your_own_value>"
        ipv6_exclude_range:
         -
            end_ip: "<your_own_value>"
            id:  "78"
            start_ip: "<your_own_value>"
        ipv6_name: "<your_own_value> (source firewall.address6.name firewall.addrgrp6.
↪name)"
        ipv6_prefix: "81"
        ipv6_split_exclude: "<your_own_value> (source firewall.address6.name firewall.
↪addrgrp6.name)"
        ipv6_split_include: "<your_own_value> (source firewall.address6.name firewall.
↪addrgrp6.name)"
        ipv6_start_ip: "<your_own_value>"
        keepalive: "85"
        keylife: "86"
        local_gw: "<your_own_value>"
        localid: "<your_own_value>"
        localid_type: "auto"
        loopback_asymroute: "enable"
```

(continues on next page)

(continued from previous page)

```
        mesh_selector_type: "disable"
        mode: "aggressive"
        mode_cfg: "disable"
        name: "default_name_94"
        nattraversal: "enable"
        negotiate_timeout: "96"
        network_id: "97"
        network_overlay: "disable"
        npu_offload: "enable"
        peer: "<your_own_value> (source user.peer.name)"
        peergrp: "<your_own_value> (source user.peergrp.name)"
        peerid: "<your_own_value>"
        peertype: "any"
        ppk: "disable"
        ppk_identity: "<your_own_value>"
        ppk_secret: "<your_own_value>"
        priority: "107"
        proposal: "des-md5"
        psksecret: "<your_own_value>"
        psksecret_remote: "<your_own_value>"
        reauth: "disable"
        rekey: "enable"
        remote_gw: "<your_own_value>"
        remotegw_ddns: "<your_own_value>"
        rsa_signature_format: "pkcs1"
        save_password: "disable"
        send_cert_chain: "enable"
        signature_hash_alg: "sha1"
        split_include_service: "<your_own_value> (source firewall.service.group.name␣
↪firewall.service.custom.name)"
        suite_b: "disable"
        type: "static"
        unity_support: "disable"
        usrgrp: "<your_own_value> (source user.group.name)"
        wizard_type: "custom"
        xauthtype: "disable"
```

6.511.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.511.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.511.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.512 fortios_vpn_ipsec_phase1_interface – Configure VPN remote gateway in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.512.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ipsec feature and phase1_interface category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.512.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.512.3 FortiOS Version Compatibility

6.512.4 Parameters

6.512.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.512.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure VPN remote gateway.
    fortios_vpn_ipsec_phase1_interface:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_ipsec_phase1_interface:
        acct_verify: "enable"
        add_gw_route: "enable"
        add_route: "disable"
        aggregate_member: "enable"
        aggregate_weight: "7"
        assign_ip: "disable"
        assign_ip_from: "range"
        authmethod: "psk"
        authmethod_remote: "psk"
        authpasswd: "<your_own_value>"
        authusr: "<your_own_value>"
        authusrgrp: "<your_own_value> (source user.group.name)"
        auto_discovery_forwarder: "enable"
        auto_discovery_psk: "enable"
        auto_discovery_receiver: "enable"
        auto_discovery_sender: "enable"
        auto_discovery_shortcuts: "independent"
        auto_negotiate: "enable"
        backup_gateway:
         -
            address: "<your_own_value>"
        banner: "<your_own_value>"
        cert_id_validation: "enable"
        certificate:
         -
            name: "default_name_26 (source vpn.certificate.local.name)"
        childless_ike: "enable"
        client_auto_negotiate: "disable"
        client_keep_alive: "disable"
        comments: "<your_own_value>"
        default_gw: "<your_own_value>"
        default_gw_priority: "32"
        dhcp_ra_giaddr: "<your_own_value>"
        dhcp6_ra_linkaddr: "<your_own_value>"
        dhgrp: "1"
```

(continues on next page)

(continued from previous page)

```
        digital_signature_auth: "enable"
        distance: "37"
        dns_mode: "manual"
        domain: "<your_own_value>"
        dpd: "disable"
        dpd_retrycount: "41"
        dpd_retryinterval: "<your_own_value>"
        eap: "enable"
        eap_exclude_peergrp: "<your_own_value> (source user.peergrp.name)"
        eap_identity: "use-id-payload"
        encap_local_gw4: "<your_own_value>"
        encap_local_gw6: "<your_own_value>"
        encap_remote_gw4: "<your_own_value>"
        encap_remote_gw6: "<your_own_value>"
        encapsulation: "none"
        encapsulation_address: "ike"
        enforce_unique_id: "disable"
        esn: "require"
        exchange_interface_ip: "enable"
        exchange_ip_addr4: "<your_own_value>"
        exchange_ip_addr6: "<your_own_value>"
        fec_base: "57"
        fec_codec: "58"
        fec_egress: "enable"
        fec_ingress: "enable"
        fec_receive_timeout: "61"
        fec_redundant: "62"
        fec_send_timeout: "63"
        forticlient_enforcement: "enable"
        fragmentation: "enable"
        fragmentation_mtu: "66"
        group_authentication: "enable"
        group_authentication_secret: "<your_own_value>"
        ha_sync_esp_seqno: "enable"
        idle_timeout: "enable"
        idle_timeoutinterval: "71"
        ike_version: "1"
        include_local_lan: "disable"
        interface: "<your_own_value> (source system.interface.name)"
        ip_fragmentation: "pre-encapsulation"
        ip_version: "4"
        ipv4_dns_server1: "<your_own_value>"
        ipv4_dns_server2: "<your_own_value>"
        ipv4_dns_server3: "<your_own_value>"
        ipv4_end_ip: "<your_own_value>"
        ipv4_exclude_range:
         -
            end_ip: "<your_own_value>"
            id:  "83"
            start_ip: "<your_own_value>"
        ipv4_name: "<your_own_value> (source firewall.address.name firewall.addrgrp.
↪name)"
        ipv4_netmask: "<your_own_value>"
        ipv4_split_exclude: "<your_own_value> (source firewall.address.name firewall.
↪addrgrp.name)"
        ipv4_split_include: "<your_own_value> (source firewall.address.name firewall.
↪addrgrp.name)"
```

(continues on next page)

(continued from previous page)

```
        ipv4_start_ip: "<your_own_value>"
        ipv4_wins_server1: "<your_own_value>"
        ipv4_wins_server2: "<your_own_value>"
        ipv6_dns_server1: "<your_own_value>"
        ipv6_dns_server2: "<your_own_value>"
        ipv6_dns_server3: "<your_own_value>"
        ipv6_end_ip: "<your_own_value>"
        ipv6_exclude_range:
         -
            end_ip: "<your_own_value>"
            id:  "98"
            start_ip: "<your_own_value>"
        ipv6_name: "<your_own_value> (source firewall.address6.name firewall.addrgrp6.
↪name)"
        ipv6_prefix: "101"
        ipv6_split_exclude: "<your_own_value> (source firewall.address6.name firewall.
↪addrgrp6.name)"
        ipv6_split_include: "<your_own_value> (source firewall.address6.name firewall.
↪addrgrp6.name)"
        ipv6_start_ip: "<your_own_value>"
        keepalive: "105"
        keylife: "106"
        local_gw: "<your_own_value>"
        local_gw6: "<your_own_value>"
        localid: "<your_own_value>"
        localid_type: "auto"
        loopback_asymroute: "enable"
        mesh_selector_type: "disable"
        mode: "aggressive"
        mode_cfg: "disable"
        monitor: "<your_own_value> (source vpn.ipsec.phase1-interface.name)"
        monitor_hold_down_delay: "116"
        monitor_hold_down_time: "<your_own_value>"
        monitor_hold_down_type: "immediate"
        monitor_hold_down_weekday: "everyday"
        name: "default_name_120"
        nattraversal: "enable"
        negotiate_timeout: "122"
        net_device: "enable"
        network_id: "124"
        network_overlay: "disable"
        npu_offload: "enable"
        passive_mode: "enable"
        peer: "<your_own_value> (source user.peer.name)"
        peergrp: "<your_own_value> (source user.peergrp.name)"
        peerid: "<your_own_value>"
        peertype: "any"
        ppk: "disable"
        ppk_identity: "<your_own_value>"
        ppk_secret: "<your_own_value>"
        priority: "135"
        proposal: "des-md5"
        psksecret: "<your_own_value>"
        psksecret_remote: "<your_own_value>"
        reauth: "disable"
        rekey: "enable"
        remote_gw: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        remote_gw6: "<your_own_value>"
        remotegw_ddns: "<your_own_value>"
        rsa_signature_format: "pkcs1"
        save_password: "disable"
        send_cert_chain: "enable"
        signature_hash_alg: "sha1"
        split_include_service: "<your_own_value> (source firewall.service.group.name␣
↪firewall.service.custom.name)"
        suite_b: "disable"
        tunnel_search: "selectors"
        type: "static"
        unity_support: "disable"
        usrgrp: "<your_own_value> (source user.group.name)"
        vni: "154"
        wizard_type: "custom"
        xauthtype: "disable"
```

6.512.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.512.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.512.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.513 fortios_vpn_ipsec_phase2 – Configure VPN autokey tunnel in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.513.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ipsec feature and phase2 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.513.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.513.3 FortiOS Version Compatibility

6.513.4 Parameters

6.513.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.513.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
```

(continues on next page)

(continued from previous page)

```
  tasks:
  - name: Configure VPN autokey tunnel.
    fortios_vpn_ipsec_phase2:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_ipsec_phase2:
        add_route: "phase1"
        auto_negotiate: "enable"
        comments: "<your_own_value>"
        dhcp_ipsec: "enable"
        dhgrp: "1"
        diffserv: "enable"
        diffservcode: "<your_own_value>"
        dst_addr_type: "subnet"
        dst_end_ip: "<your_own_value>"
        dst_end_ip6: "<your_own_value>"
        dst_name: "<your_own_value> (source firewall.address.name firewall.addrgrp.
↪name)"
        dst_name6: "<your_own_value> (source firewall.address6.name firewall.addrgrp6.
↪name)"
        dst_port: "15"
        dst_start_ip: "<your_own_value>"
        dst_start_ip6: "<your_own_value>"
        dst_subnet: "<your_own_value>"
        dst_subnet6: "<your_own_value>"
        encapsulation: "tunnel-mode"
        initiator_ts_narrow: "enable"
        ipv4_df: "enable"
        keepalive: "enable"
        keylife_type: "seconds"
        keylifekbs: "25"
        keylifeseconds: "26"
        l2tp: "enable"
        name: "default_name_28"
        pfs: "enable"
        phase1name: "<your_own_value> (source vpn.ipsec.phase1.name)"
        proposal: "null-md5"
        protocol: "32"
        replay: "enable"
        route_overlap: "use-old"
        selector_match: "exact"
        single_source: "enable"
        src_addr_type: "subnet"
        src_end_ip: "<your_own_value>"
        src_end_ip6: "<your_own_value>"
        src_name: "<your_own_value> (source firewall.address.name firewall.addrgrp.
↪name)"
        src_name6: "<your_own_value> (source firewall.address6.name firewall.addrgrp6.
↪name)"
        src_port: "42"
        src_start_ip: "<your_own_value>"
        src_start_ip6: "<your_own_value>"
        src_subnet: "<your_own_value>"
        src_subnet6: "<your_own_value>"
        use_natip: "enable"
```

6.513.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.513.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.513.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.514 fortios_vpn_ipsec_phase2_interface – Configure VPN autokey tunnel in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.514.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ipsec feature and phase2_interface category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.514.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.514.3 FortiOS Version Compatibility

6.514.4 Parameters

6.514.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.514.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure VPN autokey tunnel.
    fortios_vpn_ipsec_phase2_interface:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_ipsec_phase2_interface:
        add_route: "phase1"
        auto_discovery_forwarder: "phase1"
        auto_discovery_sender: "phase1"
        auto_negotiate: "enable"
        comments: "<your_own_value>"
        dhcp_ipsec: "enable"
        dhgrp: "1"
        diffserv: "enable"
        diffservcode: "<your_own_value>"
        dst_addr_type: "subnet"
        dst_end_ip: "<your_own_value>"
        dst_end_ip6: "<your_own_value>"
        dst_name: "<your_own_value> (source firewall.address.name firewall.addrgrp.
↪name)"
        dst_name6: "<your_own_value> (source firewall.address6.name firewall.addrgrp6.
↪name)"
        dst_port: "17"
        dst_start_ip: "<your_own_value>"
        dst_start_ip6: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        dst_subnet: "<your_own_value>"
        dst_subnet6: "<your_own_value>"
        encapsulation: "tunnel-mode"
        initiator_ts_narrow: "enable"
        ipv4_df: "enable"
        keepalive: "enable"
        keylife_type: "seconds"
        keylifekbs: "27"
        keylifeseconds: "28"
        l2tp: "enable"
        name: "default_name_30"
        pfs: "enable"
        phase1name: "<your_own_value> (source vpn.ipsec.phase1-interface.name)"
        proposal: "null-md5"
        protocol: "34"
        replay: "enable"
        route_overlap: "use-old"
        single_source: "enable"
        src_addr_type: "subnet"
        src_end_ip: "<your_own_value>"
        src_end_ip6: "<your_own_value>"
        src_name: "<your_own_value> (source firewall.address.name firewall.addrgrp.
↪name)"
        src_name6: "<your_own_value> (source firewall.address6.name firewall.addrgrp6.
↪name)"
        src_port: "43"
        src_start_ip: "<your_own_value>"
        src_start_ip6: "<your_own_value>"
        src_subnet: "<your_own_value>"
        src_subnet6: "<your_own_value>"
```

6.514.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.514.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.514.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.515 fortios_vpn_l2tp – Configure L2TP in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.515.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn feature and l2tp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.515.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.515.3 FortiOS Version Compatibility

6.515.4 Parameters

6.515.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.515.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure L2TP.
    fortios_vpn_l2tp:
      vdom:  "{{ vdom }}"
      vpn_l2tp:
        compress: "enable"
        eip: "<your_own_value>"
        enforce_ipsec: "enable"
        lcp_echo_interval: "6"
        lcp_max_echo_fails: "7"
        sip: "<your_own_value>"
        status: "enable"
        usrgrp: "<your_own_value> (source user.group.name)"
```

6.515.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.515.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.515.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.516 fortios_vpn_ocvpn – Configure Overlay Controller VPN settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.516.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn feature and ocvpn category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.516.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.516.3 FortiOS Version Compatibility

6.516.4 Parameters

6.516.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.516.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Overlay Controller VPN settings.
    fortios_vpn_ocvpn:
      vdom:  "{{ vdom }}"
      vpn_ocvpn:
        auto_discovery: "enable"
        eap: "enable"
        eap_users: "<your_own_value> (source user.group.name)"
        forticlient_access:
            auth_groups:
             -
                auth_group: "<your_own_value> (source user.group.name)"
                name: "default_name_9"
                overlays:
                 -
                    overlay_name: "<your_own_value> (source vpn.ocvpn.overlays.
↪overlay-name)"
            psksecret: "<your_own_value>"
            status: "enable"
        ha_alias: "<your_own_value>"
        ip_allocation_block: "<your_own_value>"
        multipath: "enable"
        nat: "enable"
        overlays:
         -
            assign_ip: "enable"
            id:  "20"
            inter_overlay: "allow"
            ipv4_end_ip: "<your_own_value>"
            ipv4_start_ip: "<your_own_value>"
            name: "default_name_24"
            overlay_name: "<your_own_value>"
            subnets:
             -
                id:  "27"
                interface: "<your_own_value> (source system.interface.name)"
                subnet: "<your_own_value>"
                type: "subnet"
        poll_interval: "31"
        role: "spoke"
        sdwan: "enable"
        sdwan_zone: "<your_own_value> (source system.sdwan.zone.name)"
        status: "enable"
        subnets:
         -
            id:  "37"
            interface: "<your_own_value> (source system.interface.name)"
            subnet: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        type: "subnet"
    wan_interface:
     -
        name: "default_name_42 (source system.interface.name)"
```

6.516.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.516.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.516.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.517 fortios_vpn_pptp – Configure PPTP in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.517.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn feature and pptp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.517.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.517.3 FortiOS Version Compatibility

6.517.4 Parameters

6.517.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.517.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure PPTP.
    fortios_vpn_pptp:
      vdom:  "{{ vdom }}"
      vpn_pptp:
        eip: "<your_own_value>"
        ip_mode: "range"
        local_ip: "<your_own_value>"
        sip: "<your_own_value>"
        status: "enable"
        usrgrp: "<your_own_value> (source user.group.name)"
```

6.517.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.517.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.517.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.518 fortios_vpn_ssl_client – clien in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.518.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ssl feature and client category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.518.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.518.3 FortiOS Version Compatibility

6.518.4 Parameters

6.518.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.518.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: client
    fortios_vpn_ssl_client:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_ssl_client:
        certificate: "<your_own_value> (source vpn.certificate.local.name)"
        comment: "Comment."
        distance: "5"
        interface: "<your_own_value> (source system.interface.name)"
        name: "default_name_7"
        peer: "<your_own_value> (source user.peer.name user.peergrp.name)"
        port: "9"
        priority: "10"
        psk: "<your_own_value>"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        status: "enable"
        user: "<your_own_value>"
```

6.518.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.518.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.518.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.519 fortios_vpn_ssl_settings – Configure SSL VPN in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.519.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ssl feature and settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.519.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.519.3 FortiOS Version Compatibility

6.519.4 Parameters

6.519.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.519.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure SSL VPN.
    fortios_vpn_ssl_settings:
      vdom:  "{{ vdom }}"
      vpn_ssl_settings:
        algorithm: "high"
        auth_session_check_source_ip: "enable"
        auth_timeout: "5"
        authentication_rule:
         -
            auth: "any"
            cipher: "any"
            client_cert: "enable"
            groups:
             -
                name: "default_name_11 (source user.group.name)"
            id:  "12"
            portal: "<your_own_value> (source vpn.ssl.web.portal.name)"
            realm: "<your_own_value> (source vpn.ssl.web.realm.url-path)"
            source_address:
             -
                name: "default_name_16 (source firewall.address.name firewall.addrgrp.
↪name)"
            source_address_negate: "enable"
            source_address6:
             -
                name: "default_name_19 (source firewall.address6.name firewall.
↪addrgrp6.name)"
            source_address6_negate: "enable"
```

(continues on next page)

(continued from previous page)

