Ansible Galaxy FortiOS Collection

Release 1.0

Mar 01, 2021

FortiOS/Galaxy Version Mapping Guide

1 FortiOS Galaxy Versioning 3

2 Install FortiOS Ansible Galaxy 5

3 Run Your First Playbook 7

4 Get Help 9

5 Configuration Modules 11

6 Facts Gathering Modules 917

7 Release Notes 923

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

CHAPTER 1

FortiOS Galaxy Versioning

The FortiOS galaxy collection is accommodating for all major FortiOS releases. Please choose the right Galaxy collection to install from the following table in case of any 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 `latest`	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 `latest`	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 `latest`	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: module `fortios_system_vmlicense` allows you to upload the licence with http, in this case, you should set `ansible_httpapi_use_ssl: no` and `ansible_httpapi_port: 80`

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

Get Help

4.1 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

4.2 Filing issues.

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

CHAPTER 5

Configuration Modules

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

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.1.1 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

5.1.2 Requirements

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

- ansible>=2.9.0

5.1.3 Parameters

5.1.4 Notes

Note:

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

5.1.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        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>"
```

(continues on next page)

(continued from previous page)

```
        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"
```

5.1.6 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:

5.1.7 Status

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

5.1.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*

- *Return Values*
- *Status*
- *Authors*

5.2.1 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

5.2.2 Requirements

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

- ansible>=2.9.0

5.2.3 Parameters

5.2.4 Notes

Note:

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

5.2.5 Examples

```
- hosts: fortigates
  collections:
    - 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.
    fortios_antivirus_heuristic:
      vdom:  "{{ vdom }}"
      antivirus_heuristic:
        mode: "pass"
```

5.2.6 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:

5.2.7 Status

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

5.2.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.3.1 Synopsis

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

5.3.2 Requirements

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

- ansible>=2.9.0

5.3.3 Parameters

5.3.4 Notes

Note:

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

5.3.5 Examples

```
- hosts: fortigates
  collections:
    - 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_bl_filetype: "3 (source dlp.filepattern.id)"
        analytics_db: "disable"
        analytics_max_upload: "5"
        analytics_wl_filetype: "6 (source dlp.filepattern.id)"
        av_block_log: "enable"
        av_virus_log: "enable"
        comment: "Comment."
        content_disarm:
            cover_page: "disable"
            detect_only: "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"
        extended_log: "enable"
        ftgd_analytics: "disable"
        ftp:
            archive_block: "encrypted"
```

(continues on next page)

(continued from previous page)

```
            archive_log: "encrypted"
            emulator: "enable"
            options: "scan"
            outbreak_prevention: "disabled"
        http:
            archive_block: "encrypted"
            archive_log: "encrypted"
            content_disarm: "disable"
            emulator: "enable"
            options: "scan"
            outbreak_prevention: "disabled"
        imap:
            archive_block: "encrypted"
            archive_log: "encrypted"
            content_disarm: "disable"
            emulator: "enable"
            executables: "default"
            options: "scan"
            outbreak_prevention: "disabled"
        inspection_mode: "proxy"
        mapi:
            archive_block: "encrypted"
            archive_log: "encrypted"
            emulator: "enable"
            executables: "default"
            options: "scan"
            outbreak_prevention: "disabled"
        mobile_malware_db: "disable"
        nac_quar:
            expiry: "<your_own_value>"
            infected: "none"
            log: "enable"
        name: "default_name_63"
        nntp:
            archive_block: "encrypted"
            archive_log: "encrypted"
            emulator: "enable"
            options: "scan"
            outbreak_prevention: "disabled"
        pop3:
            archive_block: "encrypted"
            archive_log: "encrypted"
            content_disarm: "disable"
            emulator: "enable"
            executables: "default"
            options: "scan"
            outbreak_prevention: "disabled"
        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"
```

(continues on next page)

(continued from previous page)

```
            archive_log: "encrypted"
            content_disarm: "disable"
            emulator: "enable"
            executables: "default"
            options: "scan"
            outbreak_prevention: "disabled"
```

5.3.6 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:

5.3.7 Status

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

5.3.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*

- *Authors*

5.4.1 Synopsis

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

5.4.2 Requirements

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

- ansible>=2.9.0

5.4.3 Parameters

5.4.4 Notes

Note:

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

5.4.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        destination: "NULL"
        drop_blocked: "imap"
        drop_heuristic: "imap"
        drop_infected: "imap"
        lowspace: "drop-new"
        maxfilesize: "9"
        quarantine_quota: "10"
        store_blocked: "imap"
        store_heuristic: "imap"
        store_infected: "imap"
```

5.4.6 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:

5.4.7 Status

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

5.4.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.5.1 Synopsis

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

5.5.2 Requirements

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

- ansible>=2.9.0

5.5.3 Parameters

5.5.4 Notes

Note:

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

5.5.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        grayware: "enable"
        override_timeout: "5"
```

5.5.6 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:

5.5.7 Status

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

5.5.8 Authors

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

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.6.1 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

5.6.2 Requirements

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

- ansible>=2.9.0

5.6.3 Parameters

5.6.4 Notes

Note:

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

5.6.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
        tag: "<your_own_value>"
        technology: "<your_own_value>"
        vendor: "<your_own_value>"
```

5.6.6 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:

5.6.7 Status

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

5.6.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.7.1 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

5.7.2 Requirements

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

- ansible>=2.9.0

5.7.3 Parameters

5.7.4 Notes

Note:

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

5.7.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       category:
        -
           id:  "6"
       comment: "Comment"
       name: "default_name_8"
       type: "application"
```

5.7.6 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:

5.7.7 Status

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

5.7.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.8.1 Synopsis

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

5.8.2 Requirements

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

- ansible>=2.9.0

5.8.3 Parameters

5.8.4 Notes

Note:

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

5.8.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      application_list:
        app_replacemsg: "disable"
        comment: "comments"
        deep_app_inspection: "disable"
        entries:
         -
            action: "pass"
            application:
             -
                id:  "9"
            behavior: "<your_own_value>"
            category:
             -
                id:  "12"
            id:  "13"
            log: "disable"
            log_packet: "disable"
            parameters:
             -
                id:  "17"
                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: "25"
            rate_duration: "26"
            rate_mode: "periodical"
            rate_track: "none"
            risk:
             -
                level: "30"
            session_ttl: "31"
            shaper: "<your_own_value> (source firewall.shaper.traffic-shaper.name)"
            shaper_reverse: "<your_own_value> (source firewall.shaper.traffic-shaper.
↪name)"
            sub_category:
             -
                id:  "35"
            technology: "<your_own_value>"
            vendor: "<your_own_value>"
        extended_log: "enable"
        name: "default_name_39"
        options: "allow-dns"
        other_application_action: "pass"
        other_application_log: "disable"
        p2p_black_list: "skype"
        replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
        unknown_application_action: "pass"
        unknown_application_log: "disable"
```

5.8.6 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:

5.8.7 Status

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

5.8.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.9.1 Synopsis

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

5.9.2 Requirements

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

- ansible>=2.9.0

5.9.3 Parameters

5.9.4 Notes

Note:

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

5.9.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
         -
            id:  "7"
            metaid: "8"
            valueid: "9"
        name: "default_name_10"
        parameter: "<your_own_value>"
        popularity: "12"
        protocol: "<your_own_value>"
        risk: "14"
        sub_category: "15"
        technology: "<your_own_value>"
        vendor: "<your_own_value>"
        weight: "18"
```

5.9.6 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:

5.9.7 Status

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

5.9.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.10.1 Synopsis

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

5.10.2 Requirements

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

- ansible>=2.9.0

5.10.3 Parameters

5.10.4 Notes

Note:

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

5.10.5 Examples

```
- hosts: fortigates
  collections:
    - 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 rule settings.
    fortios_application_rule_settings:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      application_rule_settings:
        id:  "3"
```

5.10.6 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:

5.10.7 Status

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

5.10.8 Authors

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

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.11.1 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

5.11.2 Requirements

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

- ansible>=2.9.0

5.11.3 Parameters

5.11.4 Notes

Note:

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

5.11.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
        ip_based: "enable"
        name: "default_name_6"
        protocol: "http"
        srcaddr:
         -
            name: "default_name_9 (source firewall.address.name firewall.addrgrp.name␣
↪firewall.proxy-address.name firewall.proxy-addrgrp.name)"
        srcaddr6:
         -
            name: "default_name_11 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        sso_auth_method: "<your_own_value> (source authentication.scheme.name)"
        status: "enable"
        transaction_based: "enable"
        web_auth_cookie: "enable"
```

5.11.6 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:

5.11.7 Status

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

5.11.8 Authors

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

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.12.1 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

5.12.2 Requirements

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

- ansible>=2.9.0

5.12.3 Parameters

5.12.4 Notes

Note:

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

5.12.5 Examples

```
- hosts: fortigates
  collections:
    - 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)"
        fsso_agent_for_ntlm: "<your_own_value> (source user.fsso.name)"
        fsso_guest: "enable"
        method: "ntlm"
        name: "default_name_7"
        negotiate_ntlm: "enable"
        require_tfa: "enable"
        ssh_ca: "<your_own_value> (source firewall.ssh.local-ca.name)"
        user_database:
         -
            name: "default_name_12 (source system.datasource.name user.radius.name␣
↪user.tacacs+.name user.ldap.name user.group.name)"
```

5.12.6 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:

5.12.7 Status

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

5.12.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.13.1 Synopsis

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

5.13.2 Requirements

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

- ansible>=2.9.0

5.13.3 Parameters

5.13.4 Notes

Note:

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

5.13.5 Examples

```
- hosts: fortigates
  collections:
    - 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)"
        captive_portal: "<your_own_value> (source firewall.address.name)"
        captive_portal_ip: "<your_own_value>"
        captive_portal_ip6: "<your_own_value>"
        captive_portal_port: "7"
        captive_portal_type: "fqdn"
        captive_portal6: "<your_own_value> (source firewall.address6.name)"
        sso_auth_scheme: "<your_own_value> (source authentication.scheme.name)"
```

5.13.6 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:

5.13.7 Status

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

5.13.8 Authors

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

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

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

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.14.1 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

5.14.2 Requirements

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

- ansible>=2.9.0

5.14.3 Parameters

5.14.4 Notes

Note:

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

5.14.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
      trusted: "enable"
```

5.14.6 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:

5.14.7 Status

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

5.14.8 Authors

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

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

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

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.15.1 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

5.15.2 Requirements

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

- ansible>=2.9.0

5.15.3 Parameters

5.15.4 Notes

Note:

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

5.15.5 Examples

```
- hosts: fortigates
  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:
```

(continues on next page)

(continued from previous page)

```
    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)"
```

5.15.6 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:

5.15.7 Status

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

5.15.8 Authors

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

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

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

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.16.1 Synopsis

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

5.16.2 Requirements

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

- ansible>=2.9.0

5.16.3 Parameters

5.16.4 Notes

Note:

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

5.16.5 Examples

```
- hosts: fortigates
  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:
```

(continues on next page)

(continued from previous page)

```
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    certificate_local:
      auto_regenerate_days: "3"
      auto_regenerate_days_warning: "4"
      ca_identifier:  "myId_5"
      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: "16"
      name: "default_name_17"
      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>"
```

5.16.6 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:

5.16.7 Status

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

5.16.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.17.1 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

5.17.2 Requirements

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

- ansible>=2.9.0

5.17.3 Parameters

5.17.4 Notes

Note:

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

5.17.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.17.6 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:

5.17.7 Status

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

5.17.8 Authors

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

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

5.18 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 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.18.1 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

5.18.2 Requirements

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

- ansible>=2.9.0

5.18.3 Parameters

5.18.4 Notes

Note:

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

5.18.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.18.6 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:

5.18.7 Status

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

5.18.8 Authors

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

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

5.19 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 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.19.1 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

5.19.2 Requirements

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

- ansible>=2.9.0

5.19.3 Parameters

5.19.4 Notes

Note:

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

5.19.5 Examples

```
- hosts: fortigates
  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"
```

5.19.6 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:

5.19.7 Status

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

5.19.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.20.1 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

5.20.2 Requirements

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

- ansible>=2.9.0

5.20.3 Parameters

5.20.4 Notes

Note:

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

5.20.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    dlp_sensor:
      comment: "Comment."
      dlp_log: "enable"
      extended_log: "enable"
      filter:
       -
          action: "allow"
          archive: "disable"
          company_identifier:  "myId_9"
          expiry: "<your_own_value>"
          file_size: "11"
          file_type: "12 (source dlp.filepattern.id)"
          filter_by: "credit-card"
          fp_sensitivity:
           -
              name: "default_name_15 (source dlp.fp-sensitivity.name)"
          id:  "16"
          match_percentage: "17"
          name: "default_name_18"
          proto: "smtp"
          regexp: "<your_own_value>"
          severity: "info"
          type: "file"
      flow_based: "enable"
      full_archive_proto: "smtp"
      nac_quar_log: "enable"
      name: "default_name_26"
      options: "<your_own_value>"
      replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
      summary_proto: "smtp"
```

5.20.6 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:

5.20.7 Status

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

5.20.8 Authors

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

- Nicolas Thomas (@thomnico)

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.21.1 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

5.21.2 Requirements

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

- ansible>=2.9.0

5.21.3 Parameters

5.21.4 Notes

Note:

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

5.21.5 Examples

```
- hosts: fortigates
  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)"
```

5.21.6 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:

5.21.7 Status

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

5.21.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.22.1 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

5.22.2 Requirements

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

- ansible>=2.9.0

5.22.3 Parameters

5.22.4 Notes

Note:

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

5.22.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    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"
```

5.22.6 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:

5.22.7 Status

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

5.22.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*

- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.23.1 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

5.23.2 Requirements

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

- ansible>=2.9.0

5.23.3 Parameters

5.23.4 Notes

Note:

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

5.23.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
        block_botnet: "disable"
        comment: "Comment."
        domain_filter:
            domain_filter_table: "7 (source dnsfilter.domain-filter.id)"
        external_ip_blocklist:
         -
            name: "default_name_9 (source system.external-resource.name)"
        ftgd_dns:
            filters:
             -
                action: "block"
                category: "13"
                id:  "14"
                log: "enable"
            options: "error-allow"
        log_all_domain: "enable"
        name: "default_name_18"
        redirect_portal: "<your_own_value>"
        safe_search: "disable"
        sdns_domain_log: "enable"
        sdns_ftgd_err_log: "enable"
        youtube_restrict: "strict"
```

5.23.6 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:

5.23.7 Status

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

5.23.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.24.1 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

5.24.2 Requirements

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

- ansible>=2.9.0

5.24.3 Parameters

5.24.4 Notes

Note:

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

5.24.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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:
      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>"
```

5.24.6 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:

5.24.7 Status

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

5.24.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.25.1 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

5.25.2 Requirements

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

- ansible>=2.9.0

5.25.3 Parameters

5.25.4 Notes

Note:

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

5.25.5 Examples

```
- hosts: fortigates
  collections:
    - 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_forticlient_ems:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    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"
```

5.25.6 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:

5.25.7 Status

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

5.25.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*

- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.26.1 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

5.26.2 Requirements

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

- ansible>=2.9.0

5.26.3 Parameters

5.26.4 Notes

Note:

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

5.26.5 Examples

```
- hosts: fortigates
  collections:
    - 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 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>"
```

5.26.6 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:

5.26.7 Status

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

5.26.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.27.1 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

5.27.2 Requirements

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

- ansible>=2.9.0

5.27.3 Parameters

5.27.4 Notes

Note:

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

5.27.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        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)"
```

(continues on next page)

(continued from previous page)

```
        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>"
            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>"
```

(continues on next page)

(continued from previous page)

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

5.27.6 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:

5.27.7 Status

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

5.27.8 Authors

- Link Zheng (@chillancezen)

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

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

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

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.28.1 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

5.28.2 Requirements

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

- ansible>=2.9.0

5.28.3 Parameters

5.28.4 Notes

Note:

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

5.28.5 Examples

```
- hosts: fortigates
  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>"
```

5.28.6 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:

5.28.7 Status

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

5.28.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.29.1 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

5.29.2 Requirements

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

- ansible>=2.9.0

5.29.3 Parameters

5.29.4 Notes

Note:

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

5.29.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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_ems_rest_api_call_timeout: "7"
      forticlient_keepalive_interval: "8"
      forticlient_offline_grace: "enable"
      forticlient_offline_grace_interval: "10"
      forticlient_reg_key: "<your_own_value>"
      forticlient_reg_key_enforce: "enable"
      forticlient_reg_timeout: "13"
      forticlient_sys_update_interval: "14"
      forticlient_user_avatar: "enable"
      forticlient_warning_interval: "16"
```

5.29.6 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:

5.29.7 Status

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

5.29.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.30.1 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

5.30.2 Requirements

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

- ansible>=2.9.0

5.30.3 Parameters

5.30.4 Notes

Note:

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

5.30.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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>"
       billing_start_day: "7"
       cdma_aaa_spi: "<your_own_value>"
       cdma_ha_spi: "<your_own_value>"
       cdma_nai: "<your_own_value>"
       conn_status: "11"
       description: "<your_own_value>"
       dial_mode: "dial-on-demand"
       dial_status: "14"
       ext_name: "<your_own_value>"
       ha_shared_secret: "<your_own_value>"
       id:  "17"
       ifname: "<your_own_value>"
       initiated_update: "enable"
       mode: "standalone"
       modem_passwd: "<your_own_value>"
       modem_type: "cdma"
       multi_mode: "auto"
       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: "29"
       redial: "none"
       redundant_intf: "<your_own_value>"
       roaming: "enable"
       role: "none"
       secondary_ha: "<your_own_value>"
       sim_pin: "<your_own_value>"
       vdom: "36"
       wimax_auth_protocol: "tls"
       wimax_carrier: "<your_own_value>"
       wimax_realm: "<your_own_value>"
```

5.30.6 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:

5.30.7 Status

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

5.30.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.31.1 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

5.31.2 Requirements

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

- ansible>=2.9.0

5.31.3 Parameters

5.31.4 Notes

Note:

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

5.31.5 Examples

```
- hosts: fortigates
  collections:
    - 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 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"
        color: "6"
        comment: "Comment."
        country: "<your_own_value>"
        end_ip: "<your_own_value>"
        epg_name: "<your_own_value>"
        filter: "<your_own_value>"
        fqdn: "<your_own_value>"
        list:
         -
            ip: "<your_own_value>"
        name: "default_name_15"
        obj_id: "16"
        organization: "<your_own_value>"
        policy_group: "<your_own_value>"
        sdn: "aci"
        sdn_tag: "<your_own_value>"
        start_ip: "<your_own_value>"
        subnet: "<your_own_value>"
        subnet_name: "<your_own_value>"
        tagging:
         -
            category: "<your_own_value> (source system.object-tagging.category)"
            name: "default_name_26"
            tags:
```

(continues on next page)

(continued from previous page)

```
            -
                name: "default_name_28 (source system.object-tagging.tags.name)"
        tenant: "<your_own_value>"
        type: "ipmask"
        uuid: "<your_own_value>"
        visibility: "enable"
        wildcard: "<your_own_value>"
        wildcard_fqdn: "<your_own_value>"
```

5.31.6 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:

5.31.7 Status

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

5.31.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*

- *Status*
- *Authors*

5.32.1 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

5.32.2 Requirements

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

- ansible>=2.9.0

5.32.3 Parameters

5.32.4 Notes

Note:

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

5.32.5 Examples

```
- hosts: fortigates
  collections:
    - 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."
        end_ip: "<your_own_value>"
        fqdn: "<your_own_value>"
        host: "<your_own_value>"
        host_type: "any"
        ip6: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        list:
         -
            ip: "<your_own_value>"
        name: "default_name_13"
        obj_id: "14"
        sdn: "nsx"
        start_ip: "<your_own_value>"
        subnet_segment:
         -
            name: "default_name_18"
            type: "any"
            value: "<your_own_value>"
        tagging:
         -
            category: "<your_own_value> (source system.object-tagging.category)"
            name: "default_name_23"
            tags:
             -
                name: "default_name_25 (source system.object-tagging.tags.name)"
        template: "<your_own_value> (source firewall.address6-template.name)"
        type: "ipprefix"
        uuid: "<your_own_value>"
        visibility: "enable"
```

5.32.6 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:

5.32.7 Status

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

5.32.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.33.1 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

5.33.2 Requirements

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

- ansible>=2.9.0

5.33.3 Parameters

5.33.4 Notes

Note:

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

5.33.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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:
       ip6: "<your_own_value>"
       name: "default_name_4"
       subnet_segment:
        -
           bits: "6"
           exclusive: "enable"
           id:  "8"
           name: "default_name_9"
           values:
            -
               name: "default_name_11"
               value: "<your_own_value>"
       subnet_segment_count: "13"
```

5.33.6 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:

5.33.7 Status

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

5.33.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.34.1 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

5.34.2 Requirements

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

- ansible>=2.9.0

5.34.3 Parameters

5.34.4 Notes

Note:

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

5.34.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       color: "4"
       comment: "Comment."
       member:
        -
           name: "default_name_7 (source firewall.address.name firewall.addrgrp.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"
```

5.34.6 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:

5.34.7 Status

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

5.34.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.35.1 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

5.35.2 Requirements

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

- ansible>=2.9.0

5.35.3 Parameters

5.35.4 Notes

Note:

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

5.35.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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."
       member:
        -
           name: "default_name_6 (source firewall.address6.name firewall.addrgrp6.
↪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)"
       uuid: "<your_own_value>"
       visibility: "enable"
```

5.35.6 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:

5.35.7 Status

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

5.35.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.36.1 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

5.36.2 Requirements

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

- ansible>=2.9.0

5.36.3 Parameters

5.36.4 Notes

Note:

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

5.36.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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>"
```

5.36.6 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:

5.36.7 Status

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

5.36.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*

- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.37.1 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

5.37.2 Requirements

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

- ansible>=2.9.0

5.37.3 Parameters

5.37.4 Notes

Note:

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

5.37.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
        comments: "<your_own_value>"
        dst_addr:
         -
            name: "default_name_5 (source firewall.address.name firewall.addrgrp.name)
↪"
        dstintf:
         -
            name: "default_name_7 (source system.interface.name system.zone.name)"
        nat: "disable"
        nat_ippool:
         -
            name: "default_name_10 (source firewall.ippool.name)"
        nat_port: "<your_own_value>"
        orig_addr:
         -
            name: "default_name_13 (source firewall.address.name firewall.addrgrp.
↪name)"
        orig_port: "<your_own_value>"
        policyid: "15"
        protocol: "16"
        srcintf:
         -
            name: "default_name_18 (source system.interface.name system.zone.name)"
        status: "enable"
```

5.37.6 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:

5.37.7 Status

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

5.37.8 Authors

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

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

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

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.38.1 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

5.38.2 Requirements

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

- ansible>=2.9.0

5.38.3 Parameters

5.38.4 Notes

Note:

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

5.38.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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>"
```

5.38.6 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:

5.38.7 Status

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

5.38.8 Authors

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

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

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

New in version 2.10.

- *Synopsis*
- *Requirements*

- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.39.1 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

5.39.2 Requirements

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

- ansible>=2.9.0

5.39.3 Parameters

5.39.4 Notes

Note:

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

5.39.5 Examples

```
- hosts: fortigates
  collections:
    - 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 DoS policies.
    fortios_firewall_dos_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_dos_policy:
        anomaly:
```

(continues on next page)

(continued from previous page)

```
        -
            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)"
        policyid: "17"
        service:
        -
            name: "default_name_19 (source firewall.service.custom.name firewall.
↪service.group.name)"
        srcaddr:
        -
            name: "default_name_21 (source firewall.address.name firewall.addrgrp.
↪name)"
        status: "enable"
```

5.39.6 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:

5.39.7 Status

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

5.39.8 Authors

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

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

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

New in version 2.10.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.40.1 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

5.40.2 Requirements

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

- ansible>=2.9.0

5.40.3 Parameters

5.40.4 Notes

Note:

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

5.40.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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)"
       policyid: "17"
       service:
        -
           name: "default_name_19 (source firewall.service.custom.name firewall.
↪service.group.name)"
       srcaddr:
        -
           name: "default_name_21 (source firewall.address6.name firewall.addrgrp6.
↪name)"
       status: "enable"
```

5.40.6 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:

5.40.7 Status

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

5.40.8 Authors

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

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

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

5.41 fortios_firewall_identity_based_route – Configure identity based routing in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.41.1 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

5.41.2 Requirements

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

- ansible>=2.9.0

5.41.3 Parameters

5.41.4 Notes

Note:

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

5.41.5 Examples

```
- hosts: fortigates
  collections:
    - 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)"
            gateway: "<your_own_value>"
            groups:
             -
                name: "default_name_9 (source user.group.name)"
            id:  "10"
```

5.41.6 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:

5.41.7 Status

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

5.41.8 Authors

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

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

5.42 fortios_firewall_interface_policy – Configure IPv4 interface policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.42.1 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

5.42.2 Requirements

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

- ansible>=2.9.0

5.42.3 Parameters

5.42.4 Notes

Note:

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

5.42.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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)"
       dlp_sensor_status: "enable"
       dsri: "enable"
       dstaddr:
        -
           name: "default_name_13 (source firewall.address.name firewall.addrgrp.
↪name)"
       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: "19"
       scan_botnet_connections: "disable"
       service:
        -
           name: "default_name_22 (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_26 (source firewall.address.name firewall.addrgrp.
↪name)"
       status: "enable"
       webfilter_profile: "<your_own_value> (source webfilter.profile.name)"
       webfilter_profile_status: "enable"
```

5.42.6 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:

5.42.7 Status

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

5.42.8 Authors

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

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

5.43 fortios_firewall_interface_policy6 – Configure IPv6 interface policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.43.1 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

5.43.2 Requirements

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

- ansible>=2.9.0

5.43.3 Parameters

5.43.4 Notes

Note:

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

5.43.5 Examples

```
- hosts: fortigates
  collections:
    - 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)"
        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: "19"
        scan_botnet_connections: "disable"
        service6:
         -
            name: "default_name_22 (source firewall.service.custom.name firewall.
↪service.group.name)"
        spamfilter_profile: "<your_own_value> (source spamfilter.profile.name)"
        spamfilter_profile_status: "enable"
        srcaddr6:
         -
```

(continues on next page)

(continued from previous page)

```
            name: "default_name_26 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        status: "enable"
        webfilter_profile: "<your_own_value> (source webfilter.profile.name)"
        webfilter_profile_status: "enable"
```

5.43.6 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:

5.43.7 Status

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

5.43.8 Authors

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

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

5.44 fortios_firewall_internet_service – Show Internet Service application in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.44.1 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

5.44.2 Requirements

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

- ansible>=2.9.0

5.44.3 Parameters

5.44.4 Notes

Note:

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

5.44.5 Examples

```
- hosts: fortigates
  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"
        icon_id: "11"
        id:  "12"
        name: "default_name_13"
        offset: "14"
```

(continues on next page)

(continued from previous page)

```
        reputation: "15"
        sld_id: "16"
```

5.44.6 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:

5.44.7 Status

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

5.44.8 Authors

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

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

5.45 fortios_firewall_internet_service_custom – Configure custom Internet Services in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.45.1 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

5.45.2 Requirements

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

- ansible>=2.9.0

5.45.3 Parameters

5.45.4 Notes

Note:

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

5.45.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
         -
```

(continues on next page)

(continued from previous page)

```
            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"
```

5.45.6 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:

5.45.7 Status

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

5.45.8 Authors

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

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

5.46 fortios_firewall_internet_service_custom_group – Configure custom Internet Service group in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*

- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.46.1 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

5.46.2 Requirements

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

- ansible>=2.9.0

5.46.3 Parameters

5.46.4 Notes

Note:

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

5.46.5 Examples

```
- hosts: fortigates
  collections:
    - 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."
```

(continues on next page)

(continued from previous page)

```
        member:
         -
            name: "default_name_5 (source firewall.internet-service-custom.name)"
        name: "default_name_6"
```

5.46.6 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:

5.46.7 Status

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

5.46.8 Authors

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

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

5.47 fortios_firewall_internet_service_group – Configure group of Internet Service in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.47.1 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

5.47.2 Requirements

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

- ansible>=2.9.0

5.47.3 Parameters

5.47.4 Notes

Note:

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

5.47.5 Examples

```
- hosts: fortigates
  collections:
    - 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."
        member:
         -
            id:  "5 (source firewall.internet-service.id)"
        name: "default_name_6"
```

5.47.6 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:

5.47.7 Status

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

5.47.8 Authors

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

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

5.48 fortios_firewall_ip_translation – Configure firewall IP-translation in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.48.1 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

5.48.2 Requirements

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

- ansible>=2.9.0

5.48.3 Parameters

5.48.4 Notes

Note:

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

5.48.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.48.6 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:

5.48.7 Status

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

5.48.8 Authors

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

- Nicolas Thomas (@thomnico)

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

5.49 fortios_firewall_ipmacbinding_setting – Configure IP to MAC binding settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.49.1 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

5.49.2 Requirements

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

- ansible>=2.9.0

5.49.3 Parameters

5.49.4 Notes

Note:

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

5.49.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.49.6 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:

5.49.7 Status

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

5.49.8 Authors

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

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

5.50 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 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.50.1 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

5.50.2 Requirements

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

- ansible>=2.9.0

5.50.3 Parameters

5.50.4 Notes

Note:

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

5.50.5 Examples

```
- hosts: fortigates
  collections:
    - 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 address pairs in the IP/MAC binding table.
    fortios_firewall_ipmacbinding_table:
```

(continues on next page)

(continued from previous page)

```
    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"
```

5.50.6 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:

5.50.7 Status

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

5.50.8 Authors

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

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

5.51 fortios_firewall_ippool – Configure IPv4 IP pools in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*

- *Return Values*
- *Status*
- *Authors*

5.51.1 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

5.51.2 Requirements

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

- ansible>=2.9.0

5.51.3 Parameters

5.51.4 Notes

Note:

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

5.51.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
      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>"
```

(continues on next page)

(continued from previous page)

```
        name: "default_name_9"
        num_blocks_per_user: "10"
        pba_timeout: "11"
        permit_any_host: "disable"
        source_endip: "<your_own_value>"
        source_startip: "<your_own_value>"
        startip: "<your_own_value>"
        type: "overload"
```

5.51.6 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:

5.51.7 Status

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

5.51.8 Authors

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

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

5.52 fortios_firewall_ippool6 – Configure IPv6 IP pools in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*

- *Status*
- *Authors*

5.52.1 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

5.52.2 Requirements

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

- ansible>=2.9.0

5.52.3 Parameters

5.52.4 Notes

Note:

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

5.52.5 Examples

```
- hosts: fortigates
  collections:
    - 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 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>"
```

5.52.6 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:

5.52.7 Status

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

5.52.8 Authors

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

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

5.53 fortios_firewall_ipv6_eh_filter – Configure IPv6 extension header filter in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.53.1 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

5.53.2 Requirements

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

- ansible>=2.9.0

5.53.3 Parameters

5.53.4 Notes

Note:

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

5.53.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.53.6 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:

5.53.7 Status

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

5.53.8 Authors

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

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

5.54 fortios_firewall_ldb_monitor – Configure server load balancing health monitors in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.54.1 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

5.54.2 Requirements

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

- ansible>=2.9.0

5.54.3 Parameters

5.54.4 Notes

Note:

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

5.54.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        http_get: "<your_own_value>"
        http_match: "<your_own_value>"
        http_max_redirects: "5"
        interval: "6"
        name: "default_name_7"
        port: "8"
        retry: "9"
        timeout: "10"
        type: "ping"
```

5.54.6 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:

5.54.7 Status

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

5.54.8 Authors

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

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

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

5.55 fortios_firewall_local_in_policy – Configure user defined IPv4 local-in policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.55.1 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

5.55.2 Requirements

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

- ansible>=2.9.0

5.55.3 Parameters

5.55.4 Notes

Note:

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

5.55.5 Examples

```
- hosts: fortigates
  collections:
    - 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)
↪"
        ha_mgmt_intf_only: "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)"
        srcaddr:
         -
            name: "default_name_14 (source firewall.address.name firewall.addrgrp.
↪name)"
        status: "enable"
```

5.55.6 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:

5.55.7 Status

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

5.55.8 Authors

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

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

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

5.56 fortios_firewall_local_in_policy6 – Configure user defined IPv6 local-in policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.56.1 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

5.56.2 Requirements

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

- ansible>=2.9.0

5.56.3 Parameters

5.56.4 Notes

Note:

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

5.56.5 Examples

