
Ansible Galaxy FortiOS Collection

Release 1.0

May 20, 2020

1	fortios_alertemail_setting – Configure alert email settings in Fortinet’s FortiOS and FortiGate.	1
1.1	Synopsis	1
1.2	Requirements	1
1.3	Parameters	2
1.4	Notes	2
1.5	Examples	2
1.6	Return Values	3
1.7	Status	3
1.8	Authors	3
2	fortios_antivirus_heuristic – Configure global heuristic options in Fortinet’s FortiOS and FortiGate.	5
2.1	Synopsis	5
2.2	Requirements	5
2.3	Parameters	6
2.4	Notes	6
2.5	Examples	6
2.6	Return Values	6
2.7	Status	6
2.8	Authors	6
3	fortios_antivirus_profile – Configure AntiVirus profiles in Fortinet’s FortiOS and FortiGate.	9
3.1	Synopsis	9
3.2	Requirements	9
3.3	Parameters	10
3.4	Notes	10
3.5	Examples	10
3.6	Return Values	12
3.7	Status	12
3.8	Authors	12
4	fortios_antivirus_quarantine – Configure quarantine options in Fortinet’s FortiOS and FortiGate.	13
4.1	Synopsis	13
4.2	Requirements	13
4.3	Parameters	14
4.4	Notes	14
4.5	Examples	14
4.6	Return Values	14

4.7	Status	14
4.8	Authors	15
5	fortios_antivirus_settings – Configure AntiVirus settings in Fortinet’s FortiOS and FortiGate.	17
5.1	Synopsis	17
5.2	Requirements	17
5.3	Parameters	18
5.4	Notes	18
5.5	Examples	18
5.6	Return Values	18
5.7	Status	18
5.8	Authors	18
6	fortios_application_custom – Configure custom application signatures in Fortinet’s FortiOS and FortiGate.	21
6.1	Synopsis	21
6.2	Requirements	21
6.3	Parameters	22
6.4	Notes	22
6.5	Examples	22
6.6	Return Values	22
6.7	Status	22
6.8	Authors	23
7	fortios_application_group – Configure firewall application groups in Fortinet’s FortiOS and FortiGate.	25
7.1	Synopsis	25
7.2	Requirements	25
7.3	Parameters	26
7.4	Notes	26
7.5	Examples	26
7.6	Return Values	26
7.7	Status	26
7.8	Authors	27
8	fortios_application_list – Configure application control lists in Fortinet’s FortiOS and FortiGate.	29
8.1	Synopsis	29
8.2	Requirements	29
8.3	Parameters	30
8.4	Notes	30
8.5	Examples	30
8.6	Return Values	31
8.7	Status	31
8.8	Authors	31
9	fortios_application_name – Configure application signatures in Fortinet’s FortiOS and FortiGate.	33
9.1	Synopsis	33
9.2	Requirements	33
9.3	Parameters	34
9.4	Notes	34
9.5	Examples	34
9.6	Return Values	34
9.7	Status	35
9.8	Authors	35
10	fortios_application_rule_settings – Configure application rule settings in Fortinet’s FortiOS and Forti-	

Gate.	37
10.1 Synopsis	37
10.2 Requirements	37
10.3 Parameters	38
10.4 Notes	38
10.5 Examples	38
10.6 Return Values	38
10.7 Status	38
10.8 Authors	38
11 fortios_authentication_rule – Configure Authentication Rules in Fortinet’s FortiOS and FortiGate.	41
11.1 Synopsis	41
11.2 Requirements	41
11.3 Parameters	42
11.4 Notes	42
11.5 Examples	42
11.6 Return Values	42
11.7 Status	43
11.8 Authors	43
12 fortios_authentication_scheme – Configure Authentication Schemes in Fortinet’s FortiOS and FortiGate.	45
12.1 Synopsis	45
12.2 Requirements	45
12.3 Parameters	46
12.4 Notes	46
12.5 Examples	46
12.6 Return Values	46
12.7 Status	46
12.8 Authors	47
13 fortios_authentication_setting – Configure authentication setting in Fortinet’s FortiOS and FortiGate.	49
13.1 Synopsis	49
13.2 Requirements	49
13.3 Parameters	50
13.4 Notes	50
13.5 Examples	50
13.6 Return Values	50
13.7 Status	50
13.8 Authors	50
14 fortios_certificate_ca – CA certificate in Fortinet’s FortiOS and FortiGate.	53
14.1 Synopsis	53
14.2 Requirements	53
14.3 Parameters	54
14.4 Notes	54
14.5 Examples	54
14.6 Return Values	54
14.7 Status	54
14.8 Authors	55
15 fortios_certificate_crl – Certificate Revocation List as a PEM file in Fortinet’s FortiOS and FortiGate.	57
15.1 Synopsis	57
15.2 Requirements	57
15.3 Parameters	58