```
            source_interface:
             -
                name: "default_name_22 (source system.interface.name system.zone.name)
↪"
            user_peer: "<your_own_value> (source user.peer.name)"
            users:
             -
                name: "default_name_25 (source user.local.name)"
        auto_tunnel_static_route: "enable"
        banned_cipher: "RSA"
        check_referer: "enable"
        ciphersuite: "TLS-AES-128-GCM-SHA256"
        client_sigalgs: "no-rsa-pss"
        default_portal: "<your_own_value> (source vpn.ssl.web.portal.name)"
        deflate_compression_level: "32"
        deflate_min_data_size: "33"
        dns_server1: "<your_own_value>"
        dns_server2: "<your_own_value>"
        dns_suffix: "<your_own_value>"
        dtls_hello_timeout: "37"
        dtls_max_proto_ver: "dtls1-0"
        dtls_min_proto_ver: "dtls1-0"
        dtls_tunnel: "enable"
        dual_stack_mode: "enable"
        encode_2f_sequence: "enable"
        encrypt_and_store_password: "enable"
        force_two_factor_auth: "enable"
        header_x_forwarded_for: "pass"
        hsts_include_subdomains: "enable"
        http_compression: "enable"
        http_only_cookie: "enable"
        http_request_body_timeout: "49"
        http_request_header_timeout: "50"
        https_redirect: "enable"
        idle_timeout: "52"
        ipv6_dns_server1: "<your_own_value>"
        ipv6_dns_server2: "<your_own_value>"
        ipv6_wins_server1: "<your_own_value>"
        ipv6_wins_server2: "<your_own_value>"
        login_attempt_limit: "57"
        login_block_time: "58"
        login_timeout: "59"
        port: "60"
        port_precedence: "enable"
        reqclientcert: "enable"
        route_source_interface: "enable"
        servercert: "<your_own_value> (source vpn.certificate.local.name)"
        source_address:
         -
            name: "default_name_66 (source firewall.address.name firewall.addrgrp.
↪name)"
        source_address_negate: "enable"
        source_address6:
         -
            name: "default_name_69 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        source_address6_negate: "enable"
```

(continues on next page)

(continued from previous page)

```
        source_interface:
         -
            name: "default_name_72 (source system.interface.name system.zone.name)"
        ssl_client_renegotiation: "disable"
        ssl_insert_empty_fragment: "enable"
        ssl_max_proto_ver: "tls1-0"
        ssl_min_proto_ver: "tls1-0"
        tlsv1_0: "enable"
        tlsv1_1: "enable"
        tlsv1_2: "enable"
        tlsv1_3: "enable"
        transform_backward_slashes: "enable"
        tunnel_addr_assigned_method: "first-available"
        tunnel_connect_without_reauth: "enable"
        tunnel_ip_pools:
         -
            name: "default_name_85 (source firewall.address.name firewall.addrgrp.
↪name)"
        tunnel_ipv6_pools:
         -
            name: "default_name_87 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        tunnel_user_session_timeout: "88"
        unsafe_legacy_renegotiation: "enable"
        url_obscuration: "enable"
        user_peer: "<your_own_value> (source user.peer.name)"
        wins_server1: "<your_own_value>"
        wins_server2: "<your_own_value>"
        x_content_type_options: "enable"
```

6.519.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.519.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.519.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.520 fortios_vpn_ssl_web_host_check_software – SSL-VPN host check software in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.520.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ssl_web feature and host_check_software category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.520.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.520.3 FortiOS Version Compatibility

6.520.4 Parameters

6.520.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.520.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: SSL-VPN host check software.
    fortios_vpn_ssl_web_host_check_software:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_ssl_web_host_check_software:
        check_item_list:
         -
            action: "require"
            id:  "5"
            md5s:
             -
                id:  "7"
            target: "<your_own_value>"
            type: "file"
            version: "<your_own_value>"
        guid: "<your_own_value>"
        name: "default_name_12"
        os_type: "windows"
        type: "av"
        version: "<your_own_value>"
```

6.520.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.520.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.520.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.521 fortios_vpn_ssl_web_portal – Portal in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.521.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ssl_web feature and portal category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.521.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.521.3 FortiOS Version Compatibility

6.521.4 Parameters

6.521.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.521.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Portal.
    fortios_vpn_ssl_web_portal:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_ssl_web_portal:
        allow_user_access: "web"
        auto_connect: "enable"
        bookmark_group:
         -
            bookmarks:
             -
                additional_params: "<your_own_value>"
                apptype: "citrix"
                description: "<your_own_value>"
                domain: "<your_own_value>"
                folder: "<your_own_value>"
                form_data:
                 -
                    name: "default_name_13"
                    value: "<your_own_value>"
                host: "<your_own_value>"
                listening_port: "16"
                load_balancing_info: "<your_own_value>"
                logon_password: "<your_own_value>"
                logon_user: "<your_own_value>"
                name: "default_name_20"
                port: "21"
                preconnection_blob: "<your_own_value>"
                preconnection_id: "23"
                remote_port: "24"
                security: "rdp"
                server_layout: "de-de-qwertz"
                show_status_window: "enable"
                sso: "disable"
                sso_credential: "sslvpn-login"
                sso_credential_sent_once: "enable"
                sso_password: "<your_own_value>"
                sso_username: "<your_own_value>"
                url: "myurl.com"
            name: "default_name_34"
        custom_lang: "<your_own_value> (source system.custom-language.name)"
        customize_forticlient_download_url: "enable"
        display_bookmark: "enable"
        display_connection_tools: "enable"
```

(continues on next page)

(continued from previous page)

```
        display_history: "enable"
        display_status: "enable"
        dns_server1: "<your_own_value>"
        dns_server2: "<your_own_value>"
        dns_suffix: "<your_own_value>"
        exclusive_routing: "enable"
        forticlient_download: "enable"
        forticlient_download_method: "direct"
        heading: "<your_own_value>"
        hide_sso_credential: "enable"
        host_check: "none"
        host_check_interval: "50"
        host_check_policy:
         -
            name: "default_name_52 (source vpn.ssl.web.host-check-software.name)"
        ip_mode: "range"
        ip_pools:
         -
            name: "default_name_55 (source firewall.address.name firewall.addrgrp.
↪name)"
        ipv6_dns_server1: "<your_own_value>"
        ipv6_dns_server2: "<your_own_value>"
        ipv6_exclusive_routing: "enable"
        ipv6_pools:
         -
            name: "default_name_60 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        ipv6_service_restriction: "enable"
        ipv6_split_tunneling: "enable"
        ipv6_split_tunneling_routing_address:
         -
            name: "default_name_64 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        ipv6_split_tunneling_routing_negate: "enable"
        ipv6_tunnel_mode: "enable"
        ipv6_wins_server1: "<your_own_value>"
        ipv6_wins_server2: "<your_own_value>"
        keep_alive: "enable"
        limit_user_logins: "enable"
        mac_addr_action: "allow"
        mac_addr_check: "enable"
        mac_addr_check_rule:
         -
            mac_addr_list:
             -
                addr: "<your_own_value>"
            mac_addr_mask: "76"
            name: "default_name_77"
        macos_forticlient_download_url: "<your_own_value>"
        name: "default_name_79"
        os_check: "enable"
        os_check_list:
         -
            action: "deny"
            latest_patch_level: "<your_own_value>"
            name: "default_name_84"
            tolerance: "85"
```

(continues on next page)

(continued from previous page)

```
        prefer_ipv6_dns: "enable"
        redir_url: "<your_own_value>"
        rewrite_ip_uri_ui: "enable"
        save_password: "enable"
        service_restriction: "enable"
        skip_check_for_browser: "enable"
        skip_check_for_unsupported_browser: "enable"
        skip_check_for_unsupported_os: "enable"
        smb_max_version: "smbv1"
        smb_min_version: "smbv1"
        smb_ntlmv1_auth: "enable"
        smbv1: "enable"
        split_dns:
         -
            dns_server1: "<your_own_value>"
            dns_server2: "<your_own_value>"
            domains: "<your_own_value>"
            id:  "102"
            ipv6_dns_server1: "<your_own_value>"
            ipv6_dns_server2: "<your_own_value>"
        split_tunneling: "enable"
        split_tunneling_routing_address:
         -
            name: "default_name_107 (source firewall.address.name firewall.addrgrp.
↪name)"
        split_tunneling_routing_negate: "enable"
        theme: "blue"
        transform_backward_slashes: "enable"
        tunnel_mode: "enable"
        use_sdwan: "enable"
        user_bookmark: "enable"
        user_group_bookmark: "enable"
        web_mode: "enable"
        windows_forticlient_download_url: "<your_own_value>"
        wins_server1: "<your_own_value>"
        wins_server2: "<your_own_value>"
```

6.521.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.521.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.521.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.522 fortios_vpn_ssl_web_realm – Realm in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.522.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ssl_web feature and realm category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.522.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.522.3 FortiOS Version Compatibility

6.522.4 Parameters

6.522.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.522.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Realm.
    fortios_vpn_ssl_web_realm:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_ssl_web_realm:
        login_page: "<your_own_value>"
        max_concurrent_user: "4"
        nas_ip: "<your_own_value>"
        radius_port: "6"
        radius_server: "<your_own_value> (source user.radius.name)"
        url_path: "<your_own_value>"
        virtual_host: "<your_own_value>"
        virtual_host_only: "enable"
```

6.522.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.522.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.522.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.523 fortios_vpn_ssl_web_user_bookmark – Configure SSL VPN user bookmark in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.523.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ssl_web feature and user_bookmark category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.523.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.523.3 FortiOS Version Compatibility

6.523.4 Parameters

6.523.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.523.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure SSL VPN user bookmark.
    fortios_vpn_ssl_web_user_bookmark:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_ssl_web_user_bookmark:
        bookmarks:
         -
            additional_params: "<your_own_value>"
            apptype: "citrix"
            description: "<your_own_value>"
            domain: "<your_own_value>"
            folder: "<your_own_value>"
            form_data:
             -
                name: "default_name_10"
                value: "<your_own_value>"
            host: "<your_own_value>"
            listening_port: "13"
            load_balancing_info: "<your_own_value>"
            logon_password: "<your_own_value>"
            logon_user: "<your_own_value>"
            name: "default_name_17"
            port: "18"
            preconnection_blob: "<your_own_value>"
            preconnection_id: "20"
            remote_port: "21"
            security: "rdp"
            server_layout: "de-de-qwertz"
            show_status_window: "enable"
            sso: "disable"
            sso_credential: "sslvpn-login"
            sso_credential_sent_once: "enable"
            sso_password: "<your_own_value>"
            sso_username: "<your_own_value>"
            url: "myurl.com"
        custom_lang: "<your_own_value> (source system.custom-language.name)"
        name: "default_name_32"
```

6.523.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.523.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.523.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.524 fortios_vpn_ssl_web_user_group_bookmark – Configure SSL VPN user group bookmark in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.524.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify vpn_ssl_web feature and user_group_bookmark category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.524.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.524.3 FortiOS Version Compatibility

6.524.4 Parameters

6.524.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.524.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure SSL VPN user group bookmark.
    fortios_vpn_ssl_web_user_group_bookmark:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_ssl_web_user_group_bookmark:
        bookmarks:
         -
            additional_params: "<your_own_value>"
            apptype: "citrix"
            description: "<your_own_value>"
            domain: "<your_own_value>"
            folder: "<your_own_value>"
            form_data:
             -
                name: "default_name_10"
                value: "<your_own_value>"
            host: "<your_own_value>"
            listening_port: "13"
            load_balancing_info: "<your_own_value>"
            logon_password: "<your_own_value>"
            logon_user: "<your_own_value>"
            name: "default_name_17"
            port: "18"
            preconnection_blob: "<your_own_value>"
            preconnection_id: "20"
            remote_port: "21"
            security: "rdp"
```

(continues on next page)

(continued from previous page)

```
            server_layout: "de-de-qwertz"
            show_status_window: "enable"
            sso: "disable"
            sso_credential: "sslvpn-login"
            sso_credential_sent_once: "enable"
            sso_password: "<your_own_value>"
            sso_username: "<your_own_value>"
            url: "myurl.com"
        name: "default_name_31 (source user.group.name)"
```

6.524.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.524.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.524.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.525 fortios_waf_main_class – Hidden table for datasource in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.525.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify waf feature and main_class category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.525.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.525.3 FortiOS Version Compatibility

6.525.4 Parameters

6.525.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.525.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Hidden table for datasource.
    fortios_waf_main_class:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      waf_main_class:
        id:  "3"
        name: "default_name_4"
```

6.525.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.525.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.525.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.526 fortios_waf_profile – Web application firewall configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.526.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify waf feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.526.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.526.3 FortiOS Version Compatibility

6.526.4 Parameters

6.526.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.526.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Web application firewall configuration.
    fortios_waf_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      waf_profile:
        address_list:
            blocked_address:
             -
                name: "default_name_5 (source firewall.address.name firewall.addrgrp.
↪name)"
            blocked_log: "enable"
            severity: "high"
            status: "enable"
            trusted_address:
             -
                name: "default_name_10 (source firewall.address.name firewall.addrgrp.
↪name)"
        comment: "Comment."
        constraint:
            content_length:
                action: "allow"
                length: "15"
                log: "enable"
                severity: "high"
```

(continues on next page)

(continued from previous page)

```
                status: "enable"
            exception:
             -
                address: "<your_own_value> (source firewall.address.name firewall.
↪addrgrp.name)"
                content_length: "enable"
                header_length: "enable"
                hostname: "enable"
                id:  "24"
                line_length: "enable"
                malformed: "enable"
                max_cookie: "enable"
                max_header_line: "enable"
                max_range_segment: "enable"
                max_url_param: "enable"
                method: "enable"
                param_length: "enable"
                pattern: "<your_own_value>"
                regex: "enable"
                url_param_length: "enable"
                version: "enable"
            header_length:
                action: "allow"
                length: "39"
                log: "enable"
                severity: "high"
                status: "enable"
            hostname:
                action: "allow"
                log: "enable"
                severity: "high"
                status: "enable"
            line_length:
                action: "allow"
                length: "50"
                log: "enable"
                severity: "high"
                status: "enable"
            malformed:
                action: "allow"
                log: "enable"
                severity: "high"
                status: "enable"
            max_cookie:
                action: "allow"
                log: "enable"
                max_cookie: "62"
                severity: "high"
                status: "enable"
            max_header_line:
                action: "allow"
                log: "enable"
                max_header_line: "68"
                severity: "high"
                status: "enable"
            max_range_segment:
                action: "allow"
```

(continues on next page)

(continued from previous page)

```
                log: "enable"
                max_range_segment: "74"
                severity: "high"
                status: "enable"
            max_url_param:
                action: "allow"
                log: "enable"
                max_url_param: "80"
                severity: "high"
                status: "enable"
            method:
                action: "allow"
                log: "enable"
                severity: "high"
                status: "enable"
            param_length:
                action: "allow"
                length: "90"
                log: "enable"
                severity: "high"
                status: "enable"
            url_param_length:
                action: "allow"
                length: "96"
                log: "enable"
                severity: "high"
                status: "enable"
            version:
                action: "allow"
                log: "enable"
                severity: "high"
                status: "enable"
        extended_log: "enable"
        external: "disable"
        method:
            default_allowed_methods: "get"
            log: "enable"
            method_policy:
             -
                address: "<your_own_value> (source firewall.address.name firewall.
↪addrgrp.name)"
                allowed_methods: "get"
                id:  "113"
                pattern: "<your_own_value>"
                regex: "enable"
            severity: "high"
            status: "enable"
        name: "default_name_118"
        signature:
            credit_card_detection_threshold: "120"
            custom_signature:
             -
                action: "allow"
                case_sensitivity: "disable"
                direction: "request"
                log: "enable"
                name: "default_name_126"
```

(continues on next page)

(continued from previous page)

```
                pattern: "<your_own_value>"
                severity: "high"
                status: "enable"
                target: "arg"
            disabled_signature:
             -
                id:  "132 (source waf.signature.id)"
            disabled_sub_class:
             -
                id:  "134 (source waf.sub-class.id)"
            main_class:
             -
                action: "allow"
                id:  "137 (source waf.main-class.id)"
                log: "enable"
                severity: "high"
                status: "enable"
        url_access:
         -
            access_pattern:
             -
                id:  "143"
                negate: "enable"
                pattern: "<your_own_value>"
                regex: "enable"
                srcaddr: "<your_own_value> (source firewall.address.name firewall.
↪addrgrp.name)"
            action: "bypass"
            address: "<your_own_value> (source firewall.address.name firewall.addrgrp.
↪name)"
            id:  "150"
            log: "enable"
            severity: "high"
```

6.526.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.526.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.526.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.527 fortios_waf_signature – Hidden table for datasource in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.527.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify waf feature and signature category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.527.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.527.3 FortiOS Version Compatibility

6.527.4 Parameters

6.527.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.527.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Hidden table for datasource.
    fortios_waf_signature:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      waf_signature:
        desc: "<your_own_value>"
        id:  "4"
```

6.527.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.527.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.527.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.528 fortios_waf_sub_class – Hidden table for datasource in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.528.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify waf feature and sub_class category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.528.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.528.3 FortiOS Version Compatibility

6.528.4 Parameters

6.528.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.528.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Hidden table for datasource.
  fortios_waf_sub_class:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    waf_sub_class:
      id:  "3"
      name: "default_name_4"
```

6.528.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.528.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.528.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.529 fortios_wanopt_auth_group – Configure WAN optimization authentication groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.529.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wanopt feature and auth_group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.529.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.529.3 FortiOS Version Compatibility

6.529.4 Parameters

6.529.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.529.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure WAN optimization authentication groups.
    fortios_wanopt_auth_group:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wanopt_auth_group:
```

(continues on next page)

(continued from previous page)

```
        auth_method: "cert"
        cert: "<your_own_value> (source vpn.certificate.local.name)"
        name: "default_name_5"
        peer: "<your_own_value> (source wanopt.peer.peer-host-id)"
        peer_accept: "any"
        psk: "<your_own_value>"
```

6.529.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.529.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.529.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.530 fortios_wanopt_cache_service – Designate cache-service for wan-optimization and webcache in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.530.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wanopt feature and cache_service category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.530.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.530.3 FortiOS Version Compatibility

6.530.4 Parameters

6.530.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.530.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Designate cache-service for wan-optimization and webcache.
    fortios_wanopt_cache_service:
      vdom:  "{{ vdom }}"
      wanopt_cache_service:
        acceptable_connections: "any"
        collaboration: "enable"
        device_id: "<your_own_value>"
        dst_peer:
         -
            auth_type: "7"
```

(continues on next page)

(continued from previous page)

```
            device_id: "<your_own_value>"
            encode_type: "9"
            ip: "<your_own_value>"
            priority: "11"
        prefer_scenario: "balance"
        src_peer:
         -
            auth_type: "14"
            device_id: "<your_own_value>"
            encode_type: "16"
            ip: "<your_own_value>"
            priority: "18"
```