```
- hosts: fortigates
  collections:
    - 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)"
        intf: "<your_own_value> (source system.zone.name system.interface.name)"
        policyid: "8"
        schedule: "<your_own_value> (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name firewall.schedule.group.name)"
        service:
         -
            name: "default_name_11 (source firewall.service.custom.name firewall.
↪service.group.name)"
        srcaddr:
         -
            name: "default_name_13 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        status: "enable"
```

5.56.6 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:

5.56.7 Status

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

5.56.8 Authors

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

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

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

5.57 fortios_firewall_multicast_address – Configure multicast addresses in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.57.1 Synopsis

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

5.57.2 Requirements

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

- ansible>=2.9.0

5.57.3 Parameters

5.57.4 Notes

Note:

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

5.57.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        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"
```

5.57.6 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:

5.57.7 Status

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

5.57.8 Authors

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

- Nicolas Thomas (@thomnico)

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

5.58 fortios_firewall_multicast_address6 – Configure IPv6 multicast address in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.58.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and multicast_address6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.58.2 Requirements

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

- ansible>=2.9.0

5.58.3 Parameters

5.58.4 Notes

Note:

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

5.58.5 Examples

```
- hosts: fortigates
  collections:
    - 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 }}"
      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"
```

5.58.6 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:

5.58.7 Status

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

5.58.8 Authors

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

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

5.59 fortios_firewall_multicast_policy – Configure multicast NAT policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.59.1 Synopsis

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

5.59.2 Requirements

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

- ansible>=2.9.0

5.59.3 Parameters

5.59.4 Notes

Note:

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

5.59.5 Examples

```
- hosts: fortigates
  collections:
    - 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.
    fortios_firewall_multicast_policy:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_multicast_policy:
        action: "accept"
        dnat: "<your_own_value>"
        dstaddr:
         -
            name: "default_name_6 (source firewall.multicast-address.name)"
        dstintf: "<your_own_value> (source system.interface.name system.zone.name)"
        end_port: "8"
        id:  "9"
        logtraffic: "enable"
        protocol: "11"
        snat: "enable"
        snat_ip: "<your_own_value>"
        srcaddr:
         -
            name: "default_name_15 (source firewall.address.name firewall.addrgrp.
↪name)"
        srcintf: "<your_own_value> (source system.interface.name system.zone.name)"
        start_port: "17"
        status: "enable"
```

5.59.6 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:

5.59.7 Status

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

5.59.8 Authors

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

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

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

5.60 fortios_firewall_multicast_policy6 – Configure IPv6 multicast NAT policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.60.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and multicast_policy6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.60.2 Requirements

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

- ansible>=2.9.0

5.60.3 Parameters

5.60.4 Notes

Note:

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

5.60.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        dstaddr:
         -
            name: "default_name_5 (source firewall.multicast-address6.name)"
        dstintf: "<your_own_value> (source system.interface.name system.zone.name)"
        end_port: "7"
        id:  "8"
        logtraffic: "enable"
        protocol: "10"
        srcaddr:
         -
            name: "default_name_12 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        srcintf: "<your_own_value> (source system.interface.name system.zone.name)"
        start_port: "14"
        status: "enable"
```

5.60.6 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:

5.60.7 Status

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

5.60.8 Authors

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

- Nicolas Thomas (@thomnico)

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

5.61 fortios_firewall_policy – Configure IPv4 policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.61.1 Synopsis

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

5.61.2 Requirements

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

- ansible>=2.9.0

5.61.3 Parameters

5.61.4 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.

5.61.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        app_category:
         -
            id:  "5"
        app_group:
         -
            name: "default_name_7 (source application.group.name)"
        application:
         -
            id:  "9"
        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>"
        av_profile: "<your_own_value> (source antivirus.profile.name)"
        block_notification: "enable"
        captive_portal_exempt: "enable"
        capture_packet: "enable"
        comments: "<your_own_value>"
        custom_log_fields:
         -
            field_id: "<your_own_value> (source log.custom-field.id)"
        delay_tcp_npu_session: "enable"
        devices:
         -
            name: "default_name_23 (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>"
        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:
```

(continues on next page)

(continued from previous page)

```
        -
            name: "default_name_36 (source firewall.address.name firewall.addrgrp.
↪name firewall.vip.name firewall.vipgrp.name)"
        dstaddr_negate: "enable"
        dstintf:
        -
            name: "default_name_39 (source system.interface.name system.zone.name)"
        firewall_session_dirty: "check-all"
        fixedport: "enable"
        fsso: "enable"
        fsso_agent_for_ntlm: "<your_own_value> (source user.fsso.name)"
        global_label: "<your_own_value>"
        groups:
        -
            name: "default_name_46 (source user.group.name)"
        icap_profile: "<your_own_value> (source icap.profile.name)"
        identity_based_route: "<your_own_value> (source firewall.identity-based-route.
↪name)"
        inbound: "enable"
        internet_service: "enable"
        internet_service_custom:
        -
            name: "default_name_52 (source firewall.internet-service-custom.name)"
        internet_service_id:
        -
            id:  "54 (source firewall.internet-service.id)"
        internet_service_negate: "enable"
        internet_service_src: "enable"
        internet_service_src_custom:
        -
            name: "default_name_58 (source firewall.internet-service-custom.name)"
        internet_service_src_id:
        -
            id:  "60 (source firewall.internet-service.id)"
        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"
        name: "default_name_69"
        nat: "enable"
        natinbound: "enable"
        natip: "<your_own_value>"
        natoutbound: "enable"
        ntlm: "enable"
        ntlm_enabled_browsers:
        -
            user_agent_string: "<your_own_value>"
        ntlm_guest: "enable"
        outbound: "enable"
        per_ip_shaper: "<your_own_value> (source firewall.shaper.per-ip-shaper.name)"
        permit_any_host: "enable"
        permit_stun_host: "enable"
        policyid: "82"
```

(continues on next page)

(continued from previous page)

```
        poolname:
         -
            name: "default_name_84 (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"
        radius_mac_auth_bypass: "enable"
        redirect_url: "<your_own_value>"
        replacemsg_override_group: "<your_own_value> (source system.replacemsg-group.
↪name)"
        rsso: "enable"
        rtp_addr:
         -
            name: "default_name_93 (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_100 (source firewall.service.custom.name firewall.
↪service.group.name)"
        service_negate: "enable"
        session_ttl: "102"
        spamfilter_profile: "<your_own_value> (source spamfilter.profile.name)"
        srcaddr:
         -
            name: "default_name_105 (source firewall.address.name firewall.addrgrp.
↪name)"
        srcaddr_negate: "enable"
        srcintf:
         -
            name: "default_name_108 (source system.interface.name system.zone.name)"
        ssh_filter_profile: "<your_own_value> (source ssh-filter.profile.name)"
        ssl_mirror: "enable"
        ssl_mirror_intf:
         -
            name: "default_name_112 (source system.interface.name system.zone.name)"
        ssl_ssh_profile: "<your_own_value> (source firewall.ssl-ssh-profile.name)"
        status: "enable"
        tcp_mss_receiver: "115"
        tcp_mss_sender: "116"
        tcp_session_without_syn: "all"
        timeout_send_rst: "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:  "122"
        users:
         -
```

(continues on next page)

(continued from previous page)

```
            name: "default_name_124 (source user.local.name)"
        utm_status: "enable"
        uuid: "<your_own_value>"
        vlan_cos_fwd: "127"
        vlan_cos_rev: "128"
        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)"
        wsso: "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>"
```

5.61.6 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:

5.61.7 Status

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

5.61.8 Authors

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

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

5.62 fortios_firewall_policy46 – Configure IPv4 to IPv6 policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.62.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and policy46 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.62.2 Requirements

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

- ansible>=2.9.0

5.62.3 Parameters

5.62.4 Notes

Note:

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

5.62.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       per_ip_shaper: "<your_own_value> (source firewall.shaper.per-ip-shaper.name)"
       permit_any_host: "enable"
       policyid: "13"
       poolname:
        -
           name: "default_name_15 (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_18 (source firewall.service.custom.name firewall.
↪service.group.name)"
       srcaddr:
        -
           name: "default_name_20 (source firewall.address.name firewall.addrgrp.
↪name)"
       srcintf: "<your_own_value> (source system.zone.name system.interface.name)"
       status: "enable"
       tcp_mss_receiver: "23"
       tcp_mss_sender: "24"
       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>"
```

5.62.6 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:

5.62.7 Status

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

5.62.8 Authors

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

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

5.63 fortios_firewall_policy6 – Configure IPv6 policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.63.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and policy6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.63.2 Requirements

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

- ansible>=2.9.0

5.63.3 Parameters

5.63.4 Notes

Note:

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

5.63.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
      firewall_policy6:
        action: "accept"
        app_category:
         -
            id:  "5"
        app_group:
         -
            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)"
        comments: "<your_own_value>"
        custom_log_fields:
         -
            field_id: "<your_own_value> (source log.custom-field.id)"
        devices:
         -
            name: "default_name_16 (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)"
        dscp_match: "enable"
        dscp_negate: "enable"
        dscp_value: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        dsri: "enable"
        dstaddr:
         -
            name: "default_name_27 (source firewall.address6.name firewall.addrgrp6.
↪name firewall.vip6.name firewall.vipgrp6.name)"
        dstaddr_negate: "enable"
        dstintf:
         -
            name: "default_name_30 (source system.interface.name system.zone.name)"
        firewall_session_dirty: "check-all"
        fixedport: "enable"
        global_label: "<your_own_value>"
        groups:
         -
            name: "default_name_35 (source user.group.name)"
        icap_profile: "<your_own_value> (source icap.profile.name)"
        inbound: "enable"
        ippool: "enable"
        ips_sensor: "<your_own_value> (source ips.sensor.name)"
        label: "<your_own_value>"
        logtraffic: "all"
        logtraffic_start: "enable"
        name: "default_name_43"
        nat: "enable"
        natinbound: "enable"
        natoutbound: "enable"
        outbound: "enable"
        per_ip_shaper: "<your_own_value> (source firewall.shaper.per-ip-shaper.name)"
        policyid: "49"
        poolname:
         -
            name: "default_name_51 (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_60 (source firewall.service.custom.name firewall.
↪service.group.name)"
        service_negate: "enable"
        session_ttl: "62"
        spamfilter_profile: "<your_own_value> (source spamfilter.profile.name)"
        srcaddr:
         -
            name: "default_name_65 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        srcaddr_negate: "enable"
        srcintf:
         -
            name: "default_name_68 (source system.zone.name system.interface.name)"
```

(continues on next page)

(continued from previous page)

```
        ssh_filter_profile: "<your_own_value> (source ssh-filter.profile.name)"
        ssl_mirror: "enable"
        ssl_mirror_intf:
         -
            name: "default_name_72 (source system.zone.name system.interface.name)"
        ssl_ssh_profile: "<your_own_value> (source firewall.ssl-ssh-profile.name)"
        status: "enable"
        tcp_mss_receiver: "75"
        tcp_mss_sender: "76"
        tcp_session_without_syn: "all"
        timeout_send_rst: "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:  "82"
        users:
         -
            name: "default_name_84 (source user.local.name)"
        utm_status: "enable"
        uuid: "<your_own_value>"
        vlan_cos_fwd: "87"
        vlan_cos_rev: "88"
        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)"
        webfilter_profile: "<your_own_value> (source webfilter.profile.name)"
```

5.63.6 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:

5.63.7 Status

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

5.63.8 Authors

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

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

5.64 fortios_firewall_policy64 – Configure IPv6 to IPv4 policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.64.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and policy64 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.64.2 Requirements

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

- ansible>=2.9.0

5.64.3 Parameters

5.64.4 Notes

Note:

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

5.64.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        per_ip_shaper: "<your_own_value> (source firewall.shaper.per-ip-shaper.name)"
        permit_any_host: "enable"
        policyid: "13"
        poolname:
         -
            name: "default_name_15 (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_18 (source firewall.service.custom.name firewall.
↪service.group.name)"
        srcaddr:
         -
            name: "default_name_20 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        srcintf: "<your_own_value> (source system.zone.name system.interface.name)"
        status: "enable"
        tcp_mss_receiver: "23"
        tcp_mss_sender: "24"
        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>"
```

5.64.6 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:

5.64.7 Status

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

5.64.8 Authors

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

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

5.65 fortios_firewall_profile_group – Configure profile groups in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.65.1 Synopsis

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

5.65.2 Requirements

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

- ansible>=2.9.0

5.65.3 Parameters

5.65.4 Notes

Note:

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

5.65.5 Examples

```
- hosts: fortigates
  collections:
    - 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)"
        dlp_sensor: "<your_own_value> (source dlp.sensor.name)"
        dnsfilter_profile: "<your_own_value> (source dnsfilter.profile.name)"
        icap_profile: "<your_own_value> (source icap.profile.name)"
        ips_sensor: "<your_own_value> (source ips.sensor.name)"
        name: "default_name_9"
        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)"
        voip_profile: "<your_own_value> (source voip.profile.name)"
        waf_profile: "<your_own_value> (source waf.profile.name)"
        webfilter_profile: "<your_own_value> (source webfilter.profile.name)"
```

5.65.6 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:

5.65.7 Status

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

5.65.8 Authors

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

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

5.66 fortios_firewall_profile_protocol_options – Configure protocol options in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.66.1 Synopsis

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

5.66.2 Requirements

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

- ansible>=2.9.0

5.66.3 Parameters

5.66.4 Notes

Note:

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

5.66.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        comment: "Optional comments."
        dns:
            ports: "5"
            status: "enable"
        ftp:
            comfort_amount: "8"
            comfort_interval: "9"
            inspect_all: "enable"
            options: "clientcomfort"
            oversize_limit: "12"
            ports: "13"
            scan_bzip2: "enable"
            status: "enable"
            uncompressed_nest_limit: "16"
            uncompressed_oversize_limit: "17"
        http:
            block_page_status_code: "19"
            comfort_amount: "20"
            comfort_interval: "21"
            fortinet_bar: "enable"
            fortinet_bar_port: "23"
            http_policy: "disable"
            inspect_all: "enable"
            options: "clientcomfort"
            oversize_limit: "27"
            ports: "28"
            post_lang: "jisx0201"
            range_block: "disable"
```

(continues on next page)

(continued from previous page)

```
            retry_count: "31"
            scan_bzip2: "enable"
            status: "enable"
            streaming_content_bypass: "enable"
            switching_protocols: "bypass"
            uncompressed_nest_limit: "36"
            uncompressed_oversize_limit: "37"
        imap:
            inspect_all: "enable"
            options: "fragmail"
            oversize_limit: "41"
            ports: "42"
            scan_bzip2: "enable"
            status: "enable"
            uncompressed_nest_limit: "45"
            uncompressed_oversize_limit: "46"
        mail_signature:
            signature: "<your_own_value>"
            status: "disable"
        mapi:
            options: "fragmail"
            oversize_limit: "52"
            ports: "53"
            scan_bzip2: "enable"
            status: "enable"
            uncompressed_nest_limit: "56"
            uncompressed_oversize_limit: "57"
        name: "default_name_58"
        nntp:
            inspect_all: "enable"
            options: "oversize"
            oversize_limit: "62"
            ports: "63"
            scan_bzip2: "enable"
            status: "enable"
            uncompressed_nest_limit: "66"
            uncompressed_oversize_limit: "67"
        oversize_log: "disable"
        pop3:
            inspect_all: "enable"
            options: "fragmail"
            oversize_limit: "72"
            ports: "73"
            scan_bzip2: "enable"
            status: "enable"
            uncompressed_nest_limit: "76"
            uncompressed_oversize_limit: "77"
        replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
        rpc_over_http: "enable"
        smtp:
            inspect_all: "enable"
            options: "fragmail"
            oversize_limit: "83"
            ports: "84"
            scan_bzip2: "enable"
            server_busy: "enable"
            status: "enable"
```

(continues on next page)

(continued from previous page)

```
            uncompressed_nest_limit: "88"
            uncompressed_oversize_limit: "89"
        switching_protocols_log: "disable"
```

5.66.6 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:

5.66.7 Status

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

5.66.8 Authors

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

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

5.67 fortios_firewall_proxy_address – Web proxy address configuration in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.67.1 Synopsis

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

5.67.2 Requirements

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

- ansible>=2.9.0

5.67.3 Parameters

5.67.4 Notes

Note:

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

5.67.5 Examples

```
- hosts: fortigates
  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"
        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"
```

(continues on next page)

(continued from previous page)

```
        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"
```

5.67.6 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:

5.67.7 Status

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

5.67.8 Authors

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

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

5.68 fortios_firewall_proxy_addrgrp – Web proxy address group configuration in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.68.1 Synopsis

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

5.68.2 Requirements

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

- ansible>=2.9.0

5.68.3 Parameters

5.68.4 Notes

Note:

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

5.68.5 Examples

```
- hosts: fortigates
  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:
```

(continues on next page)

(continued from previous page)

```
    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"
```

5.68.6 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:

5.68.7 Status

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

5.68.8 Authors

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

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

5.69 fortios_firewall_proxy_policy – Configure proxy policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.69.1 Synopsis

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

5.69.2 Requirements

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

- ansible>=2.9.0

5.69.3 Parameters

5.69.4 Notes

Note:

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

5.69.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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:
       action: "accept"
       application_list: "<your_own_value> (source application.list.name)"
       av_profile: "<your_own_value> (source antivirus.profile.name)"
       comments: "<your_own_value>"
       disclaimer: "disable"
       dlp_sensor: "<your_own_value> (source dlp.sensor.name)"
       dstaddr:
        -
           name: "default_name_10 (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_13 (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_15 (source system.interface.name system.zone.name)"
       global_label: "<your_own_value>"
       groups:
        -
           name: "default_name_18 (source user.group.name)"
       http_tunnel_auth: "enable"
       icap_profile: "<your_own_value> (source icap.profile.name)"
       internet_service: "enable"
       internet_service_custom:
        -
           name: "default_name_23 (source firewall.internet-service-custom.name)"
       internet_service_id:
        -
           id:  "25 (source firewall.internet-service.id)"
       internet_service_negate: "enable"
       ips_sensor: "<your_own_value> (source ips.sensor.name)"
       label: "<your_own_value>"
       logtraffic: "all"
       logtraffic_start: "enable"
       policyid: "31"
       poolname:
        -
           name: "default_name_33 (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"
```

(continues on next page)

(continued from previous page)

```
        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_43 (source firewall.service.custom.name firewall.
↪service.group.name)"
        service_negate: "enable"
        session_ttl: "45"
        spamfilter_profile: "<your_own_value> (source spamfilter.profile.name)"
        srcaddr:
         -
            name: "default_name_48 (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_51 (source firewall.address6.name firewall.addrgrp6.
↪name system.external-resource.name)"
        srcintf:
         -
            name: "default_name_53 (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"
        transparent: "enable"
        users:
         -
            name: "default_name_59 (source user.local.name)"
        utm_status: "enable"
        uuid: "<your_own_value>"
        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)"
```

5.69.6 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:

5.69.7 Status

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

5.69.8 Authors

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

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

5.70 fortios_firewall_schedule_group – Schedule group configuration in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.70.1 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

5.70.2 Requirements

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

- ansible>=2.9.0

5.70.3 Parameters

5.70.4 Notes

Note:

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

5.70.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   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"
        member:
         -
            name: "default_name_5 (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name)"
        name: "default_name_6"
```

5.70.6 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:

5.70.7 Status

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

5.70.8 Authors

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

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

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

5.71 fortios_firewall_schedule_onetime – Onetime schedule configuration in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.71.1 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

5.71.2 Requirements

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

- ansible>=2.9.0

5.71.3 Parameters

5.71.4 Notes

Note:

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

5.71.5 Examples

```
- hosts: fortigates
  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.
    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"
        name: "default_name_6"
        start: "<your_own_value>"
```

5.71.6 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:

5.71.7 Status

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

5.71.8 Authors

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

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

5.72 fortios_firewall_schedule_recurring – Recurring schedule configuration in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.72.1 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

5.72.2 Requirements

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

- ansible>=2.9.0

5.72.3 Parameters

5.72.4 Notes

Note:

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

5.72.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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:
      color: "3"
      day: "sunday"
      end: "<your_own_value>"
      name: "default_name_6"
      start: "<your_own_value>"
```

5.72.6 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:

5.72.7 Status

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

5.72.8 Authors

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

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

5.73 fortios_firewall_service_category – Configure service categories in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*

- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.73.1 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

5.73.2 Requirements

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

- ansible>=2.9.0

5.73.3 Parameters

5.73.4 Notes

Note:

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

5.73.5 Examples

```
- hosts: fortigates
  collections:
    - 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."
        name: "default_name_4"
```

5.73.6 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:

5.73.7 Status

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

5.73.8 Authors

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

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

5.74 fortios_firewall_service_custom – Configure custom services in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.74.1 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

5.74.2 Requirements

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

- ansible>=2.9.0

5.74.3 Parameters

5.74.4 Notes

Note:

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

5.74.5 Examples

```
- hosts: fortigates
  collections:
    - 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."
        fqdn: "<your_own_value>"
        helper: "auto"
```

(continues on next page)

(continued from previous page)

```
        icmpcode: "14"
        icmptype: "15"
        iprange: "<your_own_value>"
        name: "default_name_17"
        protocol: "TCP/UDP/SCTP"
        protocol_number: "19"
        proxy: "enable"
        sctp_portrange: "<your_own_value>"
        session_ttl: "22"
        tcp_halfclose_timer: "23"
        tcp_halfopen_timer: "24"
        tcp_portrange: "<your_own_value>"
        tcp_timewait_timer: "26"
        udp_idle_timer: "27"
        udp_portrange: "<your_own_value>"
        visibility: "enable"
```

5.74.6 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:

5.74.7 Status

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

5.74.8 Authors

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

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

5.75 fortios_firewall_service_group – Configure service groups in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.75.1 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

5.75.2 Requirements

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

- ansible>=2.9.0

5.75.3 Parameters

5.75.4 Notes

Note:

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

5.75.5 Examples

```
- hosts: fortigates
  collections:
    - 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 groups.
    fortios_firewall_service_group:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
      state: "present"
      access_token: "<your_own_value>"
      firewall_service_group:
        color: "3"
        comment: "Comment."
        member:
          -
            name: "default_name_6 (source firewall.service.custom.name firewall.
↪service.group.name)"
        name: "default_name_7"
        proxy: "enable"
```

5.75.6 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:

5.75.7 Status

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

5.75.8 Authors

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

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

5.76 fortios_firewall_shaper_per_ip_shaper – Configure per-IP traffic shaper in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*

- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.76.1 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

5.76.2 Requirements

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

- ansible>=2.9.0

5.76.3 Parameters

5.76.4 Notes

Note:

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

5.76.5 Examples

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

(continues on next page)

(continued from previous page)

```
        diffservcode_rev: "<your_own_value>"
        max_bandwidth: "8"
        max_concurrent_session: "9"
        name: "default_name_10"
```

5.76.6 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:

5.76.7 Status

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

5.76.8 Authors

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

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

5.77 fortios_firewall_shaper_traffic_shaper – Configure shared traffic shaper in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.77.1 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

5.77.2 Requirements

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

- ansible>=2.9.0

5.77.3 Parameters

5.77.4 Notes

Note:

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

5.77.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  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>"
        guaranteed_bandwidth: "6"
        maximum_bandwidth: "7"
        name: "default_name_8"
        per_policy: "disable"
        priority: "low"
```

5.77.6 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:

5.77.7 Status

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

5.77.8 Authors

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

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

5.78 fortios_firewall_shaping_policy – Configure shaping policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.78.1 Synopsis

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

5.78.2 Requirements

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

- ansible>=2.9.0

5.78.3 Parameters

5.78.4 Notes

Note:

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

5.78.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        application:
         -
            id:  "6"
        class_id: "7"
        comment: "Comments."
        dstaddr:
         -
            name: "default_name_10 (source firewall.address.name firewall.addrgrp.
↪name)"
        dstaddr6:
         -
            name: "default_name_12 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        dstintf:
         -
            name: "default_name_14 (source system.interface.name system.zone.name)"
        groups:
         -
            name: "default_name_16 (source user.group.name)"
        id:  "17"
        internet_service: "enable"
        internet_service_custom:
         -
            name: "default_name_20 (source firewall.internet-service-custom.name)"
        internet_service_id:
```

(continues on next page)

(continued from previous page)

```
        -
            id:  "22 (source firewall.internet-service.id)"
        internet_service_src: "enable"
        internet_service_src_custom:
        -
            name: "default_name_25 (source firewall.internet-service-custom.name)"
        internet_service_src_id:
        -
            id:  "27 (source firewall.internet-service.id)"
        ip_version: "4"
        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_32 (source firewall.service.custom.name firewall.
↪service.group.name)"
        srcaddr:
        -
            name: "default_name_34 (source firewall.address.name firewall.addrgrp.
↪name)"
        srcaddr6:
        -
            name: "default_name_36 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        status: "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:  "41"
        users:
        -
            name: "default_name_43 (source user.local.name)"
```

5.78.6 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:

5.78.7 Status

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

5.78.8 Authors

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

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

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

5.79 fortios_firewall_shaping_profile – Configure shaping profiles in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.79.1 Synopsis

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

5.79.2 Requirements

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

- ansible>=2.9.0

5.79.3 Parameters

5.79.4 Notes

Note:

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

5.79.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        profile_name: "<your_own_value>"
        shaping_entries:
         -
            class_id: "7"
            guaranteed_bandwidth_percentage: "8"
            id:  "9"
            maximum_bandwidth_percentage: "10"
            priority: "high"
```

5.79.6 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:

5.79.7 Status

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

5.79.8 Authors

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

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

5.80 fortios_firewall_sniffer – Configure sniffer in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.80.1 Synopsis

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

5.80.2 Requirements

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

- ansible>=2.9.0

5.80.3 Parameters

5.80.4 Notes

Note:

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

5.80.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       host: "myhostname"
       id:  "21"
       interface: "<your_own_value> (source system.interface.name)"
       ips_dos_status: "enable"
       ips_sensor: "<your_own_value> (source ips.sensor.name)"
       ips_sensor_status: "enable"
       ipv6: "enable"
       logtraffic: "all"
       max_packet_count: "28"
       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"
```

5.80.6 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:

5.80.7 Status

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

5.80.8 Authors

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

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

5.81 fortios_firewall_ssh_host_key – SSH proxy host public keys in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.81.1 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

5.81.2 Requirements

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

- ansible>=2.9.0

5.81.3 Parameters

5.81.4 Notes

Note:

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

5.81.5 Examples

```
- hosts: fortigates
  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"
```

5.81.6 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:

5.81.7 Status

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

5.81.8 Authors

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

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

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

5.82 fortios_firewall_ssh_local_ca – SSH proxy local CA in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.82.1 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

5.82.2 Requirements

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

- ansible>=2.9.0

5.82.3 Parameters

5.82.4 Notes

Note:

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

5.82.5 Examples

```
- hosts: fortigates
  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"
```

5.82.6 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:

5.82.7 Status

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

5.82.8 Authors

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

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

5.83 fortios_firewall_ssh_local_key – SSH proxy local keys in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.83.1 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

5.83.2 Requirements

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

- ansible>=2.9.0

5.83.3 Parameters

5.83.4 Notes

Note:

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

5.83.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  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"
```

5.83.6 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:

5.83.7 Status

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

5.83.8 Authors

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

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

5.84 fortios_firewall_ssh_setting – SSH proxy settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*

- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.84.1 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

5.84.2 Requirements

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

- ansible>=2.9.0

5.84.3 Parameters

5.84.4 Notes

Note:

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

5.84.5 Examples

```
- hosts: fortigates
  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)"
        host_trusted_checking: "enable"
```

(continues on next page)

(continued from previous page)

```
        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)"
```

5.84.6 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:

5.84.7 Status

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

5.84.8 Authors

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

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

5.85 fortios_firewall_ssl_server – Configure SSL servers in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*

- *Status*
- *Authors*

5.85.1 Synopsis

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

5.85.2 Requirements

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

- ansible>=2.9.0

5.85.3 Parameters

5.85.4 Notes

Note:

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

5.85.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        port: "7"
        ssl_algorithm: "high"
        ssl_cert: "<your_own_value> (source vpn.certificate.local.name)"
        ssl_client_renegotiation: "allow"
```

(continues on next page)

(continued from previous page)

```
        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"
```

5.85.6 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:

5.85.7 Status

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

5.85.8 Authors

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

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

5.86 fortios_firewall_ssl_setting – SSL proxy settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*

- *Authors*

5.86.1 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

5.86.2 Requirements

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

- ansible>=2.9.0

5.86.3 Parameters

5.86.4 Notes

Note:

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

5.86.5 Examples

```
- hosts: fortigates
  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"
        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"
```

5.86.6 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:

5.86.7 Status

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

5.86.8 Authors

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

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

5.87 fortios_firewall_ssl_ssh_profile – Configure SSL/SSH protocol options in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.87.1 Synopsis

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

5.87.2 Requirements

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

- ansible>=2.9.0

5.87.3 Parameters

5.87.4 Notes

Note:

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

5.87.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        caname: "<your_own_value> (source vpn.certificate.local.name)"
        comment: "Optional comments."
        ftps:
            allow_invalid_server_cert: "enable"
            client_cert_request: "bypass"
            ports: "8"
            status: "disable"
            unsupported_ssl: "bypass"
            untrusted_cert: "allow"
        https:
            allow_invalid_server_cert: "enable"
            client_cert_request: "bypass"
            ports: "15"
            status: "disable"
            unsupported_ssl: "bypass"
            untrusted_cert: "allow"
        imaps:
            allow_invalid_server_cert: "enable"
            client_cert_request: "bypass"
            ports: "22"
            status: "disable"
```

(continues on next page)

(continued from previous page)

```
            unsupported_ssl: "bypass"
            untrusted_cert: "allow"
        mapi_over_https: "enable"
        name: "default_name_27"
        pop3s:
            allow_invalid_server_cert: "enable"
            client_cert_request: "bypass"
            ports: "31"
            status: "disable"
            unsupported_ssl: "bypass"
            untrusted_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"
            client_cert_request: "bypass"
            ports: "41"
            status: "disable"
            unsupported_ssl: "bypass"
            untrusted_cert: "allow"
        ssh:
            inspect_all: "disable"
            ports: "47"
            ssh_algorithm: "compatible"
            ssh_policy_check: "disable"
            ssh_tun_policy_check: "disable"
            status: "disable"
            unsupported_version: "bypass"
        ssl:
            allow_invalid_server_cert: "enable"
            client_cert_request: "bypass"
            inspect_all: "disable"
            unsupported_ssl: "bypass"
            untrusted_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: "63"
            id:  "64"
            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_server:
         -
            ftps_client_cert_request: "bypass"
            https_client_cert_request: "bypass"
            id:  "72"
            imaps_client_cert_request: "bypass"
            ip: "<your_own_value>"
            pop3s_client_cert_request: "bypass"
```

(continues on next page)

(continued from previous page)

```
            smtps_client_cert_request: "bypass"
            ssl_other_client_cert_request: "bypass"
        untrusted_caname: "<your_own_value> (source vpn.certificate.local.name)"
        use_ssl_server: "disable"
        whitelist: "enable"
```

5.87.6 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:

5.87.7 Status

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

5.87.8 Authors

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

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

5.88 fortios_firewall_ttl_policy – Configure TTL policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.88.1 Synopsis

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

5.88.2 Requirements

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

- ansible>=2.9.0

5.88.3 Parameters

5.88.4 Notes

Note:

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

5.88.5 Examples

```
- hosts: fortigates
  collections:
    - 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)"
```

(continues on next page)

(continued from previous page)

```
        status: "enable"
        ttl: "<your_own_value>"
```

5.88.6 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:

5.88.7 Status

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

5.88.8 Authors

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

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

5.89 fortios_firewall_vip – Configure virtual IP for IPv4 in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.89.1 Synopsis

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

5.89.2 Requirements

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

- ansible>=2.9.0

5.89.3 Parameters

5.89.4 Notes

Note:

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

5.89.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
        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"
        https_cookie_secure: "disable"
        id:  "23"
        ldb_method: "static"
        mapped_addr: "<your_own_value> (source firewall.address.name)"
        mappedip:
         -
            range: "<your_own_value>"
        mappedport: "<your_own_value>"
        max_embryonic_connections: "29"
        monitor:
         -
            name: "default_name_31 (source firewall.ldb-monitor.name)"
        name: "default_name_32"
        nat_source_vip: "disable"
        outlook_web_access: "disable"
        persistence: "none"
        portforward: "disable"
        portmapping_type: "1-to-1"
        protocol: "tcp"
        realservers:
         -
            client_ip: "<your_own_value>"
            healthcheck: "disable"
            holddown_interval: "42"
            http_host: "myhostname"
            id:  "44"
            ip: "<your_own_value>"
            max_connections: "46"
            monitor: "<your_own_value> (source firewall.ldb-monitor.name)"
            port: "48"
            status: "active"
            weight: "50"
        server_type: "http"
        service:
         -
            name: "default_name_53 (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: "62"
```

(continues on next page)

(continued from previous page)

```
            versions: "ssl-3.0"
        ssl_client_fallback: "disable"
        ssl_client_renegotiation: "allow"
        ssl_client_session_state_max: "66"
        ssl_client_session_state_timeout: "67"
        ssl_client_session_state_type: "disable"
        ssl_dh_bits: "768"
        ssl_hpkp: "disable"
        ssl_hpkp_age: "71"
        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: "77"
        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"
        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: "89"
            versions: "ssl-3.0"
        ssl_server_max_version: "ssl-3.0"
        ssl_server_min_version: "ssl-3.0"
        ssl_server_session_state_max: "93"
        ssl_server_session_state_timeout: "94"
        ssl_server_session_state_type: "disable"
        type: "static-nat"
        uuid: "<your_own_value>"
        weblogic_server: "disable"
        websphere_server: "disable"
```

5.89.6 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:

5.89.7 Status

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

5.89.8 Authors

- Link Zheng (@chillancezen)

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

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

5.90 fortios_firewall_vip46 – Configure IPv4 to IPv6 virtual IPs in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.90.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vip46 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.90.2 Requirements

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

- ansible>=2.9.0

5.90.3 Parameters

5.90.4 Notes

Note:

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

5.90.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
        type: "static-nat"
        uuid: "<your_own_value>"
```

5.90.6 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:

5.90.7 Status

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

5.90.8 Authors

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

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

5.91 fortios_firewall_vip6 – Configure virtual IP for IPv6 in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.91.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vip6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.91.2 Requirements

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

- ansible>=2.9.0

5.91.3 Parameters

5.91.4 Notes

Note:

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

5.91.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        https_cookie_secure: "disable"
        id:  "18"
        ldb_method: "static"
        mappedip: "<your_own_value>"
        mappedport: "<your_own_value>"
        max_embryonic_connections: "22"
        monitor:
```

(continues on next page)

(continued from previous page)

```
        -
            name: "default_name_24 (source firewall.ldb-monitor.name)"
        name: "default_name_25"
        outlook_web_access: "disable"
        persistence: "none"
        portforward: "disable"
        protocol: "tcp"
        realservers:
        -
            client_ip: "<your_own_value>"
            healthcheck: "disable"
            holddown_interval: "33"
            http_host: "myhostname"
            id:  "35"
            ip: "<your_own_value>"
            max_connections: "37"
            monitor: "<your_own_value> (source firewall.ldb-monitor.name)"
            port: "39"
            status: "active"
            weight: "41"
        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: "49"
            versions: "ssl-3.0"
        ssl_client_fallback: "disable"
        ssl_client_renegotiation: "allow"
        ssl_client_session_state_max: "53"
        ssl_client_session_state_timeout: "54"
        ssl_client_session_state_type: "disable"
        ssl_dh_bits: "768"
        ssl_hpkp: "disable"
        ssl_hpkp_age: "58"
        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: "64"
        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"
        ssl_mode: "half"
        ssl_pfs: "require"
        ssl_send_empty_frags: "enable"
        ssl_server_algorithm: "high"
        ssl_server_cipher_suites:
```

(continues on next page)

(continued from previous page)

```
        -
            cipher: "TLS-ECDHE-RSA-WITH-CHACHA20-POLY1305-SHA256"
            priority: "76"
            versions: "ssl-3.0"
        ssl_server_max_version: "ssl-3.0"
        ssl_server_min_version: "ssl-3.0"
        ssl_server_session_state_max: "80"
        ssl_server_session_state_timeout: "81"
        ssl_server_session_state_type: "disable"
        type: "static-nat"
        uuid: "<your_own_value>"
        weblogic_server: "disable"
        websphere_server: "disable"
```

5.91.6 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:

5.91.7 Status

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

5.91.8 Authors

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

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

5.92 fortios_firewall_vip64 – Configure IPv6 to IPv4 virtual IPs in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*

- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.92.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vip64 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.92.2 Requirements

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

- ansible>=2.9.0

5.92.3 Parameters

5.92.4 Notes

Note:

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

5.92.5 Examples

```
- hosts: fortigates
  collections:
    - 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 IPs.
    fortios_firewall_vip64:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      firewall_vip64:
        arp_reply: "disable"
        color: "4"
        comment: "Comment."
```

(continues on next page)

(continued from previous page)

```
        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>"
```

5.92.6 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:

5.92.7 Status

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

5.92.8 Authors

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

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

5.93 fortios_firewall_vipgrp – Configure IPv4 virtual IP groups in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.93.1 Synopsis

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

5.93.2 Requirements

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

- ansible>=2.9.0

5.93.3 Parameters

5.93.4 Notes

Note:

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

5.93.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.93.6 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:

5.93.7 Status

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

5.93.8 Authors

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

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

5.94 fortios_firewall_vipgrp46 – Configure IPv4 to IPv6 virtual IP groups in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.94.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vipgrp46 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.94.2 Requirements

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

- ansible>=2.9.0

5.94.3 Parameters

5.94.4 Notes

Note:

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

5.94.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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>"
```

5.94.6 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:

5.94.7 Status

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

5.94.8 Authors

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

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

5.95 fortios_firewall_vipgrp6 – Configure IPv6 virtual IP groups in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.95.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vipgrp6 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.95.2 Requirements

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

- ansible>=2.9.0

5.95.3 Parameters

5.95.4 Notes

Note:

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

5.95.5 Examples

```
- hosts: fortigates
  collections:
    - 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 }}"
```

(continues on next page)

(continued from previous page)

```
    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>"
```

5.95.6 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:

5.95.7 Status

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

5.95.8 Authors

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

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

5.96 fortios_firewall_vipgrp64 – Configure IPv6 to IPv4 virtual IP groups in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*

- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.96.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify firewall feature and vipgrp64 category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.96.2 Requirements

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

- ansible>=2.9.0

5.96.3 Parameters

5.96.4 Notes

Note:

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

5.96.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
         -
```

(continues on next page)

(continued from previous page)

```
            name: "default_name_6 (source firewall.vip64.name)"
        name: "default_name_7"
        uuid: "<your_own_value>"
```

5.96.6 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:

5.96.7 Status

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

5.96.8 Authors

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

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

5.97 fortios_firewall_wildcard_fqdn_custom – Config global/VDOM Wildcard FQDN address in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.97.1 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

5.97.2 Requirements

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

- ansible>=2.9.0

5.97.3 Parameters

5.97.4 Notes

Note:

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

5.97.5 Examples

```
- hosts: fortigates
  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>"
```

5.97.6 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:

5.97.7 Status

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

5.97.8 Authors

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

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

5.98 fortios_firewall_wildcard_fqdn_group – Config global Wildcard FQDN address groups in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.98.1 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

5.98.2 Requirements

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

- ansible>=2.9.0

5.98.3 Parameters

5.98.4 Notes

Note:

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

5.98.5 Examples

```
- hosts: fortigates
  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"
```

5.98.6 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:

5.98.7 Status

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

5.98.8 Authors

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

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

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

5.99 fortios_ftp_proxy_explicit – Configure explicit FTP proxy settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.99.1 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

5.99.2 Requirements

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

- ansible>=2.9.0

5.99.3 Parameters

5.99.4 Notes

Note:

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

5.99.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        status: "enable"
```

5.99.6 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:

5.99.7 Status

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

5.99.8 Authors

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

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

5.100 fortios_icap_profile – Configure ICAP profiles in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.100.1 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

5.100.2 Requirements

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

- ansible>=2.9.0

5.100.3 Parameters

5.100.4 Notes

Note:

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

5.100.5 Examples

```
- hosts: fortigates
  collections:
    - 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 profiles.
    fortios_icap_profile:
```

(continues on next page)

(continued from previous page)

```
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    icap_profile:
      methods: "delete"
      name: "default_name_4"
      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)"
      response: "disable"
      response_failure: "error"
      response_path: "<your_own_value>"
      response_server: "<your_own_value> (source icap.server.name)"
      streaming_content_bypass: "disable"
```

5.100.6 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:

5.100.7 Status

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

5.100.8 Authors

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

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

5.101 fortios_icap_server – Configure ICAP servers in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.101.1 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

5.101.2 Requirements

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

- ansible>=2.9.0

5.101.3 Parameters

5.101.4 Notes

Note:

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

5.101.5 Examples

```
- hosts: fortigates
  collections:
    - 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 }}"
```

(continues on next page)

(continued from previous page)

```
    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"
```

5.101.6 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:

5.101.7 Status

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

5.101.8 Authors

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

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

5.102 fortios_ips_custom – Configure IPS custom signature in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*

- *Return Values*
- *Status*
- *Authors*

5.102.1 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

5.102.2 Requirements

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

- ansible>=2.9.0

5.102.3 Parameters

5.102.4 Notes

Note:

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

5.102.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
        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>"
```

5.102.6 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:

5.102.7 Status

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

5.102.8 Authors

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

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

5.103 fortios_ips_decoder – Configure IPS decoder in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*

- *Status*
- *Authors*

5.103.1 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

5.103.2 Requirements

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

- ansible>=2.9.0

5.103.3 Parameters

5.103.4 Notes

Note:

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

5.103.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.103.6 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:

5.103.7 Status

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

5.103.8 Authors

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

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

5.104 fortios_ips_global – Configure IPS global parameter in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.104.1 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

5.104.2 Requirements

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

- ansible>=2.9.0

5.104.3 Parameters

5.104.4 Notes

Note:

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

5.104.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        database: "regular"
        deep_app_insp_db_limit: "5"
        deep_app_insp_timeout: "6"
        engine_count: "7"
        exclude_signatures: "none"
        fail_open: "enable"
        intelligent_mode: "enable"
        session_limit_mode: "accurate"
        skype_client_public_ipaddr: "<your_own_value>"
        socket_size: "13"
        sync_session_ttl: "enable"
        traffic_submit: "enable"
```

5.104.6 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:

5.104.7 Status

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

5.104.8 Authors

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

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

5.105 fortios_ips_rule – Configure IPS rules in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.105.1 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

5.105.2 Requirements

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

- ansible>=2.9.0

5.105.3 Parameters

5.105.4 Notes

Note:

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

5.105.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.105.6 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:

5.105.7 Status

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

5.105.8 Authors

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

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

5.106 fortios_ips_rule_settings – Configure IPS rule setting in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.106.1 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

5.106.2 Requirements

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

- ansible>=2.9.0

5.106.3 Parameters

5.106.4 Notes

Note:

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

5.106.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.106.6 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:

5.106.7 Status

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

5.106.8 Authors

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

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

5.107 fortios_ips_sensor – Configure IPS sensor in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.107.1 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

5.107.2 Requirements

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

- ansible>=2.9.0

5.107.3 Parameters

5.107.4 Notes

Note:

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

5.107.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
            exempt_ip:
             -
                dst_ip: "<your_own_value>"
                id:  "10"
                src_ip: "<your_own_value>"
            id:  "12"
            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: "22"
            rate_duration: "23"
            rate_mode: "periodical"
            rate_track: "none"
            rule:
             -
                id:  "27"
            severity: "<your_own_value>"
            status: "disable"
        extended_log: "enable"
        filter:
         -
            action: "pass"
            application: "<your_own_value>"
            location: "<your_own_value>"
            log: "disable"
            log_packet: "disable"
            name: "default_name_37"
```

(continues on next page)

(continued from previous page)

```
            os: "<your_own_value>"
            protocol: "<your_own_value>"
            quarantine: "none"
            quarantine_expiry: "41"
            quarantine_log: "disable"
            severity: "<your_own_value>"
            status: "disable"
        name: "default_name_45"
        override:
         -
            action: "pass"
            exempt_ip:
             -
                dst_ip: "<your_own_value>"
                id:  "50"
                src_ip: "<your_own_value>"
            log: "disable"
            log_packet: "disable"
            quarantine: "none"
            quarantine_expiry: "55"
            quarantine_log: "disable"
            rule_id: "57"
            status: "disable"
        replacemsg_group: "<your_own_value> (source system.replacemsg-group.name)"
```

5.107.6 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:

5.107.7 Status

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

5.107.8 Authors

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

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

5.108 fortios_ips_settings – Configure IPS VDOM parameter in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.108.1 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

5.108.2 Requirements

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

- ansible>=2.9.0

5.108.3 Parameters

5.108.4 Notes

Note:

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

5.108.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.108.6 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:

5.108.7 Status

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

5.108.8 Authors

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

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

5.109 fortios_log_custom_field – Configure custom log fields in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*

- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.109.1 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

5.109.2 Requirements

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

- ansible>=2.9.0

5.109.3 Parameters

5.109.4 Notes

Note:

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

5.109.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
      log_custom_field:
        id:  "3"
        name: "default_name_4"
        value: "<your_own_value>"
```

5.109.6 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:

5.109.7 Status

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

5.109.8 Authors

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

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

5.110 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 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.110.1 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

5.110.2 Requirements

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

- ansible>=2.9.0

5.110.3 Parameters

5.110.4 Notes

Note:

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

5.110.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        dlp_archive: "enable"
        dns: "enable"
        event: "enable"
        filter: "<your_own_value>"
        filter_type: "include"
        forward_traffic: "enable"
        gtp: "enable"
        ha: "enable"
        ipsec: "enable"
```

(continues on next page)

(continued from previous page)

```
        ldb_monitor: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        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"
```

5.110.6 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:

5.110.7 Status

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

5.110.8 Authors

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

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

5.111 fortios_log_disk_setting – Settings for local disk logging in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.111.1 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

5.111.2 Requirements

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

- ansible>=2.9.0

5.111.3 Parameters

5.111.4 Notes

Note:

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

5.111.5 Examples

```
- hosts: fortigates
  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:
```

(continues on next page)

(continued from previous page)

```
    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"
      ips_archive: "enable"
      log_quota: "9"
      max_log_file_size: "10"
      max_policy_packet_capture_size: "11"
      maximum_log_age: "12"
      report_quota: "13"
      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: "26"
      uploadsched: "disable"
      uploadtime: "<your_own_value>"
      uploadtype: "traffic"
      uploaduser: "<your_own_value>"
```

5.111.6 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:

5.111.7 Status

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

5.111.8 Authors

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

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

5.112 fortios_log_eventfilter – Configure log event filters in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.112.1 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

5.112.2 Requirements

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

- ansible>=2.9.0

5.112.3 Parameters

5.112.4 Notes

Note:

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

5.112.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        compliance_check: "enable"
        endpoint: "enable"
        event: "enable"
        ha: "enable"
        router: "enable"
        security_rating: "enable"
        system: "enable"
        user: "enable"
        vpn: "enable"
        wan_opt: "enable"
        wireless_activity: "enable"
```

5.112.6 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:

5.112.7 Status

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

5.112.8 Authors

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

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

5.113 fortios_log_fortianalyzer2_filter – Filters for FortiAnalyzer in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.113.1 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

5.113.2 Requirements

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

- ansible>=2.9.0

5.113.3 Parameters

5.113.4 Notes

Note:

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

5.113.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
      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"
```

5.113.6 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:

5.113.7 Status

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

5.113.8 Authors

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

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

5.114 fortios_log_fortianalyzer2_setting – Global FortiAnalyzer settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.114.1 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

5.114.2 Requirements

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

- ansible>=2.9.0

5.114.3 Parameters

5.114.4 Notes

Note:

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

5.114.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       certificate: "<your_own_value> (source certificate.local.name)"
       conn_timeout: "5"
       enc_algorithm: "high-medium"
       faz_type: "7"
       hmac_algorithm: "sha256"
       ips_archive: "enable"
       mgmt_name: "<your_own_value>"
       monitor_failure_retry_period: "11"
       monitor_keepalive_period: "12"
       reliable: "enable"
       server: "192.168.100.40"
       source_ip: "84.230.14.43"
       status: "enable"
       upload_day: "<your_own_value>"
       upload_interval: "daily"
       upload_option: "store-and-upload"
       upload_time: "<your_own_value>"
```

5.114.6 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:

5.114.7 Status

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

5.114.8 Authors

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

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

5.115 fortios_log_fortianalyzer3_filter – Filters for FortiAnalyzer in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.115.1 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

5.115.2 Requirements

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

- ansible>=2.9.0

5.115.3 Parameters

5.115.4 Notes

Note:

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

5.115.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       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"
```

5.115.6 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:

5.115.7 Status

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

5.115.8 Authors

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

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

5.116 fortios_log_fortianalyzer3_setting – Global FortiAnalyzer settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.116.1 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

5.116.2 Requirements

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

- ansible>=2.9.0

5.116.3 Parameters

5.116.4 Notes

Note:

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

5.116.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       certificate: "<your_own_value> (source certificate.local.name)"
       conn_timeout: "5"
       enc_algorithm: "high-medium"
       faz_type: "7"
       hmac_algorithm: "sha256"
       ips_archive: "enable"
       mgmt_name: "<your_own_value>"
       monitor_failure_retry_period: "11"
       monitor_keepalive_period: "12"
       reliable: "enable"
       server: "192.168.100.40"
       source_ip: "84.230.14.43"
       status: "enable"
       upload_day: "<your_own_value>"
       upload_interval: "daily"
       upload_option: "store-and-upload"
       upload_time: "<your_own_value>"
```

5.116.6 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:

5.116.7 Status

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

5.116.8 Authors

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

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

5.117 fortios_log_fortianalyzer_filter – Filters for FortiAnalyzer in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.117.1 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

5.117.2 Requirements

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

- ansible>=2.9.0

5.117.3 Parameters

5.117.4 Notes

Note:

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

5.117.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       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"
```

5.117.6 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:

5.117.7 Status

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

5.117.8 Authors

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

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

5.118 fortios_log_fortianalyzer_override_filter – Override filters for FortiAnalyzer in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.118.1 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

5.118.2 Requirements

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

- ansible>=2.9.0

5.118.3 Parameters

5.118.4 Notes

Note:

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

5.118.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       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"
```

5.118.6 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:

5.118.7 Status

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

5.118.8 Authors

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

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

5.119 fortios_log_fortianalyzer_override_setting – Override FortiAnalyzer settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.119.1 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

5.119.2 Requirements

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

- ansible>=2.9.0

5.119.3 Parameters

5.119.4 Notes

Note:

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

5.119.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       certificate: "<your_own_value> (source certificate.local.name)"
       conn_timeout: "5"
       enc_algorithm: "high-medium"
       faz_type: "7"
       hmac_algorithm: "sha256"
       ips_archive: "enable"
       mgmt_name: "<your_own_value>"
       monitor_failure_retry_period: "11"
       monitor_keepalive_period: "12"
       override: "enable"
       reliable: "enable"
       server: "192.168.100.40"
       source_ip: "84.230.14.43"
       status: "enable"
       upload_day: "<your_own_value>"
       upload_interval: "daily"
       upload_option: "store-and-upload"
       upload_time: "<your_own_value>"
       use_management_vdom: "enable"
```

5.119.6 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:

5.119.7 Status

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

5.119.8 Authors

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

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

5.120 fortios_log_fortianalyzer_setting – Global FortiAnalyzer settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.120.1 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

5.120.2 Requirements

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

- ansible>=2.9.0

5.120.3 Parameters

5.120.4 Notes

Note:

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

5.120.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       certificate: "<your_own_value> (source certificate.local.name)"
       conn_timeout: "5"
       enc_algorithm: "high-medium"
       faz_type: "7"
       hmac_algorithm: "sha256"
       ips_archive: "enable"
       mgmt_name: "<your_own_value>"
       monitor_failure_retry_period: "11"
       monitor_keepalive_period: "12"
       reliable: "enable"
       server: "192.168.100.40"
       source_ip: "84.230.14.43"
       status: "enable"
       upload_day: "<your_own_value>"
       upload_interval: "daily"
       upload_option: "store-and-upload"
       upload_time: "<your_own_value>"
```

5.120.6 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:

5.120.7 Status

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

5.120.8 Authors

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

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

5.121 fortios_log_fortiguard_filter – Filters for FortiCloud in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.121.1 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

5.121.2 Requirements

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

- ansible>=2.9.0

5.121.3 Parameters

5.121.4 Notes

Note:

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

5.121.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  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"
       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"
```

5.121.6 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:

5.121.7 Status

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

5.121.8 Authors

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

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

5.122 fortios_log_fortiguard_override_filter – Override filters for FortiCloud in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.122.1 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

5.122.2 Requirements

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

- ansible>=2.9.0

5.122.3 Parameters

5.122.4 Notes

Note:

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

5.122.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       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"
```

5.122.6 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:

5.122.7 Status

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

5.122.8 Authors

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

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

5.123 fortios_log_fortiguard_override_setting – Override global FortiCloud logging settings for this VDOM in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.123.1 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

5.123.2 Requirements

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

- ansible>=2.9.0

5.123.3 Parameters

5.123.4 Notes

Note:

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

5.123.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
```

(continues on next page)

(continued from previous page)

```
  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:
      override: "enable"
      status: "enable"
      upload_day: "<your_own_value>"
      upload_interval: "daily"
      upload_option: "store-and-upload"
      upload_time: "<your_own_value>"
```

5.123.6 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:

5.123.7 Status

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

5.123.8 Authors

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

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

5.124 fortios_log_fortiguard_setting – Configure logging to FortiCloud in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*

- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.124.1 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

5.124.2 Requirements

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

- ansible>=2.9.0

5.124.3 Parameters

5.124.4 Notes

Note:

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

5.124.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        enc_algorithm: "high-medium"
        source_ip: "84.230.14.43"
```

(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>"
```

5.124.6 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:

5.124.7 Status

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

5.124.8 Authors

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

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

5.125 fortios_log_gui_display – Configure how log messages are displayed on the GUI in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.125.1 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

5.125.2 Requirements

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

- ansible>=2.9.0

5.125.3 Parameters

5.125.4 Notes

Note:

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

5.125.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.125.6 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:

5.125.7 Status

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

5.125.8 Authors

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

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

5.126 fortios_log_memory_filter – Filters for memory buffer in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.126.1 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

5.126.2 Requirements

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

- ansible>=2.9.0

5.126.3 Parameters

5.126.4 Notes

Note:

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

5.126.5 Examples

```
- hosts: fortigates
  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 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"
        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>"
        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"
```

(continues on next page)

(continued from previous page)

```
        wan_opt: "enable"
        wireless_activity: "enable"
```

5.126.6 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:

5.126.7 Status

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

5.126.8 Authors

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

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

5.127 fortios_log_memory_global_setting – Global settings for memory logging in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.127.1 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

5.127.2 Requirements

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

- ansible>=2.9.0

5.127.3 Parameters

5.127.4 Notes

Note:

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

5.127.5 Examples

```
- hosts: fortigates
  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"
```

5.127.6 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:

5.127.7 Status

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

5.127.8 Authors

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

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

5.128 fortios_log_memory_setting – Settings for memory buffer in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.128.1 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

5.128.2 Requirements

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

- ansible>=2.9.0

5.128.3 Parameters

5.128.4 Notes

Note:

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

5.128.5 Examples

```
- hosts: fortigates
  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"
```

5.128.6 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:

5.128.7 Status

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

5.128.8 Authors

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

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

5.129 fortios_log_null_device_filter – Filters for null device logging in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.129.1 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

5.129.2 Requirements

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

- ansible>=2.9.0

5.129.3 Parameters

5.129.4 Notes

Note:

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

5.129.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
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"
      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"
```

5.129.6 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:

5.129.7 Status

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

5.129.8 Authors

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

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

5.130 fortios_log_null_device_setting – Settings for null device logging in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.130.1 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

5.130.2 Requirements

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

- ansible>=2.9.0

5.130.3 Parameters

5.130.4 Notes

Note:

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

5.130.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.130.6 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:

5.130.7 Status

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

5.130.8 Authors

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

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

5.131 fortios_log_setting – Configure general log settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*

- *Return Values*
- *Status*
- *Authors*

5.131.1 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

5.131.2 Requirements

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

- ansible>=2.9.0

5.131.3 Parameters

5.131.4 Notes

Note:

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

5.131.5 Examples

```
- hosts: fortigates
  collections:
    - 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 }}"
      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"
        fwpolicy_implicit_log: "enable"
        fwpolicy6_implicit_log: "enable"
```

(continues on next page)

(continued from previous page)

```
        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"
        user_anonymize: "enable"
```

5.131.6 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:

5.131.7 Status

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

5.131.8 Authors

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

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

5.132 fortios_log_syslogd2_filter – Filters for remote system server in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*

- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.132.1 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

5.132.2 Requirements

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

- ansible>=2.9.0

5.132.3 Parameters

5.132.4 Notes

Note:

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

5.132.5 Examples

```
- hosts: fortigates
  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"
```

(continues on next page)

(continued from previous page)

```
        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"
```

5.132.6 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:

5.132.7 Status

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

5.132.8 Authors

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

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

5.133 fortios_log_syslogd2_setting – Global settings for remote syslog server in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*

- *Return Values*
- *Status*
- *Authors*

5.133.1 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

5.133.2 Requirements

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

- ansible>=2.9.0

5.133.3 Parameters

5.133.4 Notes

Note:

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

5.133.5 Examples

```
- hosts: fortigates
  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"
```

(continues on next page)

(continued from previous page)

```
        format: "default"
        mode: "udp"
        port: "12"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        status: "enable"
```

5.133.6 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:

5.133.7 Status

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

5.133.8 Authors

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

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

5.134 fortios_log_syslogd3_filter – Filters for remote system server in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*

- *Authors*

5.134.1 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

5.134.2 Requirements

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

- ansible>=2.9.0

5.134.3 Parameters

5.134.4 Notes

Note:

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

5.134.5 Examples

```
- hosts: fortigates
  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"
        gtp: "enable"
        local_traffic: "enable"
        multicast_traffic: "enable"
        netscan_discovery: "<your_own_value>"
        netscan_vulnerability: "<your_own_value>"
        severity: "emergency"
```

(continues on next page)

(continued from previous page)

```
        sniffer_traffic: "enable"
        ssh: "enable"
        voip: "enable"
```

5.134.6 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:

5.134.7 Status

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

5.134.8 Authors

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

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

5.135 fortios_log_syslogd3_setting – Global settings for remote syslog server in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.135.1 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

5.135.2 Requirements

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

- ansible>=2.9.0

5.135.3 Parameters

5.135.4 Notes

Note:

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

5.135.5 Examples

```
- hosts: fortigates
  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"
        mode: "udp"
        port: "12"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        status: "enable"
```

5.135.6 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:

5.135.7 Status

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

5.135.8 Authors

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

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

5.136 fortios_log_syslogd4_filter – Filters for remote system server in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.136.1 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

5.136.2 Requirements

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

- ansible>=2.9.0

5.136.3 Parameters

5.136.4 Notes

Note:

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

5.136.5 Examples

```
- hosts: fortigates
  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"
        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"
```

5.136.6 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:

5.136.7 Status

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

5.136.8 Authors

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

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

5.137 fortios_log_syslogd4_setting – Global settings for remote syslog server in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.137.1 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

5.137.2 Requirements

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

- ansible>=2.9.0

5.137.3 Parameters

5.137.4 Notes

Note:

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

5.137.5 Examples

```
- hosts: fortigates
  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"
        mode: "udp"
        port: "12"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        status: "enable"
```

5.137.6 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:

5.137.7 Status

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

5.137.8 Authors

- Link Zheng (@chillancezen)

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

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

5.138 fortios_log_syslogd_filter – Filters for remote system server in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.138.1 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

5.138.2 Requirements

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

- ansible>=2.9.0

5.138.3 Parameters

5.138.4 Notes

Note:

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

5.138.5 Examples

```
- hosts: fortigates
  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"
        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"
```

5.138.6 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:

5.138.7 Status

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

5.138.8 Authors

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

- Nicolas Thomas (@thomnico)

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

5.139 fortios_log_syslogd_override_filter – Override filters for remote system server in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.139.1 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

5.139.2 Requirements

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

- ansible>=2.9.0

5.139.3 Parameters

5.139.4 Notes

Note:

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

5.139.5 Examples

```
- hosts: fortigates
  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"
        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"
```

5.139.6 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:

5.139.7 Status

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

5.139.8 Authors

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

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

5.140 fortios_log_syslogd_override_setting – Override settings for remote syslog server in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.140.1 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

5.140.2 Requirements

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

- ansible>=2.9.0

5.140.3 Parameters

5.140.4 Notes

Note:

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

5.140.5 Examples

```
- hosts: fortigates
  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"
        mode: "udp"
        override: "enable"
        port: "13"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        status: "enable"
```

5.140.6 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:

5.140.7 Status

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

5.140.8 Authors

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

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

5.141 fortios_log_syslogd_setting – Global settings for remote syslog server in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.141.1 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

5.141.2 Requirements

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

- ansible>=2.9.0

5.141.3 Parameters

5.141.4 Notes

Note:

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

5.141.5 Examples

```
- hosts: fortigates
  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"
        mode: "udp"
        port: "12"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        status: "enable"
```

5.141.6 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:

5.141.7 Status

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

5.141.8 Authors

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

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

5.142 fortios_log_threat_weight – Configure threat weight settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.142.1 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

5.142.2 Requirements

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

- ansible>=2.9.0

5.142.3 Parameters

5.142.4 Notes

Note:

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

5.142.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
            high: "22"
            low: "23"
            medium: "24"
        malware_detected: "disable"
        status: "enable"
        url_block_detected: "disable"
        web:
         -
            category: "29"
            id:  "30"
            level: "disable"
```

5.142.6 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:

5.142.7 Status

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

5.142.8 Authors

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

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

5.143 fortios_log_webtrends_filter – Filters for WebTrends in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.143.1 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

5.143.2 Requirements

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

- ansible>=2.9.0

5.143.3 Parameters

5.143.4 Notes

Note:

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

5.143.5 Examples

```
- hosts: fortigates
  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"
        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"
```

5.143.6 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:

5.143.7 Status

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

5.143.8 Authors

- Link Zheng (@chillancezen)

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

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

5.144 fortios_log_webtrends_setting – Settings for WebTrends in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.144.1 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

5.144.2 Requirements

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

- ansible>=2.9.0

5.144.3 Parameters

5.144.4 Notes

Note:

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

5.144.5 Examples

```
- hosts: fortigates
  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"
```

5.144.6 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:

5.144.7 Status

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

5.144.8 Authors

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

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

5.145 fortios_registration_forticare – Add a FortiCare license in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.145.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify registration feature and forticare category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.5

5.145.2 Requirements

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

- ansible>=2.9.0

5.145.3 Parameters

5.145.4 Notes

Note:

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

5.145.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_use_ssl: no
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 80
tasks:
- name: Add a FortiCare license.
  fortios_registration_forticare:
    vdom:  "{{ vdom }}"
    registration_forticare:
      registration_code: "<your_own_value>"
```

5.145.6 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:

5.145.7 Status

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

5.145.8 Authors

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

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

5.146 fortios_registration_vdom – Add a VDOM license in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*

- *Authors*

5.146.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify registration feature and vdom category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.5

5.146.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.146.3 Parameters

5.146.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.146.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: no
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 80
  tasks:
  - name: Add a VDOM license.
    fortios_registration_vdom:
      vdom:  "{{ vdom }}"
      registration_vdom:
        license: "<your_own_value>"
```

5.146.6 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:

5.146.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.146.8 Authors

- Frank Shen (@frankshen01)
- Link Zheng (@chillancezen)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.147 fortios_report_chart – Report chart widget configuration in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.147.1 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

5.147.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.147.3 Parameters

5.147.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.147.5 Examples

```
- hosts: fortigates
  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>"
```

(continues on next page)

(continued from previous page)

```
            id:  "28"
            status: "enable"
        favorite: "no"
        graph_type: "none"
        legend: "enable"
        legend_font_size: "33"
        name: "default_name_34"
        period: "last24h"
        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>"
```

5.147.6 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:

5.147.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.147.8 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.148 fortios_report_dataset – Report dataset configuration in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.148.1 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

5.148.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.148.3 Parameters

5.148.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.148.5 Examples

```
- hosts: fortigates
  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>"
```

5.148.6 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:

5.148.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.148.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.149 fortios_report_layout – Report layout configuration in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.149.1 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

5.149.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.149.3 Parameters

5.149.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.149.5 Examples