6.530.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.530.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.530.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.531 fortios_wanopt_content_delivery_network_rule – Configure WAN optimization content delivery network rules in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.531.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wanopt feature and content_delivery_network_rule category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.531.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.531.3 FortiOS Version Compatibility

6.531.4 Parameters

6.531.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.531.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure WAN optimization content delivery network rules.
    fortios_wanopt_content_delivery_network_rule:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    state: "present"
    access_token: "<your_own_value>"
    wanopt_content_delivery_network_rule:
      category: "vcache"
      comment: "Comment about this CDN-rule."
      host_domain_name_suffix:
       -
          name: "default_name_6"
      name: "default_name_7"
      request_cache_control: "enable"
      response_cache_control: "enable"
      response_expires: "enable"
      rules:
       -
          content_id:
              end_direction: "forward"
              end_skip: "14"
              end_str: "<your_own_value>"
              range_str: "<your_own_value>"
              start_direction: "forward"
              start_skip: "18"
              start_str: "<your_own_value>"
              target: "path"
          match_entries:
           -
              id:  "22"
              pattern:
               -
                  string: "<your_own_value>"
              target: "path"
          match_mode: "all"
          name: "default_name_27"
          skip_entries:
           -
              id:  "29"
              pattern:
               -
                  string: "<your_own_value>"
              target: "path"
          skip_rule_mode: "all"
      status: "enable"
      text_response_vcache: "enable"
      updateserver: "enable"
```

6.531.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.531.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.531.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.532 fortios_wanopt_peer – Configure WAN optimization peers in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.532.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wanopt feature and peer category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.532.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.532.3 FortiOS Version Compatibility

6.532.4 Parameters

6.532.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.532.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure WAN optimization peers.
    fortios_wanopt_peer:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wanopt_peer:
        ip: "<your_own_value>"
        peer_host_id: "myhostname"
```

6.532.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.532.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.532.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.533 fortios_wanopt_profile – Configure WAN optimization profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.533.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wanopt feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.533.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.533.3 FortiOS Version Compatibility

6.533.4 Parameters

6.533.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.533.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure WAN optimization profiles.
    fortios_wanopt_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wanopt_profile:
        auth_group: "<your_own_value> (source wanopt.auth-group.name)"
        cifs:
            byte_caching: "enable"
            log_traffic: "enable"
            port: "7"
            prefer_chunking: "dynamic"
            protocol_opt: "protocol"
            secure_tunnel: "enable"
            status: "enable"
            tunnel_sharing: "private"
        comments: "<your_own_value>"
        ftp:
            byte_caching: "enable"
            log_traffic: "enable"
            port: "17"
            prefer_chunking: "dynamic"
            protocol_opt: "protocol"
            secure_tunnel: "enable"
            ssl: "enable"
            status: "enable"
            tunnel_sharing: "private"
        http:
            byte_caching: "enable"
            log_traffic: "enable"
            port: "27"
            prefer_chunking: "dynamic"
            protocol_opt: "protocol"
            secure_tunnel: "enable"
            ssl: "enable"
            ssl_port: "32"
            status: "enable"
            tunnel_non_http: "enable"
            tunnel_sharing: "private"
            unknown_http_version: "reject"
        mapi:
            byte_caching: "enable"
            log_traffic: "enable"
            port: "40"
            secure_tunnel: "enable"
```

(continues on next page)

(continued from previous page)

```
            status: "enable"
            tunnel_sharing: "private"
        name: "default_name_44"
        tcp:
            byte_caching: "enable"
            byte_caching_opt: "mem-only"
            log_traffic: "enable"
            port: "<your_own_value>"
            secure_tunnel: "enable"
            ssl: "enable"
            ssl_port: "52"
            status: "enable"
            tunnel_sharing: "private"
        transparent: "enable"
```

6.533.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.533.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.533.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.534 fortios_wanopt_remote_storage – Configure a remote cache device as Web cache storage in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Synopsis*

6.534.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wanopt feature and remote_storage category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.534.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.534.3 FortiOS Version Compatibility

6.534.4 Parameters

6.534.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.534.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure a remote cache device as Web cache storage.
```

(continues on next page)

(continued from previous page)

```
    fortios_wanopt_remote_storage:
      vdom:  "{{ vdom }}"
      wanopt_remote_storage:
        local_cache_id: "<your_own_value>"
        remote_cache_id: "<your_own_value>"
        remote_cache_ip: "<your_own_value>"
        status: "disable"
```

6.534.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.534.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.534.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.535 fortios_wanopt_settings – Configure WAN optimization settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.535.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wanopt feature and settings category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.535.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.535.3 FortiOS Version Compatibility

6.535.4 Parameters

6.535.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.535.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure WAN optimization settings.
    fortios_wanopt_settings:
      vdom:  "{{ vdom }}"
      wanopt_settings:
        auto_detect_algorithm: "simple"
        host_id: "myhostname"
        tunnel_ssl_algorithm: "high"
```

6.535.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.535.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.535.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.536 fortios_wanopt_webcache – Configure global Web cache settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.536.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wanopt feature and webcache category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.536.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.536.3 FortiOS Version Compatibility

6.536.4 Parameters

6.536.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.536.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure global Web cache settings.
    fortios_wanopt_webcache:
      vdom:  "{{ vdom }}"
      wanopt_webcache:
        always_revalidate: "enable"
        cache_by_default: "enable"
        cache_cookie: "enable"
        cache_expired: "enable"
        default_ttl: "7"
        external: "enable"
        fresh_factor: "9"
        host_validate: "enable"
        ignore_conditional: "enable"
        ignore_ie_reload: "enable"
        ignore_ims: "enable"
        ignore_pnc: "enable"
        max_object_size: "15"
        max_ttl: "16"
        min_ttl: "17"
        neg_resp_time: "18"
        reval_pnc: "enable"
```

6.536.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.536.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.536.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.537 fortios_web_proxy_debug_url – Configure debug URL addresses in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.537.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify web_proxy feature and debug_url category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.537.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.537.3 FortiOS Version Compatibility

6.537.4 Parameters

6.537.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.537.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure debug URL addresses.
    fortios_web_proxy_debug_url:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      web_proxy_debug_url:
        exact: "enable"
        name: "default_name_4"
        status: "enable"
        url_pattern: "<your_own_value>"
```

6.537.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.537.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.537.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.538 fortios_web_proxy_explicit – Configure explicit Web proxy settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.538.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify web_proxy feature and explicit category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.538.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.538.3 FortiOS Version Compatibility

6.538.4 Parameters

6.538.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.538.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure explicit Web proxy settings.
    fortios_web_proxy_explicit:
      vdom:  "{{ vdom }}"
      web_proxy_explicit:
        ftp_incoming_port: "<your_own_value>"
        ftp_over_http: "enable"
        http_incoming_port: "<your_own_value>"
        https_incoming_port: "<your_own_value>"
        https_replacement_message: "enable"
        incoming_ip: "<your_own_value>"
        incoming_ip6: "<your_own_value>"
        ipv6_status: "enable"
        message_upon_server_error: "enable"
        outgoing_ip: "<your_own_value>"
        outgoing_ip6: "<your_own_value>"
        pac_file_data: "<your_own_value>"
        pac_file_name: "<your_own_value>"
        pac_file_server_port: "<your_own_value>"
        pac_file_server_status: "enable"
        pac_file_url: "<your_own_value>"
        pac_policy:
         -
            comments: "<your_own_value>"
            dstaddr:
             -
                name: "default_name_22 (source firewall.address.name firewall.addrgrp.
↪name)"
            pac_file_data: "<your_own_value>"
            pac_file_name: "<your_own_value>"
            policyid: "25"
            srcaddr:
```

(continues on next page)

(continued from previous page)

```
            -
               name: "default_name_27 (source firewall.address.name firewall.addrgrp.
↪name firewall.proxy-address.name firewall.proxy-addrgrp.name)"
            srcaddr6:
            -
               name: "default_name_29 (source firewall.address6.name firewall.
↪addrgrp6.name)"
            status: "enable"
        pref_dns_result: "ipv4"
        realm: "<your_own_value>"
        sec_default_action: "accept"
        socks: "enable"
        socks_incoming_port: "<your_own_value>"
        ssl_algorithm: "high"
        status: "enable"
        strict_guest: "enable"
        trace_auth_no_rsp: "enable"
        unknown_http_version: "reject"
```

6.538.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.538.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.538.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.539 fortios_web_proxy_forward_server – Configure forward-server addresses in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.539.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify web_proxy feature and forward_server category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.539.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.539.3 FortiOS Version Compatibility

6.539.4 Parameters

6.539.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.539.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure forward-server addresses.
  fortios_web_proxy_forward_server:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    web_proxy_forward_server:
      addr_type: "ip"
      comment: "Comment."
      fqdn: "<your_own_value>"
      healthcheck: "disable"
      ip: "<your_own_value>"
      monitor: "<your_own_value>"
      name: "default_name_9"
      password: "<your_own_value>"
      port: "11"
      server_down_option: "block"
      username: "<your_own_value>"
```

6.539.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.539.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.539.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.540 fortios_web_proxy_forward_server_group – Configure a forward server group consisting or multiple forward servers. Supports failover and load balancing in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.540.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify web_proxy feature and forward_server_group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.540.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.540.3 FortiOS Version Compatibility

6.540.4 Parameters

6.540.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.540.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure a forward server group consisting or multiple forward servers.␣
↪Supports failover and load balancing.
    fortios_web_proxy_forward_server_group:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      web_proxy_forward_server_group:
        affinity: "enable"
        group_down_option: "block"
        ldb_method: "weighted"
        name: "default_name_6"
        server_list:
         -
            name: "default_name_8 (source web-proxy.forward-server.name)"
            weight: "9"
```

6.540.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.540.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.540.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.541 fortios_web_proxy_global – Configure Web proxy global settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.541.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify web_proxy feature and global category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.541.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.541.3 FortiOS Version Compatibility

6.541.4 Parameters

6.541.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.541.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Web proxy global settings.
    fortios_web_proxy_global:
      vdom:  "{{ vdom }}"
      web_proxy_global:
        fast_policy_match: "enable"
        forward_proxy_auth: "enable"
        forward_server_affinity_timeout: "5"
        learn_client_ip: "enable"
        learn_client_ip_from_header: "true-client-ip"
        learn_client_ip_srcaddr:
         -
            name: "default_name_9 (source firewall.address.name firewall.addrgrp.name)
↪"
        learn_client_ip_srcaddr6:
         -
            name: "default_name_11 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        max_message_length: "12"
        max_request_length: "13"
        max_waf_body_cache_length: "14"
        proxy_fqdn: "<your_own_value>"
        src_affinity_exempt_addr: "<your_own_value>"
        src_affinity_exempt_addr6: "<your_own_value>"
        ssl_ca_cert: "<your_own_value> (source vpn.certificate.local.name)"
        ssl_cert: "<your_own_value> (source vpn.certificate.local.name)"
        strict_web_check: "enable"
        tunnel_non_http: "enable"
        unknown_http_version: "reject"
        webproxy_profile: "<your_own_value> (source web-proxy.profile.name)"
```

6.541.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.541.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.541.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.542 fortios_web_proxy_profile – Configure web proxy profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.542.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify web_proxy feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.542.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.542.3 FortiOS Version Compatibility

6.542.4 Parameters

6.542.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.542.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure web proxy profiles.
    fortios_web_proxy_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      web_proxy_profile:
        header_client_ip: "pass"
        header_front_end_https: "pass"
        header_via_request: "pass"
        header_via_response: "pass"
        header_x_authenticated_groups: "pass"
        header_x_authenticated_user: "pass"
        header_x_forwarded_for: "pass"
        headers:
         -
            action: "add-to-request"
            add_option: "append"
            base64_encoding: "disable"
            content: "<your_own_value>"
            dstaddr:
             -
                name: "default_name_16 (source firewall.address.name firewall.addrgrp.
↪name)"
            dstaddr6:
             -
                name: "default_name_18 (source firewall.address6.name firewall.
↪addrgrp6.name)"
            id:  "19"
            name: "default_name_20"
            protocol: "https"
        log_header_change: "enable"
        name: "default_name_23"
        strip_encoding: "enable"
```

6.542.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.542.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.542.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.543 fortios_web_proxy_url_match – Exempt URLs from web proxy forwarding and caching in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.543.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify web_proxy feature and url_match category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.543.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.543.3 FortiOS Version Compatibility

6.543.4 Parameters

6.543.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.543.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Exempt URLs from web proxy forwarding and caching.
    fortios_web_proxy_url_match:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      web_proxy_url_match:
        cache_exemption: "enable"
        comment: "Comment."
        forward_server: "<your_own_value> (source web-proxy.forward-server.name web-
↪proxy.forward-server-group.name)"
        name: "default_name_6"
        status: "enable"
        url_pattern: "<your_own_value>"
```

6.543.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.543.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.543.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.544 fortios_web_proxy_wisp – Configure Wireless Internet service provider (WISP) servers in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.544.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify web_proxy feature and wisp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.544.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.544.3 FortiOS Version Compatibility

6.544.4 Parameters

6.544.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.544.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Wireless Internet service provider (WISP) servers.
    fortios_web_proxy_wisp:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      web_proxy_wisp:
        comment: "Comment."
        max_connections: "4"
        name: "default_name_5"
        outgoing_ip: "<your_own_value>"
        server_ip: "<your_own_value>"
        server_port: "8"
        timeout: "9"
```

6.544.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.544.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.544.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.545 fortios_webfilter_content – Configure Web filter banned word table in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.545.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify webfilter feature and content category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.545.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.545.3 FortiOS Version Compatibility

6.545.4 Parameters

6.545.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.545.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Web filter banned word table.
    fortios_webfilter_content:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      webfilter_content:
        comment: "Optional comments."
        entries:
         -
            action: "block"
            lang: "western"
            name: "default_name_7"
            pattern_type: "wildcard"
            score: "9"
            status: "enable"
        id:  "11"
        name: "default_name_12"
```

6.545.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.545.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.545.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.546 fortios_webfilter_content_header – Configure content types used by Web filter in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.546.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify webfilter feature and content_header category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.546.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.546.3 FortiOS Version Compatibility

6.546.4 Parameters

6.546.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.546.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure content types used by Web filter.
    fortios_webfilter_content_header:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      webfilter_content_header:
        comment: "Optional comments."
        entries:
         -
            action: "block"
            category: "<your_own_value>"
            pattern: "<your_own_value>"
        id:  "8"
        name: "default_name_9"
```

6.546.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.546.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.546.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.547 fortios_webfilter_fortiguard – Configure FortiGuard Web Filter service in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.547.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify webfilter feature and fortiguard category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.547.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.547.3 FortiOS Version Compatibility

6.547.4 Parameters

6.547.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.547.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiGuard Web Filter service.
    fortios_webfilter_fortiguard:
      vdom:  "{{ vdom }}"
      webfilter_fortiguard:
        cache_mem_percent: "3"
        cache_mode: "ttl"
        cache_prefix_match: "enable"
        close_ports: "enable"
        ovrd_auth_https: "enable"
        ovrd_auth_port: "8"
        ovrd_auth_port_http: "9"
        ovrd_auth_port_https: "10"
        ovrd_auth_port_https_flow: "11"
        ovrd_auth_port_warning: "12"
        request_packet_size_limit: "13"
        warn_auth_https: "enable"
```

6.547.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.547.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.547.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.548 fortios_webfilter_ftgd_local_cat – Configure FortiGuard Web Filter local categories in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.548.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify webfilter feature and ftgd_local_cat category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.548.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.548.3 FortiOS Version Compatibility

6.548.4 Parameters

6.548.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.548.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiGuard Web Filter local categories.
    fortios_webfilter_ftgd_local_cat:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      webfilter_ftgd_local_cat:
        desc: "<your_own_value>"
        id:  "4"
        status: "enable"
```

6.548.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.548.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.548.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.549 fortios_webfilter_ftgd_local_rating – Configure local FortiGuard Web Filter local ratings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.549.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify webfilter feature and ftgd_local_rating category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.549.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.549.3 FortiOS Version Compatibility

6.549.4 Parameters

6.549.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.549.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure local FortiGuard Web Filter local ratings.
  fortios_webfilter_ftgd_local_rating:
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    webfilter_ftgd_local_rating:
      comment: "Comment."
      rating: "<your_own_value>"
      status: "enable"
      url: "myurl.com"
```

6.549.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.549.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.549.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.550 fortios_webfilter_ips_urlfilter_cache_setting – Configure IPS URL filter cache settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.550.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify webfilter feature and ips_urlfilter_cache_setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.550.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.550.3 FortiOS Version Compatibility

6.550.4 Parameters

6.550.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.550.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPS URL filter cache settings.
    fortios_webfilter_ips_urlfilter_cache_setting:
      vdom:  "{{ vdom }}"
      webfilter_ips_urlfilter_cache_setting:
```

(continues on next page)

(continued from previous page)

```
        dns_retry_interval: "3"
        extended_ttl: "4"
```

6.550.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.550.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.550.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.551 fortios_webfilter_ips_urlfilter_setting – Configure IPS URL filter settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.551.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify webfilter feature and ips_urlfilter_setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.551.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.551.3 FortiOS Version Compatibility

6.551.4 Parameters

6.551.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.551.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPS URL filter settings.
    fortios_webfilter_ips_urlfilter_setting:
      vdom:  "{{ vdom }}"
      webfilter_ips_urlfilter_setting:
        device: "<your_own_value> (source system.interface.name)"
        distance: "4"
        gateway: "<your_own_value>"
        geo_filter: "<your_own_value>"
```

6.551.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.551.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.551.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.552 fortios_webfilter_ips_urlfilter_setting6 – Configure IPS URL filter settings for IPv6 in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.552.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify webfilter feature and ips_urlfilter_setting6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.552.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.552.3 FortiOS Version Compatibility

6.552.4 Parameters

6.552.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.552.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IPS URL filter settings for IPv6.
    fortios_webfilter_ips_urlfilter_setting6:
      vdom:  "{{ vdom }}"
      webfilter_ips_urlfilter_setting6:
        device: "<your_own_value> (source system.interface.name)"
        distance: "4"
        gateway6: "<your_own_value>"
        geo_filter: "<your_own_value>"
```

6.552.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.552.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.552.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.553 fortios_webfilter_override – Configure FortiGuard Web Filter administrative overrides in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.553.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify webfilter feature and override category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.553.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.553.3 FortiOS Version Compatibility

6.553.4 Parameters

6.553.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.553.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiGuard Web Filter administrative overrides.
    fortios_webfilter_override:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      webfilter_override:
        expires: "<your_own_value>"
        id:  "4"
        initiator: "<your_own_value>"
        ip: "<your_own_value>"
        ip6: "<your_own_value>"
        new_profile: "<your_own_value> (source webfilter.profile.name)"
        old_profile: "<your_own_value> (source webfilter.profile.name)"
        scope: "user"
        status: "enable"
        user: "<your_own_value>"
        user_group: "<your_own_value> (source user.group.name)"
```

6.553.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.553.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.553.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.554 fortios_webfilter_profile – Configure Web filter profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.554.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify webfilter feature and profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.554.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.554.3 FortiOS Version Compatibility

6.554.4 Parameters

6.554.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.554.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Web filter profiles.
    fortios_webfilter_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      webfilter_profile:
        antiphish:
            authentication: "domain-controller"
            check_basic_auth: "enable"
            check_uri: "enable"
            check_username_only: "enable"
            custom_patterns:
             -
                category: "username"
                pattern: "<your_own_value>"
                type: "regex"
            default_action: "exempt"
            domain_controller: "<your_own_value> (source credential-store.domain-
↪controller.server-name)"
            inspection_entries:
             -
                action: "exempt"
                fortiguard_category: "<your_own_value>"
                name: "default_name_17"
            ldap: "<your_own_value> (source user.ldap.name)"
            max_body_len: "19"
            status: "enable"
        comment: "Optional comments."
        extended_log: "enable"
        feature_set: "flow"
        file_filter:
            entries:
             -
                action: "log"
                comment: "Comment."
                direction: "incoming"
                file_type:
                 -
                    name: "default_name_30 (source antivirus.filetype.name)"
                filter: "<your_own_value>"
                password_protected: "yes"
                protocol: "http"
            log: "enable"
            scan_archive_contents: "enable"
            status: "enable"
```

(continues on next page)

(continued from previous page)

```
        ftgd_wf:
            exempt_quota: "<your_own_value>"
            filters:
             -
                action: "block"
                auth_usr_grp:
                 -
                    name: "default_name_42 (source user.group.name)"
                category: "43"
                id:  "44"
                log: "enable"
                override_replacemsg: "<your_own_value>"
                warn_duration: "<your_own_value>"
                warning_duration_type: "session"
                warning_prompt: "per-domain"
            max_quota_timeout: "50"
            options: "error-allow"
            ovrd: "<your_own_value>"
            quota:
             -
                category: "<your_own_value>"
                duration: "<your_own_value>"
                id:  "56"
                override_replacemsg: "<your_own_value>"
                type: "time"
                unit: "B"
                value: "60"
            rate_crl_urls: "disable"
            rate_css_urls: "disable"
            rate_image_urls: "disable"
            rate_javascript_urls: "disable"
        https_replacemsg: "enable"
        inspection_mode: "proxy"
        log_all_url: "enable"
        name: "default_name_68"
        options: "activexfilter"
        override:
            ovrd_cookie: "allow"
            ovrd_dur: "<your_own_value>"
            ovrd_dur_mode: "constant"
            ovrd_scope: "user"
            ovrd_user_group:
             -
                name: "default_name_76 (source user.group.name)"
            profile:
             -
                name: "default_name_78 (source webfilter.profile.name)"
            profile_attribute: "User-Name"
            profile_type: "list"
        ovrd_perm: "bannedword-override"
        post_action: "normal"
        replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
        url_extraction:
            redirect_header: "<your_own_value>"
            redirect_no_content: "enable"
            redirect_url: "<your_own_value>"
            server_fqdn: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        status: "enable"
    web:
        allowlist: "exempt-av"
        blacklist: "enable"
        blocklist: "enable"
        bword_table: "94 (source webfilter.content.id)"
        bword_threshold: "95"
        content_header_list: "96 (source webfilter.content-header.id)"
        keyword_match:
         -
            pattern: "<your_own_value>"
        log_search: "enable"
        safe_search: "url"
        urlfilter_table: "101 (source webfilter.urlfilter.id)"
        whitelist: "exempt-av"
        youtube_restrict: "none"
    web_antiphishing_log: "enable"
    web_content_log: "enable"
    web_extended_all_action_log: "enable"
    web_filter_activex_log: "enable"
    web_filter_applet_log: "enable"
    web_filter_command_block_log: "enable"
    web_filter_cookie_log: "enable"
    web_filter_cookie_removal_log: "enable"
    web_filter_js_log: "enable"
    web_filter_jscript_log: "enable"
    web_filter_referer_log: "enable"
    web_filter_unknown_log: "enable"
    web_filter_vbs_log: "enable"
    web_ftgd_err_log: "enable"
    web_ftgd_quota_usage: "enable"
    web_invalid_domain_log: "enable"
    web_url_log: "enable"
    wisp: "enable"
    wisp_algorithm: "primary-secondary"
    wisp_servers:
     -
        name: "default_name_124 (source web-proxy.wisp.name)"
    youtube_channel_filter:
     -
        channel_id: "<your_own_value>"
        comment: "Comment."
        id:  "128"
    youtube_channel_status: "disable"
```

6.554.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.554.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.554.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.555 fortios_webfilter_search_engine – Configure web filter search engines in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.555.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify webfilter feature and search_engine category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.555.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.555.3 FortiOS Version Compatibility

6.555.4 Parameters

6.555.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.555.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure web filter search engines.
    fortios_webfilter_search_engine:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      webfilter_search_engine:
        charset: "utf-8"
        hostname: "myhostname"
        name: "default_name_5"
        query: "<your_own_value>"
        safesearch: "disable"
        safesearch_str: "<your_own_value>"
        url: "myurl.com"
```

6.555.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.555.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.555.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.556 fortios_webfilter_status – Display rating info in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.556.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify webfilter feature and status category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.556.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.556.3 FortiOS Version Compatibility

6.556.4 Parameters

6.556.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.556.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Display rating info.
    fortios_webfilter_status:
      vdom:  "{{ vdom }}"
      webfilter_status:
        <refresh_rate>: "<your_own_value>"
```

6.556.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.556.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.556.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.557 fortios_webfilter_urlfilter – Configure URL filter lists in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.557.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify webfilter feature and urlfilter category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.557.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.557.3 FortiOS Version Compatibility

6.557.4 Parameters

6.557.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.557.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure URL filter lists.
    fortios_webfilter_urlfilter:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      webfilter_urlfilter:
        comment: "Optional comments."
        entries:
         -
            action: "exempt"
            antiphish_action: "block"
            dns_address_family: "ipv4"
            exempt: "av"
            id:  "9"
            referrer_host: "myhostname"
            status: "enable"
            type: "simple"
            url: "myurl.com"
            web_proxy_profile: "<your_own_value> (source web-proxy.profile.name)"
        id:  "15"
        ip_addr_block: "enable"
        name: "default_name_17"
        one_arm_ips_urlfilter: "enable"
```

6.557.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.557.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.557.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.558 fortios_wireless_controller_access_control_list – Configure WiFi bridge access control list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.558.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and access_control_list category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.558.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.558.3 FortiOS Version Compatibility

6.558.4 Parameters

6.558.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.558.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure WiFi bridge access control list.
    fortios_wireless_controller_access_control_list:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_access_control_list:
        comment: "Description."
        layer3_ipv4_rules:
         -
            action: "allow"
            comment: "Description."
            dstaddr: "<your_own_value>"
            dstport: "8"
            protocol: "9"
            rule_id: "10"
            srcaddr: "<your_own_value>"
            srcport: "12"
        layer3_ipv6_rules:
         -
            action: "allow"
            comment: "Description."
            dstaddr: "<your_own_value>"
            dstport: "17"
            protocol: "18"
            rule_id: "19"
            srcaddr: "<your_own_value>"
            srcport: "21"
        name: "default_name_22"
```

6.558.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.558.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.558.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.559 fortios_wireless_controller_address – Configure the client with its MAC address in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.559.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and address category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.559.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.559.3 FortiOS Version Compatibility

6.559.4 Parameters

6.559.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.559.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure the client with its MAC address.
    fortios_wireless_controller_address:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_address:
        id:  "3"
        mac: "<your_own_value>"
        policy: "allow"
```

6.559.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.559.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.559.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.560 fortios_wireless_controller_addrgrp – Configure the MAC address group in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.560.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and addrgrp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.560.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.560.3 FortiOS Version Compatibility

6.560.4 Parameters

6.560.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.560.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure the MAC address group.
    fortios_wireless_controller_addrgrp:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_addrgrp:
        addresses:
         -
            id:  "4 (source wireless-controller.address.id)"
        default_policy: "allow"
        id:  "6"
```

6.560.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.560.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.560.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.561 fortios_wireless_controller_ap_status – Configure access point status (rogue | accepted | suppressed) in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.561.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and ap_status category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.561.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.561.3 FortiOS Version Compatibility

6.561.4 Parameters

6.561.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.561.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure access point status (rogue | accepted | suppressed).
    fortios_wireless_controller_ap_status:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_ap_status:
        bssid: "<your_own_value>"
        id:  "4"
        ssid: "<your_own_value>"
        status: "rogue"
```

6.561.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.561.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.561.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.562 fortios_wireless_controller_apcfg_profile – Configure AP local configuration profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.562.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and apcfg_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.562.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.562.3 FortiOS Version Compatibility

6.562.4 Parameters

6.562.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.562.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure AP local configuration profiles.
    fortios_wireless_controller_apcfg_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_apcfg_profile:
        ac_ip: "<your_own_value>"
        ac_port: "4"
        ac_timer: "5"
        ac_type: "default"
        command_list:
         -
            id:  "8"
            name: "default_name_9"
            passwd_value: "<your_own_value>"
            type: "non-password"
            value: "<your_own_value>"
        comment: "Comment."
        name: "default_name_14"
```

6.562.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.562.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.562.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.563 fortios_wireless_controller_arrp_profile – Configure WiFi Automatic Radio Resource Provisioning (ARRP) profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.563.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and arrp_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.563.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.563.3 FortiOS Version Compatibility

6.563.4 Parameters

6.563.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.563.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure WiFi Automatic Radio Resource Provisioning (ARRP) profiles.
    fortios_wireless_controller_arrp_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_arrp_profile:
        comment: "Comment."
        include_dfs_channel: "yes"
        include_weather_channel: "yes"
        monitor_period: "6"
        name: "default_name_7"
        selection_period: "8"
        threshold_ap: "9"
        threshold_channel_load: "10"
        threshold_noise_floor: "<your_own_value>"
        threshold_rx_errors: "12"
        threshold_spectral_rssi: "<your_own_value>"
        threshold_tx_retries: "14"
        weight_channel_load: "15"
        weight_dfs_channel: "16"
        weight_managed_ap: "17"
        weight_noise_floor: "18"
        weight_rogue_ap: "19"
        weight_spectral_rssi: "20"
        weight_weather_channel: "21"
```

6.563.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.563.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.563.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.564 fortios_wireless_controller_ble_profile – Configure Bluetooth Low Energy profile in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.564.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and ble_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.564.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.564.3 FortiOS Version Compatibility

6.564.4 Parameters

6.564.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.564.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Bluetooth Low Energy profile.
    fortios_wireless_controller_ble_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_ble_profile:
        advertising: "ibeacon"
        beacon_interval: "4"
        ble_scanning: "enable"
        comment: "Comment."
        eddystone_instance: "<your_own_value>"
        eddystone_namespace: "<your_own_value>"
        eddystone_url: "<your_own_value>"
        eddystone_url_encode_hex: "<your_own_value>"
        ibeacon_uuid: "<your_own_value>"
        major_id: "12"
        minor_id: "13"
        name: "default_name_14"
        txpower: "0"
```

6.564.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.564.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.564.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.565 fortios_wireless_controller_bonjour_profile – Configure Bonjour profiles. Bonjour is Apple's zero configuration networking protocol. Bonjour profiles allow APs and FortiAPs to connnect to networks using Bonjour in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.565.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and bonjour_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.565.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.565.3 FortiOS Version Compatibility

6.565.4 Parameters

6.565.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.565.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Bonjour profiles. Bonjour is Apple's zero configuration␣
↪networking protocol. Bonjour profiles allow APs and FortiAPs to connnect to
     networks using Bonjour.
    fortios_wireless_controller_bonjour_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_bonjour_profile:
        comment: "Comment."
        name: "default_name_4"
        policy_list:
         -
            description: "<your_own_value>"
            from_vlan: "<your_own_value>"
            policy_id: "8"
            services: "all"
            to_vlan: "<your_own_value>"
```

6.565.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.565.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.565.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.566 fortios_wireless_controller_client_info – Wireless controller client-info in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.566.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and client_info category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.566.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.566.3 FortiOS Version Compatibility

6.566.4 Parameters

6.566.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.566.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Wireless controller client-info.
    fortios_wireless_controller_client_info:
      vdom:  "{{ vdom }}"
      wireless_controller_client_info:
        <vfid>: "<your_own_value>"
```

6.566.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.566.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.566.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.567 fortios_wireless_controller_global – Configure wireless controller global settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.567.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and global category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.567.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.567.3 FortiOS Version Compatibility

6.567.4 Parameters

6.567.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.567.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Configure wireless controller global settings.
  fortios_wireless_controller_global:
    vdom:  "{{ vdom }}"
    wireless_controller_global:
      ap_log_server: "enable"
      ap_log_server_ip: "<your_own_value>"
      ap_log_server_port: "5"
      control_message_offload: "ebp-frame"
      data_ethernet_II: "enable"
      discovery_mc_addr: "<your_own_value>"
      fiapp_eth_type: "9"
      image_download: "enable"
      ipsec_base_ip: "<your_own_value>"
      link_aggregation: "enable"
      location: "<your_own_value>"
      max_clients: "14"
      max_retransmit: "15"
      mesh_eth_type: "16"
      name: "default_name_17"
      rogue_scan_mac_adjacency: "18"
      wtp_share: "enable"
```

6.567.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.567.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.567.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.568 fortios_wireless_controller_hotspot20_anqp_3gpp_cellular – Configure 3GPP public land mobile network (PLMN) in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.568.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller_hotspot20 feature and anqp_3gpp_cellular category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.568.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.568.3 FortiOS Version Compatibility

6.568.4 Parameters

6.568.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.568.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure 3GPP public land mobile network (PLMN).
    fortios_wireless_controller_hotspot20_anqp_3gpp_cellular:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_hotspot20_anqp_3gpp_cellular:
        mcc_mnc_list:
         -
            id:  "4"
            mcc: "<your_own_value>"
            mnc: "<your_own_value>"
        name: "default_name_7"
```

6.568.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.568.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.568.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.569 fortios_wireless_controller_hotspot20_anqp_ip_address_type – Configure IP address type availability in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.569.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller_hotspot20 feature and anqp_ip_address_type category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.569.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.569.3 FortiOS Version Compatibility

6.569.4 Parameters

6.569.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.569.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure IP address type availability.
    fortios_wireless_controller_hotspot20_anqp_ip_address_type:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_hotspot20_anqp_ip_address_type:
        ipv4_address_type: "not-available"
        ipv6_address_type: "not-available"
        name: "default_name_5"
```

6.569.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.569.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.569.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.570 fortios_wireless_controller_hotspot20_anqp_nai_realm – Configure network access identifier (NAI) realm in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.570.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller_hotspot20 feature and anqp_nai_realm category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.570.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.570.3 FortiOS Version Compatibility

6.570.4 Parameters

6.570.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.570.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure network access identifier (NAI) realm.
    fortios_wireless_controller_hotspot20_anqp_nai_realm:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_hotspot20_anqp_nai_realm:
        nai_list:
         -
            eap_method:
             -
                auth_param:
                 -
                    id:  "6"
                    index: "7"
                    val: "eap-identity"
                index: "9"
                method: "eap-identity"
            encoding: "disable"
            nai_realm: "<your_own_value>"
            name: "default_name_13"
        name: "default_name_14"
```

6.570.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.570.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.570.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.571 fortios_wireless_controller_hotspot20_anqp_network_auth_type – Configure network authentication type in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.571.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller_hotspot20 feature and anqp_network_auth_type category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.571.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.571.3 FortiOS Version Compatibility

6.571.4 Parameters

6.571.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.571.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure network authentication type.
    fortios_wireless_controller_hotspot20_anqp_network_auth_type:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_hotspot20_anqp_network_auth_type:
        auth_type: "acceptance-of-terms"
        name: "default_name_4"
        url: "myurl.com"
```

6.571.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.571.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.571.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.572 fortios_wireless_controller_hotspot20_anqp_roaming_consortium – Configure roaming consortium in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.572.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller_hotspot20 feature and anqp_roaming_consortium category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.572.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.572.3 FortiOS Version Compatibility

6.572.4 Parameters

6.572.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.572.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure roaming consortium.
    fortios_wireless_controller_hotspot20_anqp_roaming_consortium:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_hotspot20_anqp_roaming_consortium:
        name: "default_name_3"
        oi_list:
         -
            comment: "Comment."
            index: "6"
            oi: "<your_own_value>"
```

6.572.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.572.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.572.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.573 fortios_wireless_controller_hotspot20_anqp_venue_name – Configure venue name duple in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.573.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller_hotspot20 feature and anqp_venue_name category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.573.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.573.3 FortiOS Version Compatibility

6.573.4 Parameters

6.573.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.573.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure venue name duple.
    fortios_wireless_controller_hotspot20_anqp_venue_name:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_hotspot20_anqp_venue_name:
        name: "default_name_3"
        value_list:
         -
            index: "5"
            lang: "<your_own_value>"
            value: "<your_own_value>"
```

6.573.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.573.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.573.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.574 fortios_wireless_controller_hotspot20_h2qp_conn_capability – Configure connection capability in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.574.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller_hotspot20 feature and h2qp_conn_capability category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.574.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.574.3 FortiOS Version Compatibility

6.574.4 Parameters

6.574.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.574.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure connection capability.
    fortios_wireless_controller_hotspot20_h2qp_conn_capability:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_hotspot20_h2qp_conn_capability:
        esp_port: "closed"
        ftp_port: "closed"
        http_port: "closed"
        icmp_port: "closed"
        ikev2_port: "closed"
        ikev2_xx_port: "closed"
        name: "default_name_9"
        pptp_vpn_port: "closed"
        ssh_port: "closed"
        tls_port: "closed"
        voip_tcp_port: "closed"
        voip_udp_port: "closed"
```

6.574.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.574.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.574.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.575 fortios_wireless_controller_hotspot20_h2qp_operator_name – Configure operator friendly name in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.575.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller_hotspot20 feature and h2qp_operator_name category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.575.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.575.3 FortiOS Version Compatibility