```
- hosts: fortigates
  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>"
```

5.149.6 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:

5.149.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.149.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.150 fortios_report_setting – Report setting configuration in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.150.1 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

5.150.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.150.3 Parameters

5.150.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.150.5 Examples

```
- hosts: fortigates
  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"
```

5.150.6 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:

5.150.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.150.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.151 fortios_report_style – Report style configuration in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.151.1 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

5.151.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.151.3 Parameters

5.151.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.151.5 Examples

```
- hosts: fortigates
  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:
```

(continues on next page)

(continued from previous page)

```
    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>"
```

5.151.6 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:

5.151.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.151.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.152 fortios_report_theme – Report themes configuratio in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.152.1 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

5.152.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.152.3 Parameters

5.152.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.152.5 Examples

```
- hosts: fortigates
  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>"
        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>"
```

5.152.6 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:

5.152.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.152.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.153 fortios_router_access_list – Configure access lists in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.153.1 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

5.153.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.153.3 Parameters

5.153.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.153.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
            id:  "9"
            prefix: "<your_own_value>"
            wildcard: "<your_own_value>"
```

5.153.6 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:

5.153.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.153.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.154 fortios_router_access_list6 – Configure IPv6 access lists in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.154.1 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

5.154.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.154.3 Parameters

5.154.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.154.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.154.6 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:

5.154.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.154.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.155 fortios_router_aspath_list – Configure Autonomous System (AS) path lists in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.155.1 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

5.155.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.155.3 Parameters

5.155.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.155.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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>"
```

5.155.6 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:

5.155.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.155.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.156 fortios_router_auth_path – Configure authentication based routing in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.156.1 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

5.156.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.156.3 Parameters

5.156.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.156.5 Examples

```
- hosts: fortigates
  collections:
    - 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 }}"
```

(continues on next page)

(continued from previous page)

```
    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"
```

5.156.6 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:

5.156.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.156.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.157 fortios_router_bfd – Configure BFD in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*

- *Authors*

5.157.1 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

5.157.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.157.3 Parameters

5.157.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.157.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.157.6 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:

5.157.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.157.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.158 fortios_router_bfd6 – Configure IPv6 BFD in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.158.1 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

5.158.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.158.3 Parameters

5.158.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.158.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.158.6 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:

5.158.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.158.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.159 fortios_router_bgp – Configure BGP in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.159.1 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

5.159.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.159.3 Parameters

5.159.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.159.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure BGP.
    fortios_router_bgp:
      vdom:  "{{ vdom }}"
      router_bgp:
        admin_distance:
         -
            distance: "4"
            id:  "5"
            neighbour_prefix: "<your_own_value>"
            route_list: "<your_own_value> (source router.access-list.name)"
        aggregate_address:
         -
            as_set: "enable"
            id:  "10"
            prefix: "<your_own_value>"
            summary_only: "enable"
        aggregate_address6:
         -
            as_set: "enable"
            id:  "15"
            prefix6: "<your_own_value>"
            summary_only: "enable"
        always_compare_med: "enable"
        as: "19"
        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: "27"
        confederation_peers:
         -
            peer: "<your_own_value>"
        dampening: "enable"
        dampening_max_suppress_time: "31"
        dampening_reachability_half_life: "32"
        dampening_reuse: "33"
        dampening_route_map: "<your_own_value> (source router.route-map.name)"
        dampening_suppress: "35"
        dampening_unreachability_half_life: "36"
        default_local_preference: "37"
        deterministic_med: "enable"
        distance_external: "39"
```

(continues on next page)

(continued from previous page)

```
        distance_internal: "40"
        distance_local: "41"
        ebgp_multipath: "enable"
        enforce_first_as: "enable"
        fast_external_failover: "enable"
        graceful_end_on_timer: "enable"
        graceful_restart: "enable"
        graceful_restart_time: "47"
        graceful_stalepath_time: "48"
        graceful_update_delay: "49"
        holdtime_timer: "50"
        ibgp_multipath: "enable"
        ignore_optional_capability: "enable"
        keepalive_timer: "53"
        log_neighbour_changes: "enable"
        neighbor:
         -
            activate: "enable"
            activate6: "enable"
            advertisement_interval: "58"
            allowas_in: "59"
            allowas_in_enable: "enable"
            allowas_in_enable6: "enable"
            allowas_in6: "62"
            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: "80"
            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: "90"
            filter_list_in: "<your_own_value> (source router.aspath-list.name)"
            filter_list_in6: "<your_own_value> (source router.aspath-list.name)"
```

(continues on next page)

(continued from previous page)

```
            filter_list_out: "<your_own_value> (source router.aspath-list.name)"
            filter_list_out6: "<your_own_value> (source router.aspath-list.name)"
            holdtime_timer: "95"
            interface: "<your_own_value> (source system.interface.name)"
            ip: "<your_own_value>"
            keep_alive_timer: "98"
            link_down_failover: "enable"
            local_as: "100"
            local_as_no_prepend: "enable"
            local_as_replace_as: "enable"
            maximum_prefix: "103"
            maximum_prefix_threshold: "104"
            maximum_prefix_threshold6: "105"
            maximum_prefix_warning_only: "enable"
            maximum_prefix_warning_only6: "enable"
            maximum_prefix6: "108"
            next_hop_self: "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: "118"
            remove_private_as: "enable"
            remove_private_as6: "enable"
            restart_time: "121"
            retain_stale_time: "122"
            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_out6: "<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: "141"
        neighbor_group:
          -
            activate: "enable"
            activate6: "enable"
            advertisement_interval: "145"
            allowas_in: "146"
            allowas_in_enable: "enable"
            allowas_in_enable6: "enable"
```

(continues on next page)

(continued from previous page)

```
            allowas_in6: "149"
            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: "163"
            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: "173"
            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: "178"
            interface: "<your_own_value> (source system.interface.name)"
            keep_alive_timer: "180"
            link_down_failover: "enable"
            local_as: "182"
            local_as_no_prepend: "enable"
            local_as_replace_as: "enable"
            maximum_prefix: "185"
            maximum_prefix_threshold: "186"
            maximum_prefix_threshold6: "187"
            maximum_prefix_warning_only: "enable"
            maximum_prefix_warning_only6: "enable"
            maximum_prefix6: "190"
            name: "default_name_191"
            next_hop_self: "enable"
            next_hop_self6: "enable"
            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: "200"
            remove_private_as: "enable"
            remove_private_as6: "enable"
            restart_time: "203"
```

(continues on next page)

(continued from previous page)

```
            retain_stale_time: "204"
            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_out6: "<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: "223"
        neighbor_range:
         -
            id:  "225"
            max_neighbor_num: "226"
            neighbor_group: "<your_own_value> (source router.bgp.neighbor-group.name)"
            prefix: "<your_own_value>"
        network:
         -
            backdoor: "enable"
            id:  "231"
            prefix: "<your_own_value>"
            route_map: "<your_own_value> (source router.route-map.name)"
        network_import_check: "enable"
        network6:
         -
            backdoor: "enable"
            id:  "237"
            prefix6: "<your_own_value>"
            route_map: "<your_own_value> (source router.route-map.name)"
        redistribute:
         -
            name: "default_name_241"
            route_map: "<your_own_value> (source router.route-map.name)"
            status: "enable"
        redistribute6:
         -
            name: "default_name_245"
            route_map: "<your_own_value> (source router.route-map.name)"
            status: "enable"
        router_id: "<your_own_value>"
        scan_time: "249"
        synchronization: "enable"
```

5.159.6 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:

5.159.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.159.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.160 fortios_router_community_list – Configure community lists in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.160.1 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

5.160.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.160.3 Parameters

5.160.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.160.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.160.6 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:

5.160.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.160.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.161 fortios_router_isis – Configure IS-IS in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.161.1 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

5.161.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.161.3 Parameters

5.161.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.161.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
            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"
            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>"
```

(continues on next page)

(continued from previous page)

```
        summary_address:
         -
            id:  "87"
            level: "level-1-2"
            prefix: "<your_own_value>"
        summary_address6:
         -
            id:  "91"
            level: "level-1-2"
            prefix6: "<your_own_value>"
```

5.161.6 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:

5.161.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.161.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.162 fortios_router_key_chain – Configure key-chain in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*

- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.162.1 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

5.162.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.162.3 Parameters

5.162.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.162.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
            key_string: "<your_own_value>"
            send_lifetime: "<your_own_value>"
        name: "default_name_8"
```

5.162.6 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:

5.162.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.162.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.163 fortios_router_multicast – Configure router multicast in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.163.1 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

5.163.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.163.3 Parameters

5.163.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.163.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
                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"
            rp_candidate: "enable"
            rp_candidate_group: "<your_own_value> (source router.access-list.name)"
            rp_candidate_interval: "29"
            rp_candidate_priority: "30"
            state_refresh_interval: "31"
            static_group: "<your_own_value> (source router.multicast-flow.name)"
            ttl_threshold: "33"
        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: "40"
            bsr_interface: "<your_own_value> (source system.interface.name)"
            bsr_priority: "42"
            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: "47"
            message_interval: "48"
            null_register_retries: "49"
            register_rate_limit: "50"
            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: "55"
            rp_address:
             -
                group: "<your_own_value> (source router.access-list.name)"
                id:  "58"
                ip_address: "<your_own_value>"
            rp_register_keepalive: "60"
            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: "65"
        route_threshold: "66"
```

5.163.6 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:

5.163.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.163.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.164 fortios_router_multicast6 – Configure IPv6 multicast in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.164.1 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

5.164.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.164.3 Parameters

5.164.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.164.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.164.6 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:

5.164.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.164.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.165 fortios_router_multicast_flow – Configure multicast-flow in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.165.1 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

5.165.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.165.3 Parameters

5.165.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.165.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.165.6 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:

5.165.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.165.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.166 fortios_router_ospf – Configure OSPF in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.166.1 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

5.166.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.166.3 Parameters

5.166.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.166.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
            default_cost: "6"
            filter_list:
             -
                direction: "in"
                id:  "9"
                list: "<your_own_value> (source router.access-list.name router.prefix-
↪list.name)"
            id:  "11"
            nssa_default_information_originate: "enable"
            nssa_default_information_originate_metric: "13"
            nssa_default_information_originate_metric_type: "1"
            nssa_redistribution: "enable"
            nssa_translator_role: "candidate"
            range:
             -
                advertise: "disable"
                id:  "19"
                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: "29"
                hello_interval: "30"
                md5_key: "<your_own_value>"
                name: "default_name_32"
                peer: "<your_own_value>"
                retransmit_interval: "34"
                transmit_delay: "35"
        auto_cost_ref_bandwidth: "36"
        bfd: "enable"
        database_overflow: "enable"
```

(continues on next page)

(continued from previous page)

```
        database_overflow_max_lsas: "39"
        database_overflow_time_to_recover: "40"
        default_information_metric: "41"
        default_information_metric_type: "1"
        default_information_originate: "enable"
        default_information_route_map: "<your_own_value> (source router.route-map.
↪name)"
        default_metric: "45"
        distance: "46"
        distance_external: "47"
        distance_inter_area: "48"
        distance_intra_area: "49"
        distribute_list:
         -
            access_list: "<your_own_value> (source router.access-list.name)"
            id:  "52"
            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: "58"
            id:  "59"
            ip: "<your_own_value>"
            poll_interval: "61"
            priority: "62"
        network:
         -
            area: "<your_own_value>"
            id:  "65"
            prefix: "<your_own_value>"
        ospf_interface:
         -
            authentication: "none"
            authentication_key: "<your_own_value>"
            bfd: "global"
            cost: "71"
            database_filter_out: "enable"
            dead_interval: "73"
            hello_interval: "74"
            hello_multiplier: "75"
            interface: "<your_own_value> (source system.interface.name)"
            ip: "<your_own_value>"
            md5_key: "<your_own_value>"
            mtu: "79"
            mtu_ignore: "enable"
            name: "default_name_81"
            network_type: "broadcast"
            prefix_length: "83"
            priority: "84"
            resync_timeout: "85"
            retransmit_interval: "86"
            status: "disable"
            transmit_delay: "88"
        passive_interface:
```

(continues on next page)

(continued from previous page)

```
        -
            name: "default_name_90 (source system.interface.name)"
        redistribute:
        -
            metric: "92"
            metric_type: "1"
            name: "default_name_94"
            routemap: "<your_own_value> (source router.route-map.name)"
            status: "enable"
            tag: "97"
        restart_mode: "none"
        restart_period: "99"
        rfc1583_compatible: "enable"
        router_id: "<your_own_value>"
        spf_timers: "<your_own_value>"
        summary_address:
        -
            advertise: "disable"
            id:  "105"
            prefix: "<your_own_value>"
            tag: "107"
```

5.166.6 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:

5.166.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.166.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.167 fortios_router_ospf6 – Configure IPv6 OSPF in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.167.1 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

5.167.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.167.3 Parameters

5.167.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.167.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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:
        -
           default_cost: "5"
           id:  "6"
           nssa_default_information_originate: "enable"
           nssa_default_information_originate_metric: "8"
           nssa_default_information_originate_metric_type: "1"
           nssa_redistribution: "enable"
           nssa_translator_role: "candidate"
           range:
            -
               advertise: "disable"
               id:  "14"
               prefix6: "<your_own_value>"
           stub_type: "no-summary"
           type: "regular"
           virtual_link:
            -
               dead_interval: "19"
               hello_interval: "20"
               name: "default_name_21"
               peer: "<your_own_value>"
               retransmit_interval: "23"
               transmit_delay: "24"
       auto_cost_ref_bandwidth: "25"
       bfd: "enable"
       default_information_metric: "27"
       default_information_metric_type: "1"
       default_information_originate: "enable"
       default_information_route_map: "<your_own_value> (source router.route-map.
↪name)"
       default_metric: "31"
       log_neighbour_changes: "enable"
       ospf6_interface:
        -
           area_id: "<your_own_value>"
           bfd: "global"
           cost: "36"
           dead_interval: "37"
           hello_interval: "38"
           interface: "<your_own_value> (source system.interface.name)"
           name: "default_name_40"
           neighbor:
            -
               cost: "42"
               ip6: "<your_own_value>"
               poll_interval: "44"
               priority: "45"
```

(continues on next page)

(continued from previous page)

```
            network_type: "broadcast"
            priority: "47"
            retransmit_interval: "48"
            status: "disable"
            transmit_delay: "50"
        passive_interface:
         -
            name: "default_name_52 (source system.interface.name)"
        redistribute:
         -
            metric: "54"
            metric_type: "1"
            name: "default_name_56"
            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:  "63"
            prefix6: "<your_own_value>"
            tag: "65"
```

5.167.6 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:

5.167.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.167.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.168 fortios_router_policy – Configure IPv4 routing policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.168.1 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

5.168.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.168.3 Parameters

5.168.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.168.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
 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)"
       output_device: "<your_own_value> (source system.interface.name)"
       protocol: "16"
       seq_num: "17"
       src:
        -
           subnet: "<your_own_value>"
       src_negate: "enable"
       srcaddr:
        -
           name: "default_name_22 (source firewall.address.name firewall.addrgrp.
↪name)"
       start_port: "23"
       start_source_port: "24"
       status: "enable"
       tos: "<your_own_value>"
       tos_mask: "<your_own_value>"
```

5.168.6 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:

5.168.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.168.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.169 fortios_router_policy6 – Configure IPv6 routing policies in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.169.1 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

5.169.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.169.3 Parameters

5.169.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.169.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.169.6 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:

5.169.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.169.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.170 fortios_router_prefix_list – Configure IPv4 prefix lists in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.170.1 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

5.170.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.170.3 Parameters

5.170.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.170.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.170.6 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:

5.170.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.170.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.171 fortios_router_prefix_list6 – Configure IPv6 prefix lists in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.171.1 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

5.171.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.171.3 Parameters

5.171.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.171.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.171.6 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:

5.171.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.171.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.172 fortios_router_rip – Configure RIP in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.172.1 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

5.172.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.172.3 Parameters

5.172.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.172.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
           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)"
```

(continues on next page)

(continued from previous page)

```
        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"
```

5.172.6 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:

5.172.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.172.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.173 fortios_router_ripng – Configure RIPng in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*

- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.173.1 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

5.173.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.173.3 Parameters

5.173.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.173.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
        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"
            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"
```

5.173.6 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:

5.173.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.173.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.174 fortios_router_route_map – Configure route maps in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.174.1 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

5.174.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.174.3 Parameters

5.174.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.174.5 Examples

```
- hosts: fortigates
  collections:
    - 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.
    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"
            set_aggregator_as: "21"
            set_aggregator_ip: "<your_own_value>"
            set_aspath:
             -
                as: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
            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: "31"
            set_dampening_reachability_half_life: "32"
            set_dampening_reuse: "33"
            set_dampening_suppress: "34"
            set_dampening_unreachability_half_life: "35"
            set_extcommunity_rt:
             -
                community: "<your_own_value>"
            set_extcommunity_soo:
             -
                community: "<your_own_value>"
            set_flags: "40"
            set_ip_nexthop: "<your_own_value>"
            set_ip6_nexthop: "<your_own_value>"
            set_ip6_nexthop_local: "<your_own_value>"
            set_local_preference: "44"
            set_metric: "45"
            set_metric_type: "1"
            set_origin: "none"
            set_originator_id: "<your_own_value>"
            set_route_tag: "49"
            set_tag: "50"
            set_weight: "51"
```

5.174.6 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:

5.174.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.174.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.175 fortios_router_setting – Configure router settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.175.1 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

5.175.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.175.3 Parameters

5.175.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.175.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        hostname: "myhostname"
        show_filter: "<your_own_value> (source router.prefix-list.name)"
```

5.175.6 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:

5.175.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.175.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.176 fortios_router_static – Configure IPv4 static routing tables in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.176.1 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

5.176.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.176.3 Parameters

5.176.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.176.5 Examples

```
- hosts: fortigates
  collections:
    - 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 static routing tables.
    fortios_router_static:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
      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"
        seq_num: "16"
        src: "<your_own_value>"
        status: "enable"
        virtual_wan_link: "enable"
        vrf: "20"
        weight: "21"
```

5.176.6 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:

5.176.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.176.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.177 fortios_router_static6 – Configure IPv6 static routing tables in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.177.1 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

5.177.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.177.3 Parameters

5.177.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.177.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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>"
       gateway: "<your_own_value>"
       priority: "11"
       seq_num: "12"
       status: "enable"
       virtual_wan_link: "enable"
```

5.177.6 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:

5.177.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.177.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.178 fortios_spamfilter_bwl – Configure anti-spam black/white list in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.178.1 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

5.178.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.178.3 Parameters

5.178.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.178.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.178.6 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:

5.178.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.178.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.179 fortios_spamfilter_bword – Configure AntiSpam banned word list in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.179.1 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

5.179.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.179.3 Parameters

5.179.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.179.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.179.6 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:

5.179.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.179.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.180 fortios_spamfilter_dnsbl – Configure AntiSpam DNSBL/ORBL in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.180.1 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

5.180.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.180.3 Parameters

5.180.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.180.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.180.6 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:

5.180.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.180.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.181 fortios_spamfilter_fortishield – Configure FortiGuard - Anti-Spam in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.181.1 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

5.181.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.181.3 Parameters

5.181.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.181.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    vdom:  "{{ vdom }}"
    spamfilter_fortishield:
      spam_submit_force: "enable"
      spam_submit_srv: "<your_own_value>"
      spam_submit_txt2htm: "enable"
```

5.181.6 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:

5.181.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.181.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.182 fortios_spamfilter_iptrust – Configure AntiSpam IP trust in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.182.1 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

5.182.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.182.3 Parameters

5.182.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.182.5 Examples

```
- hosts: fortigates
  collections:
    - 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_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"
```

5.182.6 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:

5.182.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.182.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.183 fortios_spamfilter_mheader – Configure AntiSpam MIME header in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.183.1 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

5.183.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.183.3 Parameters

5.183.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.183.5 Examples

```
- hosts: fortigates
  collections:
    - 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_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"
```

5.183.6 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:

5.183.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.183.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.184 fortios_spamfilter_options – Configure AntiSpam options in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.184.1 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

5.184.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.184.3 Parameters

5.184.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.184.5 Examples

```
- hosts: fortigates
  collections:
    - 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_spamfilter_options:
      vdom:  "{{ vdom }}"
      spamfilter_options:
        dns_timeout: "3"
```

5.184.6 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:

5.184.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.184.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.185 fortios_spamfilter_profile – Configure AntiSpam profiles in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.185.1 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

5.185.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.185.3 Parameters

5.185.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.185.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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:
           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"
```

5.185.6 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:

5.185.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.185.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.186 fortios_ssh_filter_profile – SSH filter profile in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.186.1 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

5.186.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.186.3 Parameters

5.186.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.186.5 Examples

```
- hosts: fortigates
  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"
        log: "x11"
        name: "default_name_6"
        shell_commands:
         -
            action: "block"
            alert: "enable"
            id:  "10"
            log: "enable"
            pattern: "<your_own_value>"
            severity: "low"
            type: "simple"
```

5.186.6 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:

5.186.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.186.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.187 fortios_switch_controller_802_1x_settings – Configure global 802.1X settings in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.187.1 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

5.187.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.187.3 Parameters

5.187.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.187.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.187.6 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:

5.187.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.187.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.188 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 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.188.1 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

5.188.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.188.3 Parameters

5.188.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.188.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.188.6 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:

5.188.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.188.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.189 fortios_switch_controller_global – Configure FortiSwitch global settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.189.1 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

5.189.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.189.3 Parameters

5.189.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.189.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
      default_virtual_switch_vlan: "<your_own_value> (source system.interface.name)"
      disable_discovery:
       -
          name: "default_name_6"
      https_image_push: "enable"
      mac_aging_interval: "8"
      mac_retention_period: "9"
```

5.189.6 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:

5.189.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.189.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.190 fortios_switch_controller_igmp_snooping – Configure FortiSwitch IGMP snooping global settings in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.190.1 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

5.190.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.190.3 Parameters

5.190.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.190.5 Examples

```
- hosts: fortigates
  collections:
    - 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 }}"
```

(continues on next page)

(continued from previous page)

```
    switch_controller_igmp_snooping:
      aging_time: "3"
      flood_unknown_multicast: "enable"
```

5.190.6 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:

5.190.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.190.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.191 fortios_switch_controller_lldp_profile – Configure FortiSwitch LLDP profiles in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.191.1 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

5.191.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.191.3 Parameters

5.191.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.191.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        custom_tlvs:
         -
            information_string: "<your_own_value>"
            name: "default_name_11"
            oui: "<your_own_value>"
            subtype: "13"
        med_network_policy:
```

(continues on next page)

(continued from previous page)

```
        -
            dscp: "15"
            name: "default_name_16"
            priority: "17"
            status: "disable"
            vlan: "19"
        med_tlvs: "inventory-management"
        name: "default_name_21"
```

5.191.6 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:

5.191.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.191.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.192 fortios_switch_controller_lldp_settings – Configure FortiSwitch LLDP settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*

- *Status*
- *Authors*

5.192.1 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

5.192.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.192.3 Parameters

5.192.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.192.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        fast_start_interval: "3"
        management_interface: "internal"
        status: "enable"
        tx_hold: "6"
        tx_interval: "7"
```

5.192.6 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:

5.192.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.192.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.193 fortios_switch_controller_mac_sync_settings – Configure global MAC synchronization settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.193.1 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

5.193.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.193.3 Parameters

5.193.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.193.5 Examples

```
- hosts: fortigates
  collections:
    - 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 }}"
      switch_controller_mac_sync_settings:
        mac_sync_interval: "3"
```

5.193.6 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:

5.193.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.193.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.194 fortios_switch_controller_managed_switch – Configure FortiSwitch devices that are managed by this FortiGate in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.194.1 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

5.194.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.194.3 Parameters

5.194.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.194.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        connected: "8"
        custom_command:
         -
            command_entry: "<your_own_value>"
            command_name: "<your_own_value> (source switch-controller.custom-command.
↪command-name)"
        delayed_restart_trigger: "12"
        description: "<your_own_value>"
        directly_connected: "14"
        dynamic_capability: "15"
        dynamically_discovered: "16"
        fsw_wan1_admin: "discovered"
        fsw_wan1_peer: "<your_own_value>"
        fsw_wan2_admin: "discovered"
        fsw_wan2_peer: "<your_own_value>"
        igmp_snooping:
            aging_time: "22"
            flood_unknown_multicast: "enable"
            local_override: "enable"
        max_allowed_trunk_members: "25"
        mirror:
         -
            dst: "<your_own_value>"
            name: "default_name_28"
            src_egress:
             -
                name: "default_name_30"
            src_ingress:
             -
                name: "default_name_32"
            status: "active"
            switching_packet: "enable"
        name: "default_name_35"
        owner_vdom: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        poe_pre_standard_detection: "enable"
        ports:
         -
            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: "53"
            fgt_peer_device_name: "<your_own_value>"
            fgt_peer_port_name: "<your_own_value>"
            fiber_port: "56"
            flags: "57"
            fortilink_port: "58"
            igmp_snooping: "enable"
            igmps_flood_reports: "enable"
            igmps_flood_traffic: "enable"
            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: "66"
            lldp_profile: "<your_own_value> (source switch-controller.lldp-profile.
↪name)"
            lldp_status: "disable"
            loop_guard: "enabled"
            loop_guard_timeout: "70"
            max_bundle: "71"
            mclag: "enable"
            member_withdrawal_behavior: "forward"
            members:
             -
                member_name: "<your_own_value>"
            min_bundle: "76"
            mode: "static"
            poe_capable: "78"
            poe_pre_standard_detection: "enable"
            poe_status: "enable"
            port_name: "<your_own_value>"
            port_number: "82"
            port_owner: "<your_own_value>"
            port_prefix_type: "84"
            port_security_policy: "<your_own_value> (source switch-controller.
↪security-policy.802-1X.name switch-controller.security-policy.captive-portal
```

(continues on next page)

(continued from previous page)

```
              .name)"
            port_selection_criteria: "src-mac"
            qos_policy: "<your_own_value> (source switch-controller.qos.qos-policy.
↪name)"
            sample_direction: "tx"
            sflow_counter_interval: "89"
            sflow_sample_rate: "90"
            sflow_sampler: "enabled"
            speed: "10half"
            speed_mask: "93"
            stacking_port: "94"
            status: "up"
            stp_bpdu_guard: "enabled"
            stp_bpdu_guard_timeout: "97"
            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: "104"
            vlan: "<your_own_value> (source system.interface.name)"
        pre_provisioned: "106"
        staged_image_version: "<your_own_value>"
        storm_control:
            broadcast: "enable"
            local_override: "enable"
            rate: "111"
            unknown_multicast: "enable"
            unknown_unicast: "enable"
        stp_settings:
            forward_time: "115"
            hello_time: "116"
            local_override: "enable"
            max_age: "118"
            max_hops: "119"
            name: "default_name_120"
            pending_timer: "121"
            revision: "122"
            status: "enable"
        switch_device_tag: "<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"
        type: "virtual"
        version: "134"
```

5.194.6 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:

5.194.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.194.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.195 fortios_switch_controller_network_monitor_settings – Configure network monitor settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.195.1 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

5.195.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.195.3 Parameters

5.195.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.195.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.195.6 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:

5.195.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.195.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.196 fortios_switch_controller_qos_dot1p_map – Configure FortiSwitch QoS 802.1p in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.196.1 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

5.196.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.196.3 Parameters

5.196.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.196.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
        name: "default_name_4"
        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"
```

5.196.6 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:

5.196.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.196.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.197 fortios_switch_controller_qos_ip_dscp_map – Configure FortiSwitch QoS IP precedence/DSCP in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.197.1 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

5.197.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.197.3 Parameters

5.197.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.197.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.197.6 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:

5.197.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.197.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.198 fortios_switch_controller_qos_qos_policy – Configure FortiSwitch QoS policy in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.198.1 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

5.198.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.198.3 Parameters

5.198.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.198.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
      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)"
```

5.198.6 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:

5.198.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.198.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.199 fortios_switch_controller_qos_queue_policy – Configure FortiSwitch QoS egress queue policy in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*

- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.199.1 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

5.199.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.199.3 Parameters

5.199.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.199.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    -
      description: "<your_own_value>"
      drop_policy: "taildrop"
      max_rate: "6"
      min_rate: "7"
      name: "default_name_8"
      weight: "9"
  name: "default_name_10"
  schedule: "strict"
```

5.199.6 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:

5.199.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.199.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.200 fortios_switch_controller_quarantine – Configure FortiSwitch quarantine support in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*

- *Return Values*
- *Status*
- *Authors*

5.200.1 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

5.200.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.200.3 Parameters

5.200.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.200.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.200.6 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:

5.200.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.200.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.201 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.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.201.1 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

5.201.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.201.3 Parameters

5.201.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.201.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        eap_passthru: "disable"
        guest_auth_delay: "7"
        guest_vlan: "disable"
        guest_vlan_id: "<your_own_value> (source system.interface.name)"
        guest_vlanid: "10"
        mac_auth_bypass: "disable"
        name: "default_name_12"
        policy_type: "802.1X"
        radius_timeout_overwrite: "disable"
        security_mode: "802.1X"
        user_group:
         -
            name: "default_name_17 (source user.group.name)"
```

5.201.6 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:

5.201.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.201.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.202 fortios_switch_controller_security_policy_captive_portal – Names of VLANs that use captive portal authentication in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.202.1 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

5.202.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.202.3 Parameters

5.202.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.202.5 Examples

```
- hosts: fortigates
  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)"
```

5.202.6 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:

5.202.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.202.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.203 fortios_switch_controller_sflow – Configure FortiSwitch sFlow in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.203.1 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

5.203.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.203.3 Parameters

5.203.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.203.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.203.6 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:

5.203.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.203.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.204 fortios_switch_controller_storm_control – Configure FortiSwitch storm control in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.204.1 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

5.204.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.204.3 Parameters

5.204.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.204.5 Examples

```
- hosts: fortigates
  collections:
    - 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.
    fortios_switch_controller_storm_control:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
    switch_controller_storm_control:
      broadcast: "enable"
      rate: "4"
      unknown_multicast: "enable"
      unknown_unicast: "enable"
```

5.204.6 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:

5.204.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.204.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.205 fortios_switch_controller_stp_settings – Configure FortiSwitch spanning tree protocol (STP) in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*

- *Authors*

5.205.1 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

5.205.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.205.3 Parameters

5.205.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.205.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.205.6 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:

5.205.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.205.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.206 fortios_switch_controller_switch_group – Configure FortiSwitch switch groups in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.206.1 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

5.206.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.206.3 Parameters

5.206.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.206.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
        members:
         -
            name: "default_name_5 (source switch-controller.managed-switch.switch-id)"
        name: "default_name_6"
```

5.206.6 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:

5.206.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.206.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.207 fortios_switch_controller_switch_interface_tag – Configure switch object tags in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.207.1 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

5.207.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.207.3 Parameters

5.207.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.207.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.207.6 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:

5.207.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.207.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.208 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 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.208.1 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

5.208.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.208.3 Parameters

5.208.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.208.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.208.6 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:

5.208.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.208.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.209 fortios_switch_controller_switch_profile – Configure FortiSwitch switch profile in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.209.1 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

5.209.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.209.3 Parameters

5.209.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.209.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    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"
```

5.209.6 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:

5.209.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.209.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.210 fortios_switch_controller_system – Configure system-wide switch controller settings in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*

- *Status*
- *Authors*

5.210.1 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

5.210.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.210.3 Parameters

5.210.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.210.5 Examples

```
- hosts: fortigates
  collections:
    - 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-wide switch controller settings.
    fortios_switch_controller_system:
      vdom:  "{{ vdom }}"
      switch_controller_system:
        parallel_process: "3"
        parallel_process_override: "disable"
```

5.210.6 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:

5.210.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.210.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.211 fortios_switch_controller_virtual_port_pool – Configure virtual pool in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.211.1 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

5.211.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.211.3 Parameters

5.211.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.211.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.211.6 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:

5.211.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.211.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.212 fortios_switch_controller_vlan – Configure VLANs for switch controller in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.212.1 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

5.212.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.212.3 Parameters

5.212.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.212.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   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"
```

5.212.6 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:

5.212.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.212.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.213 fortios_system_3g_modem_custom – 3G MODEM custom in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.213.1 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

5.213.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.213.3 Parameters

5.213.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.213.5 Examples

```
- hosts: fortigates
  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>"
        product_id: "<your_own_value>"
        vendor: "<your_own_value>"
        vendor_id: "<your_own_value>"
```

5.213.6 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:

5.213.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.213.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.214 fortios_system_accprofile – Configure access profiles for system administrators in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.214.1 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

5.214.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.214.3 Parameters

5.214.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.214.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       utmgrp: "none"
       utmgrp_permission:
           antivirus: "none"
           application_control: "none"
           data_loss_prevention: "none"
           dnsfilter: "none"
           endpoint_control: "none"
           icap: "none"
           ips: "none"
           spamfilter: "none"
           voip: "none"
           waf: "none"
           webfilter: "none"
       vpngrp: "none"
       wanoptgrp: "none"
       wifi: "none"
```

5.214.6 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:

5.214.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.214.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.215 fortios_system_admin – Configure admin users in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.215.1 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

5.215.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.215.3 Parameters

5.215.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.215.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        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"
            scope: "global"
            widget:
             -
```

(continues on next page)

(continued from previous page)

```
            fabric_device: "<your_own_value>"
            filters:
             -
                id:  "23"
                key: "<your_own_value>"
                value: "<your_own_value>"
            height: "26"
            id:  "27"
            industry: "default"
            interface: "<your_own_value> (source system.interface.name)"
            region: "default"
            report_by: "source"
            sort_by: "<your_own_value>"
            timeframe: "realtime"
            title: "<your_own_value>"
            type: "sysinfo"
            visualization: "table"
            width: "37"
            x_pos: "38"
            y_pos: "39"
        gui_global_menu_favorites:
         -
            id:  "41"
        gui_vdom_menu_favorites:
         -
            id:  "43"
        hidden: "44"
        history0: "<your_own_value>"
        history1: "<your_own_value>"
        ip6_trusthost1: "<your_own_value>"
        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_61"
        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)"
```

(continues on next page)

(continued from previous page)

```
        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"
        vdom:
         -
            name: "default_name_89 (source system.vdom.name)"
        wildcard: "enable"
```

5.215.6 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:

5.215.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.215.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.216 fortios_system_affinity_interrupt – Configure interrupt affinity in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.216.1 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

5.216.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.216.3 Parameters

5.216.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.216.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    system_affinity_interrupt:
      affinity_cpumask: "<your_own_value>"
      id:  "4"
      interrupt: "<your_own_value>"
```

5.216.6 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:

5.216.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.216.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.217 fortios_system_affinity_packet_redistribution – Configure packet redistribution in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*

- *Status*
- *Authors*

5.217.1 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

5.217.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.217.3 Parameters

5.217.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.217.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.217.6 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:

5.217.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.217.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.218 fortios_system_alarm – Configure alarm in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.218.1 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

5.218.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.218.3 Parameters

5.218.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.218.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
            user_auth_lockout_threshold: "24"
        status: "enable"
```

5.218.6 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:

5.218.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.218.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.219 fortios_system_alias – Configure alias command in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.219.1 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

5.219.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.219.3 Parameters

5.219.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.219.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.219.6 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:

5.219.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.219.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.220 fortios_system_api_user – Configure API users in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.220.1 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

5.220.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.220.3 Parameters

5.220.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.220.5 Examples

```
- hosts: fortigates
  collections:
    - 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)"
```

5.220.6 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:

5.220.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.220.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.221 fortios_system_arp_table – Configure ARP table in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.221.1 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

5.221.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.221.3 Parameters

5.221.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.221.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.221.6 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:

5.221.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.221.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.222 fortios_system_auto_install – Configure USB auto installation in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.222.1 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

5.222.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.222.3 Parameters

5.222.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.222.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.222.6 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:

5.222.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.222.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.223 fortios_system_auto_script – Configure auto script in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.223.1 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

5.223.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.223.3 Parameters

5.223.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.223.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure auto script.
    fortios_system_auto_script:
```

(continues on next page)

(continued from previous page)

```
    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"
```

5.223.6 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:

5.223.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.223.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.224 fortios_system_automation_action – Action for automation stitches in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*

- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.224.1 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

5.224.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.224.3 Parameters

5.224.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.224.5 Examples

```
- hosts: fortigates
  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 }}"
      state: "present"
      access_token: "<your_own_value>"
      system_automation_action:
        action_type: "email"
        aws_api_id: "<your_own_value>"
        aws_api_key: "<your_own_value>"
        aws_api_path: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        aws_api_stage: "<your_own_value>"
        aws_region: "<your_own_value>"
        email_subject: "<your_own_value>"
        email_to:
         -
            name: "default_name_11"
        headers:
         -
            header: "<your_own_value>"
        http_body: "<your_own_value>"
        method: "post"
        minimum_interval: "16"
        name: "default_name_17"
        port: "18"
        protocol: "http"
        uri: "<your_own_value>"
```

5.224.6 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:

5.224.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.224.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.225 fortios_system_automation_destination – Automation destinations in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.225.1 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

5.225.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.225.3 Parameters

5.225.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.225.5 Examples

```
- hosts: fortigates
  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 }}"
```

(continues on next page)

(continued from previous page)

```
    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"
```

5.225.6 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:

5.225.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.225.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.226 fortios_system_automation_stitch – Automation stitches in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*

- *Return Values*
- *Status*
- *Authors*

5.226.1 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

5.226.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.226.3 Parameters

5.226.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.226.5 Examples

```
- hosts: fortigates
  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)"
        destination:
         -
            name: "default_name_6 (source system.automation-destination.name)"
```

(continues on next page)

(continued from previous page)

```
        name: "default_name_7"
        status: "enable"
        trigger: "<your_own_value> (source system.automation-trigger.name)"
```

5.226.6 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:

5.226.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.226.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.227 fortios_system_automation_trigger – Trigger for automation stitches in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.227.1 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

5.227.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.227.3 Parameters

5.227.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.227.5 Examples

```
- hosts: fortigates
  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:
        event_type: "ioc"
        ioc_level: "medium"
        license_type: "forticare-support"
        logid: "6"
        name: "default_name_7"
        trigger_day: "8"
        trigger_frequency: "hourly"
        trigger_hour: "10"
        trigger_minute: "11"
        trigger_type: "event-based"
        trigger_weekday: "sunday"
```

5.227.6 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:

5.227.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.227.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.228 fortios_system_autoupdate_push_update – Configure push updates in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.228.1 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

5.228.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.228.3 Parameters

5.228.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.228.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.228.6 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:

5.228.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.228.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.229 fortios_system_autoupdate_schedule – Configure update schedule in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.229.1 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

5.229.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.229.3 Parameters

5.229.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.229.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.229.6 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:

5.229.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.229.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.230 fortios_system_autoupdate_tunneling – Configure web proxy tunnelling for the FDN in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.230.1 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

5.230.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.230.3 Parameters

5.230.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.230.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    vdom:  "{{ vdom }}"
    system_autoupdate_tunneling:
      address: "<your_own_value>"
      password: "<your_own_value>"
      port: "5"
      status: "enable"
      username: "<your_own_value>"
```

5.230.6 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:

5.230.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.230.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.231 fortios_system_central_management – Configure central management in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*

- *Status*
- *Authors*

5.231.1 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

5.231.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.231.3 Parameters

5.231.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.231.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        enc_algorithm: "default"
        fmg: "<your_own_value>"
        fmg_source_ip: "<your_own_value>"
        fmg_source_ip6: "<your_own_value>"
        include_default_servers: "enable"
        mode: "normal"
```

(continues on next page)

(continued from previous page)

```
        schedule_config_restore: "enable"
        schedule_script_restore: "enable"
        serial_number: "<your_own_value>"
        server_list:
         -
            addr_type: "ipv4"
            fqdn: "<your_own_value>"
            id:  "19"
            server_address: "<your_own_value>"
            server_address6: "<your_own_value>"
            server_type: "update"
        type: "fortimanager"
        vdom: "<your_own_value> (source system.vdom.name)"
```

5.231.6 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:

5.231.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.231.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.232 fortios_system_cluster_sync – Configure FortiGate Session Life Support Protocol (FGSP) session synchronization in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*

- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.232.1 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

5.232.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.232.3 Parameters

5.232.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.232.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
        down_intfs_before_sess_sync:
         -
            name: "default_name_4 (source system.interface.name)"
        hb_interval: "5"
        hb_lost_threshold: "6"
        peerip: "<your_own_value>"
        peervd: "<your_own_value> (source system.vdom.name)"
        session_sync_filter:
            custom_service:
             -
                dst_port_range: "<your_own_value>"
                id:  "12"
                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)"
        slave_add_ike_routes: "enable"
        sync_id: "21"
        syncvd:
         -
            name: "default_name_23 (source system.vdom.name)"
```

5.232.6 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:

5.232.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.232.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.233 fortios_system_console – Configure console in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.233.1 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

5.233.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.233.3 Parameters

5.233.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.233.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
      login: "enable"
      mode: "batch"
      output: "standard"
```

5.233.6 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:

5.233.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.233.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.234 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 2.9.

- *Synopsis*
- *Requirements*

- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.234.1 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

5.234.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.234.3 Parameters

5.234.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.234.5 Examples

```
- hosts: fortigates
  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:
        configuration_sync: "default"
        fabric_device:
```

(continues on next page)

(continued from previous page)

```
        -
            device_ip: "<your_own_value>"
            device_type: "fortimail"
            login: "<your_own_value>"
            name: "default_name_8"
            password: "<your_own_value>"
        fixed_key: "<your_own_value>"
        group_name: "<your_own_value>"
        group_password: "<your_own_value>"
        management_ip: "<your_own_value>"
        status: "enable"
        trusted_list:
         -
            action: "accept"
            downstream_authorization: "enable"
            ha_members: "<your_own_value>"
            serial: "<your_own_value>"
        upstream_ip: "<your_own_value>"
        upstream_port: "21"
```

5.234.6 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:

5.234.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.234.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.235 fortios_system_custom_language – Configure custom languages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.235.1 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

5.235.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.235.3 Parameters

5.235.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.235.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    system_custom_language:
      comments: "<your_own_value>"
      filename: "<your_own_value>"
      name: "default_name_5"
```

5.235.6 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:

5.235.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.235.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.236 fortios_system_ddns – Configure DDNS in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*

- *Status*
- *Authors*

5.236.1 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

5.236.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.236.3 Parameters

5.236.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.236.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure DDNS.
    fortios_system_ddns:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_ddns:
        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"
```

(continues on next page)

(continued from previous page)

```
        ddns_server_ip: "<your_own_value>"
        ddns_sn: "<your_own_value>"
        ddns_ttl: "13"
        ddns_username: "<your_own_value>"
        ddns_zone: "<your_own_value>"
        ddnsid: "16"
        monitor_interface:
         -
            interface_name: "<your_own_value> (source system.interface.name)"
        ssl_certificate: "<your_own_value> (source certificate.local.name)"
        update_interval: "20"
        use_public_ip: "disable"
```

5.236.6 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:

5.236.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.236.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.237 fortios_system_dedicated_mgmt – Configure dedicated management in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*

- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.237.1 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

5.237.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.237.3 Parameters

5.237.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.237.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

(continues on next page)

(continued from previous page)

```
        interface: "<your_own_value> (source system.interface.name)"
        status: "enable"
```

5.237.6 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:

5.237.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.237.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.238 fortios_system_dhcp6_server – Configure DHCPv6 servers in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.238.1 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

5.238.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.238.3 Parameters

5.238.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.238.5 Examples

```
- hosts: fortigates
  collections:
    - 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_service: "delegated"
        domain: "<your_own_value>"
        id:  "9"
        interface: "<your_own_value> (source system.interface.name)"
        ip_mode: "range"
        ip_range:
         -
            end_ip: "<your_own_value>"
            id:  "14"
```

(continues on next page)

(continued from previous page)

```
            start_ip: "<your_own_value>"
        lease_time: "16"
        option1: "<your_own_value>"
        option2: "<your_own_value>"
        option3: "<your_own_value>"
        prefix_range:
         -
            end_prefix: "<your_own_value>"
            id:  "22"
            prefix_length: "23"
            start_prefix: "<your_own_value>"
        rapid_commit: "disable"
        status: "disable"
        subnet: "<your_own_value>"
        upstream_interface: "<your_own_value> (source system.interface.name)"
```

5.238.6 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:

5.238.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.238.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.239 fortios_system_dhcp_server – Configure DHCP servers in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*

- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.239.1 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

5.239.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.239.3 Parameters

5.239.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.239.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
        auto_configuration: "disable"
        conflicted_ip_timeout: "4"
        ddns_auth: "disable"
        ddns_key: "<your_own_value>"
        ddns_keyname: "<your_own_value>"
        ddns_server_ip: "<your_own_value>"
        ddns_ttl: "9"
        ddns_update: "disable"
        ddns_update_override: "disable"
        ddns_zone: "<your_own_value>"
        default_gateway: "<your_own_value>"
        dns_server1: "<your_own_value>"
        dns_server2: "<your_own_value>"
        dns_server3: "<your_own_value>"
        dns_service: "local"
        domain: "<your_own_value>"
        exclude_range:
         -
            end_ip: "<your_own_value>"
            id:  "21"
            start_ip: "<your_own_value>"
        filename: "<your_own_value>"
        forticlient_on_net_status: "disable"
        id:  "25"
        interface: "<your_own_value> (source system.interface.name)"
        ip_mode: "range"
        ip_range:
         -
            end_ip: "<your_own_value>"
            id:  "30"
            start_ip: "<your_own_value>"
        ipsec_lease_hold: "32"
        lease_time: "33"
        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: "42"
            id:  "43"
            ip: "<your_own_value>"
            type: "hex"
            value: "<your_own_value>"
        reserved_address:
         -
            action: "assign"
            description: "<your_own_value>"
            id:  "50"
            ip: "<your_own_value>"
            mac: "<your_own_value>"
        server_type: "regular"
        status: "disable"
        tftp_server:
```

(continues on next page)

(continued from previous page)

```
        -
            tftp_server: "<your_own_value>"
        timezone: "01"
        timezone_option: "disable"
        vci_match: "disable"
        vci_string:
        -
            vci_string: "<your_own_value>"
        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>"
```

5.239.6 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:

5.239.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.239.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.240 fortios_system_dns – Configure DNS in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*

- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.240.1 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

5.240.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.240.3 Parameters

5.240.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.240.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        domain: "<your_own_value>"
        ip6_primary: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        ip6_secondary: "<your_own_value>"
        primary: "<your_own_value>"
        secondary: "<your_own_value>"
        source_ip: "84.230.14.43"
```

5.240.6 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:

5.240.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.240.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.241 fortios_system_dns_database – Configure DNS databases in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.241.1 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

5.241.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.241.3 Parameters

5.241.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.241.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
            type: "A"
        domain: "<your_own_value>"
        forwarder: "<your_own_value>"
        ip_master: "<your_own_value>"
        name: "default_name_19"
        primary_name: "<your_own_value>"
        source_ip: "84.230.14.43"
        status: "enable"
        ttl: "23"
        type: "master"
        view: "shadow"
```

5.241.6 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:

5.241.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.241.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.242 fortios_system_dns_server – Configure DNS servers in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*

- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.242.1 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

5.242.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.242.3 Parameters

5.242.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.242.5 Examples

```
- hosts: fortigates
  collections:
    - 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)"
        mode: "recursive"
        name: "default_name_5 (source system.interface.name)"
```

5.242.6 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:

5.242.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.242.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.243 fortios_system_dscp_based_priority – Configure DSCP based priority table in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.243.1 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

5.243.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.243.3 Parameters

5.243.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.243.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.243.6 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:

5.243.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.243.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.244 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 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.244.1 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

5.244.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.244.3 Parameters

5.244.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.244.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        password: "<your_own_value>"
        port: "5"
        reply_to: "<your_own_value>"
        security: "none"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        source_ip6: "<your_own_value>"
        type: "custom"
        username: "<your_own_value>"
        validate_server: "enable"
```

5.244.6 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:

5.244.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.244.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.245 fortios_system_external_resource – Configure external resource in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.245.1 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

5.245.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.245.3 Parameters

5.245.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.245.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
        last_update: "<your_own_value>"
        name: "default_name_6"
        refresh_rate: "7"
        resource: "<your_own_value>"
        status: "enable"
        type: "category"
```

5.245.6 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:

5.245.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.245.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.246 fortios_system_fips_cc – Configure FIPS-CC mode in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.246.1 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

5.246.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.246.3 Parameters

5.246.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.246.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.246.6 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:

5.246.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.246.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.247 fortios_system_fm – Configure FM in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*

- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.247.1 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

5.247.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.247.3 Parameters

5.247.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.247.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
        status: "enable"
        vdom: "<your_own_value> (source system.vdom.name)"
```

5.247.6 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:

5.247.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.247.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.248 fortios_system_fortiguard – Configure FortiGuard services in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.248.1 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

5.248.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.248.3 Parameters

5.248.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.248.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        ddns_server_ip: "<your_own_value>"
        ddns_server_port: "11"
        load_balance_servers: "12"
        outbreak_prevention_cache: "enable"
        outbreak_prevention_cache_mpercent: "14"
        outbreak_prevention_cache_ttl: "15"
        outbreak_prevention_expiration: "16"
        outbreak_prevention_force_off: "enable"
```

(continues on next page)

(continued from previous page)

```
        outbreak_prevention_license: "18"
        outbreak_prevention_timeout: "19"
        port: "53"
        sdns_server_ip: "<your_own_value>"
        sdns_server_port: "22"
        service_account_id: "<your_own_value>"
        source_ip: "84.230.14.43"
        source_ip6: "<your_own_value>"
        update_server_location: "usa"
        webfilter_cache: "enable"
        webfilter_cache_ttl: "28"
        webfilter_expiration: "29"
        webfilter_force_off: "enable"
        webfilter_license: "31"
        webfilter_timeout: "32"
```

5.248.6 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:

5.248.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.248.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.249 fortios_system_fortimanager – Configure FortiManager in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*

- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.249.1 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

5.249.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.249.3 Parameters

5.249.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.249.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
        central_mgmt_schedule_config_restore: "enable"
        central_mgmt_schedule_script_restore: "enable"
        ip: "<your_own_value>"
        ipsec: "enable"
        vdom: "<your_own_value> (source system.vdom.name)"
```

5.249.6 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:

5.249.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.249.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.250 fortios_system_fortisandbox – Configure FortiSandbox in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.250.1 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

5.250.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.250.3 Parameters

5.250.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.250.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        status: "enable"
```

5.250.6 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:

5.250.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.250.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.251 fortios_system_fsso_polling – Configure Fortinet Single Sign On (FSSO) server in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.251.1 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

5.251.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.251.3 Parameters

5.251.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.251.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.251.6 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:

5.251.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.251.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.252 fortios_system_ftm_push – Configure FortiToken Mobile push services in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.252.1 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

5.252.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.252.3 Parameters

5.252.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.252.5 Examples

```
- hosts: fortigates
  collections:
    - 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_ip: "<your_own_value>"
        server_port: "4"
        status: "enable"
```

5.252.6 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:

5.252.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.252.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.253 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 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.253.1 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

5.253.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.253.3 Parameters

5.253.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.253.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure geographical location mapping for IP address(es) to override␣
↪mappings from FortiGuard.
```

(continues on next page)

(continued from previous page)

```
    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>"
        name: "default_name_9"
```

5.253.6 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:

5.253.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.253.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.254 fortios_system_global – Configure global attributes in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*

- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.254.1 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

5.254.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.254.3 Parameters

5.254.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.254.5 Examples

```
- hosts: fortigates
  collections:
    - 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.
    fortios_system_global:
      vdom:  "{{ vdom }}"
      system_global:
        admin_concurrent: "enable"
        admin_console_timeout: "4"
        admin_https_pki_required: "enable"
        admin_https_redirect: "enable"
        admin_https_ssl_versions: "tlsv1-0"
```

(continues on next page)

(continued from previous page)

```
        admin_lockout_duration: "8"
        admin_lockout_threshold: "9"
        admin_login_max: "10"
        admin_maintainer: "enable"
        admin_port: "12"
        admin_restrict_local: "enable"
        admin_scp: "enable"
        admin_server_cert: "<your_own_value> (source certificate.local.name)"
        admin_sport: "16"
        admin_ssh_grace_time: "17"
        admin_ssh_password: "enable"
        admin_ssh_port: "19"
        admin_ssh_v1: "enable"
        admin_telnet_port: "21"
        admintimeout: "22"
        alias: "<your_own_value>"
        allow_traffic_redirect: "enable"
        anti_replay: "disable"
        arp_max_entry: "26"
        asymroute: "enable"
        auth_cert: "<your_own_value> (source certificate.local.name)"
        auth_http_port: "29"
        auth_https_port: "30"
        auth_keepalive: "enable"
        auth_session_limit: "block-new"
        auto_auth_extension_device: "enable"
        av_affinity: "<your_own_value>"
        av_failopen: "pass"
        av_failopen_session: "enable"
        batch_cmdb: "enable"
        block_session_timer: "38"
        br_fdb_max_entry: "39"
        cert_chain_max: "40"
        cfg_revert_timeout: "41"
        cfg_save: "automatic"
        check_protocol_header: "loose"
        check_reset_range: "strict"
        cli_audit_log: "enable"
        clt_cert_req: "enable"
        compliance_check: "enable"
        compliance_check_time: "<your_own_value>"
        cpu_use_threshold: "49"
        csr_ca_attribute: "enable"
        daily_restart: "enable"
        device_identification_active_scan_delay: "52"
        device_idle_timeout: "53"
        dh_params: "1024"
        dst: "enable"
        endpoint_control_fds_access: "enable"
        endpoint_control_portal_port: "57"
        failtime: "58"
        fds_statistics: "enable"
        fds_statistics_period: "60"
        fgd_alert_subscription: "advisory"
        fortiextender: "enable"
        fortiextender_data_port: "63"
        fortiextender_vlan_mode: "enable"
```

(continues on next page)

(continued from previous page)

```
        fortiservice_port: "65"
        gui_certificates: "enable"
        gui_custom_language: "enable"
        gui_device_latitude: "<your_own_value>"
        gui_device_longitude: "<your_own_value>"
        gui_display_hostname: "enable"
        gui_ipv6: "enable"
        gui_lines_per_page: "72"
        gui_theme: "green"
        gui_wireless_opensecurity: "enable"
        honor_df: "enable"
        hostname: "myhostname"
        igmp_state_limit: "77"
        interval: "78"
        ip_src_port_range: "<your_own_value>"
        ips_affinity: "<your_own_value>"
        ipsec_asic_offload: "enable"
        ipsec_hmac_offload: "enable"
        ipv6_accept_dad: "83"
        ipv6_allow_anycast_probe: "enable"
        language: "english"
        ldapconntimeout: "86"
        lldp_transmission: "enable"
        log_ssl_connection: "enable"
        log_uuid: "disable"
        login_timestamp: "enable"
        long_vdom_name: "enable"
        management_vdom: "<your_own_value> (source system.vdom.name)"
        max_dlpstat_memory: "93"
        max_route_cache_size: "94"
        mc_ttl_notchange: "enable"
        memory_use_threshold_extreme: "96"
        memory_use_threshold_green: "97"
        memory_use_threshold_red: "98"
        miglogd_children: "99"
        multi_factor_authentication: "optional"
        multicast_forward: "enable"
        ndp_max_entry: "102"
        per_user_bwl: "enable"
        policy_auth_concurrent: "104"
        post_login_banner: "disable"
        pre_login_banner: "enable"
        private_data_encryption: "disable"
        proxy_auth_lifetime: "enable"
        proxy_auth_lifetime_timeout: "109"
        proxy_auth_timeout: "110"
        proxy_cipher_hardware_acceleration: "disable"
        proxy_kxp_hardware_acceleration: "disable"
        proxy_re_authentication_mode: "session"
        proxy_worker_count: "114"
        radius_port: "115"
        reboot_upon_config_restore: "enable"
        refresh: "117"
        remoteauthtimeout: "118"
        reset_sessionless_tcp: "enable"
        restart_time: "<your_own_value>"
        revision_backup_on_logout: "enable"
```

(continues on next page)

(continued from previous page)

```
        revision_image_auto_backup: "enable"
        scanunit_count: "123"
        security_rating_result_submission: "enable"
        security_rating_run_on_schedule: "enable"
        send_pmtu_icmp: "enable"
        snat_route_change: "enable"
        special_file_23_support: "disable"
        ssh_cbc_cipher: "enable"
        ssh_hmac_md5: "enable"
        ssh_kex_sha1: "enable"
        ssl_static_key_ciphers: "enable"
        sslvpn_cipher_hardware_acceleration: "enable"
        sslvpn_kxp_hardware_acceleration: "enable"
        sslvpn_max_worker_count: "135"
        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: "141"
        tcp_halfclose_timer: "142"
        tcp_halfopen_timer: "143"
        tcp_option: "enable"
        tcp_timewait_timer: "145"
        tftp: "enable"
        timezone: "01"
        tp_mc_skip_policy: "enable"
        traffic_priority: "tos"
        traffic_priority_level: "low"
        two_factor_email_expiry: "151"
        two_factor_fac_expiry: "152"
        two_factor_ftk_expiry: "153"
        two_factor_ftm_expiry: "154"
        two_factor_sms_expiry: "155"
        udp_idle_timer: "156"
        user_server_cert: "<your_own_value> (source certificate.local.name)"
        vdom_admin: "enable"
        vip_arp_range: "unlimited"
        virtual_server_count: "160"
        virtual_server_hardware_acceleration: "disable"
        wad_csvc_cs_count: "162"
        wad_csvc_db_count: "163"
        wad_source_affinity: "disable"
        wad_worker_count: "165"
        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: "170"
```

5.254.6 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:

5.254.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.254.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.255 fortios_system_gre_tunnel – Configure GRE tunnel in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.255.1 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

5.255.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.255.3 Parameters

5.255.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.255.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        dscp_copying: "disable"
        interface: "<your_own_value> (source system.interface.name)"
        ip_version: "4"
        keepalive_failtimes: "8"
        keepalive_interval: "9"
        key_inbound: "10"
        key_outbound: "11"
        local_gw: "<your_own_value>"
        local_gw6: "<your_own_value>"
        name: "default_name_14"
        remote_gw: "<your_own_value>"
        remote_gw6: "<your_own_value>"
        sequence_number_reception: "disable"
        sequence_number_transmission: "disable"
```

5.255.6 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:

5.255.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.255.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.256 fortios_system_ha – Configure HA in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.256.1 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

5.256.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.256.3 Parameters

5.256.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.256.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        ftp_proxy_threshold: "<your_own_value>"
        gratuitous_arps: "enable"
        group_id: "10"
        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:  "18"
            interface: "<your_own_value> (source system.interface.name)"
        ha_mgmt_status: "enable"
        ha_uptime_diff_margin: "21"
        hb_interval: "22"
        hb_lost_threshold: "23"
        hbdev: "<your_own_value>"
        hc_eth_type: "<your_own_value>"
        hello_holddown: "26"
        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>"
```

(continues on next page)

(continued from previous page)

```
        link_failed_signal: "enable"
        load_balance_all: "enable"
        memory_compatible_mode: "enable"
        memory_threshold: "<your_own_value>"
        mode: "standalone"
        monitor: "<your_own_value> (source system.interface.name)"
        multicast_ttl: "38"
        nntp_proxy_threshold: "<your_own_value>"
        override: "enable"
        override_wait_time: "41"
        password: "<your_own_value>"
        pingserver_failover_threshold: "43"
        pingserver_flip_timeout: "44"
        pingserver_monitor_interface: "<your_own_value> (source system.interface.name)
↪"
        pingserver_slave_force_reset: "enable"
        pop3_proxy_threshold: "<your_own_value>"
        priority: "48"
        route_hold: "49"
        route_ttl: "50"
        route_wait: "51"
        schedule: "none"
        secondary_vcluster:
            monitor: "<your_own_value> (source system.interface.name)"
            override: "enable"
            override_wait_time: "56"
            pingserver_failover_threshold: "57"
            pingserver_monitor_interface: "<your_own_value> (source system.interface.
↪name)"
            pingserver_slave_force_reset: "enable"
            priority: "60"
            vcluster_id: "61"
            vdom: "<your_own_value>"
        session_pickup: "enable"
        session_pickup_connectionless: "enable"
        session_pickup_delay: "enable"
        session_pickup_expectation: "enable"
        session_pickup_nat: "enable"
        session_sync_dev: "<your_own_value> (source system.interface.name)"
        smtp_proxy_threshold: "<your_own_value>"
        standalone_config_sync: "enable"
        standalone_mgmt_vdom: "enable"
        sync_config: "enable"
        sync_packet_balance: "enable"
        unicast_hb: "enable"
        unicast_hb_netmask: "<your_own_value>"
        unicast_hb_peerip: "<your_own_value>"
        uninterruptible_upgrade: "enable"
        vcluster_id: "78"
        vcluster2: "enable"
        vdom: "<your_own_value>"
        weight: "<your_own_value>"
```

5.256.6 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:

5.256.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.256.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.257 fortios_system_ha_monitor – Configure HA monitor in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.257.1 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

5.257.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.257.3 Parameters

5.257.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.257.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.257.6 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:

5.257.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.257.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.258 fortios_system_interface – Configure interfaces in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.258.1 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

5.258.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.258.3 Parameters

5.258.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.258.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        bfd: "global"
        bfd_desired_min_tx: "13"
        bfd_detect_mult: "14"
        bfd_required_min_rx: "15"
        broadcast_forticlient_discovery: "enable"
        broadcast_forward: "enable"
        captive_portal: "18"
        cli_conn_status: "19"
        color: "20"
        dedicated_to: "none"
        defaultgw: "enable"
        description: "<your_own_value>"
        detected_peer_mtu: "24"
        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: "32"
        dhcp_client_identifier:  "myId_33"
        dhcp_relay_agent_option: "enable"
        dhcp_relay_ip: "<your_own_value>"
        dhcp_relay_service: "disable"
        dhcp_relay_type: "regular"
        dhcp_renew_time: "38"
        disc_retry_timeout: "39"
        disconnect_threshold: "40"
        distance: "41"
```

(continues on next page)

(continued from previous page)

```
        dns_server_override: "enable"
        drop_fragment: "enable"
        drop_overlapped_fragment: "enable"
        egress_shaping_profile: "<your_own_value>"
        endpoint_compliance: "enable"
        estimated_downstream_bandwidth: "47"
        estimated_upstream_bandwidth: "48"
        explicit_ftp_proxy: "enable"
        explicit_web_proxy: "enable"
        external: "enable"
        fail_action_on_extender: "soft-restart"
        fail_alert_interfaces:
         -
            name: "default_name_54 (source system.interface.name)"
        fail_alert_method: "link-failed-signal"
        fail_detect: "enable"
        fail_detect_option: "detectserver"
        fortiheartbeat: "enable"
        fortilink: "enable"
        fortilink_backup_link: "60"
        fortilink_split_interface: "enable"
        fortilink_stacking: "enable"
        forward_domain: "63"
        gwdetect: "enable"
        ha_priority: "65"
        icmp_redirect: "enable"
        ident_accept: "enable"
        idle_timeout: "68"
        inbandwidth: "69"
        ingress_spillover_threshold: "70"
        interface: "<your_own_value> (source system.interface.name)"
        internal: "72"
        ip: "<your_own_value>"
        ipmac: "enable"
        ips_sniffer_mode: "enable"
        ipunnumbered: "<your_own_value>"
        ipv6:
            autoconf: "enable"
            dhcp6_client_options: "rapid"
            dhcp6_information_request: "enable"
            dhcp6_prefix_delegation: "enable"
            dhcp6_prefix_hint: "<your_own_value>"
            dhcp6_prefix_hint_plt: "83"
            dhcp6_prefix_hint_vlt: "84"
            dhcp6_relay_ip: "<your_own_value>"
            dhcp6_relay_service: "disable"
            dhcp6_relay_type: "regular"
            ip6_address: "<your_own_value>"
            ip6_allowaccess: "ping"
            ip6_default_life: "90"
            ip6_delegated_prefix_list:
             -
                autonomous_flag: "enable"
                onlink_flag: "enable"
                prefix_id: "94"
                rdnss: "<your_own_value>"
                rdnss_service: "delegated"
```

(continues on next page)

(continued from previous page)