6.575.4 Parameters

6.575.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.575.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure operator friendly name.
    fortios_wireless_controller_hotspot20_h2qp_operator_name:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_hotspot20_h2qp_operator_name:
        name: "default_name_3"
        value_list:
         -
            index: "5"
            lang: "<your_own_value>"
            value: "<your_own_value>"
```

6.575.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.575.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.575.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.576 fortios_wireless_controller_hotspot20_h2qp_osu_provider – Configure online sign up (OSU) provider list in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.576.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller_hotspot20 feature and h2qp_osu_provider category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.576.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.576.3 FortiOS Version Compatibility

6.576.4 Parameters

6.576.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.576.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure online sign up (OSU) provider list.
    fortios_wireless_controller_hotspot20_h2qp_osu_provider:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_hotspot20_h2qp_osu_provider:
        friendly_name:
         -
            friendly_name: "<your_own_value>"
            index: "5"
            lang: "<your_own_value>"
        icon: "<your_own_value> (source wireless-controller.hotspot20.icon.name)"
        name: "default_name_8"
        osu_method: "oma-dm"
        osu_nai: "<your_own_value>"
        server_uri: "<your_own_value>"
        service_description:
         -
            lang: "<your_own_value>"
            service_description: "<your_own_value>"
            service_id: "15"
```

6.576.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.576.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.576.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.577 fortios_wireless_controller_hotspot20_h2qp_wan_metric – Configure WAN metrics in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.577.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller_hotspot20 feature and h2qp_wan_metric category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.577.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.577.3 FortiOS Version Compatibility

6.577.4 Parameters

6.577.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.577.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure WAN metrics.
    fortios_wireless_controller_hotspot20_h2qp_wan_metric:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_hotspot20_h2qp_wan_metric:
        downlink_load: "3"
        downlink_speed: "4"
        link_at_capacity: "enable"
        link_status: "up"
        load_measurement_duration: "7"
        name: "default_name_8"
        symmetric_wan_link: "symmetric"
        uplink_load: "10"
        uplink_speed: "11"
```

6.577.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.577.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.577.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.578 fortios_wireless_controller_hotspot20_hs_profile – Configure hotspot profile in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.578.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller_hotspot20 feature and hs_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.578.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.578.3 FortiOS Version Compatibility

6.578.4 Parameters

6.578.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.578.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure hotspot profile.
    fortios_wireless_controller_hotspot20_hs_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_hotspot20_hs_profile:
        plmn_3gpp: "<your_own_value> (source wireless-controller.hotspot20.anqp-3gpp-
↪cellular.name)"
        access_network_asra: "enable"
        access_network_esr: "enable"
        access_network_internet: "enable"
        access_network_type: "private-network"
        access_network_uesa: "enable"
        anqp_domain_id: "9"
        bss_transition: "enable"
        conn_cap: "<your_own_value> (source wireless-controller.hotspot20.h2qp-conn-
↪capability.name)"
        deauth_request_timeout: "12"
        dgaf: "enable"
        domain_name: "<your_own_value>"
        gas_comeback_delay: "15"
        gas_fragmentation_limit: "16"
        hessid: "<your_own_value>"
        ip_addr_type: "<your_own_value> (source wireless-controller.hotspot20.anqp-ip-
↪address-type.name)"
        l2tif: "enable"
        nai_realm: "<your_own_value> (source wireless-controller.hotspot20.anqp-nai-
↪realm.name)"
        name: "default_name_21"
        network_auth: "<your_own_value> (source wireless-controller.hotspot20.anqp-
↪network-auth-type.name)"
        oper_friendly_name: "<your_own_value> (source wireless-controller.hotspot20.
↪h2qp-operator-name.name)"
        osu_provider:
          -
            name: "default_name_25 (source wireless-controller.hotspot20.h2qp-osu-
↪provider.name)"
        osu_ssid: "<your_own_value>"
        pame_bi: "disable"
        proxy_arp: "enable"
        qos_map: "<your_own_value> (source wireless-controller.hotspot20.qos-map.name)
↪"
        roaming_consortium: "<your_own_value> (source wireless-controller.hotspot20.
↪anqp-roaming-consortium.name)"
        venue_group: "unspecified"
        venue_name: "<your_own_value> (source wireless-controller.hotspot20.anqp-
↪venue-name.name)"
```

(continues on next page)

(continued from previous page)

```
        venue_type: "unspecified"
        wan_metrics: "<your_own_value> (source wireless-controller.hotspot20.h2qp-wan-
↪metric.name)"
        wnm_sleep_mode: "enable"
```

6.578.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.578.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.578.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.579 fortios_wireless_controller_hotspot20_icon – Configure OSU provider icon in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.579.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller_hotspot20 feature and icon category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.579.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.579.3 FortiOS Version Compatibility

6.579.4 Parameters

6.579.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.579.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure OSU provider icon.
    fortios_wireless_controller_hotspot20_icon:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_hotspot20_icon:
        icon_list:
         -
            file: "<your_own_value>"
            height: "5"
            lang: "<your_own_value>"
            name: "default_name_7"
            type: "bmp"
```

(continues on next page)

(continued from previous page)

```
            width: "9"
        name: "default_name_10"
```

6.579.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.579.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.579.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.580 fortios_wireless_controller_hotspot20_qos_map – Configure QoS map set in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.580.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller_hotspot20 feature and qos_map category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.580.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.580.3 FortiOS Version Compatibility

6.580.4 Parameters

6.580.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.580.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure QoS map set.
    fortios_wireless_controller_hotspot20_qos_map:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_hotspot20_qos_map:
        dscp_except:
         -
            dscp: "4"
            index: "5"
            up: "6"
        dscp_range:
         -
            high: "8"
            index: "9"
            low: "10"
            up: "11"
        name: "default_name_12"
```

6.580.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.580.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.580.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.581 fortios_wireless_controller_inter_controller – Configure inter wireless controller operation in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.581.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and inter_controller category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.581.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.581.3 FortiOS Version Compatibility

6.581.4 Parameters

6.581.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.581.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure inter wireless controller operation.
    fortios_wireless_controller_inter_controller:
      vdom:  "{{ vdom }}"
      wireless_controller_inter_controller:
        fast_failover_max: "3"
        fast_failover_wait: "4"
        inter_controller_key: "<your_own_value>"
        inter_controller_mode: "disable"
        inter_controller_peer:
         -
            id:  "8"
            peer_ip: "<your_own_value>"
            peer_port: "10"
            peer_priority: "primary"
        inter_controller_pri: "primary"
```

6.581.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.581.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.581.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.582 fortios_wireless_controller_log – Configure wireless controller event log filters in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.582.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and log category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.582.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.582.3 FortiOS Version Compatibility

6.582.4 Parameters

6.582.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.582.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure wireless controller event log filters.
    fortios_wireless_controller_log:
      vdom:  "{{ vdom }}"
      wireless_controller_log:
        addrgrp_log: "emergency"
        ble_log: "emergency"
        clb_log: "emergency"
        dhcp_starv_log: "emergency"
        led_sched_log: "emergency"
        radio_event_log: "emergency"
        rogue_event_log: "emergency"
        sta_event_log: "emergency"
        sta_locate_log: "emergency"
        status: "enable"
        wids_log: "emergency"
        wtp_event_log: "emergency"
```

6.582.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.582.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.582.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.583 fortios_wireless_controller_mpsk_profile – Configure MPSK profile in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.583.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and mpsk_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.583.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.583.3 FortiOS Version Compatibility

6.583.4 Parameters

6.583.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.583.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure MPSK profile.
    fortios_wireless_controller_mpsk_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_mpsk_profile:
        mpsk_concurrent_clients: "3"
        mpsk_group:
         -
            mpsk_key:
             -
                comment: "Comment."
                concurrent_client_limit_type: "default"
                concurrent_clients: "8"
                mac: "<your_own_value>"
                mpsk_schedules:
                 -
                    name: "default_name_11 (source firewall.schedule.group.name␣
↪firewall.schedule.recurring.name firewall.schedule.onetime.name)"
                name: "default_name_12"
                passphrase: "<your_own_value>"
            name: "default_name_14"
            vlan_id: "15"
            vlan_type: "no-vlan"
        name: "default_name_17"
```

6.583.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.583.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.583.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.584 fortios_wireless_controller_nac_profile – Configure WiFi network access control (NAC) profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.584.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and nac_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.584.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.584.3 FortiOS Version Compatibility

6.584.4 Parameters

6.584.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.584.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure WiFi network access control (NAC) profiles.
    fortios_wireless_controller_nac_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_nac_profile:
        comment: "Comment."
        name: "default_name_4"
        onboarding_vlan: "<your_own_value> (source system.interface.name)"
```

6.584.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.584.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.584.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.585 fortios_wireless_controller_qos_profile – Configure WiFi quality of service (QoS) profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.585.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and qos_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.585.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.585.3 FortiOS Version Compatibility

6.585.4 Parameters

6.585.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.585.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure WiFi quality of service (QoS) profiles.
    fortios_wireless_controller_qos_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_qos_profile:
        bandwidth_admission_control: "enable"
        bandwidth_capacity: "4"
        burst: "enable"
        call_admission_control: "enable"
        call_capacity: "7"
        comment: "Comment."
        downlink: "9"
        downlink_sta: "10"
        dscp_wmm_be:
         -
            id:  "12"
        dscp_wmm_bk:
         -
            id:  "14"
        dscp_wmm_mapping: "enable"
        dscp_wmm_vi:
         -
            id:  "17"
        dscp_wmm_vo:
         -
            id:  "19"
        name: "default_name_20"
```

(continues on next page)

(continued from previous page)

```
        uplink: "21"
        uplink_sta: "22"
        wmm: "enable"
        wmm_be_dscp: "24"
        wmm_bk_dscp: "25"
        wmm_dscp_marking: "enable"
        wmm_uapsd: "enable"
        wmm_vi_dscp: "28"
        wmm_vo_dscp: "29"
```

6.585.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.585.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.585.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.586 fortios_wireless_controller_region – Configure FortiAP regions (for floor plans and maps) in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.586.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and region category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.586.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.586.3 FortiOS Version Compatibility

6.586.4 Parameters

6.586.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.586.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure FortiAP regions (for floor plans and maps).
    fortios_wireless_controller_region:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_region:
```

(continues on next page)

(continued from previous page)

```
        comments: "<your_own_value>"
        grayscale: "enable"
        image_type: "png"
        name: "default_name_6"
        opacity: "7"
```

6.586.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.586.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.586.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.587 fortios_wireless_controller_rf_analysis – Wireless controller rf-analysis in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Authors*

6.587.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and rf_analysis category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.587.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.587.3 FortiOS Version Compatibility

6.587.4 Parameters

6.587.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.587.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Wireless controller rf-analysis.
    fortios_wireless_controller_rf_analysis:
      vdom:  "{{ vdom }}"
      wireless_controller_rf_analysis:
        <wtp_id>: "<your_own_value>"
```

6.587.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.587.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.587.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.588 fortios_wireless_controller_setting – VDOM wireless controller configuration in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.588.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and setting category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.588.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.588.3 FortiOS Version Compatibility

6.588.4 Parameters

6.588.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.588.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: VDOM wireless controller configuration.
    fortios_wireless_controller_setting:
      vdom:  "{{ vdom }}"
      wireless_controller_setting:
        account_id: "<your_own_value>"
        country: "NA"
        darrp_optimize: "5"
        darrp_optimize_schedules:
         -
            name: "default_name_7 (source firewall.schedule.group.name firewall.
↪schedule.recurring.name firewall.schedule.onetime.name)"
        device_holdoff: "8"
        device_idle: "9"
        device_weight: "10"
        duplicate_ssid: "enable"
        fake_ssid_action: "log"
        fapc_compatibility: "enable"
        offending_ssid:
         -
            action: "log"
            id:  "16"
            ssid_pattern: "<your_own_value>"
        phishing_ssid_detect: "enable"
        wfa_compatibility: "enable"
```

6.588.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.588.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.588.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.589 fortios_wireless_controller_snmp – Configure SNMP in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.589.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and snmp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.589.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.589.3 FortiOS Version Compatibility

6.589.4 Parameters

6.589.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.589.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure SNMP.
    fortios_wireless_controller_snmp:
      vdom:  "{{ vdom }}"
      wireless_controller_snmp:
        community:
         -
            hosts:
             -
                id:  "5"
                ip: "<your_own_value>"
            id:  "7"
            name: "default_name_8"
            query_v1_status: "enable"
            query_v2c_status: "enable"
            status: "enable"
            trap_v1_status: "enable"
            trap_v2c_status: "enable"
        contact_info: "<your_own_value>"
        engine_id: "<your_own_value>"
        trap_high_cpu_threshold: "16"
        trap_high_mem_threshold: "17"
        user:
         -
            auth_proto: "md5"
            auth_pwd: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
            name: "default_name_21"
            notify_hosts: "<your_own_value>"
            priv_proto: "aes"
            priv_pwd: "<your_own_value>"
            queries: "enable"
            security_level: "no-auth-no-priv"
            status: "enable"
            trap_status: "enable"
```

6.589.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.589.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.589.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.590 fortios_wireless_controller_spectral_info – Wireless controller spectrum analysis in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.590.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and spectral_info category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.590.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.590.3 FortiOS Version Compatibility

6.590.4 Parameters

6.590.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.590.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Wireless controller spectrum analysis.
    fortios_wireless_controller_spectral_info:
      vdom:  "{{ vdom }}"
      wireless_controller_spectral_info:
        set_wtp_id: "<your_own_value>"
```

6.590.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.590.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.590.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.591 fortios_wireless_controller_ssid_policy – Configure WiFi SSID policies in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.591.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and ssid_policy category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.591.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.591.3 FortiOS Version Compatibility

6.591.4 Parameters

6.591.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.591.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure WiFi SSID policies.
    fortios_wireless_controller_ssid_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_ssid_policy:
        description: "<your_own_value>"
        name: "default_name_4"
        vlan: "<your_own_value> (source system.interface.name)"
```

6.591.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.591.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.591.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.592 fortios_wireless_controller_status – Wireless controller status in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.592.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and status category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.592.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.592.3 FortiOS Version Compatibility

6.592.4 Parameters

6.592.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.592.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Wireless controller status.
    fortios_wireless_controller_status:
      vdom:  "{{ vdom }}"
      wireless_controller_status:
        set_1_2: "<your_own_value>"
```

6.592.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.592.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.592.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.593 fortios_wireless_controller_timers – Configure CAPWAP timers in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.593.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and timers category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.593.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.593.3 FortiOS Version Compatibility

6.593.4 Parameters

6.593.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.593.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure CAPWAP timers.
    fortios_wireless_controller_timers:
      vdom:  "{{ vdom }}"
      wireless_controller_timers:
        ble_scan_report_intv: "3"
        client_idle_timeout: "4"
        darrp_day: "sunday"
        darrp_optimize: "6"
        darrp_time:
         -
            time: "<your_own_value>"
        discovery_interval: "9"
        drma_interval: "10"
        echo_interval: "11"
        fake_ap_log: "12"
        ipsec_intf_cleanup: "13"
        radio_stats_interval: "14"
        rogue_ap_log: "15"
        sta_capability_interval: "16"
        sta_locate_timer: "17"
        sta_stats_interval: "18"
        vap_stats_interval: "19"
```

6.593.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.593.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.593.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.594 fortios_wireless_controller_utm_profile – Configure UTM (Unified Threat Management) profile in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.594.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and utm_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.594.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.594.3 FortiOS Version Compatibility

6.594.4 Parameters

6.594.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.594.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure UTM (Unified Threat Management) profile.
    fortios_wireless_controller_utm_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_utm_profile:
        antivirus_profile: "<your_own_value> (source antivirus.profile.name)"
        application_list: "<your_own_value> (source application.list.name)"
        comment: "Comment."
        ips_sensor: "<your_own_value> (source ips.sensor.name)"
        name: "default_name_7"
        scan_botnet_connections: "disable"
        utm_log: "enable"
        webfilter_profile: "<your_own_value> (source webfilter.profile.name)"
```

6.594.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.594.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.594.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.595 fortios_wireless_controller_vap – Configure Virtual Access Points (VAPs) in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.595.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and vap category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.595.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.595.3 FortiOS Version Compatibility

6.595.4 Parameters

6.595.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.595.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Virtual Access Points (VAPs).
    fortios_wireless_controller_vap:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_vap:
        access_control_list: "<your_own_value> (source wireless-controller.access-
↪control-list.name)"
        acct_interim_interval: "4"
        additional_akms: "akm6"
        address_group: "<your_own_value> (source wireless-controller.addrgrp.id)"
        alias: "<your_own_value>"
        atf_weight: "8"
        auth: "psk"
        broadcast_ssid: "enable"
        broadcast_suppression: "dhcp-up"
        bss_color_partial: "enable"
        bstm_disassociation_imminent: "enable"
        bstm_load_balancing_disassoc_timer: "14"
        bstm_rssi_disassoc_timer: "15"
        captive_portal_ac_name: "<your_own_value>"
        captive_portal_auth_timeout: "17"
        captive_portal_macauth_radius_secret: "<your_own_value>"
        captive_portal_macauth_radius_server: "<your_own_value>"
        captive_portal_radius_secret: "<your_own_value>"
        captive_portal_radius_server: "<your_own_value>"
        captive_portal_session_timeout_interval: "22"
        dhcp_address_enforcement: "enable"
        dhcp_lease_time: "24"
        dhcp_option43_insertion: "enable"
        dhcp_option82_circuit_id_insertion: "style-1"
        dhcp_option82_insertion: "enable"
        dhcp_option82_remote_id_insertion: "style-1"
        dynamic_vlan: "enable"
        eap_reauth: "enable"
        eap_reauth_intv: "31"
        eapol_key_retries: "disable"
        encrypt: "TKIP"
        external_fast_roaming: "enable"
        external_logout: "<your_own_value>"
        external_web: "<your_own_value>"
        external_web_format: "auto-detect"
        fast_bss_transition: "disable"
        fast_roaming: "enable"
        ft_mobility_domain: "40"
        ft_over_ds: "disable"
        ft_r0_key_lifetime: "42"
```

(continues on next page)

(continued from previous page)