```
            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: "102"
        ip6_link_mtu: "103"
        ip6_manage_flag: "enable"
        ip6_max_interval: "105"
        ip6_min_interval: "106"
        ip6_mode: "static"
        ip6_other_flag: "enable"
        ip6_prefix_list:
         -
            autonomous_flag: "enable"
            dnssl:
             -
                domain: "<your_own_value>"
            onlink_flag: "enable"
            preferred_life_time: "114"
            prefix: "<your_own_value>"
            rdnss: "<your_own_value>"
            valid_life_time: "117"
        ip6_reachable_time: "118"
        ip6_retrans_time: "119"
        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: "126"
        nd_timestamp_delta: "127"
        nd_timestamp_fuzz: "128"
        vrip6_link_local: "<your_own_value>"
        vrrp_virtual_mac6: "enable"
        vrrp6:
         -
            accept_mode: "enable"
            adv_interval: "133"
            preempt: "enable"
            priority: "135"
            start_time: "136"
            status: "enable"
            vrdst6: "<your_own_value>"
            vrgrp: "139"
            vrid: "140"
            vrip6: "<your_own_value>"
    l2forward: "enable"
    lacp_ha_slave: "enable"
    lacp_mode: "static"
    lacp_speed: "slow"
    lcp_echo_interval: "146"
    lcp_max_echo_fails: "147"
    link_up_delay: "148"
    lldp_transmission: "enable"
```

(continues on next page)

(continued from previous page)

```
        macaddr: "<your_own_value>"
        managed_device:
         -
            name: "default_name_152"
        management_ip: "<your_own_value>"
        member:
         -
            interface_name: "<your_own_value> (source system.interface.name)"
        min_links: "156"
        min_links_down: "operational"
        mode: "static"
        mtu: "159"
        mtu_override: "enable"
        name: "default_name_161"
        ndiscforward: "enable"
        netbios_forward: "disable"
        netflow_sampler: "disable"
        outbandwidth: "165"
        padt_retry_timeout: "166"
        password: "<your_own_value>"
        ping_serv_status: "168"
        polling_interval: "169"
        pppoe_unnumbered_negotiate: "enable"
        pptp_auth_type: "auto"
        pptp_client: "enable"
        pptp_password: "<your_own_value>"
        pptp_server_ip: "<your_own_value>"
        pptp_timeout: "175"
        pptp_user: "<your_own_value>"
        preserve_session_route: "enable"
        priority: "178"
        priority_override: "enable"
        proxy_captive_portal: "enable"
        redundant_interface: "<your_own_value>"
        remote_ip: "<your_own_value>"
        replacemsg_override_group: "<your_own_value>"
        role: "lan"
        sample_direction: "tx"
        sample_rate: "186"
        scan_botnet_connections: "disable"
        secondary_IP: "enable"
        secondaryip:
         -
            allowaccess: "ping"
            detectprotocol: "ping"
            detectserver: "<your_own_value>"
            gwdetect: "enable"
            ha_priority: "194"
            id:  "195"
            ip: "<your_own_value>"
            ping_serv_status: "197"
        security_exempt_list: "<your_own_value>"
        security_external_logout: "<your_own_value>"
        security_external_web: "<your_own_value>"
        security_groups:
         -
            name: "default_name_202"
```

(continues on next page)

(continued from previous page)

```
        security_mac_auth_bypass: "enable"
        security_mode: "none"
        security_redirect_url: "<your_own_value>"
        service_name: "<your_own_value>"
        sflow_sampler: "enable"
        snmp_index: "208"
        speed: "auto"
        spillover_threshold: "210"
        src_check: "enable"
        status: "up"
        stpforward: "enable"
        stpforward_mode: "rpl-all-ext-id"
        subst: "enable"
        substitute_dst_mac: "<your_own_value>"
        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_igmp_snooping: "enable"
        switch_controller_learning_limit: "224"
        tagging:
         -
            category: "<your_own_value> (source system.object-tagging.category)"
            name: "default_name_227"
            tags:
             -
                name: "default_name_229 (source system.object-tagging.tags.name)"
        tcp_mss: "230"
        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: "240"
        vlanforward: "enable"
        vlanid: "242"
        vrf: "243"
        vrrp:
         -
            accept_mode: "enable"
            adv_interval: "246"
            preempt: "enable"
            priority: "248"
            proxy_arp:
             -
                id:  "250"
                ip: "<your_own_value>"
            start_time: "252"
            status: "enable"
            version: "2"
            vrdst: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
            vrdst_priority: "256"
            vrgrp: "257"
            vrid: "258"
            vrip: "<your_own_value>"
        vrrp_virtual_mac: "enable"
        wccp: "enable"
        weight: "262"
        wins_ip: "<your_own_value>"
```

5.258.6 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:

5.258.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.258.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.259 fortios_system_ipip_tunnel – Configure IP in IP Tunneling in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*

- *Status*
- *Authors*

5.259.1 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

5.259.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.259.3 Parameters

5.259.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.259.5 Examples

```
- hosts: fortigates
  collections:
    - 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 }}"
      state: "present"
      access_token: "<your_own_value>"
      system_ipip_tunnel:
        interface: "<your_own_value> (source system.interface.name)"
        local_gw: "<your_own_value>"
        name: "default_name_5"
        remote_gw: "<your_own_value>"
```

5.259.6 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:

5.259.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.259.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.260 fortios_system_ips_urlfilter_dns – Configure IPS URL filter DNS servers in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.260.1 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

5.260.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.260.3 Parameters

5.260.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.260.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.260.6 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:

5.260.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.260.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.261 fortios_system_ips_urlfilter_dns6 – Configure IPS URL filter IPv6 DNS servers in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.261.1 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

5.261.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.261.3 Parameters

5.261.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.261.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.261.6 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:

5.261.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.261.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.262 fortios_system_ipv6_neighbor_cache – Configure IPv6 neighbor cache table in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.262.1 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

5.262.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.262.3 Parameters

5.262.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.262.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    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>"
```

5.262.6 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:

5.262.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.262.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.263 fortios_system_ipv6_tunnel – Configure IPv6/IPv4 in IPv6 tunnel in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*

- *Status*
- *Authors*

5.263.1 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

5.263.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.263.3 Parameters

5.263.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.263.5 Examples

```
- hosts: fortigates
  collections:
    - 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/IPv4 in IPv6 tunnel.
    fortios_system_ipv6_tunnel:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_ipv6_tunnel:
        destination: "<your_own_value>"
        interface: "<your_own_value> (source system.interface.name)"
        name: "default_name_5"
        source: "<your_own_value>"
```

5.263.6 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:

5.263.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.263.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.264 fortios_system_link_monitor – Configure Link Health Monitor in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.264.1 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

5.264.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.264.3 Parameters

5.264.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.264.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        failtime: "4"
        gateway_ip: "<your_own_value>"
        gateway_ip6: "<your_own_value>"
        ha_priority: "7"
        http_get: "<your_own_value>"
        http_match: "<your_own_value>"
        interval: "10"
        name: "default_name_11"
        packet_size: "12"
        password: "<your_own_value>"
        port: "14"
        protocol: "ping"
        recoverytime: "16"
        security_mode: "none"
        server:
         -
            address: "<your_own_value>"
        source_ip: "84.230.14.43"
        source_ip6: "<your_own_value>"
        srcintf: "<your_own_value> (source system.interface.name)"
```

(continues on next page)

(continued from previous page)

```
        status: "enable"
        update_cascade_interface: "enable"
        update_static_route: "enable"
```

5.264.6 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:

5.264.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.264.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.265 fortios_system_lte_modem – Configure USB LTE/WIMAX devices in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.265.1 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

5.265.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.265.3 Parameters

5.265.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.265.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        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>"
```

5.265.6 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:

5.265.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.265.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.266 fortios_system_mac_address_table – Configure MAC address tables in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.266.1 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

5.266.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.266.3 Parameters

5.266.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.266.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.266.6 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:

5.266.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.266.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.267 fortios_system_management_tunnel – Management tunnel configuration in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.267.1 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

5.267.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.267.3 Parameters

5.267.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.267.5 Examples

```
- hosts: fortigates
  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"
```

5.267.6 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:

5.267.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.267.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.268 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 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.268.1 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

5.268.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.268.3 Parameters

5.268.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.268.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
```

(continues on next page)

(continued from previous page)

```
    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"
```

5.268.6 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:

5.268.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.268.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.269 fortios_system_modem – Configure MODEM in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.269.1 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

5.269.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.269.3 Parameters

5.269.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.269.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        priority: "40"
        redial: "none"
        reset: "42"
        status: "enable"
```

(continues on next page)

(continued from previous page)

```
        traffic_check: "enable"
        username1: "<your_own_value>"
        username2: "<your_own_value>"
        username3: "<your_own_value>"
        wireless_port: "48"
```

5.269.6 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:

5.269.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.269.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.270 fortios_system_nat64 – Configure NAT64 in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.270.1 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

5.270.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.270.3 Parameters

5.270.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.270.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        nat64_prefix: "<your_own_value>"
        secondary_prefix:
         -
            name: "default_name_7"
            nat64_prefix: "<your_own_value>"
        secondary_prefix_status: "enable"
        status: "enable"
```

5.270.6 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:

5.270.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.270.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.271 fortios_system_netflow – Configure NetFlow in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.271.1 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

5.271.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.271.3 Parameters

5.271.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.271.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.271.6 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:

5.271.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.271.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.272 fortios_system_network_visibility – Configure network visibility settings in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.272.1 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

5.272.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.272.3 Parameters

5.272.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.272.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.272.6 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:

5.272.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.272.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.273 fortios_system_ntp – Configure system NTP information in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.273.1 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

5.273.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.273.3 Parameters

5.273.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.273.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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:
       interface:
        -
           interface_name: "<your_own_value> (source system.interface.name)"
       ntpserver:
        -
           authentication: "enable"
           id:  "7"
           key: "<your_own_value>"
           key_id: "9"
           ntpv3: "enable"
           server: "192.168.100.40"
       ntpsync: "enable"
       server_mode: "enable"
       source_ip: "84.230.14.43"
       syncinterval: "15"
       type: "fortiguard"
```

5.273.6 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:

5.273.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.273.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.274 fortios_system_object_tagging – Configure object tagging in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.274.1 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

5.274.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.274.3 Parameters

5.274.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.274.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.274.6 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:

5.274.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.274.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.275 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 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.275.1 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

5.275.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.275.3 Parameters

5.275.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.275.5 Examples

```
- hosts: fortigates
  collections:
    - 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.
```

(continues on next page)

(continued from previous page)

```
    fortios_system_password_policy:
      vdom:  "{{ vdom }}"
      system_password_policy:
        apply_to: "admin-password"
        change_4_characters: "enable"
        expire_day: "5"
        expire_status: "enable"
        min_lower_case_letter: "7"
        min_non_alphanumeric: "8"
        min_number: "9"
        min_upper_case_letter: "10"
        minimum_length: "11"
        reuse_password: "enable"
        status: "enable"
```

5.275.6 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:

5.275.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.275.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.276 fortios_system_password_policy_guest_admin – Configure the password policy for guest administrators in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*

- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.276.1 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

5.276.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.276.3 Parameters

5.276.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.276.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
        expire_day: "5"
        expire_status: "enable"
        min_lower_case_letter: "7"
        min_non_alphanumeric: "8"
        min_number: "9"
        min_upper_case_letter: "10"
        minimum_length: "11"
        reuse_password: "enable"
        status: "enable"
```

5.276.6 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:

5.276.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.276.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.277 fortios_system_physical_switch – Configure physical switches in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*

- *Return Values*
- *Status*
- *Authors*

5.277.1 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

5.277.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.277.3 Parameters

5.277.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.277.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
            speed: "auto"
            status: "up"
```

5.277.6 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:

5.277.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.277.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.278 fortios_system_pppoe_interface – Configure the PPPoE interfaces in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.278.1 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

5.278.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.278.3 Parameters

5.278.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.278.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

(continues on next page)

(continued from previous page)

```
        pppoe_unnumbered_negotiate: "enable"
        service_name: "<your_own_value>"
        username: "<your_own_value>"
```

5.278.6 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:

5.278.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.278.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.279 fortios_system_probe_response – Configure system probe response in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.279.1 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

5.279.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.279.3 Parameters

5.279.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.279.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.279.6 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:

5.279.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.279.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.280 fortios_system_proxy_arp – Configure proxy-ARP in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.280.1 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

5.280.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.280.3 Parameters

5.280.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.280.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.280.6 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:

5.280.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.280.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.281 fortios_system_replacemsg_admin – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.281.1 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

5.281.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.281.3 Parameters

5.281.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.281.5 Examples

```
- hosts: fortigates
  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:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

5.281.6 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:

5.281.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.281.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.282 fortios_system_replacemsg_alertmail – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.282.1 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

5.282.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.282.3 Parameters

5.282.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.282.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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>"
```

5.282.6 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:

5.282.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.282.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.283 fortios_system_replacemsg_auth – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*

- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.283.1 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

5.283.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.283.3 Parameters

5.283.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.283.5 Examples

```
- hosts: fortigates
  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>"
```

(continues on next page)

(continued from previous page)

```
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

5.283.6 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:

5.283.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.283.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.284 fortios_system_replacemsg_device_detection_portal – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.284.1 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

5.284.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.284.3 Parameters

5.284.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.284.5 Examples

```
- hosts: fortigates
  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>"
```

5.284.6 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:

5.284.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.284.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.285 fortios_system_replacemsg_ec – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.285.1 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

5.285.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.285.3 Parameters

5.285.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.285.5 Examples

```
- hosts: fortigates
  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>"
```

5.285.6 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:

5.285.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.285.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.286 fortios_system_replacemsg_fortiguard_wf – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.286.1 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

5.286.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.286.3 Parameters

5.286.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.286.5 Examples

```
- hosts: fortigates
  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_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>"
```

5.286.6 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:

5.286.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.286.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.287 fortios_system_replacemsg_ftp – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.287.1 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

5.287.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.287.3 Parameters

5.287.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.287.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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>"
    system_replacemsg_ftp:
      buffer: "<your_own_value>"
      format: "none"
      header: "none"
      msg_type: "<your_own_value>"
```

5.287.6 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:

5.287.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.287.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.288 fortios_system_replacemsg_group – Configure replacement message groups in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*

- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.288.1 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

5.288.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.288.3 Parameters

5.288.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.288.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
        -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        alertmail:
        -
            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>"
        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>"
        nac_quar:
         -
            buffer: "<your_own_value>"
            format: "none"
            header: "none"
            msg_type: "<your_own_value>"
        name: "default_name_65"
        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"
            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>"
```

5.288.6 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:

5.288.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.288.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.289 fortios_system_replacemsg_http – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.289.1 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

5.289.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.289.3 Parameters

5.289.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.289.5 Examples

```
- hosts: fortigates
  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 }}"
      state: "present"
      access_token: "<your_own_value>"
      system_replacemsg_http:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

5.289.6 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:

5.289.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.289.8 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.290 fortios_system_replacemsg_icap – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.290.1 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

5.290.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.290.3 Parameters

5.290.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.290.5 Examples

```
- hosts: fortigates
  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>"
```

5.290.6 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:

5.290.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.290.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.291 fortios_system_replacemsg_image – Configure replacement message images in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.291.1 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

5.291.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.291.3 Parameters

5.291.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.291.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.291.6 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:

5.291.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.291.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.292 fortios_system_replacemsg_mail – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*

- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.292.1 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

5.292.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.292.3 Parameters

5.292.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.292.5 Examples

```
- hosts: fortigates
  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"
```

(continues on next page)

(continued from previous page)

```
        header: "none"
        msg_type: "<your_own_value>"
```

5.292.6 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:

5.292.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.292.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.293 fortios_system_replacemsg_nac_quar – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.293.1 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

5.293.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.293.3 Parameters

5.293.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.293.5 Examples

```
- hosts: fortigates
  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>"
```

5.293.6 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:

5.293.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.293.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.294 fortios_system_replacemsg_nntp – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.294.1 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

5.294.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.294.3 Parameters

5.294.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.294.5 Examples

```
- hosts: fortigates
  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_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>"
```

5.294.6 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:

5.294.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.294.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.295 fortios_system_replacemsg_spam – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.295.1 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

5.295.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.295.3 Parameters

5.295.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.295.5 Examples

```
- hosts: fortigates
  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>"
      system_replacemsg_spam:
        buffer: "<your_own_value>"
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

5.295.6 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:

5.295.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.295.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.296 fortios_system_replacemsg_sslvpn – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.296.1 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

5.296.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.296.3 Parameters

5.296.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.296.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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>"
```

5.296.6 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:

5.296.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.296.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.297 fortios_system_replacemsg_traffic_quota – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*

- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.297.1 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

5.297.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.297.3 Parameters

5.297.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.297.5 Examples

```
- hosts: fortigates
  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>"
```

(continues on next page)

(continued from previous page)

```
        format: "none"
        header: "none"
        msg_type: "<your_own_value>"
```

5.297.6 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:

5.297.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.297.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.298 fortios_system_replacemsg_utm – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.298.1 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

5.298.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.298.3 Parameters

5.298.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.298.5 Examples

```
- hosts: fortigates
  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>"
```

5.298.6 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:

5.298.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.298.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.299 fortios_system_replacemsg_webproxy – Replacement messages in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.299.1 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

5.299.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.299.3 Parameters

5.299.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.299.5 Examples

```
- hosts: fortigates
  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>"
```

5.299.6 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:

5.299.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.299.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.300 fortios_system_resource_limits – Configure resource limits in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.300.1 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

5.300.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.300.3 Parameters

5.300.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.300.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.300.6 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:

5.300.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.300.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.301 fortios_system_sdn_connector – Configure connection to SDN Connector in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.301.1 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

5.301.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.301.3 Parameters

5.301.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.301.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
        azure_region: "global"
        client_id: "<your_own_value>"
        client_secret: "<your_own_value>"
        external_ip:
         -
            name: "default_name_8"
        name: "default_name_9"
        nic:
         -
            ip:
             -
                name: "default_name_12"
                public_ip: "<your_own_value>"
            name: "default_name_14"
        password: "<your_own_value>"
        region: "<your_own_value>"
        resource_group: "<your_own_value>"
        route:
         -
            name: "default_name_19"
        route_table:
         -
            name: "default_name_21"
            route:
             -
                name: "default_name_23"
                next_hop: "<your_own_value>"
        secret_key: "<your_own_value>"
        server: "192.168.100.40"
        server_port: "27"
        status: "disable"
        subscription_id: "<your_own_value>"
        tenant_id: "<your_own_value>"
        type: "aci"
        update_interval: "32"
        username: "<your_own_value>"
        vpc_id: "<your_own_value>"
```

5.301.6 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:

5.301.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.301.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.302 fortios_system_session_helper – Configure session helper in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.302.1 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

5.302.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.302.3 Parameters

5.302.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.302.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.302.6 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:

5.302.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.302.8 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.303 fortios_system_session_ttl – Configure global session TTL timers for this FortiGate in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.303.1 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

5.303.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.303.3 Parameters

5.303.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.303.5 Examples

```
- hosts: fortigates
  collections:
    - 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 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>"
```

5.303.6 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:

5.303.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.303.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.304 fortios_system_settings – Configure VDOM settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.304.1 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

5.304.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.304.3 Parameters

5.304.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.304.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
 tasks:
 - name: Configure VDOM settings.
   fortios_system_settings:
     vdom:  "{{ vdom }}"
     system_settings:
       allow_subnet_overlap: "enable"
       asymroute: "enable"
       asymroute_icmp: "enable"
       asymroute6: "enable"
       asymroute6_icmp: "enable"
       bfd: "enable"
       bfd_desired_min_tx: "9"
       bfd_detect_mult: "10"
       bfd_dont_enforce_src_port: "enable"
       bfd_required_min_rx: "12"
       block_land_attack: "disable"
       central_nat: "enable"
       comments: "<your_own_value>"
       compliance_check: "enable"
       default_voip_alg_mode: "proxy-based"
       deny_tcp_with_icmp: "enable"
       device: "<your_own_value> (source system.interface.name)"
       dhcp_proxy: "enable"
       dhcp_server_ip: "<your_own_value>"
       dhcp6_server_ip: "<your_own_value>"
       discovered_device_timeout: "23"
       ecmp_max_paths: "24"
       email_portal_check_dns: "disable"
       firewall_session_dirty: "check-all"
       fw_session_hairpin: "enable"
       gateway: "<your_own_value>"
       gateway6: "<your_own_value>"
       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_36"
       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_fortiap_split_tunneling: "enable"
       gui_fortiextender_controller: "enable"
```

(continues on next page)

(continued from previous page)

```
        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_policy_based_ipsec: "enable"
        gui_policy_learning: "enable"
        gui_replacement_message_groups: "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_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"
        http_external_dest: "fortiweb"
        ike_dn_format: "with-space"
        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_transmission: "enable"
        mac_ttl: "89"
        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"
        sccp_port: "97"
        ses_denied_traffic: "enable"
        sip_helper: "enable"
        sip_nat_trace: "enable"
        sip_ssl_port: "101"
        sip_tcp_port: "102"
        sip_udp_port: "103"
        snat_hairpin_traffic: "enable"
        ssl_ssh_profile: "<your_own_value> (source firewall.ssl-ssh-profile.name)"
        status: "enable"
        strict_src_check: "enable"
```

(continues on next page)

(continued from previous page)

```
        tcp_session_without_syn: "enable"
        utf8_spam_tagging: "enable"
        v4_ecmp_mode: "source-ip-based"
        vpn_stats_log: "ipsec"
        vpn_stats_period: "112"
        wccp_cache_engine: "enable"
```

5.304.6 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:

5.304.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.304.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.305 fortios_system_sflow – Configure sFlow in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*

- *Authors*

5.305.1 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

5.305.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.305.3 Parameters

5.305.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.305.5 Examples

```
- hosts: fortigates
  collections:
    - 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.
    fortios_system_sflow:
      vdom:  "{{ vdom }}"
      system_sflow:
        collector_ip: "<your_own_value>"
        collector_port: "4"
        source_ip: "84.230.14.43"
```

5.305.6 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:

5.305.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.305.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.306 fortios_system_sit_tunnel – Configure IPv6 tunnel over IPv4 in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.306.1 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

5.306.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.306.3 Parameters

5.306.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.306.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        destination: "<your_own_value>"
        interface: "<your_own_value> (source system.interface.name)"
        ip6: "<your_own_value>"
        name: "default_name_6"
        source: "<your_own_value>"
```

5.306.6 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:

5.306.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.306.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.307 fortios_system_sms_server – Configure SMS server for sending SMS messages to support user authentication in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.307.1 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

5.307.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.307.3 Parameters

5.307.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.307.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.307.6 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:

5.307.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.307.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.308 fortios_system_snmp_community – SNMP community configuration in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.308.1 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

5.308.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.308.3 Parameters

5.308.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.308.5 Examples

```
- hosts: fortigates
  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:
```

(continues on next page)

(continued from previous page)

```
    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"
      trap_v1_lport: "23"
      trap_v1_rport: "24"
      trap_v1_status: "enable"
      trap_v2c_lport: "26"
      trap_v2c_rport: "27"
      trap_v2c_status: "enable"
```

5.308.6 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:

5.308.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.308.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.309 fortios_system_snmp_sysinfo – SNMP system info configuration in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.309.1 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

5.309.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.309.3 Parameters

5.309.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.309.5 Examples

```
- hosts: fortigates
  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"
```

5.309.6 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:

5.309.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.309.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.310 fortios_system_snmp_user – SNMP user configuration in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.310.1 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

5.310.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.310.3 Parameters

5.310.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.310.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.310.6 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:

5.310.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.310.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.311 fortios_system_storage – Configure logical storage in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.311.1 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

5.311.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.311.3 Parameters

5.311.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.311.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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: "mix"
      wanopt_mode: "mix"
```

5.311.6 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:

5.311.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.311.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.312 fortios_system_stp – Configure Spanning Tree Protocol (STP) in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.312.1 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

5.312.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.312.3 Parameters

5.312.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.312.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    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"
```

5.312.6 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:

5.312.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.312.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.313 fortios_system_switch_interface – Configure software switch interfaces by grouping physical and WiFi interfaces in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*

- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.313.1 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

5.313.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.313.3 Parameters

5.313.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.313.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        member:
```

(continues on next page)

(continued from previous page)

```
    -
      interface_name: "<your_own_value> (source system.interface.name)"
    name: "default_name_6"
    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)"
```

5.313.6 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:

5.313.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.313.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.314 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 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*

- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.314.1 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

5.314.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.314.3 Parameters

5.314.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.314.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
        priority: "low"
        tos: "5"
```

5.314.6 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:

5.314.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.314.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.315 fortios_system_vdom – Configure virtual domain in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.315.1 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

5.315.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.315.3 Parameters

5.315.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.315.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        name: "default_name_3"
        short_name: "<your_own_value>"
        temporary: "5"
        vcluster_id: "6"
```

5.315.6 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:

5.315.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.315.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.316 fortios_system_vdom_dns – Configure DNS servers for a non-management VDOM in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.316.1 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

5.316.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.316.3 Parameters

5.316.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.316.5 Examples

```
- hosts: fortigates
  collections:
    - 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 for a non-management VDOM.
    fortios_system_vdom_dns:
      vdom:  "{{ vdom }}"
      system_vdom_dns:
        ip6_primary: "<your_own_value>"
        ip6_secondary: "<your_own_value>"
        primary: "<your_own_value>"
        secondary: "<your_own_value>"
        source_ip: "84.230.14.43"
        vdom_dns: "enable"
```

5.316.6 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:

5.316.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.316.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.317 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 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.317.1 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

5.317.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.317.3 Parameters

5.317.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.317.5 Examples

```
- hosts: fortigates
  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)"
```

5.317.6 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:

5.317.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.317.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.318 fortios_system_vdom_link – Configure VDOM links in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.318.1 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

5.318.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.318.3 Parameters

5.318.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.318.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.318.6 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:

5.318.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.318.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.319 fortios_system_vdom_netflow – Configure NetFlow per VDOM in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*

- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.319.1 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

5.319.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.319.3 Parameters

5.319.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.319.5 Examples

```
- hosts: fortigates
  collections:
    - 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 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"
```

5.319.6 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:

5.319.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.319.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.320 fortios_system_vdom_property – Configure VDOM property in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.320.1 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

5.320.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.320.3 Parameters

5.320.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.320.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        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>"
```

5.320.6 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:

5.320.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.320.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.321 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 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.321.1 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

5.321.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.321.3 Parameters

5.321.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.321.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.321.6 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:

5.321.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.321.8 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.322 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 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.322.1 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

5.322.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.322.3 Parameters

5.322.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.322.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.322.6 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:

5.322.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.322.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.323 fortios_system_virtual_switch – Configure virtual hardware switch interfaces in Fortinet's FortiOS and FortiGate.

New in version 2.10.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.323.1 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

5.323.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.323.3 Parameters

5.323.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.323.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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>"
           name: "default_name_7"
           speed: "auto"
           status: "up"
       span: "disable"
       span_dest_port: "<your_own_value>"
       span_direction: "rx"
       span_source_port: "<your_own_value>"
```

5.323.6 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:

5.323.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.323.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.324 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 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.324.1 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

5.324.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.324.3 Parameters

5.324.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.324.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
```

(continues on next page)

(continued from previous page)

```
  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"
           failtime: "8"
           http_get: "<your_own_value>"
           http_match: "<your_own_value>"
           interval: "11"
           members:
            -
               seq_num: "13 (source system.virtual-wan-link.members.seq-num)"
           name: "default_name_14"
           packet_size: "15"
           password: "<your_own_value>"
           port: "17"
           protocol: "ping"
           recoverytime: "19"
           security_mode: "none"
           server: "192.168.100.40"
           sla:
            -
               id:  "23"
               jitter_threshold: "24"
               latency_threshold: "25"
               link_cost_factor: "latency"
               packetloss_threshold: "27"
           threshold_alert_jitter: "28"
           threshold_alert_latency: "29"
           threshold_alert_packetloss: "30"
           threshold_warning_jitter: "31"
           threshold_warning_latency: "32"
           threshold_warning_packetloss: "33"
           update_cascade_interface: "enable"
           update_static_route: "enable"
       load_balance_mode: "source-ip-based"
       members:
        -
           gateway: "<your_own_value>"
           gateway6: "<your_own_value>"
           ingress_spillover_threshold: "40"
           interface: "<your_own_value> (source system.interface.name)"
           priority: "42"
           seq_num: "43"
           source: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
            source6: "<your_own_value>"
            spillover_threshold: "46"
            status: "disable"
            volume_ratio: "48"
            weight: "49"
        service:
         -
            addr_mode: "ipv4"
            bandwidth_weight: "52"
            dscp_forward: "enable"
            dscp_forward_tag: "<your_own_value>"
            dscp_reverse: "enable"
            dscp_reverse_tag: "<your_own_value>"
            dst:
             -
                name: "default_name_58 (source firewall.address.name firewall.addrgrp.
↪name)"
            dst_negate: "enable"
            dst6:
             -
                name: "default_name_61 (source firewall.address6.name firewall.
↪addrgrp6.name)"
            end_port: "62"
            groups:
             -
                name: "default_name_64 (source user.group.name)"
            health_check: "<your_own_value> (source system.virtual-wan-link.health-
↪check.name)"
            id:  "66"
            input_device:
             -
                name: "default_name_68 (source system.interface.name)"
            internet_service: "enable"
            internet_service_ctrl:
             -
                id:  "71"
            internet_service_ctrl_group:
             -
                name: "default_name_73 (source application.group.name)"
            internet_service_custom:
             -
                name: "default_name_75 (source firewall.internet-service-custom.name)"
            internet_service_custom_group:
             -
                name: "default_name_77 (source firewall.internet-service-custom-group.
↪name)"
            internet_service_group:
             -
                name: "default_name_79 (source firewall.internet-service-group.name)"
            internet_service_id:
             -
                id:  "81 (source firewall.internet-service.id)"
            jitter_weight: "82"
            latency_weight: "83"
            link_cost_factor: "latency"
            link_cost_threshold: "85"
            member: "86"
```

(continues on next page)

(continued from previous page)

```
            mode: "auto"
            name: "default_name_88"
            packet_loss_weight: "89"
            priority_members:
             -
                seq_num: "91 (source system.virtual-wan-link.members.seq-num)"
            protocol: "92"
            quality_link: "93"
            route_tag: "94"
            sla:
             -
                health_check: "<your_own_value> (source system.virtual-wan-link.
↪health-check.name)"
                id:  "97"
            src:
             -
                name: "default_name_99 (source firewall.address.name firewall.addrgrp.
↪name)"
            src_negate: "enable"
            src6:
             -
                name: "default_name_102 (source firewall.address6.name firewall.
↪addrgrp6.name)"
            start_port: "103"
            status: "enable"
            tos: "<your_own_value>"
            tos_mask: "<your_own_value>"
            users:
             -
                name: "default_name_108 (source user.local.name)"
        status: "disable"
```

5.324.6 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:

5.324.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.324.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.325 fortios_system_virtual_wire_pair – Configure virtual wire pairs in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.325.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and virtual_wire_pair category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.325.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.325.3 Parameters

5.325.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.325.5 Examples

```
- hosts: fortigates
  collections:
    - 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 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"
```

5.325.6 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:

5.325.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.325.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.326 fortios_system_vmlicense – Update VM license using uploaded file. Reboots immediately if successful in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.326.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and vmlicense category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.5

5.326.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.326.3 Parameters

5.326.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.326.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
```

(continues on next page)

(continued from previous page)

```
  vdom: "root"
  ansible_httpapi_use_ssl: no
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 80
  license_file: ./FGVMXXXXXX-VM00.lic
  license_file_content: "{{ lookup( 'file', license_file) }}"
  encoded_license: "{{ license_file_content | string | b64encode }}"
tasks:
- name: Update VM license using uploaded file. Reboots immediately if successful.
  fortios_system_vmlicense:
    vdom:  "{{ vdom }}"
    system_vmlicense:
      file_content: "{{ encoded_license }}"
```

5.326.6 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:

5.326.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.326.8 Authors

- Frank Shen(@frankshen01)
- Link Zheng (@chillancezen)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.327 fortios_system_vxlan – Configure VXLAN devices in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*

- *Return Values*
- *Status*
- *Authors*

5.327.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and vxlan category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.327.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.327.3 Parameters

5.327.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.327.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        name: "default_name_7"
        remote_ip:
```

(continues on next page)

(continued from previous page)

```
        -
            ip: "<your_own_value>"
        remote_ip6:
        -
            ip6: "<your_own_value>"
        vni: "12"
```

5.327.6 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:

5.327.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.327.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.328 fortios_system_wccp – Configure WCCP in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*

- *Authors*

5.328.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and wccp category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.328.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.328.3 Parameters

5.328.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.328.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
        assignment_weight: "7"
        authentication: "enable"
        cache_engine_method: "GRE"
        cache_id: "<your_own_value>"
        forward_method: "GRE"
```

(continues on next page)

(continued from previous page)

```
        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>"
        service_id: "<your_own_value>"
        service_type: "auto"
```

5.328.6 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:

5.328.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.328.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.329 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 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.329.1 Synopsis

- This module is able to configure a FortiGate or FortiOS (FOS) device by allowing the user to set and modify system feature and zone category. Examples include all parameters and values need to be adjusted to datasources before usage. Tested with FOS v6.0.0

5.329.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.329.3 Parameters

5.329.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.329.5 Examples

```
- hosts: fortigates
  collections:
    - 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.
```

(continues on next page)

(continued from previous page)

```
    fortios_system_zone:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      system_zone:
        interface:
         -
            interface_name: "<your_own_value> (source system.interface.name)"
        intrazone: "allow"
        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)"
```

5.329.6 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:

5.329.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.329.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.330 fortios_user_adgrp – Configure FSSO groups in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.330.1 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

5.330.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.330.3 Parameters

5.330.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.330.5 Examples

```
- hosts: fortigates
  collections:
    - 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 }}"
```

(continues on next page)

(continued from previous page)

```
    state: "present"
    access_token: "<your_own_value>"
    user_adgrp:
      name: "default_name_3"
      server_name: "<your_own_value> (source user.fsso.name)"
```

5.330.6 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:

5.330.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.330.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.331 fortios_user_device – Configure devices in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.331.1 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

5.331.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.331.3 Parameters

5.331.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.331.5 Examples

```
- hosts: fortigates
  collections:
    - 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)"
```

(continues on next page)

(continued from previous page)

```
        type: "unknown"
        user: "<your_own_value>"
```

5.331.6 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:

5.331.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.331.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.332 fortios_user_device_access_list – Configure device access control lists in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.332.1 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

5.332.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.332.3 Parameters

5.332.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.332.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.332.6 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:

5.332.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.332.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.333 fortios_user_device_category – Configure device categories in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.333.1 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

5.333.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.333.3 Parameters

5.333.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.333.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.333.6 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:

5.333.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.333.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.334 fortios_user_device_group – Configure device groups in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.334.1 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

5.334.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.334.3 Parameters

5.334.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.334.5 Examples

```
- hosts: fortigates
  collections:
    - 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 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)"
```

5.334.6 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:

5.334.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.334.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.335 fortios_user_domain_controller – Configure domain controller entries in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.335.1 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

5.335.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.335.3 Parameters

5.335.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.335.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        domain_name: "<your_own_value>"
        ip_address: "<your_own_value>"
        ldap_server: "<your_own_value> (source user.ldap.name)"
        name: "default_name_6"
        port: "7"
```

5.335.6 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:

5.335.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.335.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.336 fortios_user_fortitoken – Configure FortiToken in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.336.1 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

5.336.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.336.3 Parameters

5.336.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.336.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.336.6 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:

5.336.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.336.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.337 fortios_user_fsso – Configure Fortinet Single Sign On (FSSO) agents in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.337.1 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

5.337.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.337.3 Parameters

5.337.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.337.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    vdom:  "{{ vdom }}"
    state: "present"
    access_token: "<your_own_value>"
    user_fsso:
      ldap_server: "<your_own_value> (source user.ldap.name)"
      name: "default_name_4"
      password: "<your_own_value>"
      password2: "<your_own_value>"
      password3: "<your_own_value>"
      password4: "<your_own_value>"
      password5: "<your_own_value>"
      port: "10"
      port2: "11"
      port3: "12"
      port4: "13"
      port5: "14"
      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>"
```

5.337.6 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:

5.337.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.337.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.338 fortios_user_fsso_polling – Configure FSSO active directory servers for polling mode in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.338.1 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

5.338.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.338.3 Parameters

5.338.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.338.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       password: "<your_own_value>"
       polling_frequency: "10"
       port: "11"
       server: "192.168.100.40"
       status: "enable"
       user: "<your_own_value>"
```

5.338.6 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:

5.338.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.338.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.339 fortios_user_group – Configure user groups in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.339.1 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

5.339.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.339.3 Parameters

5.339.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.339.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       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>"
           mobile_phone: "<your_own_value>"
           name: "default_name_17"
           password: "<your_own_value>"
           sponsor: "<your_own_value>"
           user_id: "<your_own_value>"
       http_digest_realm: "<your_own_value>"
       id:  "22"
       match:
        -
           group_name: "<your_own_value>"
           id:  "25"
           server_name: "<your_own_value> (source user.radius.name user.ldap.name␣
↪user.tacacs+.name)"
       max_accounts: "27"
       member:
        -
           name: "default_name_29 (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_32"
       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"
```

5.339.6 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:

5.339.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.339.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.340 fortios_user_krb_keytab – Configure Kerberos keytab entries in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.340.1 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

5.340.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.340.3 Parameters

5.340.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.340.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        principal: "<your_own_value>"
```

5.340.6 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:

5.340.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.340.8 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.341 fortios_user_ldap – Configure LDAP server entries in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.341.1 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

5.341.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.341.3 Parameters

5.341.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.341.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        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>"
        member_attr: "<your_own_value>"
        name: "default_name_13"
        password: "<your_own_value>"
        password_expiry_warning: "enable"
        password_renewal: "enable"
        port: "17"
        secondary_server: "<your_own_value>"
        secure: "disable"
        server: "192.168.100.40"
        source_ip: "84.230.14.43"
        tertiary_server: "<your_own_value>"
        type: "simple"
        username: "<your_own_value>"
```

5.341.6 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:

5.341.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.341.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.342 fortios_user_local – Configure local users in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.342.1 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

5.342.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.342.3 Parameters

5.342.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.342.5 Examples

```
- hosts: fortigates
  collections:
    - 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_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)"
        two_factor: "disable"
        type: "password"
        workstation: "<your_own_value>"
```

5.342.6 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:

5.342.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.342.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.343 fortios_user_password_policy – Configure user password policy in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.343.1 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

5.343.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.343.3 Parameters

5.343.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.343.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        name: "default_name_4"
        warn_days: "5"
```

5.343.6 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:

5.343.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.343.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.344 fortios_user_peer – Configure peer users in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.344.1 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

5.344.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.344.3 Parameters

5.344.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.344.5 Examples

```
- hosts: fortigates
  collections:
    - 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 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"
```

5.344.6 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:

5.344.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.344.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.345 fortios_user_peergrp – Configure peer groups in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.345.1 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

5.345.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.345.3 Parameters

5.345.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.345.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.345.6 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:

5.345.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.345.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.346 fortios_user_pop3 – POP3 server entry configuration in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.346.1 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

5.346.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.346.3 Parameters

5.346.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.346.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  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"
```

5.346.6 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:

5.346.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.346.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.347 fortios_user_quarantine – Configure quarantine support in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*

- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.347.1 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

5.347.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.347.3 Parameters

5.347.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.347.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        quarantine: "enable"
        targets:
         -
```

(continues on next page)

(continued from previous page)

```
            description: "<your_own_value>"
            entry_id: "6"
            mac: "<your_own_value>"
            tag:
             -
                tags: "<your_own_value>"
```

5.347.6 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:

5.347.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.347.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.348 fortios_user_radius – Configure RADIUS server entries in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*

- *Authors*

5.348.1 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

5.348.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.348.3 Parameters

5.348.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.348.5 Examples

```
- hosts: fortigates
  collections:
    - 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 }}"
      state: "present"
      access_token: "<your_own_value>"
      user_radius:
        accounting_server:
         -
            id:  "4"
            port: "5"
            secret: "<your_own_value>"
            server: "192.168.100.40"
            source_ip: "84.230.14.43"
            status: "enable"
        acct_all_servers: "enable"
```

(continues on next page)

(continued from previous page)

```
        acct_interim_interval: "11"
        all_usergroup: "disable"
        auth_type: "auto"
        class:
         -
            name: "default_name_15"
        h3c_compatibility: "enable"
        name: "default_name_17"
        nas_ip: "<your_own_value>"
        password_encoding: "auto"
        password_renewal: "enable"
        radius_coa: "enable"
        radius_port: "22"
        rsso: "enable"
        rsso_context_timeout: "24"
        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: "30"
        rsso_radius_response: "enable"
        rsso_radius_server_port: "32"
        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"
        tertiary_secret: "<your_own_value>"
        tertiary_server: "<your_own_value>"
        timeout: "45"
        use_management_vdom: "enable"
        username_case_sensitive: "enable"
```

5.348.6 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:

5.348.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.348.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.349 fortios_user_security_exempt_list – Configure security exemption list in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.349.1 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

5.349.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.349.3 Parameters

5.349.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.349.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
             -
                name: "default_name_14 (source firewall.address.name firewall.addrgrp.
↪name)"
```

5.349.6 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:

5.349.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.349.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.350 fortios_user_setting – Configure user authentication setting in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.350.1 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

5.350.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.350.3 Parameters

5.350.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.350.5 Examples

```
- hosts: fortigates
  collections:
    - 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_portal_timeout: "10"
        auth_ports:
         -
            id:  "12"
            port: "13"
            type: "http"
        auth_secure_http: "enable"
        auth_ssl_allow_renegotiation: "enable"
        auth_timeout: "17"
        auth_timeout_type: "idle-timeout"
        auth_type: "http"
        radius_ses_timeout_act: "hard-timeout"
```

5.350.6 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:

5.350.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.350.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.351 fortios_user_tacacsplus – Configure TACACS+ server entries in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.351.1 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

5.351.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.351.3 Parameters

5.351.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.351.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        authen_type: "mschap"
        authorization: "enable"
        key: "<your_own_value>"
        name: "default_name_6"
        port: "7"
        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>"
```

5.351.6 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:

5.351.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.351.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.352 fortios_voip_profile – Configure VoIP profiles in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.352.1 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

5.352.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.352.3 Parameters

5.352.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.352.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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:
       comment: "Comment."
       name: "default_name_4"
       sccp:
           block_mcast: "disable"
           log_call_summary: "disable"
           log_violations: "disable"
           max_calls: "9"
           status: "disable"
           verify_header: "disable"
       sip:
           ack_rate: "13"
           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: "31"
           call_keepalive: "32"
           cancel_rate: "33"
           contact_fixup: "disable"
           hnt_restrict_source_ip: "disable"
           hosted_nat_traversal: "disable"
           info_rate: "37"
           invite_rate: "38"
           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"
```

(continues on next page)

(continued from previous page)

```
            malformed_header_max_forwards: "discard"
            malformed_header_p_asserted_identity: "discard"
            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: "71"
            max_dialogs: "72"
            max_idle_dialogs: "73"
            max_line_length: "74"
            message_rate: "75"
            nat_trace: "disable"
            no_sdp_fixup: "disable"
            notify_rate: "78"
            open_contact_pinhole: "disable"
            open_record_route_pinhole: "disable"
            open_register_pinhole: "disable"
            open_via_pinhole: "disable"
            options_rate: "83"
            prack_rate: "84"
            preserve_override: "disable"
            provisional_invite_expiry_time: "86"
            publish_rate: "87"
            refer_rate: "88"
            register_contact_trace: "disable"
            register_rate: "90"
            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"
            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)"
```

(continues on next page)

(continued from previous page)

```
            status: "disable"
            strict_register: "disable"
            subscribe_rate: "106"
            unknown_header: "discard"
            update_rate: "108"
```

5.352.6 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:

5.352.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.352.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.353 fortios_vpn_certificate_ca – CA certificate in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.353.1 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

5.353.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.353.3 Parameters

5.353.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.353.5 Examples

```
- hosts: fortigates
  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 }}"
      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"
        trusted: "enable"
```

5.353.6 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:

5.353.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.353.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.354 fortios_vpn_certificate_crl – Certificate Revocation List as a PEM file in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.354.1 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

5.354.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.354.3 Parameters

5.354.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.354.5 Examples

```
- hosts: fortigates
  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 }}"
      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)"
```

5.354.6 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:

5.354.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.354.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.355 fortios_vpn_certificate_local – Local keys and certificates in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.355.1 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

5.355.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.355.3 Parameters

5.355.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.355.5 Examples

```
- hosts: fortigates
  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_vpn_certificate_local:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      vpn_certificate_local:
        auto_regenerate_days: "3"
        auto_regenerate_days_warning: "4"
        ca_identifier:  "myId_5"
        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: "16"
        name: "default_name_17"
        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>"
```

5.355.6 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:

5.355.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.355.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.356 fortios_vpn_certificate_ocsp_server – OCSP server configuration in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.356.1 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

5.356.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.356.3 Parameters

5.356.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.356.5 Examples

```
- hosts: fortigates
  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"
```

5.356.6 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:

5.356.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.356.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.357 fortios_vpn_certificate_remote – Remote certificate as a PEM file in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.357.1 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

5.357.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.357.3 Parameters

5.357.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.357.5 Examples

```
- hosts: fortigates
  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"
```

5.357.6 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:

5.357.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.357.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.358 fortios_vpn_certificate_setting – VPN certificate setting in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.358.1 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

5.358.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.358.3 Parameters

5.358.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.358.5 Examples

```
- hosts: fortigates
  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_rsa1024: "<your_own_value> (source vpn.certificate.local.name)"
        certname_rsa2048: "<your_own_value> (source vpn.certificate.local.name)"
        check_ca_cert: "enable"
        check_ca_chain: "enable"
        cmp_save_extra_certs: "enable"
        cn_match: "substring"
        ocsp_default_server: "<your_own_value> (source vpn.certificate.ocsp-server.
↪name)"
        ocsp_status: "enable"
        ssl_ocsp_option: "certificate"
        ssl_ocsp_status: "enable"
        strict_crl_check: "enable"
        strict_ocsp_check: "enable"
        subject_match: "substring"
```

5.358.6 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:

5.358.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.358.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.359 fortios_vpn_ipsec_concentrator – Concentrator configuration in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.359.1 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

5.359.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.359.3 Parameters

5.359.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.359.5 Examples

```
- hosts: fortigates
  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"
```

5.359.6 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:

5.359.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.359.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.360 fortios_vpn_ipsec_forticlient – Configure FortiClient policy realm in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.360.1 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

5.360.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.360.3 Parameters

5.360.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.360.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
    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)"
```

5.360.6 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:

5.360.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.360.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.361 fortios_vpn_ipsec_manualkey – Configure IPsec manual keys in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*

- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.361.1 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

5.361.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.361.3 Parameters

5.361.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.361.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   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:
```

(continues on next page)

(continued from previous page)

```
        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>"
```

5.361.6 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:

5.361.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.361.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.362 fortios_vpn_ipsec_manualkey_interface – Configure IPsec manual keys in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*

- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.362.1 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

5.362.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.362.3 Parameters

5.362.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.362.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   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"
```

(continues on next page)

(continued from previous page)

```
        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>"
```

5.362.6 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:

5.362.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.362.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.363 fortios_vpn_ipsec_phase1 – Configure VPN remote gateway in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*

- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.363.1 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

5.363.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.363.3 Parameters

5.363.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.363.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

(continues on next page)

(continued from previous page)

```
        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"
        autoconfig: "disable"
        backup_gateway:
         -
            address: "<your_own_value>"
        banner: "<your_own_value>"
        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>"
        dhgrp: "1"
        digital_signature_auth: "enable"
        distance: "26"
        dns_mode: "manual"
        domain: "<your_own_value>"
        dpd: "disable"
        dpd_retrycount: "30"
        dpd_retryinterval: "<your_own_value>"
        eap: "enable"
        eap_identity: "use-id-payload"
        enforce_unique_id: "disable"
        forticlient_enforcement: "enable"
        fragmentation: "enable"
        fragmentation_mtu: "37"
        group_authentication: "enable"
        group_authentication_secret: "<your_own_value>"
        ha_sync_esp_seqno: "enable"
        idle_timeout: "enable"
        idle_timeoutinterval: "42"
        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:  "52"
            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:  "67"
            start_ip: "<your_own_value>"
        ipv6_name: "<your_own_value> (source firewall.address6.name firewall.addrgrp6.
↪name)"
        ipv6_prefix: "70"
        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: "74"
        keylife: "75"
        local_gw: "<your_own_value>"
        localid: "<your_own_value>"
        localid_type: "auto"
        mesh_selector_type: "disable"
        mode: "aggressive"
        mode_cfg: "disable"
        name: "default_name_82"
        nattraversal: "enable"
        negotiate_timeout: "84"
        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: "93"
        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)"
```

(continues on next page)

(continued from previous page)

```
        wizard_type: "custom"
        xauthtype: "disable"
```

5.363.6 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:

5.363.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.363.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.364 fortios_vpn_ipsec_phase1_interface – Configure VPN remote gateway in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.364.1 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

5.364.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.364.3 Parameters

5.364.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.364.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        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"
```

(continues on next page)

(continued from previous page)

```
        auto_discovery_sender: "enable"
        auto_negotiate: "enable"
        backup_gateway:
         -
            address: "<your_own_value>"
        banner: "<your_own_value>"
        certificate:
         -
            name: "default_name_22 (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: "28"
        dhgrp: "1"
        digital_signature_auth: "enable"
        distance: "31"
        dns_mode: "manual"
        domain: "<your_own_value>"
        dpd: "disable"
        dpd_retrycount: "35"
        dpd_retryinterval: "<your_own_value>"
        eap: "enable"
        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"
        exchange_interface_ip: "enable"
        forticlient_enforcement: "enable"
        fragmentation: "enable"
        fragmentation_mtu: "49"
        group_authentication: "enable"
        group_authentication_secret: "<your_own_value>"
        ha_sync_esp_seqno: "enable"
        idle_timeout: "enable"
        idle_timeoutinterval: "54"
        ike_version: "1"
        include_local_lan: "disable"
        interface: "<your_own_value> (source system.interface.name)"
        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:  "65"
            start_ip: "<your_own_value>"
        ipv4_name: "<your_own_value> (source firewall.address.name firewall.addrgrp.
↪name)"
        ipv4_netmask: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
        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:  "80"
            start_ip: "<your_own_value>"
        ipv6_name: "<your_own_value> (source firewall.address6.name firewall.addrgrp6.
↪name)"
        ipv6_prefix: "83"
        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: "87"
        keylife: "88"
        local_gw: "<your_own_value>"
        local_gw6: "<your_own_value>"
        localid: "<your_own_value>"
        localid_type: "auto"
        mesh_selector_type: "disable"
        mode: "aggressive"
        mode_cfg: "disable"
        monitor: "<your_own_value> (source vpn.ipsec.phase1-interface.name)"
        monitor_hold_down_delay: "97"
        monitor_hold_down_time: "<your_own_value>"
        monitor_hold_down_type: "immediate"
        monitor_hold_down_weekday: "everyday"
        name: "default_name_101"
        nattraversal: "enable"
        negotiate_timeout: "103"
        net_device: "enable"
        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: "114"
        proposal: "des-md5"
        psksecret: "<your_own_value>"
        psksecret_remote: "<your_own_value>"
        reauth: "disable"
        rekey: "enable"
```

(continues on next page)

(continued from previous page)

```
        remote_gw: "<your_own_value>"
        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: "133"
        wizard_type: "custom"
        xauthtype: "disable"
```

5.364.6 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:

5.364.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.364.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.365 fortios_vpn_ipsec_phase2 – Configure VPN autokey tunnel in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.365.1 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

5.365.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.365.3 Parameters

5.365.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.365.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
      vdom:  "{{ vdom }}"
```

(continues on next page)

(continued from previous page)

```
      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"
        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: "13"
        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"
        keepalive: "enable"
        keylife_type: "seconds"
        keylifekbs: "21"
        keylifeseconds: "22"
        l2tp: "enable"
        name: "default_name_24"
        pfs: "enable"
        phase1name: "<your_own_value> (source vpn.ipsec.phase1.name)"
        proposal: "null-md5"
        protocol: "28"
        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: "38"
        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"
```

5.365.6 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:

5.365.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.365.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.366 fortios_vpn_ipsec_phase2_interface – Configure VPN autokey tunnel in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.366.1 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

5.366.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.366.3 Parameters

5.366.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.366.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        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"
        keepalive: "enable"
        keylife_type: "seconds"
        keylifekbs: "23"
        keylifeseconds: "24"
        l2tp: "enable"
        name: "default_name_26"
        pfs: "enable"
        phase1name: "<your_own_value> (source vpn.ipsec.phase1-interface.name)"
```

(continues on next page)

(continued from previous page)

```
        proposal: "null-md5"
        protocol: "30"
        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: "39"
        src_start_ip: "<your_own_value>"
        src_start_ip6: "<your_own_value>"
        src_subnet: "<your_own_value>"
        src_subnet6: "<your_own_value>"
```

5.366.6 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:

5.366.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.366.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.367 fortios_vpn_l2tp – Configure L2TP in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.367.1 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

5.367.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.367.3 Parameters

5.367.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.367.5 Examples

```
- hosts: fortigates
  collections:
    - 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 }}"
```

(continues on next page)

(continued from previous page)

```
    vpn_l2tp:
      eip: "<your_own_value>"
      enforce_ipsec: "enable"
      sip: "<your_own_value>"
      status: "enable"
      usrgrp: "<your_own_value> (source user.group.name)"
```

5.367.6 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:

5.367.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.367.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.368 fortios_vpn_ocvpn – Configure One-Click VPN settings in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*

- *Authors*

5.368.1 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

5.368.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.368.3 Parameters

5.368.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.368.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   ansible_httpapi_port: 443
  tasks:
  - name: Configure One-Click VPN settings.
    fortios_vpn_ocvpn:
      vdom:  "{{ vdom }}"
      vpn_ocvpn:
        poll_interval: "3"
        status: "enable"
        subnets:
         -
            id:  "6"
            subnet: "<your_own_value>"
```

5.368.6 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:

5.368.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.368.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.369 fortios_vpn_pptp – Configure PPTP in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.369.1 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

5.369.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.369.3 Parameters

5.369.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.369.5 Examples

```
- hosts: fortigates
  collections:
    - 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)"
```

5.369.6 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:

5.369.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.369.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.370 fortios_vpn_ssl_settings – Configure SSL VPN in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.370.1 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

5.370.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.370.3 Parameters

5.370.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.370.5 Examples

```
- hosts: fortigates
  collections:
    - 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_timeout: "4"
        authentication_rule:
         -
            auth: "any"
            cipher: "any"
            client_cert: "enable"
            groups:
             -
                name: "default_name_10 (source user.group.name)"
            id:  "11"
            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_15 (source firewall.address.name firewall.addrgrp.
↪name)"
            source_address_negate: "enable"
            source_address6:
             -
                name: "default_name_18 (source firewall.address6.name firewall.
↪addrgrp6.name)"
            source_address6_negate: "enable"
            source_interface:
             -
                name: "default_name_21 (source system.interface.name system.zone.name)
↪"
            users:
             -
                name: "default_name_23 (source user.local.name)"
        auto_tunnel_static_route: "enable"
        banned_cipher: "RSA"
        check_referer: "enable"
        default_portal: "<your_own_value> (source vpn.ssl.web.portal.name)"
        deflate_compression_level: "28"
        deflate_min_data_size: "29"
        dns_server1: "<your_own_value>"
        dns_server2: "<your_own_value>"
        dns_suffix: "<your_own_value>"
        dtls_hello_timeout: "33"
        dtls_tunnel: "enable"
```

(continues on next page)

(continued from previous page)

```
        force_two_factor_auth: "enable"
        header_x_forwarded_for: "pass"
        http_compression: "enable"
        http_only_cookie: "enable"
        http_request_body_timeout: "39"
        http_request_header_timeout: "40"
        https_redirect: "enable"
        idle_timeout: "42"
        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: "47"
        login_block_time: "48"
        login_timeout: "49"
        port: "50"
        port_precedence: "enable"
        reqclientcert: "enable"
        route_source_interface: "enable"
        servercert: "<your_own_value> (source vpn.certificate.local.name)"
        source_address:
         -
            name: "default_name_56 (source firewall.address.name firewall.addrgrp.
↪name)"
        source_address_negate: "enable"
        source_address6:
         -
            name: "default_name_59 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        source_address6_negate: "enable"
        source_interface:
         -
            name: "default_name_62 (source system.interface.name system.zone.name)"
        ssl_big_buffer: "enable"
        ssl_client_renegotiation: "disable"
        ssl_insert_empty_fragment: "enable"
        sslv3: "enable"
        tlsv1_0: "enable"
        tlsv1_1: "enable"
        tlsv1_2: "enable"
        tunnel_ip_pools:
         -
            name: "default_name_71 (source firewall.address.name firewall.addrgrp.
↪name)"
        tunnel_ipv6_pools:
         -
            name: "default_name_73 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        unsafe_legacy_renegotiation: "enable"
        url_obscuration: "enable"
        wins_server1: "<your_own_value>"
        wins_server2: "<your_own_value>"
        x_content_type_options: "enable"
```

5.370.6 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:

5.370.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.370.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.371 fortios_vpn_ssl_web_host_check_software – SSL-VPN host check software in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.371.1 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

5.371.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.371.3 Parameters

5.371.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.371.5 Examples

```
- hosts: fortigates
  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>"
```

5.371.6 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:

5.371.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.371.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.372 fortios_vpn_ssl_web_portal – Portal in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.372.1 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

5.372.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.372.3 Parameters

5.372.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.372.5 Examples

```
- hosts: fortigates
  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>"
                folder: "<your_own_value>"
                form_data:
                 -
                    name: "default_name_12"
                    value: "<your_own_value>"
                host: "<your_own_value>"
                listening_port: "15"
                logon_password: "<your_own_value>"
                logon_user: "<your_own_value>"
                name: "default_name_18"
                port: "19"
                remote_port: "20"
                security: "rdp"
                server_layout: "en-us-qwerty"
                show_status_window: "enable"
                sso: "disable"
                sso_credential: "sslvpn-login"
                sso_credential_sent_once: "enable"
                sso_password: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
                sso_username: "<your_own_value>"
                url: "myurl.com"
            name: "default_name_30"
        custom_lang: "<your_own_value> (source system.custom-language.name)"
        customize_forticlient_download_url: "enable"
        display_bookmark: "enable"
        display_connection_tools: "enable"
        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>"
        host_check: "none"
        host_check_interval: "45"
        host_check_policy:
         -
            name: "default_name_47 (source vpn.ssl.web.host-check-software.name)"
        ip_mode: "range"
        ip_pools:
         -
            name: "default_name_50 (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_55 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        ipv6_service_restriction: "enable"
        ipv6_split_tunneling: "enable"
        ipv6_split_tunneling_routing_address:
         -
            name: "default_name_59 (source firewall.address6.name firewall.addrgrp6.
↪name)"
        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: "70"
            name: "default_name_71"
        macos_forticlient_download_url: "<your_own_value>"
        name: "default_name_73"
        os_check: "enable"
        os_check_list:
```

(continues on next page)

(continued from previous page)

```
        -
            action: "deny"
            latest_patch_level: "<your_own_value>"
            name: "default_name_78"
            tolerance: "79"
        redir_url: "<your_own_value>"
        save_password: "enable"
        service_restriction: "enable"
        skip_check_for_unsupported_browser: "enable"
        skip_check_for_unsupported_os: "enable"
        smb_ntlmv1_auth: "enable"
        split_dns:
        -
            dns_server1: "<your_own_value>"
            dns_server2: "<your_own_value>"
            domains: "<your_own_value>"
            id:  "90"
            ipv6_dns_server1: "<your_own_value>"
            ipv6_dns_server2: "<your_own_value>"
        split_tunneling: "enable"
        split_tunneling_routing_address:
        -
            name: "default_name_95 (source firewall.address.name firewall.addrgrp.
↪name)"
        theme: "blue"
        tunnel_mode: "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>"
```

5.372.6 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:

5.372.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.372.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.373 fortios_vpn_ssl_web_realm – Realm in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.373.1 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

5.373.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.373.3 Parameters

5.373.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.373.5 Examples

```
- hosts: fortigates
  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"
        url_path: "<your_own_value>"
        virtual_host: "<your_own_value>"
```

5.373.6 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:

5.373.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.373.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.374 fortios_vpn_ssl_web_user_bookmark – Configure SSL VPN user bookmark in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.374.1 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

5.374.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.374.3 Parameters

5.374.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.374.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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>"
           folder: "<your_own_value>"
           form_data:
            -
               name: "default_name_9"
               value: "<your_own_value>"
           host: "<your_own_value>"
           listening_port: "12"
           logon_password: "<your_own_value>"
           logon_user: "<your_own_value>"
           name: "default_name_15"
           port: "16"
           remote_port: "17"
           security: "rdp"
           server_layout: "en-us-qwerty"
           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_28"
```

5.374.6 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:

5.374.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.374.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.375 fortios_vpn_ssl_web_user_group_bookmark – Configure SSL VPN user group bookmark in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.375.1 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

5.375.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.375.3 Parameters

5.375.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.375.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
            folder: "<your_own_value>"
            form_data:
             -
                name: "default_name_9"
                value: "<your_own_value>"
            host: "<your_own_value>"
            listening_port: "12"
            logon_password: "<your_own_value>"
            logon_user: "<your_own_value>"
            name: "default_name_15"
            port: "16"
            remote_port: "17"
            security: "rdp"
            server_layout: "en-us-qwerty"
            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_27 (source user.group.name)"
```

5.375.6 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:

5.375.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.375.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.376 fortios_waf_main_class – Hidden table for datasource in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.376.1 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

5.376.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.376.3 Parameters

5.376.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.376.5 Examples

```
- hosts: fortigates
  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"
```

5.376.6 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:

5.376.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.376.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.377 fortios_waf_profile – Web application firewall configuration in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.377.1 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

5.377.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.377.3 Parameters

5.377.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.377.5 Examples

```
- hosts: fortigates
  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"
                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"
```

(continues on next page)

(continued from previous page)

```
            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"
            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"
```

(continues on next page)

(continued from previous page)

```
                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"
                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:
```

(continues on next page)

(continued from previous page)

```
            -
                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"
```

5.377.6 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:

5.377.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.377.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.378 fortios_waf_signature – Hidden table for datasource in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*

- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.378.1 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

5.378.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.378.3 Parameters

5.378.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.378.5 Examples

```
- hosts: fortigates
  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"
```

5.378.6 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:

5.378.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.378.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.379 fortios_waf_sub_class – Hidden table for datasource in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.379.1 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

5.379.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.379.3 Parameters

5.379.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.379.5 Examples

```
- hosts: fortigates
  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_sub_class:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      waf_sub_class:
        id:  "3"
        name: "default_name_4"
```

5.379.6 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:

5.379.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.379.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.380 fortios_wanopt_auth_group – Configure WAN optimization authentication groups in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.380.1 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

5.380.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.380.3 Parameters

5.380.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.380.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        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>"
```

5.380.6 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:

5.380.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.380.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.381 fortios_wanopt_cache_service – Designate cache-service for wan-optimization and webcache in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.381.1 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

5.381.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.381.3 Parameters

5.381.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.381.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
```

(continues on next page)

(continued from previous page)

```
  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"
          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"
```

5.381.6 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:

5.381.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.381.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.382 fortios_wanopt_content_delivery_network_rule – Configure WAN optimization content delivery network rules in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.382.1 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

5.382.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.382.3 Parameters

5.382.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.382.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
```

(continues on next page)

(continued from previous page)

```
  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 }}"
     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"
```

5.382.6 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:

5.382.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.382.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.383 fortios_wanopt_peer – Configure WAN optimization peers in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.383.1 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

5.383.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.383.3 Parameters

5.383.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.383.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.383.6 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:

5.383.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.383.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.384 fortios_wanopt_profile – Configure WAN optimization profiles in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.384.1 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

5.384.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.384.3 Parameters

5.384.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.384.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
            secure_tunnel: "enable"
            status: "enable"
            tunnel_sharing: "private"
        comments: "<your_own_value>"
        ftp:
            byte_caching: "enable"
            log_traffic: "enable"
            port: "16"
            prefer_chunking: "dynamic"
            secure_tunnel: "enable"
            status: "enable"
            tunnel_sharing: "private"
        http:
            byte_caching: "enable"
            log_traffic: "enable"
            port: "24"
            prefer_chunking: "dynamic"
            secure_tunnel: "enable"
            ssl: "enable"
            ssl_port: "28"
            status: "enable"
            tunnel_non_http: "enable"
            tunnel_sharing: "private"
            unknown_http_version: "reject"
        mapi:
            byte_caching: "enable"
            log_traffic: "enable"
            port: "36"
            secure_tunnel: "enable"
            status: "enable"
            tunnel_sharing: "private"
        name: "default_name_40"
        tcp:
```

(continues on next page)

(continued from previous page)