```
        gas_comeback_delay: "43"
        gas_fragmentation_limit: "44"
        gtk_rekey: "enable"
        gtk_rekey_intv: "46"
        high_efficiency: "enable"
        hotspot20_profile: "<your_own_value> (source wireless-controller.hotspot20.hs-
↪profile.name)"
        igmp_snooping: "enable"
        intra_vap_privacy: "enable"
        ip: "<your_own_value>"
        ipv6_rules: "drop-icmp6ra"
        key: "<your_own_value>"
        keyindex: "54"
        ldpc: "disable"
        local_authentication: "enable"
        local_bridging: "enable"
        local_lan: "allow"
        local_standalone: "enable"
        local_standalone_nat: "enable"
        mac_auth_bypass: "enable"
        mac_called_station_delimiter: "hyphen"
        mac_calling_station_delimiter: "hyphen"
        mac_case: "uppercase"
        mac_filter: "enable"
        mac_filter_list:
         -
            id:  "67"
            mac: "<your_own_value>"
            mac_filter_policy: "allow"
        mac_filter_policy_other: "allow"
        mac_password_delimiter: "hyphen"
        mac_username_delimiter: "hyphen"
        max_clients: "73"
        max_clients_ap: "74"
        mbo: "disable"
        mbo_cell_data_conn_pref: "excluded"
        me_disable_thresh: "77"
        mesh_backhaul: "enable"
        mpsk: "enable"
        mpsk_concurrent_clients: "80"
        mpsk_key:
         -
            comment: "Comment."
            concurrent_clients: "<your_own_value>"
            key_name: "<your_own_value>"
            mpsk_schedules:
             -
                name: "default_name_86 (source firewall.schedule.group.name firewall.
↪schedule.recurring.name firewall.schedule.onetime.name)"
            passphrase: "<your_own_value>"
        mpsk_profile: "<your_own_value> (source wireless-controller.mpsk-profile.name)
↪"
        mu_mimo: "enable"
        multicast_enhance: "enable"
        multicast_rate: "0"
        nac: "enable"
        nac_profile: "<your_own_value> (source wireless-controller.nac-profile.name)"
```

(continues on next page)

(continued from previous page)

```
        name: "default_name_94"
        neighbor_report_dual_band: "disable"
        okc: "disable"
        owe_groups: "19"
        owe_transition: "disable"
        owe_transition_ssid: "<your_own_value>"
        passphrase: "<your_own_value>"
        pmf: "disable"
        pmf_assoc_comeback_timeout: "102"
        pmf_sa_query_retry_timeout: "103"
        port_macauth: "disable"
        port_macauth_reauth_timeout: "105"
        port_macauth_timeout: "106"
        portal_message_override_group: "<your_own_value> (source system.replacemsg-
↪group.name)"
        portal_message_overrides:
            auth_disclaimer_page: "<your_own_value>"
            auth_login_failed_page: "<your_own_value>"
            auth_login_page: "<your_own_value>"
            auth_reject_page: "<your_own_value>"
        portal_type: "auth"
        primary_wag_profile: "<your_own_value> (source wireless-controller.wag-
↪profile.name)"
        probe_resp_suppression: "enable"
        probe_resp_threshold: "<your_own_value>"
        ptk_rekey: "enable"
        ptk_rekey_intv: "118"
        qos_profile: "<your_own_value> (source wireless-controller.qos-profile.name)"
        quarantine: "enable"
        radio_2g_threshold: "<your_own_value>"
        radio_5g_threshold: "<your_own_value>"
        radio_sensitivity: "enable"
        radius_mac_auth: "enable"
        radius_mac_auth_server: "<your_own_value> (source user.radius.name)"
        radius_mac_auth_usergroups:
         -
            name: "default_name_127"
        radius_server: "<your_own_value> (source user.radius.name)"
        rates_11a: "1"
        rates_11ac_ss12: "mcs0/1"
        rates_11ac_ss34: "mcs0/3"
        rates_11bg: "1"
        rates_11n_ss12: "mcs0/1"
        rates_11n_ss34: "mcs16/3"
        sae_groups: "19"
        sae_password: "<your_own_value>"
        schedule: "<your_own_value>"
        secondary_wag_profile: "<your_own_value> (source wireless-controller.wag-
↪profile.name)"
        security: "open"
        security_exempt_list: "<your_own_value> (source user.security-exempt-list.
↪name)"
        security_obsolete_option: "enable"
        security_redirect_url: "<your_own_value>"
        selected_usergroups:
         -
            name: "default_name_144 (source user.group.name)"
```

(continues on next page)

(continued from previous page)

```
        split_tunneling: "enable"
        ssid: "<your_own_value>"
        sticky_client_remove: "enable"
        sticky_client_threshold_2g: "<your_own_value>"
        sticky_client_threshold_5g: "<your_own_value>"
        target_wake_time: "enable"
        tkip_counter_measure: "enable"
        tunnel_echo_interval: "152"
        tunnel_fallback_interval: "153"
        usergroup:
         -
            name: "default_name_155 (source user.group.name)"
        utm_profile: "<your_own_value> (source wireless-controller.utm-profile.name)"
        vdom: "<your_own_value> (source system.vdom.name)"
        vlan_auto: "enable"
        vlan_pool:
         -
            id:  "160"
            wtp_group: "<your_own_value> (source wireless-controller.wtp-group.name)"
        vlan_pooling: "wtp-group"
        vlanid: "163"
        voice_enterprise: "disable"
```

6.595.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.595.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.595.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.596 fortios_wireless_controller_vap_group – Configure virtual Access Point (VAP) groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.596.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and vap_group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.596.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.596.3 FortiOS Version Compatibility

6.596.4 Parameters

6.596.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.596.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure virtual Access Point (VAP) groups.
    fortios_wireless_controller_vap_group:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_vap_group:
        comment: "Comment."
        name: "default_name_4"
        vaps:
         -
            name: "default_name_6 (source wireless-controller.vap.name)"
```

6.596.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.596.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.596.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.597 fortios_wireless_controller_vap_status – Wireless controller VAP-status in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.597.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and vap_status category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.597.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.597.3 FortiOS Version Compatibility

6.597.4 Parameters

6.597.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.597.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_port: 443
tasks:
- name: Wireless controller VAP-status.
  fortios_wireless_controller_vap_status:
    vdom:  "{{ vdom }}"
    wireless_controller_vap_status:
      set_1: "<your_own_value>"
```

6.597.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.597.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.597.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.598 fortios_wireless_controller_wag_profile – Configure wireless access gateway (WAG) profiles used for tunnels on AP in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.598.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and wag_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.598.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.598.3 FortiOS Version Compatibility

6.598.4 Parameters

6.598.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.598.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure wireless access gateway (WAG) profiles used for tunnels on AP.
    fortios_wireless_controller_wag_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_wag_profile:
        comment: "Comment."
        dhcp_ip_addr: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        name: "default_name_5"
        ping_interval: "6"
        ping_number: "7"
        return_packet_timeout: "8"
        tunnel_type: "l2tpv3"
        wag_ip: "<your_own_value>"
        wag_port: "11"
```

6.598.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.598.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.598.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.599 fortios_wireless_controller_wids_profile – Configure wireless intrusion detection system (WIDS) profiles in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.599.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and wids_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.599.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.599.3 FortiOS Version Compatibility

6.599.4 Parameters

6.599.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.599.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure wireless intrusion detection system (WIDS) profiles.
    fortios_wireless_controller_wids_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_wids_profile:
        ap_auto_suppress: "enable"
        ap_bgscan_disable_day: "sunday"
```

(continues on next page)

(continued from previous page)

```
        ap_bgscan_disable_end: "<your_own_value>"
        ap_bgscan_disable_schedules:
         -
            name: "default_name_7 (source firewall.schedule.group.name firewall.
↪schedule.recurring.name firewall.schedule.onetime.name)"
        ap_bgscan_disable_start: "<your_own_value>"
        ap_bgscan_duration: "9"
        ap_bgscan_idle: "10"
        ap_bgscan_intv: "11"
        ap_bgscan_period: "12"
        ap_bgscan_report_intv: "13"
        ap_fgscan_report_intv: "14"
        ap_scan: "disable"
        ap_scan_passive: "enable"
        ap_scan_threshold: "<your_own_value>"
        asleap_attack: "enable"
        assoc_flood_thresh: "19"
        assoc_flood_time: "20"
        assoc_frame_flood: "enable"
        auth_flood_thresh: "22"
        auth_flood_time: "23"
        auth_frame_flood: "enable"
        comment: "Comment."
        deauth_broadcast: "enable"
        deauth_unknown_src_thresh: "27"
        eapol_fail_flood: "enable"
        eapol_fail_intv: "29"
        eapol_fail_thresh: "30"
        eapol_logoff_flood: "enable"
        eapol_logoff_intv: "32"
        eapol_logoff_thresh: "33"
        eapol_pre_fail_flood: "enable"
        eapol_pre_fail_intv: "35"
        eapol_pre_fail_thresh: "36"
        eapol_pre_succ_flood: "enable"
        eapol_pre_succ_intv: "38"
        eapol_pre_succ_thresh: "39"
        eapol_start_flood: "enable"
        eapol_start_intv: "41"
        eapol_start_thresh: "42"
        eapol_succ_flood: "enable"
        eapol_succ_intv: "44"
        eapol_succ_thresh: "45"
        invalid_mac_oui: "enable"
        long_duration_attack: "enable"
        long_duration_thresh: "48"
        name: "default_name_49"
        null_ssid_probe_resp: "enable"
        sensor_mode: "disable"
        spoofed_deauth: "enable"
        weak_wep_iv: "enable"
        wireless_bridge: "enable"
```

6.599.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.599.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.599.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.600 fortios_wireless_controller_wtp – Configure Wireless Termination Points (WTPs), that is, FortiAPs or APs to be managed by FortiGate in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.600.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and wtp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.600.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.600.3 FortiOS Version Compatibility

6.600.4 Parameters

6.600.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.600.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure Wireless Termination Points (WTPs), that is, FortiAPs or APs to␣
↪be managed by FortiGate.
    fortios_wireless_controller_wtp:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_wtp:
        admin: "discovered"
        allowaccess: "telnet"
        apcfg_profile: "<your_own_value> (source wireless-controller.apcfg-profile.
↪name)"
        bonjour_profile: "<your_own_value> (source wireless-controller.bonjour-
↪profile.name)"
        coordinate_enable: "enable"
        coordinate_latitude: "<your_own_value>"
        coordinate_longitude: "<your_own_value>"
        coordinate_x: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        coordinate_y: "<your_own_value>"
        firmware_provision: "<your_own_value>"
        image_download: "enable"
        index: "14"
        ip_fragment_preventing: "tcp-mss-adjust"
        lan:
            port_esl_mode: "offline"
            port_esl_ssid: "<your_own_value> (source system.interface.name)"
            port_mode: "offline"
            port_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port1_mode: "offline"
            port1_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port2_mode: "offline"
            port2_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port3_mode: "offline"
            port3_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port4_mode: "offline"
            port4_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port5_mode: "offline"
            port5_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port6_mode: "offline"
            port6_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port7_mode: "offline"
            port7_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port8_mode: "offline"
            port8_ssid: "<your_own_value> (source wireless-controller.vap.name)"
        led_state: "enable"
        location: "<your_own_value>"
        login_passwd: "<your_own_value>"
        login_passwd_change: "yes"
        mesh_bridge_enable: "default"
        name: "default_name_42"
        override_allowaccess: "enable"
        override_ip_fragment: "enable"
        override_lan: "enable"
        override_led_state: "enable"
        override_login_passwd_change: "enable"
        override_split_tunnel: "enable"
        override_wan_port_mode: "enable"
        radio_1:
            auto_power_high: "51"
            auto_power_level: "enable"
            auto_power_low: "53"
            auto_power_target: "<your_own_value>"
            band: "802.11a"
            channel:
             -
                chan: "<your_own_value>"
            drma_manual_mode: "ap"
            override_analysis: "enable"
            override_band: "enable"
            override_channel: "enable"
            override_txpower: "enable"
            override_vaps: "enable"
            power_level: "64"
            power_mode: "dBm"
            power_value: "66"
```

(continues on next page)

(continued from previous page)

```
            radio_id: "67"
            spectrum_analysis: "enable"
            vap_all: "enable"
            vaps:
             -
                name: "default_name_71 (source wireless-controller.vap-group.name␣
↪wireless-controller.vap.name)"
        radio_2:
            auto_power_high: "73"
            auto_power_level: "enable"
            auto_power_low: "75"
            auto_power_target: "<your_own_value>"
            band: "802.11a"
            channel:
             -
                chan: "<your_own_value>"
            drma_manual_mode: "ap"
            override_analysis: "enable"
            override_band: "enable"
            override_channel: "enable"
            override_txpower: "enable"
            override_vaps: "enable"
            power_level: "86"
            power_mode: "dBm"
            power_value: "88"
            radio_id: "89"
            spectrum_analysis: "enable"
            vap_all: "enable"
            vaps:
             -
                name: "default_name_93 (source wireless-controller.vap-group.name␣
↪wireless-controller.vap.name)"
        radio_3:
            auto_power_high: "95"
            auto_power_level: "enable"
            auto_power_low: "97"
            auto_power_target: "<your_own_value>"
            band: "802.11a"
            channel:
             -
                chan: "<your_own_value>"
            drma_manual_mode: "ap"
            override_analysis: "enable"
            override_band: "enable"
            override_channel: "enable"
            override_txpower: "enable"
            override_vaps: "enable"
            power_level: "108"
            power_mode: "dBm"
            power_value: "110"
            radio_id: "111"
            spectrum_analysis: "enable"
            vap_all: "enable"
            vaps:
             -
                name: "default_name_115 (source wireless-controller.vap-group.name␣
↪system.interface.name)"
```

(continues on next page)

(continued from previous page)

```
        radio_4:
            auto_power_high: "117"
            auto_power_level: "enable"
            auto_power_low: "119"
            auto_power_target: "<your_own_value>"
            band: "802.11a"
            channel:
             -
                chan: "<your_own_value>"
            drma_manual_mode: "ap"
            override_analysis: "enable"
            override_band: "enable"
            override_channel: "enable"
            override_txpower: "enable"
            override_vaps: "enable"
            power_level: "130"
            power_mode: "dBm"
            power_value: "132"
            spectrum_analysis: "enable"
            vap_all: "enable"
            vaps:
             -
                name: "default_name_136 (source wireless-controller.vap-group.name␣
↪system.interface.name)"
        region: "<your_own_value> (source wireless-controller.region.name)"
        region_x: "<your_own_value>"
        region_y: "<your_own_value>"
        split_tunneling_acl:
         -
            dest_ip: "<your_own_value>"
            id:  "142"
        split_tunneling_acl_local_ap_subnet: "enable"
        split_tunneling_acl_path: "tunnel"
        tun_mtu_downlink: "145"
        tun_mtu_uplink: "146"
        uuid: "<your_own_value>"
        wan_port_mode: "wan-lan"
        wtp_id: "<your_own_value>"
        wtp_mode: "normal"
        wtp_profile: "<your_own_value> (source wireless-controller.wtp-profile.name)"
```

6.600.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.600.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.600.9 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.601 fortios_wireless_controller_wtp_group – Configure WTP groups in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.601.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and wtp_group category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.601.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.601.3 FortiOS Version Compatibility

6.601.4 Parameters

6.601.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.601.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure WTP groups.
    fortios_wireless_controller_wtp_group:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_wtp_group:
        name: "default_name_3"
        platform_type: "AP-11N"
        wtps:
         -
            wtp_id: "<your_own_value> (source wireless-controller.wtp.wtp-id)"
```

6.601.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.601.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.601.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.602 fortios_wireless_controller_wtp_profile – Configure WTP profiles or FortiAP profiles that define radio settings for manageable FortiAP platforms in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.602.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and wtp_profile category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.602.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.602.3 FortiOS Version Compatibility

6.602.4 Parameters

6.602.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.602.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure WTP profiles or FortiAP profiles that define radio settings for␣
↪manageable FortiAP platforms.
    fortios_wireless_controller_wtp_profile:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      wireless_controller_wtp_profile:
        allowaccess: "telnet"
        ap_country: "NA"
        ap_handoff: "enable"
        apcfg_profile: "<your_own_value> (source wireless-controller.apcfg-profile.
↪name)"
        ble_profile: "<your_own_value> (source wireless-controller.ble-profile.name)"
        comment: "Comment."
        control_message_offload: "ebp-frame"
        deny_mac_list:
         -
            id:  "11"
            mac: "<your_own_value>"
        dtls_in_kernel: "enable"
        dtls_policy: "clear-text"
        energy_efficient_ethernet: "enable"
        ext_info_enable: "enable"
        frequency_handoff: "enable"
        handoff_roaming: "enable"
        handoff_rssi: "19"
        handoff_sta_thresh: "20"
        ip_fragment_preventing: "tcp-mss-adjust"
        lan:
            port_esl_mode: "offline"
            port_esl_ssid: "<your_own_value> (source system.interface.name)"
            port_mode: "offline"
            port_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port1_mode: "offline"
            port1_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port2_mode: "offline"
            port2_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port3_mode: "offline"
            port3_ssid: "<your_own_value> (source wireless-controller.vap.name)"
```

(continues on next page)

(continued from previous page)

```
            port4_mode: "offline"
            port4_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port5_mode: "offline"
            port5_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port6_mode: "offline"
            port6_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port7_mode: "offline"
            port7_ssid: "<your_own_value> (source wireless-controller.vap.name)"
            port8_mode: "offline"
            port8_ssid: "<your_own_value> (source wireless-controller.vap.name)"
        lbs:
            aeroscout: "enable"
            aeroscout_ap_mac: "bssid"
            aeroscout_mmu_report: "enable"
            aeroscout_mu: "enable"
            aeroscout_mu_factor: "48"
            aeroscout_mu_timeout: "49"
            aeroscout_server_ip: "<your_own_value>"
            aeroscout_server_port: "51"
            ekahau_blink_mode: "enable"
            ekahau_tag: "<your_own_value>"
            erc_server_ip: "<your_own_value>"
            erc_server_port: "55"
            fortipresence: "foreign"
            fortipresence_ble: "enable"
            fortipresence_frequency: "58"
            fortipresence_port: "59"
            fortipresence_project: "<your_own_value>"
            fortipresence_rogue: "enable"
            fortipresence_secret: "<your_own_value>"
            fortipresence_server: "<your_own_value>"
            fortipresence_unassoc: "enable"
            station_locate: "enable"
        led_schedules:
         -
            name: "default_name_67 (source firewall.schedule.group.name firewall.
↪schedule.recurring.name)"
        led_state: "enable"
        lldp: "enable"
        login_passwd: "<your_own_value>"
        login_passwd_change: "yes"
        max_clients: "72"
        name: "default_name_73"
        platform:
            ddscan: "enable"
            mode: "single-5G"
            type: "AP-11N"
        poe_mode: "auto"
        radio_1:
            airtime_fairness: "enable"
            amsdu: "enable"
            ap_handoff: "enable"
            ap_sniffer_addr: "<your_own_value>"
            ap_sniffer_bufsize: "84"
            ap_sniffer_chan: "85"
            ap_sniffer_ctl: "enable"
            ap_sniffer_data: "enable"
```