```
            byte_caching: "enable"
            byte_caching_opt: "mem-only"
            log_traffic: "enable"
            port: "<your_own_value>"
            secure_tunnel: "enable"
            ssl: "enable"
            ssl_port: "48"
            status: "enable"
            tunnel_sharing: "private"
        transparent: "enable"
```

5.384.6 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:

5.384.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.384.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.385 fortios_wanopt_remote_storage – Configure a remote cache device as Web cache storage in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*

- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.385.1 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

5.385.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.385.3 Parameters

5.385.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.385.5 Examples

```
- hosts: fortigates
  collections:
    - 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.
    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"
```

5.385.6 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:

5.385.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.385.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.386 fortios_wanopt_settings – Configure WAN optimization settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.386.1 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

5.386.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.386.3 Parameters

5.386.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.386.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.386.6 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:

5.386.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.386.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.387 fortios_wanopt_webcache – Configure global Web cache settings in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.387.1 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

5.387.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.387.3 Parameters

5.387.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.387.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.387.6 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:

5.387.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.387.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.388 fortios_web_proxy_debug_url – Configure debug URL addresses in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.388.1 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

5.388.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.388.3 Parameters

5.388.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.388.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.388.6 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:

5.388.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.388.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.389 fortios_web_proxy_explicit – Configure explicit Web proxy settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.389.1 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

5.389.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.389.3 Parameters

5.389.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.389.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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:
            -
               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"
```

5.389.6 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:

5.389.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.389.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.390 fortios_web_proxy_forward_server – Configure forward-server addresses in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.390.1 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

5.390.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.390.3 Parameters

5.390.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.390.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
   ansible_httpapi_use_ssl: yes
   ansible_httpapi_validate_certs: no
   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"
        port: "10"
        server_down_option: "block"
```

5.390.6 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:

5.390.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.390.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.391 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 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.391.1 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

5.391.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.391.3 Parameters

5.391.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.391.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.391.6 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:

5.391.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.391.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.392 fortios_web_proxy_global – Configure Web proxy global settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.392.1 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

5.392.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.392.3 Parameters

5.392.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.392.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
        strict_web_check: "enable"
        tunnel_non_http: "enable"
        unknown_http_version: "reject"
        webproxy_profile: "<your_own_value> (source web-proxy.profile.name)"
```

5.392.6 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:

5.392.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.392.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.393 fortios_web_proxy_profile – Configure web proxy profiles in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.393.1 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

5.393.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.393.3 Parameters

5.393.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.393.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
            content: "<your_own_value>"
            id:  "13"
            name: "default_name_14"
        log_header_change: "enable"
        name: "default_name_16"
        strip_encoding: "enable"
```

5.393.6 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:

5.393.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.393.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.394 fortios_web_proxy_url_match – Exempt URLs from web proxy forwarding and caching in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.394.1 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

5.394.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.394.3 Parameters

5.394.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.394.5 Examples

```
- hosts: fortigates
  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>"
```

5.394.6 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:

5.394.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.394.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.395 fortios_web_proxy_wisp – Configure Wireless Internet service provider (WISP) servers in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.395.1 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

5.395.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.395.3 Parameters

5.395.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.395.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.395.6 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:

5.395.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.395.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.396 fortios_webfilter_content – Configure Web filter banned word table in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.396.1 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

5.396.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.396.3 Parameters

5.396.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.396.5 Examples

```
- hosts: fortigates
  collections:
    - 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 }}"
```

(continues on next page)

(continued from previous page)

```
    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"
```

5.396.6 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:

5.396.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.396.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.397 fortios_webfilter_content_header – Configure content types used by Web filter in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*

- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.397.1 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

5.397.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.397.3 Parameters

5.397.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.397.5 Examples

```
- hosts: fortigates
  collections:
    - 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."
```

(continues on next page)

(continued from previous page)

```
        entries:
         -
            action: "block"
            category: "<your_own_value>"
            pattern: "<your_own_value>"
        id:  "8"
        name: "default_name_9"
```

5.397.6 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:

5.397.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.397.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.398 fortios_webfilter_fortiguard – Configure FortiGuard Web Filter service in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*

- *Status*
- *Authors*

5.398.1 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

5.398.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.398.3 Parameters

5.398.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.398.5 Examples

```
- hosts: fortigates
  collections:
    - 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_warning: "11"
```

(continues on next page)

(continued from previous page)

```
        request_packet_size_limit: "12"
        warn_auth_https: "enable"
```

5.398.6 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:

5.398.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.398.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.399 fortios_webfilter_ftgd_local_cat – Configure FortiGuard Web Filter local categories in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.399.1 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

5.399.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.399.3 Parameters

5.399.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.399.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.399.6 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:

5.399.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.399.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.400 fortios_webfilter_ftgd_local_rating – Configure local FortiGuard Web Filter local ratings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.400.1 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

5.400.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.400.3 Parameters

5.400.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.400.5 Examples

```
- hosts: fortigates
  collections:
    - 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 FortiGuard Web Filter local ratings.
    fortios_webfilter_ftgd_local_rating:
      vdom:  "{{ vdom }}"
      state: "present"
      access_token: "<your_own_value>"
      webfilter_ftgd_local_rating:
        rating: "<your_own_value>"
        status: "enable"
        url: "myurl.com"
```

5.400.6 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:

5.400.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.400.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.401 fortios_webfilter_ips_urlfilter_cache_setting – Configure IPS URL filter cache settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.401.1 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

5.401.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.401.3 Parameters

5.401.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.401.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        dns_retry_interval: "3"
        extended_ttl: "4"
```

5.401.6 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:

5.401.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.401.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.402 fortios_webfilter_ips_urlfilter_setting – Configure IPS URL filter settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.402.1 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

5.402.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.402.3 Parameters

5.402.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.402.5 Examples

```
- hosts: fortigates
  collections:
    - 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 }}"
```

(continues on next page)

(continued from previous page)

```
    webfilter_ips_urlfilter_setting:
      device: "<your_own_value> (source system.interface.name)"
      distance: "4"
      gateway: "<your_own_value>"
      geo_filter: "<your_own_value>"
```

5.402.6 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:

5.402.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.402.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.403 fortios_webfilter_ips_urlfilter_setting6 – Configure IPS URL filter settings for IPv6 in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.403.1 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

5.403.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.403.3 Parameters

5.403.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.403.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.403.6 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:

5.403.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.403.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.404 fortios_webfilter_override – Configure FortiGuard Web Filter administrative overrides in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.404.1 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

5.404.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.404.3 Parameters

5.404.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.404.5 Examples

```
- hosts: fortigates
  collections:
    - 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)"
```

5.404.6 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:

5.404.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.404.8 Authors

- Link Zheng (@chillancezen)

- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.405 fortios_webfilter_profile – Configure Web filter profiles in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.405.1 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

5.405.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.405.3 Parameters

5.405.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.405.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        comment: "Optional comments."
        extended_log: "enable"
        ftgd_wf:
            exempt_quota: "<your_own_value>"
            filters:
             -
                action: "block"
                auth_usr_grp:
                 -
                    name: "default_name_10 (source user.group.name)"
                category: "11"
                id:  "12"
                log: "enable"
                override_replacemsg: "<your_own_value>"
                warn_duration: "<your_own_value>"
                warning_duration_type: "session"
                warning_prompt: "per-domain"
            max_quota_timeout: "18"
            options: "error-allow"
            ovrd: "<your_own_value>"
            quota:
             -
                category: "<your_own_value>"
                duration: "<your_own_value>"
                id:  "24"
                override_replacemsg: "<your_own_value>"
                type: "time"
                unit: "B"
                value: "28"
            rate_crl_urls: "disable"
            rate_css_urls: "disable"
            rate_image_urls: "disable"
            rate_javascript_urls: "disable"
        https_replacemsg: "enable"
        inspection_mode: "proxy"
```

(continues on next page)

(continued from previous page)

```
        log_all_url: "enable"
        name: "default_name_36"
        options: "activexfilter"
        override:
            ovrd_cookie: "allow"
            ovrd_dur: "<your_own_value>"
            ovrd_dur_mode: "constant"
            ovrd_scope: "user"
            ovrd_user_group:
             -
                name: "default_name_44 (source user.group.name)"
            profile:
             -
                name: "default_name_46 (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)"
        web:
            blacklist: "enable"
            bword_table: "54 (source webfilter.content.id)"
            bword_threshold: "55"
            content_header_list: "56 (source webfilter.content-header.id)"
            keyword_match:
             -
                pattern: "<your_own_value>"
            log_search: "enable"
            safe_search: "url"
            urlfilter_table: "61 (source webfilter.urlfilter.id)"
            whitelist: "exempt-av"
            youtube_restrict: "none"
        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_83 (source web-proxy.wisp.name)"
        youtube_channel_filter:
         -
            channel_id: "<your_own_value>"
            comment: "Comment."
```

(continues on next page)

(continued from previous page)

```
            id:  "87"
        youtube_channel_status: "disable"
```

5.405.6 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:

5.405.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.405.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.406 fortios_webfilter_search_engine – Configure web filter search engines in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.406.1 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

5.406.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.406.3 Parameters

5.406.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.406.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.406.6 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:

5.406.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.406.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.407 fortios_webfilter_urlfilter – Configure URL filter lists in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.407.1 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

5.407.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.407.3 Parameters

5.407.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.407.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
            dns_address_family: "ipv4"
            exempt: "av"
            id:  "8"
            referrer_host: "myhostname"
            status: "enable"
            type: "simple"
            url: "myurl.com"
            web_proxy_profile: "<your_own_value> (source web-proxy.profile.name)"
        id:  "14"
        ip_addr_block: "enable"
        name: "default_name_16"
        one_arm_ips_urlfilter: "enable"
```

5.407.6 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:

5.407.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.407.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.408 fortios_wireless_controller_ap_status – Configure access point status (rogue | accepted | suppressed) in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.408.1 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

5.408.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.408.3 Parameters

5.408.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.408.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.408.6 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:

5.408.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.408.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.409 fortios_wireless_controller_ble_profile – Configure Bluetooth Low Energy profile in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.409.1 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

5.409.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.409.3 Parameters

5.409.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.409.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.409.6 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:

5.409.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.409.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.410 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 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.410.1 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

5.410.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.410.3 Parameters

5.410.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.410.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.410.6 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:

5.410.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.410.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.411 fortios_wireless_controller_global – Configure wireless controller global settings in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.411.1 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

5.411.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.411.3 Parameters

5.411.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.411.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  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"
```

5.411.6 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:

5.411.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.411.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.412 fortios_wireless_controller_hotspot20_anqp_3gpp_cellular – Configure 3GPP public land mobile network (PLMN) in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.412.1 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

5.412.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.412.3 Parameters

5.412.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.412.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.412.6 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:

5.412.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.412.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.413 fortios_wireless_controller_hotspot20_anqp_ip_address_type – Configure IP address type availability in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.413.1 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

5.413.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.413.3 Parameters

5.413.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.413.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    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"
```

5.413.6 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:

5.413.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.413.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.414 fortios_wireless_controller_hotspot20_anqp_nai_realm – Configure network access identifier (NAI) realm in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*

- *Return Values*
- *Status*
- *Authors*

5.414.1 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

5.414.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.414.3 Parameters

5.414.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.414.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
                 -
```

(continues on next page)

(continued from previous page)

```
                    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"
```

5.414.6 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:

5.414.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.414.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.415 fortios_wireless_controller_hotspot20_anqp_network_auth_type – Configure network authentication type in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*

- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.415.1 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

5.415.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.415.3 Parameters

5.415.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.415.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.415.6 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:

5.415.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.415.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.416 fortios_wireless_controller_hotspot20_anqp_roaming_consortium – Configure roaming consortium in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.416.1 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

5.416.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.416.3 Parameters

5.416.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.416.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.416.6 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:

5.416.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.416.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.417 fortios_wireless_controller_hotspot20_anqp_venue_name – Configure venue name duple in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.417.1 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

5.417.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.417.3 Parameters

5.417.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.417.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.417.6 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:

5.417.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.417.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.418 fortios_wireless_controller_hotspot20_h2qp_conn_capability – Configure connection capability in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.418.1 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

5.418.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.418.3 Parameters

5.418.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.418.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.418.6 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:

5.418.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.418.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.419 fortios_wireless_controller_hotspot20_h2qp_operator_name – Configure operator friendly name in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.419.1 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

5.419.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.419.3 Parameters

5.419.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.419.5 Examples

```
- hosts: fortigates
  collections:
    - 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>"
```

5.419.6 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:

5.419.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.419.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.420 fortios_wireless_controller_hotspot20_h2qp_osu_provider – Configure online sign up (OSU) provider list in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.420.1 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

5.420.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.420.3 Parameters

5.420.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.420.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.420.6 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:

5.420.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.420.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.421 fortios_wireless_controller_hotspot20_h2qp_wan_metric – Configure WAN metrics in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.421.1 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

5.421.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.421.3 Parameters

5.421.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.421.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
```

5.421.6 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:

5.421.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.421.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.422 fortios_wireless_controller_hotspot20_hs_profile – Configure hotspot profile in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.422.1 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

5.422.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.422.3 Parameters

5.422.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.422.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    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)"
      venue_type: "unspecified"
      wan_metrics: "<your_own_value> (source wireless-controller.hotspot20.h2qp-wan-
↪metric.name)"
      wnm_sleep_mode: "enable"
```

5.422.6 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:

5.422.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.422.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.423 fortios_wireless_controller_hotspot20_icon – Configure OSU provider icon in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.423.1 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

5.423.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.423.3 Parameters

5.423.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.423.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
            width: "9"
        name: "default_name_10"
```

5.423.6 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:

5.423.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.423.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.424 fortios_wireless_controller_hotspot20_qos_map – Configure QoS map set in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.424.1 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

5.424.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.424.3 Parameters

5.424.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.424.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.424.6 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:

5.424.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.424.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.425 fortios_wireless_controller_inter_controller – Configure inter wireless controller operation in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.425.1 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

5.425.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.425.3 Parameters

5.425.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.425.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
```

5.425.6 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:

5.425.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.425.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.426 fortios_wireless_controller_qos_profile – Configure WiFi quality of service (QoS) profiles in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.426.1 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

5.426.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.426.3 Parameters

5.426.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.426.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
   vdom: "root"
```

(continues on next page)

(continued from previous page)

```
  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"
       uplink: "21"
       uplink_sta: "22"
       wmm: "enable"
       wmm_uapsd: "enable"
```

5.426.6 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:

5.426.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.426.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.427 fortios_wireless_controller_setting – VDOM wireless controller configuration in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.427.1 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

5.427.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.427.3 Parameters

5.427.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.427.5 Examples

```
- hosts: fortigates
  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"
        duplicate_ssid: "enable"
        fapc_compatibility: "enable"
```

5.427.6 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:

5.427.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.427.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.428 fortios_wireless_controller_timers – Configure CAPWAP timers in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.428.1 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

5.428.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.428.3 Parameters

5.428.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.428.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    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"
      echo_interval: "10"
      fake_ap_log: "11"
      ipsec_intf_cleanup: "12"
      radio_stats_interval: "13"
      rogue_ap_log: "14"
      sta_capability_interval: "15"
      sta_locate_timer: "16"
      sta_stats_interval: "17"
      vap_stats_interval: "18"
```

5.428.6 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:

5.428.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.428.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.429 fortios_wireless_controller_utm_profile – Configure UTM (Unified Threat Management) profile in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.429.1 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

5.429.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.429.3 Parameters

5.429.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.429.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
```

(continues on next page)

(continued from previous page)

```
    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)"
```

5.429.6 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:

5.429.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.429.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.430 fortios_wireless_controller_vap – Configure Virtual Access Points (VAPs) in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*

- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.430.1 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

5.430.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.430.3 Parameters

5.430.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.430.5 Examples

```
- hosts: fortigates
  collections:
    - 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:
        acct_interim_interval: "3"
        alias: "<your_own_value>"
        auth: "psk"
```

(continues on next page)

(continued from previous page)

```
        broadcast_ssid: "enable"
        broadcast_suppression: "dhcp-up"
        captive_portal_ac_name: "<your_own_value>"
        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: "13"
        dhcp_lease_time: "14"
        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: "20"
        eapol_key_retries: "disable"
        encrypt: "TKIP"
        external_fast_roaming: "enable"
        external_logout: "<your_own_value>"
        external_web: "<your_own_value>"
        fast_bss_transition: "disable"
        fast_roaming: "enable"
        ft_mobility_domain: "28"
        ft_over_ds: "disable"
        ft_r0_key_lifetime: "30"
        gtk_rekey: "enable"
        gtk_rekey_intv: "32"
        hotspot20_profile: "<your_own_value>"
        intra_vap_privacy: "enable"
        ip: "<your_own_value>"
        key: "<your_own_value>"
        keyindex: "37"
        ldpc: "disable"
        local_authentication: "enable"
        local_bridging: "enable"
        local_lan: "allow"
        local_standalone: "enable"
        local_standalone_nat: "enable"
        mac_auth_bypass: "enable"
        mac_filter: "enable"
        mac_filter_list:
         -
            id:  "47"
            mac: "<your_own_value>"
            mac_filter_policy: "allow"
        mac_filter_policy_other: "allow"
        max_clients: "51"
        max_clients_ap: "52"
        me_disable_thresh: "53"
        mesh_backhaul: "enable"
        mpsk: "enable"
        mpsk_concurrent_clients: "56"
        mpsk_key:
         -
            comment: "Comment."
            concurrent_clients: "<your_own_value>"
            key_name: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```
            passphrase: "<your_own_value>"
        multicast_enhance: "enable"
        multicast_rate: "0"
        name: "default_name_64"
        okc: "disable"
        passphrase: "<your_own_value>"
        pmf: "disable"
        pmf_assoc_comeback_timeout: "68"
        pmf_sa_query_retry_timeout: "69"
        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>"
        portal_type: "auth"
        probe_resp_suppression: "enable"
        probe_resp_threshold: "<your_own_value>"
        ptk_rekey: "enable"
        ptk_rekey_intv: "80"
        qos_profile: "<your_own_value>"
        quarantine: "enable"
        radius_mac_auth: "enable"
        radius_mac_auth_server: "<your_own_value>"
        radius_server: "<your_own_value>"
        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"
        schedule: "<your_own_value>"
        security: "open"
        security_exempt_list: "<your_own_value>"
        security_obsolete_option: "enable"
        security_redirect_url: "<your_own_value>"
        selected_usergroups:
         -
            name: "default_name_98"
        split_tunneling: "enable"
        ssid: "<your_own_value>"
        tkip_counter_measure: "enable"
        usergroup:
         -
            name: "default_name_103"
        utm_profile: "<your_own_value>"
        vdom: "<your_own_value> (source system.vdom.name)"
        vlan_auto: "enable"
        vlan_pool:
         -
            id:  "108"
            wtp_group: "<your_own_value>"
        vlan_pooling: "wtp-group"
        vlanid: "111"
        voice_enterprise: "disable"
```

5.430.6 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:

5.430.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.430.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.431 fortios_wireless_controller_vap_group – Configure virtual Access Point (VAP) groups in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.431.1 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

5.431.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.431.3 Parameters

5.431.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.431.5 Examples

```
- hosts: fortigates
  collections:
    - 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)"
```

5.431.6 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:

5.431.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.431.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.432 fortios_wireless_controller_wids_profile – Configure wireless intrusion detection system (WIDS) profiles in Fortinet's FortiOS and FortiGate.

New in version 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.432.1 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

5.432.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.432.3 Parameters

5.432.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.432.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        ap_bgscan_disable_end: "<your_own_value>"
        ap_bgscan_disable_start: "<your_own_value>"
        ap_bgscan_duration: "7"
        ap_bgscan_idle: "8"
        ap_bgscan_intv: "9"
        ap_bgscan_period: "10"
        ap_bgscan_report_intv: "11"
        ap_fgscan_report_intv: "12"
        ap_scan: "disable"
        ap_scan_passive: "enable"
        asleap_attack: "enable"
        assoc_flood_thresh: "16"
        assoc_flood_time: "17"
        assoc_frame_flood: "enable"
        auth_flood_thresh: "19"
        auth_flood_time: "20"
        auth_frame_flood: "enable"
        comment: "Comment."
        deauth_broadcast: "enable"
        deauth_unknown_src_thresh: "24"
        eapol_fail_flood: "enable"
        eapol_fail_intv: "26"
        eapol_fail_thresh: "27"
        eapol_logoff_flood: "enable"
        eapol_logoff_intv: "29"
        eapol_logoff_thresh: "30"
```

(continues on next page)

(continued from previous page)

```
        eapol_pre_fail_flood: "enable"
        eapol_pre_fail_intv: "32"
        eapol_pre_fail_thresh: "33"
        eapol_pre_succ_flood: "enable"
        eapol_pre_succ_intv: "35"
        eapol_pre_succ_thresh: "36"
        eapol_start_flood: "enable"
        eapol_start_intv: "38"
        eapol_start_thresh: "39"
        eapol_succ_flood: "enable"
        eapol_succ_intv: "41"
        eapol_succ_thresh: "42"
        invalid_mac_oui: "enable"
        long_duration_attack: "enable"
        long_duration_thresh: "45"
        name: "default_name_46"
        null_ssid_probe_resp: "enable"
        sensor_mode: "disable"
        spoofed_deauth: "enable"
        weak_wep_iv: "enable"
        wireless_bridge: "enable"
```

5.432.6 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:

5.432.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.432.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.433 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 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.433.1 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

5.433.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.433.3 Parameters

5.433.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.433.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
```

(continues on next page)

(continued from previous page)

```
  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"
       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>"
       coordinate_y: "<your_own_value>"
       image_download: "enable"
       index: "12"
       ip_fragment_preventing: "tcp-mss-adjust"
       lan:
           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_38"
       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:
```

(continues on next page)

(continued from previous page)

```
            auto_power_high: "47"
            auto_power_level: "enable"
            auto_power_low: "49"
            band: "802.11a"
            channel:
             -
                chan: "<your_own_value>"
            override_analysis: "enable"
            override_band: "enable"
            override_channel: "enable"
            override_txpower: "enable"
            override_vaps: "enable"
            power_level: "58"
            radio_id: "59"
            spectrum_analysis: "enable"
            vap_all: "enable"
            vaps:
             -
                name: "default_name_63 (source wireless-controller.vap-group.name␣
↪wireless-controller.vap.name)"
        radio_2:
            auto_power_high: "65"
            auto_power_level: "enable"
            auto_power_low: "67"
            band: "802.11a"
            channel:
             -
                chan: "<your_own_value>"
            override_analysis: "enable"
            override_band: "enable"
            override_channel: "enable"
            override_txpower: "enable"
            override_vaps: "enable"
            power_level: "76"
            radio_id: "77"
            spectrum_analysis: "enable"
            vap_all: "enable"
            vaps:
             -
                name: "default_name_81 (source wireless-controller.vap-group.name␣
↪wireless-controller.vap.name)"
        split_tunneling_acl:
         -
            dest_ip: "<your_own_value>"
            id:  "84"
        split_tunneling_acl_local_ap_subnet: "enable"
        split_tunneling_acl_path: "tunnel"
        tun_mtu_downlink: "87"
        tun_mtu_uplink: "88"
        wan_port_mode: "wan-lan"
        wtp_id: "<your_own_value>"
        wtp_mode: "normal"
        wtp_profile: "<your_own_value> (source wireless-controller.wtp-profile.name)"
```

5.433.6 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:

5.433.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.433.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.434 fortios_wireless_controller_wtp_group – Configure WTP groups in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.434.1 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

5.434.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.434.3 Parameters

5.434.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.434.5 Examples

```
- hosts: fortigates
  collections:
    - 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)"
```

5.434.6 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:

5.434.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.434.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

5.435 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 2.8.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

5.435.1 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

5.435.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

5.435.3 Parameters

5.435.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks

5.435.5 Examples

```
- hosts: fortigates
  collections:
    - 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"
        ble_profile: "<your_own_value> (source wireless-controller.ble-profile.name)"
        comment: "Comment."
        control_message_offload: "ebp-frame"
        deny_mac_list:
         -
            id:  "9"
            mac: "<your_own_value>"
        dtls_in_kernel: "enable"
        dtls_policy: "clear-text"
        energy_efficient_ethernet: "enable"
        ext_info_enable: "enable"
        handoff_roaming: "enable"
        handoff_rssi: "16"
        handoff_sta_thresh: "17"
        ip_fragment_preventing: "tcp-mss-adjust"
        lan:
            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"
```

(continues on next page)

(continued from previous page)

```
            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: "43"
            aeroscout_mu_timeout: "44"
            aeroscout_server_ip: "<your_own_value>"
            aeroscout_server_port: "46"
            ekahau_blink_mode: "enable"
            ekahau_tag: "<your_own_value>"
            erc_server_ip: "<your_own_value>"
            erc_server_port: "50"
            fortipresence: "foreign"
            fortipresence_frequency: "52"
            fortipresence_port: "53"
            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_61 (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: "66"
        name: "default_name_67"
        platform:
            type: "AP-11N"
        poe_mode: "auto"
        radio_1:
            amsdu: "enable"
            ap_handoff: "enable"
            ap_sniffer_addr: "<your_own_value>"
            ap_sniffer_bufsize: "75"
            ap_sniffer_chan: "76"
            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: "82"
            auto_power_level: "enable"
```

(continues on next page)

(continued from previous page)

```
            auto_power_low: "84"
            band: "802.11a"
            bandwidth_admission_control: "enable"
            bandwidth_capacity: "87"
            beacon_interval: "88"
            call_admission_control: "enable"
            call_capacity: "90"
            channel:
             -
                chan: "<your_own_value>"
            channel_bonding: "80MHz"
            channel_utilization: "enable"
            coexistence: "enable"
            darrp: "enable"
            dtim: "97"
            frag_threshold: "98"
            frequency_handoff: "enable"
            max_clients: "100"
            max_distance: "101"
            mode: "disabled"
            power_level: "103"
            powersave_optimize: "tim"
            protection_mode: "rtscts"
            radio_id: "106"
            rts_threshold: "107"
            short_guard_interval: "enable"
            spectrum_analysis: "enable"
            transmit_optimize: "disable"
            vap_all: "enable"
            vaps:
             -
                name: "default_name_113 (source wireless-controller.vap-group.name␣
↪wireless-controller.vap.name)"
            wids_profile: "<your_own_value> (source wireless-controller.wids-profile.
↪name)"
        radio_2:
            amsdu: "enable"
            ap_handoff: "enable"
            ap_sniffer_addr: "<your_own_value>"
            ap_sniffer_bufsize: "119"
            ap_sniffer_chan: "120"
            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: "126"
            auto_power_level: "enable"
            auto_power_low: "128"
            band: "802.11a"
            bandwidth_admission_control: "enable"
            bandwidth_capacity: "131"
            beacon_interval: "132"
            call_admission_control: "enable"
            call_capacity: "134"
            channel:
             -
```

(continues on next page)

(continued from previous page)

```
                chan: "<your_own_value>"
            channel_bonding: "80MHz"
            channel_utilization: "enable"
            coexistence: "enable"
            darrp: "enable"
            dtim: "141"
            frag_threshold: "142"
            frequency_handoff: "enable"
            max_clients: "144"
            max_distance: "145"
            mode: "disabled"
            power_level: "147"
            powersave_optimize: "tim"
            protection_mode: "rtscts"
            radio_id: "150"
            rts_threshold: "151"
            short_guard_interval: "enable"
            spectrum_analysis: "enable"
            transmit_optimize: "disable"
            vap_all: "enable"
            vaps:
             -
                name: "default_name_157 (source wireless-controller.vap-group.name␣
↪wireless-controller.vap.name)"
            wids_profile: "<your_own_value> (source wireless-controller.wids-profile.
↪name)"
        split_tunneling_acl:
         -
            dest_ip: "<your_own_value>"
            id:  "161"
        split_tunneling_acl_local_ap_subnet: "enable"
        split_tunneling_acl_path: "tunnel"
        tun_mtu_downlink: "164"
        tun_mtu_uplink: "165"
        wan_port_mode: "wan-lan"
```

5.435.6 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:

5.435.7 Status

- This module is not guaranteed to have a backwards compatible interface.

5.435.8 Authors

- Link Zheng (@chillancezen)
- Jie Xue (@JieX19)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Miguel 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 6

Facts Gathering Modules

The Modules to gather FortiOS fatcs are invoking `GET` requests for FortiOS managed objects or procedures.

6.1 fortios_facts – Get facts about fortios devices (about to be deprecated).

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

6.1.1 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.

6.1.2 Requirements

The below requirements are needed on the host that executes this module.

- galaxy collection fortinet.fortios

6.1.3 Parameters

6.1.4 Notes

Note:

- httpapi mode is the new recommended way for any network modules
- the module is going to be deprecated in next major release.

6.1.5 Examples

```
- hosts: localhost
  vars:
    host: "192.168.122.40"
    username: "admin"
    password: ""
    vdom: "root"
    ssl_verify: "False"

  tasks:
  - name: gather basic system status facts
    fortios_facts:
      host:  "{{ host }}"
      username: "{{ username }}"
      password: "{{ password }}"
      vdom:  "{{ vdom }}"
      gather_subset:
        - fact: 'system_status_select'

  - name: gather all physical interfaces status facts
    fortios_facts:
      host:  "{{ host }}"
      username: "{{ username }}"
      password: "{{ password }}"
      vdom:  "{{ vdom }}"
      gather_subset:
        - fact: 'system_interface_select'

  - name: gather gather all physical and vlan interfaces status facts
    fortios_facts:
      host:  "{{ host }}"
      username: "{{ username }}"
      password: "{{ password }}"
      vdom:  "{{ vdom }}"
      gather_subset:
        - fact: 'system_interface_select'
```

(continues on next page)

(continued from previous page)

```
        filters:
          - include_vlan: true

- name: gather basic system info and physical interface port3 status facts
  fortios_facts:
    host:  "{{ host }}"
    username: "{{ username }}"
    password: "{{ password }}"
    vdom:  "{{ vdom }}"
    gather_subset:
      - fact: 'system_status_select'
      - fact: 'system_interface_select'
        filters:
          - interface_name: 'port3'
```

6.1.6 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:

6.1.7 Status

- This module is not guaranteed to have a backwards compatible interface.

6.1.8 Authors

- Don Yao (@fortinetps)
- Miguel Angel 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_configuration_fact – Retrieve Facts of FortiOS Configurable Objects.

New in version 2.10.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*

- *Return Values*
- *Status*
- *Authors*

6.2.1 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.

6.2.2 Requirements

The below requirements are needed on the host that executes this module.

- install galaxy collection fortinet.fortios

6.2.3 Parameters

6.2.4 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.
- 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.

6.2.5 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 all
    fortios_configuration_fact:
      vdom: ""
      access_token: ""
      selector: log_custom-field
```

(continues on next page)

(continued from previous page)

```
- 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
```

6.2.6 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:

6.2.7 Status

- This module is not guaranteed to have a backwards compatible interface.

6.2.8 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.

CHAPTER 7

Release Notes

7.1 Multiversions Note

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",
    "system_version": "v6.2.0"
}
...
```

Simply installing a matched FortiOS collection can prevent potential compatibility issues.

7.2 Release Galaxy 1.1.9

7.2.1 Release Targets

- fos_v6.0.0/galaxy_1.1.9

7.2.2 Bug Fixes

- Fix legacy module `fortios_system_config_backup_restore`

7.3 Release Galaxy 1.1.6 . . . 1.1.8

7.3.1 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

7.3.2 Bug Fixes

- Fixed module construction for legacy module `fortios_facts`.
- Sorted selector list of module `fortios_configuration_fact`.

7.4 Release Galaxy 1.1.3 . . . 1.1.5

7.4.1 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

7.4.2 Bug Fixes

- Fixed a fatal error: `mkey` not recognized in plugin due to wrong naming convention.

7.5 Release Galaxy 1.1.0 . . . 1.1.2

7.5.1 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

7.5.2 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`).

7.5.3 Bug Fixes

- Github Issue #65

7.6 Release Galaxy 1.0.10 . . . 10.0.13

7.6.1 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

7.6.2 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

Continued on next page

Table 1 – continued from previous page

#	Module Name	New in 6.2	New in 6.4
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
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

Continued on next page

Table 1 – continued from previous page

#	Module Name	New in 6.2	New in 6.4
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
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

Continued on next page

Table 1 – continued from previous page

#	Module Name	New in 6.2	New in 6.4
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
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

Continued on next page

Table 1 – continued from previous page

#	Module Name	New in 6.2	New in 6.4
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

7.6.3 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.

7.6.4 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`.