(continues on next page)

(continued from previous page)

```
            ap_sniffer_mgmt_beacon: "enable"
            ap_sniffer_mgmt_other: "enable"
            ap_sniffer_mgmt_probe: "enable"
            auto_power_high: "91"
            auto_power_level: "enable"
            auto_power_low: "93"
            auto_power_target: "<your_own_value>"
            band: "802.11a"
            band_5g_type: "5g-full"
            bandwidth_admission_control: "enable"
            bandwidth_capacity: "98"
            beacon_interval: "99"
            bss_color: "100"
            call_admission_control: "enable"
            call_capacity: "102"
            channel:
             -
                chan: "<your_own_value>"
            channel_bonding: "80MHz"
            channel_utilization: "enable"
            coexistence: "enable"
            darrp: "enable"
            drma: "disable"
            drma_sensitivity: "low"
            dtim: "111"
            frag_threshold: "112"
            frequency_handoff: "enable"
            iperf_protocol: "udp"
            iperf_server_port: "115"
            max_clients: "116"
            max_distance: "117"
            mode: "disabled"
            power_level: "119"
            power_mode: "dBm"
            power_value: "121"
            powersave_optimize: "tim"
            protection_mode: "rtscts"
            radio_id: "124"
            rts_threshold: "125"
            sam_bssid: "<your_own_value>"
            sam_captive_portal: "enable"
            sam_password: "<your_own_value>"
            sam_report_intv: "129"
            sam_security_type: "open"
            sam_server: "<your_own_value>"
            sam_ssid: "<your_own_value>"
            sam_test: "ping"
            sam_username: "<your_own_value>"
            short_guard_interval: "enable"
            spectrum_analysis: "enable"
            transmit_optimize: "disable"
            vap_all: "enable"
            vaps:
             -
                name: "default_name_140 (source wireless-controller.vap-group.name␣
↪wireless-controller.vap.name)"
            wids_profile: "<your_own_value> (source wireless-controller.wids-profile.
↪name)"
```

(continues on next page)

(continued from previous page)

```
            zero_wait_dfs: "enable"
        radio_2:
            airtime_fairness: "enable"
            amsdu: "enable"
            ap_handoff: "enable"
            ap_sniffer_addr: "<your_own_value>"
            ap_sniffer_bufsize: "148"
            ap_sniffer_chan: "149"
            ap_sniffer_ctl: "enable"
            ap_sniffer_data: "enable"
            ap_sniffer_mgmt_beacon: "enable"
            ap_sniffer_mgmt_other: "enable"
            ap_sniffer_mgmt_probe: "enable"
            auto_power_high: "155"
            auto_power_level: "enable"
            auto_power_low: "157"
            auto_power_target: "<your_own_value>"
            band: "802.11a"
            band_5g_type: "5g-full"
            bandwidth_admission_control: "enable"
            bandwidth_capacity: "162"
            beacon_interval: "163"
            bss_color: "164"
            call_admission_control: "enable"
            call_capacity: "166"
            channel:
              -
                chan: "<your_own_value>"
            channel_bonding: "80MHz"
            channel_utilization: "enable"
            coexistence: "enable"
            darrp: "enable"
            drma: "disable"
            drma_sensitivity: "low"
            dtim: "175"
            frag_threshold: "176"
            frequency_handoff: "enable"
            iperf_protocol: "udp"
            iperf_server_port: "179"
            max_clients: "180"
            max_distance: "181"
            mode: "disabled"
            power_level: "183"
            power_mode: "dBm"
            power_value: "185"
            powersave_optimize: "tim"
            protection_mode: "rtscts"
            radio_id: "188"
            rts_threshold: "189"
            sam_bssid: "<your_own_value>"
            sam_captive_portal: "enable"
            sam_password: "<your_own_value>"
            sam_report_intv: "193"
            sam_security_type: "open"
            sam_server: "<your_own_value>"
            sam_ssid: "<your_own_value>"
            sam_test: "ping"
```

(continues on next page)

(continued from previous page)

```
            sam_username: "<your_own_value>"
            short_guard_interval: "enable"
            spectrum_analysis: "enable"
            transmit_optimize: "disable"
            vap_all: "enable"
            vaps:
             -
                name: "default_name_204 (source wireless-controller.vap-group.name␣
↪wireless-controller.vap.name)"
            wids_profile: "<your_own_value> (source wireless-controller.wids-profile.
↪name)"
            zero_wait_dfs: "enable"
        radio_3:
            airtime_fairness: "enable"
            amsdu: "enable"
            ap_handoff: "enable"
            ap_sniffer_addr: "<your_own_value>"
            ap_sniffer_bufsize: "212"
            ap_sniffer_chan: "213"
            ap_sniffer_ctl: "enable"
            ap_sniffer_data: "enable"
            ap_sniffer_mgmt_beacon: "enable"
            ap_sniffer_mgmt_other: "enable"
            ap_sniffer_mgmt_probe: "enable"
            auto_power_high: "219"
            auto_power_level: "enable"
            auto_power_low: "221"
            auto_power_target: "<your_own_value>"
            band: "802.11a"
            band_5g_type: "5g-full"
            bandwidth_admission_control: "enable"
            bandwidth_capacity: "226"
            beacon_interval: "227"
            bss_color: "228"
            call_admission_control: "enable"
            call_capacity: "230"
            channel:
             -
                chan: "<your_own_value>"
            channel_bonding: "160MHz"
            channel_utilization: "enable"
            coexistence: "enable"
            darrp: "enable"
            drma: "disable"
            drma_sensitivity: "low"
            dtim: "239"
            frag_threshold: "240"
            frequency_handoff: "enable"
            iperf_protocol: "udp"
            iperf_server_port: "243"
            max_clients: "244"
            max_distance: "245"
            mode: "disabled"
            power_level: "247"
            power_mode: "dBm"
            power_value: "249"
            powersave_optimize: "tim"
```

(continues on next page)

(continued from previous page)

```
            protection_mode: "rtscts"
            radio_id: "252"
            rts_threshold: "253"
            sam_bssid: "<your_own_value>"
            sam_captive_portal: "enable"
            sam_password: "<your_own_value>"
            sam_report_intv: "257"
            sam_security_type: "open"
            sam_server: "<your_own_value>"
            sam_ssid: "<your_own_value>"
            sam_test: "ping"
            sam_username: "<your_own_value>"
            short_guard_interval: "enable"
            spectrum_analysis: "enable"
            transmit_optimize: "disable"
            vap_all: "enable"
            vaps:
             -
                name: "default_name_268 (source wireless-controller.vap-group.name␣
↪system.interface.name)"
            wids_profile: "<your_own_value> (source wireless-controller.wids-profile.
↪name)"
            zero_wait_dfs: "enable"
        radio_4:
            airtime_fairness: "enable"
            amsdu: "enable"
            ap_handoff: "enable"
            ap_sniffer_addr: "<your_own_value>"
            ap_sniffer_bufsize: "276"
            ap_sniffer_chan: "277"
            ap_sniffer_ctl: "enable"
            ap_sniffer_data: "enable"
            ap_sniffer_mgmt_beacon: "enable"
            ap_sniffer_mgmt_other: "enable"
            ap_sniffer_mgmt_probe: "enable"
            auto_power_high: "283"
            auto_power_level: "enable"
            auto_power_low: "285"
            auto_power_target: "<your_own_value>"
            band: "802.11a"
            band_5g_type: "5g-full"
            bandwidth_admission_control: "enable"
            bandwidth_capacity: "290"
            beacon_interval: "291"
            bss_color: "292"
            call_admission_control: "enable"
            call_capacity: "294"
            channel:
             -
                chan: "<your_own_value>"
            channel_bonding: "160MHz"
            channel_utilization: "enable"
            coexistence: "enable"
            darrp: "enable"
            drma: "disable"
            drma_sensitivity: "low"
            dtim: "303"
```

(continues on next page)

(continued from previous page)

```
            frag_threshold: "304"
            frequency_handoff: "enable"
            iperf_protocol: "udp"
            iperf_server_port: "307"
            max_clients: "308"
            max_distance: "309"
            mode: "disabled"
            power_level: "311"
            power_mode: "dBm"
            power_value: "313"
            powersave_optimize: "tim"
            protection_mode: "rtscts"
            rts_threshold: "316"
            sam_bssid: "<your_own_value>"
            sam_captive_portal: "enable"
            sam_password: "<your_own_value>"
            sam_report_intv: "320"
            sam_security_type: "open"
            sam_server: "<your_own_value>"
            sam_ssid: "<your_own_value>"
            sam_test: "ping"
            sam_username: "<your_own_value>"
            short_guard_interval: "enable"
            spectrum_analysis: "enable"
            transmit_optimize: "disable"
            vap_all: "enable"
            vaps:
             -
                name: "default_name_331 (source wireless-controller.vap-group.name␣
↪system.interface.name)"
            wids_profile: "<your_own_value> (source wireless-controller.wids-profile.
↪name)"
            zero_wait_dfs: "enable"
        split_tunneling_acl:
         -
            dest_ip: "<your_own_value>"
            id:  "336"
        split_tunneling_acl_local_ap_subnet: "enable"
        split_tunneling_acl_path: "tunnel"
        tun_mtu_downlink: "339"
        tun_mtu_uplink: "340"
        wan_port_mode: "wan-lan"
```

6.602.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.602.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.602.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

6.603 fortios_wireless_controller_wtp_status – Wireless controller WTP-status in Fortinet's FortiOS and FortiGate.

New in version 2.10.

6.603.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify wireless_controller feature and wtp_status category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

6.603.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

6.603.3 FortiOS Version Compatibility

6.603.4 Parameters

6.603.5 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

6.603.6 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Wireless controller WTP-status.
    fortios_wireless_controller_wtp_status:
      vdom:  "{{ vdom }}"
      wireless_controller_wtp_status:
        <wtp_id>: "<your_own_value>"
```

6.603.7 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

6.603.8 Status

- This module is not guaranteed to have a backwards compatible interface.

6.603.9 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

CHAPTER 7

Monitor Modules

The Modules to build FortiOS monitor API requests to FortiOS appliances.

7.1 fortios_monitor – Ansible Module for FortiOS Monitor API.

New in version 2.10.

7.1.1 Synopsis

- Request FortiOS appliances to perform specific actions or procedures. This module contain all the FortiOS monitor API.

7.1.2 Requirements

The below requirements are needed on the host that executes this module.

- install galaxy collection fortinet.fortios >= `2.0.0`.

7.1.3 Parameters

7.1.4 Notes

Note:

- Different `selector` may have different parameters, users are expected to look up them in the dropdown list above..
- For some selectors, no `params` are allowed to appear.
- Not all parameters are required for a selector.
- This module is exclusivly for FortiOS monitor API.
- The result of API request is stored in `results`.

7.1.5 Examples

```
- hosts: fortigate03
  connection: httpapi
  collections:
  - fortinet.fortios
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:

  - name: Activate FortiToken
    fortios_monitor:
       vdom: "root"
       access_token: "<fortios_access_token>"
       selector: 'activate.user.fortitoken'
       params:
           tokens: '<token string>'

  - name: Reboot This Device
    fortios_monitor:
       vdom: "root"
       access_token: "<fortios_access_token>"
       selector: 'reboot.system.os'
       params:
           event_log_message: 'Reboot Request From Ansible'
```

7.1.6 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

7.1.7 Status

- This module is not guaranteed to have a backwards compatible interface.

7.1.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@fshen01)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

CHAPTER 8

Facts Gathering Modules

The Modules to gather FortiOS fatcs are invoking `GET` requests for FortiOS managed objects or procedures.

8.1 fortios_configuration_fact – Retrieve Facts of FortiOS Configurable Objects.

New in version 2.10.

8.1.1 Synopsis

- Collects facts from network devices running the fortios operating system. This module places the facts gathered in the fact tree keyed by the respective resource name. This facts module will only collect those facts which user specified in playbook.

8.1.2 Requirements

The below requirements are needed on the host that executes this module.

- install galaxy collection fortinet.fortios >= `2.0.0`.

8.1.3 Parameters

8.1.4 Notes

Note:

- Different `selector` may have different parameters, users are expected to look up them for a specific selector.
- For some selectors, the objects are global, no `params` are allowed to appear.
- If `params` is empty a non-unique object, the whole object list is returned.
- This module has support for all configuration API, excluding any monitor API.
- The result of API request is stored in `results` as a list.
- There are three filtering parameters: `filters`, `sorters` and `formatters`, please see filtering spec for more information.

8.1.5 Examples

```
- hosts: fortigateslab
  connection: httpapi
  collections:
    - fortinet.fortios
  vars:
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
    vdom: "root"
  tasks:
  - name: Get multiple selectors info concurrently
    fortios_configuration_fact:
        selectors:
            - selector: firewall_address
              params:
                name: "gmail.com"
        - selector: system_interface
        - selector: log_eventfilter
          params: {}

  - name: fact gathering with filters
    fortios_configuration_fact:
        vdom: ""
        filters:
         - name==port1
         - vlanid==0
        sorters:
         - name,vlanid
```

(continues on next page)

(continued from previous page)

```
        - management-ip
      formatters:
        - name
        - management-ip
        - vlanid
      selector: 'system_interface'

- name: get all
  fortios_configuration_fact:
    vdom: ""
    access_token: ""
    selector: log_custom-field

- name: get single
  fortios_configuration_fact:
    vdom: ""
    access_token: ""
    selector: log_custom-field
    #optionally list or single get
    params:
      id: "3"

- name: fetch one firewall address
  fortios_configuration_fact:
    selector: firewall_address
    params:
      name: "login.microsoft.com"

- name: fetch all firewall addresses
  fortios_configuration_fact:
    selector: firewall_address
```

8.1.6 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

8.1.7 Status

- This module is not guaranteed to have a backwards compatible interface.

8.1.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@fshen01)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

8.2 fortios_monitor_fact – Retrieve Facts of FortiOS Monitor Objects.

New in version 2.10.

8.2.1 Synopsis

- Collects monitor facts from network devices running the fortios operating system. This facts module will only collect those facts which user specified in playbook.

8.2.2 Requirements

The below requirements are needed on the host that executes this module.

- install galaxy collection fortinet.fortios >= `2.0.0`.

8.2.3 Parameters

8.2.4 Notes

Note:

- Different `selector` may have different parameters, users are expected to look up them for a specific selector.
- For some selectors, the objects are global, no `params` are allowed to appear.
- Not all parameters are required for a slector.
- This module is exclusivly for FortiOS monitor API.
- The result of API request is stored in `results`.
- There are three filtering parameters: `filters`, `sorters` and `formatters`, please see filtering spec for more information.

8.2.5 Examples

```
- hosts: fortigate03
  connection: httpapi
  collections:
  - fortinet.fortios
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:

  - fortios_monitor_fact:
      vdom: ""
      enable_log: true
      formatters:
          - model_name
      filters:
          - model_name==FortiGat
      selector: 'system_status'

  - name: fact gathering
    fortios_monitor_fact:
      vdom: ""
      access_token: ""
      selector: 'firewall_acl'

  - name: fact gathering
    fortios_monitor_fact:
      vdom: ""
      access_token: ""
      selector: 'firewall_security-policy'
      params:
          policyid: '1'
```

8.2.6 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

8.2.7 Status

- This module is not guaranteed to have a backwards compatible interface.

8.2.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@fshen01)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

8.3 fortios_log_fact – Retrieve Log Data of Fortios Log Objects.

New in version 2.10.

8.3.1 Synopsis

- Collects log data from network devices running the fortios operating system. This module will only collect the log data specified in the playbook.

8.3.2 Requirements

The below requirements are needed on the host that executes this module.

- install galaxy collection fortinet.fortios >= `2.1.0`.

8.3.3 Parameters

8.3.4 Notes

Note:

- Different `selector` may have different parameters, users are expected to look up them for a specific selector.
- For some selectors, the objects are global, no `params` are allowed to appear.
- Not all parameters are required for a slector.
- This module is exclusivly for FortiOS monitor API.
- The result of API request is stored in `results`.
- There are three filtering parameters: `filters`, `sorters` and `formatters`, please see filtering spec for more information.

8.3.5 Examples

```
- hosts: fortigate03
  connection: httpapi
  collections:
  - fortinet.fortios
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Get system event log with logid==0100032038
    fortios_log_fact:
      filters:
        - logid==0100032038
      selector: "disk_event_system"
      params:
        rows: 100

  - name: Get a description of the quarantined virus file
    fortios_log_fact:
      selector: "forticloud_virus_archive"
```

8.3.6 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

8.3.7 Status

- This module is not guaranteed to have a backwards compatible interface.

8.3.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@fshen01)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

CHAPTER 9

Generic Modules

The Modules to build flexible raw requests to FortiOS appliances.

9.1 fortios_json_generic – Configure Fortinet's FortiOS and FortiGate with json generic method.

9.1.1 Synopsis

This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set any category supported by FortiAPI with raw json. All parameters and values included in examples need to be adjusted to datasources before usage.

9.1.2 Requirements

The below requirements are needed on the host that executes this module.

- install galaxy collection `fortinet.fortios` >= 2.0.0

9.1.3 Parameters

9.1.4 Examples

host

```
[fortigates]
fortigate01 ansible_host=192.168.52.177 ansible_user="admin" ansible_password="admin"

[fortigates:vars]
ansible_network_os=fortios
```

sample1.yml

```
---
- hosts: fortigates
  connection: httpapi
  collections:
    - fortinet.fortios
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443

  tasks:
  - name: test add with string
    fortios_json_generic:
      vdom:  "{{ vdom }}"
      json_generic:
        method: "POST"
        path: "/api/v2/cmdb/firewall/address"
        jsonbody: |
          {
          "name": "111",
          "type": "geography",
          "fqdn": "",
          "country": "AL",
          "comment": "ccc",
          "visibility": "enable",
          "associated-interface": "port1",
          "allow-routing": "disable"
          }
    register: info

  - name: display vars
    debug: msg="{{info}}"
```

sample2.yml

```
---
- hosts: fortigates
  connection: httpapi
  collections:
    - fortinet.fortios
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443

  tasks:
  - name: test delete
    fortios_json_generic:
      vdom:  "{{ vdom }}"
      json_generic:
        method: "DELETE"
        path: "/api/v2/cmdb/firewall/address/111"
        specialparams: "testpara1=1&testpara2=2"
    register: info

  - name: display vars
    debug: msg="{{info}}"

  - name: test add with dict
    fortios_json_generic:
      vdom:  "{{ vdom }}"
      json_generic:
        method: "POST"
        path: "/api/v2/cmdb/firewall/address"
        dictbody:
          name: "111"
          type: "geography"
          fqdn: ""
          country: "AL"
          comment: "ccc"
          visibility: "enable"
          associated-interface: "port1"
          allow-routing: "disable"
    register: info

  - name: display vars
    debug: msg="{{info}}"

  - name: test delete
    fortios_json_generic:
      vdom:  "{{ vdom }}"
      json_generic:
        method: "DELETE"
        path: "/api/v2/cmdb/firewall/address/111"
    register: info

  - name: display vars
    debug: msg="{{info}}"

  - name: test add with string
    fortios_json_generic:
```

(continues on next page)

(continued from previous page)

```
      vdom:  "{{ vdom }}"
      json_generic:
        method: "POST"
        path: "/api/v2/cmdb/firewall/address"
        jsonbody: |
          {
          "name": "111",
          "type": "geography",
          "fqdn": "",
          "country": "AL",
          "comment": "ccc",
          "visibility": "enable",
          "associated-interface": "port1",
          "allow-routing": "disable"
          }
    register: info

  - name: display vars
    debug: msg="{{info}}"
```

sample3.yml

```
---
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443

  tasks:
  - name: test firewall policy order modification
    fortios_json_generic:
      vdom:  "{{ vdom }}"
      json_generic:
            method: "PUT"
            path: "/api/v2/cmdb/firewall/policy/1"
            specialparams: "action=move&after=2"
    register: info

  - name: display vars
    debug: msg="{{info}}"
```

9.1.5 Return Values

Common return values are documented: https://docs.ansible.com/ansible/latest/reference_appendices/common_return_values.html#common-return-values, the following are the fields unique to this module:

9.1.6 Status

- This module is ported from https://github.com/fortinet/ansible-fortios-generic

9.1.7 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Frank Shen (@fshen01)
- Hongbin Lu (@fgtdev-hblu)

9.1.8 Warning

It's preferred to use `FortiOS Ansible Collection Included Modules` unless some features are not available there.

CHAPTER 10

Release Notes

10.1 Release Galaxy 2.1.0

10.1.1 Release Targets

FortiOS Galaxy 2.1.0 is based on 2.0.2

10.1.2 Features

- Support Fortios 7.0.
- Support Log APIs.
- New module fortios_monitor_fact.

10.1.3 Bug Fixes

- Fix the unexpected warning caused by optinal params in `fortios_monitor_fact` and `fortios_monitor`.
- Disable check_mode feature from all global objects of configuration modules due to 'state' issue.
- Fix a bug in IP_PREFIX.match().
- Fix the issue that the `server_type` is not updated in `fortios_system_central_management`.

10.2 Release Galaxy 2.0.2

10.2.1 Release Targets

FortiOS Galaxy 2.0.2 is based on 2.0.1

10.2.2 Features

- Support `check_mode` in all cofigurationAPI-based modules.
- Improve `fortios_configuration_fact` to use multiple selectors concurrently.
- Support moving policy in `firewall_central_snat_map`.
- Support filtering for fact gathering modules `fortios_configuration_fact` and `fortios_monitor_fact`.
- Unify schemas for monitor API.

10.2.3 Bug Fixes

- Fix the authorization fails at log in with username and password in FOS7.0.
- Github Issue #103
- Github Issue #105

10.3 Release Galaxy 2.0.1

10.3.1 Release Targets

FortiOS Galaxy is based on `2.0.0`.

10.3.2 Features

- fixed `pylint` minor errors.

10.4 Release Galaxy 2.0.0

10.4.1 Release Targets

FortiOS Galaxy 2.0.0 is a major ansible release for all v6.x.x FOS virtual and hardware platforms.

10.4.2 Features

- Full support for gathering facts of both configuration(`fortios_configuration_fact`) and monitor(`fortios_monitor_fact`) objects or runtime data.
- Support for requesting Monitor API via module `fortios_monitor`.

- Ported FortiOS generic module: `fortios_json_generic`.
- Unified collections for all 6.x FOS releases, Ansible detects versioning mismatch at runtime.
- Explicit logging option: `enable_log`.
- Deprecated second-layer `state` module parameter.

10.4.3 Compatibility Notes

As a major release, it semantically breaks backward compability, some modules are removed as new full-fledged replacements come into being.

- For deprecated modules, please find the alternatives in **Deprecated Modules** section.
- Other existing modules are kepted compatible.

10.4.4 Deprecated Modules

- `fortios_facts`: find full selectors in modules `fortios_configuration_fact` and `fortios_monitor_fact`.
- `fortios_registration_forticare`: replaced by module `fortios_monitor`, see selector `add-license.registration.forticare`.
- `fortios_registration_vdom`: replaced by module `fortios_monitor`, see selector `add-license.registration.vdom`.
- `fortios_system_vmlicense`: replaced by module `fortios_monitor`, see selector `upload.system.vmlicense`.
- **`fortios_system_config_backup_restore`: it was a complexed module.**
  - To backup the FOS system, use module `fortios_monitor_fact` and its selector `system_config_backup`.
  - To restore the configuration, use module `fortios_monitor` and its selector `restore.system.config`.

10.5 Legacy Multiversions Note(Prior to 2.0.0)

The FortiOS Galaxy namespace: `fortinet.fortios` hosts Ansible modules for multiple FortiOS major releases.

A mismatched Ansible collection version for a FortiOS device can cause a warning:

```
[WARNING]: Ansible has detected version mismatch between FortOS system and galaxy,␣
↪see more details by specifying option -vvv
```

you can find more details with `-vvv` option when running a playbook:

```
...
"version_check_warning": {
    "ansible_collection_version": "v6.0.0 (galaxy: 1.0.13)",
    "matched": false,
    "message": "Please follow steps in FortiOS versioning notes: https://ansible-
↪galaxy-fortios-docs.readthedocs.io/en/latest/version.html",
```

(continues on next page)

(continued from previous page)

```
    "system_version": "v6.2.0"
}
...
```

Simply installing a matched FortiOS collection can prevent potential compatibility issues.

10.6 Release Galaxy 1.1.9

10.6.1 Release Targets

- fos_v6.0.0/galaxy_1.1.9

10.6.2 Bug Fixes

- Fix legacy module `fortios_system_config_backup_restore`

10.7 Release Galaxy 1.1.6 . . . 1.1.8

10.7.1 Release Targets

There are multiple Galaxy releases dedicated to different FortiOS major releases.

- fos_v6.2.0/galaxy_1.1.6
- fos_v6.4.0/galaxy_1.1.7
- fos_v6.0.0/galaxy_1.1.8

10.7.2 Bug Fixes

- Fixed module construction for legacy module `fortios_facts`.
- Sorted selector list of module `fortios_configuration_fact`.

10.8 Release Galaxy 1.1.3 . . . 1.1.5

10.8.1 Release Targets

There are multiple Galaxy releases dedicated to different FortiOS major releases.

- fos_v6.2.0/galaxy_1.1.3
- fos_v6.4.0/galaxy_1.1.4
- fos_v6.0.0/galaxy_1.1.5

10.8.2 Bug Fixes

- Fixed a fatal error: `mkey` not recognized in plugin due to wrong naming convention.

10.9 Release Galaxy 1.1.0 . . . 1.1.2

10.9.1 Release Targets

There are multiple Galaxy releases dedicated to different FortiOS major releases.

- fos_v6.2.0/galaxy_1.1.0
- fos_v6.4.0/galaxy_1.1.1
- fos_v6.0.0/galaxy_1.1.2

10.9.2 Features

- Support check mode for modules.
- Deprecate `fortiosapi` legacy connection mode.
- Support access token based authentication.
- Fully support fact gathering for all configuration API (`fortios_configuration_fact`).
- Suport Ansible 2.10 base framework.
- Support moving objects to different orders (`fortios_firewall_policy`).

10.9.3 Bug Fixes

- Github Issue #65

10.10 Release Galaxy 1.0.10 . . . 10.0.13

10.10.1 Release Targets

There are multiple Galaxy releases dedicated to different FortiOS major releases.

- fos_v6.0.0/galaxy_1.0.13
- fos_v6.0.5/galaxy_1.0.12
- fos_v6.4.0/galaxy_1.0.11
- fos_v6.2.0/galaxy_1.0.10

10.10.2 New Modules

#	Module Name	New in 6.2	New in 6.4
1	fortios_cifs_domain_controller	yes	yes
2	fortios_cifs_profile	yes	yes
3	fortios_dlp_sensitivity	yes	yes
4	fortios_emailfilter_bwl	yes	yes
5	fortios_emailfilter_bword	yes	yes
6	fortios_emailfilter_dnsbl	yes	yes
7	fortios_emailfilter_fortishield	yes	yes
8	fortios_emailfilter_iptrust	yes	yes
9	fortios_emailfilter_mheader	yes	yes
10	fortios_emailfilter_options	yes	yes
11	fortios_emailfilter_profile	yes	yes
12	fortios_endpoint_control_fctems	yes	yes
13	fortios_firewall_consolidated_policy	yes	yes
14	fortios_firewall_internet_service_addition	yes	yes
15	fortios_firewall_internet_service_cat_definition	yes	no
16	fortios_firewall_internet_service_definition	yes	yes
17	fortios_firewall_internet_service_extension	yes	yes
18	fortios_log_fortianalyzer2_override_filter	yes	yes
19	fortios_log_fortianalyzer2_override_setting	yes	yes
20	fortios_log_fortianalyzer3_override_filter	yes	yes
21	fortios_log_fortianalyzer3_override_setting	yes	yes
22	fortios_log_fortianalyzer_cloud_filter	yes	yes
23	fortios_log_fortianalyzer_cloud_override_filter	yes	yes
24	fortios_log_fortianalyzer_cloud_override_setting	yes	yes
25	fortios_log_fortianalyzer_cloud_setting	yes	yes
26	fortios_log_syslogd2_override_filter	yes	yes
27	fortios_log_syslogd2_override_setting	yes	yes
28	fortios_log_syslogd3_override_filter	yes	yes
29	fortios_log_syslogd3_override_setting	yes	yes
30	fortios_log_syslogd4_override_filter	yes	yes
31	fortios_log_syslogd4_override_setting	yes	yes
32	fortios_switch_controller_auto_config_custom	yes	yes
33	fortios_switch_controller_auto_config_default	yes	yes
34	fortios_switch_controller_auto_config_policy	yes	yes
35	fortios_switch_controller_flow_tracking	yes	yes
36	fortios_switch_controller_location	yes	yes
37	fortios_switch_controller_security_policy_local_access	yes	yes
38	fortios_switch_controller_storm_control_policy	yes	yes
39	fortios_switch_controller_stp_instance	yes	yes
40	fortios_switch_controller_traffic_policy	yes	yes
41	fortios_switch_controller_traffic_sniffer	yes	yes
42	fortios_system_ipsec_aggregate	yes	yes
43	fortios_system_lldp_network_policy	yes	yes
44	fortios_system_nd_proxy	yes	yes
45	fortios_system_npu	yes	yes
46	fortios_system_ptp	yes	yes
47	fortios_system_saml	yes	yes

Continued on next page

Table 1 – continued from previous page

#	Module Name	New in 6.2	New in 6.4
48	fortios_system_speed_test_server	yes	yes
49	fortios_system_sso_admin	yes	yes
50	fortios_user_exchange	yes	yes
51	fortios_wireless_controller_address	yes	yes
52	fortios_wireless_controller_addrgrp	yes	yes
53	fortios_wireless_controller_log	yes	yes
54	fortios_wireless_controller_region	yes	yes
55	fortios_wireless_controller_snmp	yes	yes
56	fortios_certificate_remote	no	yes
57	fortios_credential_store_domain_controller	no	yes
58	fortios_dpdk_cpus	no	yes
59	fortios_dpdk_global	no	yes
60	fortios_extender_modem_status	no	yes
61	fortios_extender_sys_info	no	yes
62	fortios_firewall_city	no	yes
63	fortios_firewall_country	no	yes
64	fortios_firewall_decrypted_traffic_mirror	no	yes
65	fortios_firewall_internet_service_botnet	no	yes
66	fortios_firewall_internet_service_ipbl_reason	no	yes
67	fortios_firewall_internet_service_ipbl_vendor	no	yes
68	fortios_firewall_internet_service_list	no	yes
69	fortios_firewall_internet_service_name	no	yes
70	fortios_firewall_internet_service_owner	no	yes
71	fortios_firewall_internet_service_reputation	no	yes
72	fortios_firewall_internet_service_sld	no	yes
73	fortios_firewall_iprope_list	no	yes
74	fortios_firewall_proute	no	yes
75	fortios_firewall_region	no	yes
76	fortios_firewall_security_policy	no	yes
77	fortios_firewall_traffic_class	no	yes
78	fortios_firewall_vendor_mac	no	yes
79	fortios_hardware_nic	no	yes
80	fortios_ips_view_map	no	yes
81	fortios_switch_controller_initial_config_template	no	yes
82	fortios_switch_controller_initial_config_vlans	no	yes
83	fortios_switch_controller_mac_policy	no	yes
84	fortios_switch_controller_nac_device	no	yes
85	fortios_switch_controller_nac_settings	no	yes
86	fortios_switch_controller_poe	no	yes
87	fortios_switch_controller_port_policy	no	yes
88	fortios_switch_controller_remote_log	no	yes
89	fortios_switch_controller_snmp_community	no	yes
90	fortios_switch_controller_snmp_sysinfo	no	yes
91	fortios_switch_controller_snmp_trap_threshold	no	yes
92	fortios_switch_controller_snmp_user	no	yes
93	fortios_switch_controller_vlan_policy	no	yes
94	fortios_system_geneve	no	yes
95	fortios_system_geoip_country	no	yes
96	fortios_system_performance_top	no	yes

Continued on next page

Table 1 – continued from previous page

#	Module Name	New in 6.2	New in 6.4
97	fortios_system_standalone_cluster	no	yes
98	fortios_test_acd	no	yes
99	fortios_test_acid	no	yes
100	fortios_test_autod	no	yes
101	fortios_test_awsd	no	yes
102	fortios_test_azd	no	yes
103	fortios_test_bfd	no	yes
104	fortios_test_csfd	no	yes
105	fortios_test_ddnscd	no	yes
106	fortios_test_dhcp6c	no	yes
107	fortios_test_dhcp6r	no	yes
108	fortios_test_dhcprelay	no	yes
109	fortios_test_dlpfingerprint	no	yes
110	fortios_test_dlpfpcache	no	yes
111	fortios_test_dnsproxy	no	yes
112	fortios_test_dsd	no	yes
113	fortios_test_fas	no	yes
114	fortios_test_fcnacd	no	yes
115	fortios_test_fnbamd	no	yes
116	fortios_test_forticldd	no	yes
117	fortios_test_forticron	no	yes
118	fortios_test_fsd	no	yes
119	fortios_test_fsvrd	no	yes
120	fortios_test_ftpd	no	yes
121	fortios_test_gcpd	no	yes
122	fortios_test_harelay	no	yes
123	fortios_test_hasync	no	yes
124	fortios_test_hatalk	no	yes
125	fortios_test_imap	no	yes
126	fortios_test_info_sslvpnd	no	yes
127	fortios_test_init	no	yes
128	fortios_test_iotd	no	yes
129	fortios_test_ipamd	no	yes
130	fortios_test_ipldbd	no	yes
131	fortios_test_ipsengine	no	yes
132	fortios_test_ipsmonitor	no	yes
133	fortios_test_ipsufd	no	yes
134	fortios_test_kubed	no	yes
135	fortios_test_l2tpcd	no	yes
136	fortios_test_lnkmtd	no	yes
137	fortios_test_lted	no	yes
138	fortios_test_miglogd	no	yes
139	fortios_test_mrd	no	yes
140	fortios_test_netxd	no	yes
141	fortios_test_nntp	no	yes
142	fortios_test_ocid	no	yes
143	fortios_test_openstackd	no	yes
144	fortios_test_ovrd	no	yes
145	fortios_test_pop3	no	yes

Continued on next page

Table 1 – continued from previous page

#	Module Name	New in 6.2	New in 6.4
146	fortios_test_pptpcd	no	yes
147	fortios_test_quarantined	no	yes
148	fortios_test_radius_das	no	yes
149	fortios_test_radiusd	no	yes
150	fortios_test_radvd	no	yes
151	fortios_test_reportd	no	yes
152	fortios_test_sdncd	no	yes
153	fortios_test_sepmd	no	yes
154	fortios_test_sessionsync	no	yes
155	fortios_test_sflowd	no	yes
156	fortios_test_smtp	no	yes
157	fortios_test_snmpd	no	yes
158	fortios_test_uploadd	no	yes
159	fortios_test_urlfilter	no	yes
160	fortios_test_vmwd	no	yes
161	fortios_test_wad	no	yes
162	fortios_test_wccpd	no	yes
163	fortios_test_wf_monitor	no	yes
164	fortios_test_zebos_launcher	no	yes
165	fortios_user_nac_policy	no	yes
166	fortios_user_saml	no	yes
167	fortios_vpn_ike_gateway	no	yes
168	fortios_webfilter_status	no	yes
169	fortios_wireless_controller_access_control_list	no	yes
170	fortios_wireless_controller_apcfg_profile	no	yes
171	fortios_wireless_controller_client_info	no	yes
172	fortios_wireless_controller_rf_analysis	no	yes
173	fortios_wireless_controller_spectral_info	no	yes
174	fortios_wireless_controller_status	no	yes
175	fortios_wireless_controller_vap_status	no	yes
176	fortios_wireless_controller_wag_profile	no	yes
177	fortios_wireless_controller_wtp_status	no	yes

10.10.3 Features

- Support special identifier validation and restoration in Ansible modules.
- Support more valid identifiers: `3gpp_plmn`, `802_1X_settings`, `802.1_tlvs` and `802.3_tlvs`.
- Support `revision_change` in response since fortigate 6.2.3.
- Support Underscore to hypen conversion.
- Support licence modules: `fortios_system_vmlicense`, `fortios_registration_forticare` and `fortios_registration_vdom`.
- Support raw json encoding for generic module.

10.10.4 Bug Fixes

- Fix `fgd_alert_subscription` multiple choices problem for module `fortios_system_global`.
- Fix `proposal` exceptional multilist for module `fortios_vpn_ipsec_phase2_interface`.

- Fix issue #26 of ansible_fgt_modules.
- Fix issue #24 of ansible_fgt_modules.
- Fix `events` exceptional multilist for module `fortios_system_snmp_community`.
- Fix py2/py3 compability issue for httpapi plugin fortios.
- Fix the mkey encoding in fortios api URL.
- Fix `banned_cipher` exceptional multilist for module `fortios_vpn_ssl_settings`.