15.4	Notes	58
15.5	Examples	58
15.6	Return Values	58
15.7	Status	58
15.8	Authors	59
16	fortios_certificate_local – Local keys and certificates in Fortinet’s FortiOS and FortiGate.	61
16.1	Synopsis	61
16.2	Requirements	61
16.3	Parameters	62
16.4	Notes	62
16.5	Examples	62
16.6	Return Values	63
16.7	Status	63
16.8	Authors	63
17	fortios_dlp_filepattern – Configure file patterns used by DLP blocking in Fortinet’s FortiOS and FortiGate.	65
17.1	Synopsis	65
17.2	Requirements	65
17.3	Parameters	66
17.4	Notes	66
17.5	Examples	66
17.6	Return Values	66
17.7	Status	66
17.8	Authors	66
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.	69
18.1	Synopsis	69
18.2	Requirements	69
18.3	Parameters	70
18.4	Notes	70
18.5	Examples	70
18.6	Return Values	71
18.7	Status	71
18.8	Authors	71
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.	73
19.1	Synopsis	73
19.2	Requirements	73
19.3	Parameters	74
19.4	Notes	74
19.5	Examples	74
19.6	Return Values	74
19.7	Status	74
19.8	Authors	74
20	fortios_dlp_sensor – Configure DLP sensors in Fortinet’s FortiOS and FortiGate.	77
20.1	Synopsis	77
20.2	Requirements	77
20.3	Parameters	78
20.4	Notes	78
20.5	Examples	78

20.6	Return Values	79
20.7	Status	79
20.8	Authors	79
21	fortios_dlp_settings – Designate logical storage for DLP fingerprint database in Fortinet’s FortiOS and FortiGate.	81
21.1	Synopsis	81
21.2	Requirements	81
21.3	Parameters	82
21.4	Notes	82
21.5	Examples	82
21.6	Return Values	82
21.7	Status	82
21.8	Authors	82
22	fortios_dnsfilter_domain_filter – Configure DNS domain filters in Fortinet’s FortiOS and FortiGate.	85
22.1	Synopsis	85
22.2	Requirements	85
22.3	Parameters	86
22.4	Notes	86
22.5	Examples	86
22.6	Return Values	86
22.7	Status	86
22.8	Authors	87
23	fortios_dnsfilter_profile – Configure DNS domain filter profiles in Fortinet’s FortiOS and FortiGate.	89
23.1	Synopsis	89
23.2	Requirements	89
23.3	Parameters	90
23.4	Notes	90
23.5	Examples	90
23.6	Return Values	91
23.7	Status	91
23.8	Authors	91
24	fortios_endpoint_control_client – Configure endpoint control client lists in Fortinet’s FortiOS and FortiGate.	93
24.1	Synopsis	93
24.2	Requirements	93
24.3	Parameters	94
24.4	Notes	94
24.5	Examples	94
24.6	Return Values	94
24.7	Status	94
24.8	Authors	94
25	fortios_endpoint_control_forticlient_ems – Configure FortiClient Enterprise Management Server (EMS) entries in Fortinet’s FortiOS and FortiGate.	97
25.1	Synopsis	97
25.2	Requirements	97
25.3	Parameters	98
25.4	Notes	98
25.5	Examples	98
25.6	Return Values	98
25.7	Status	98

25.8	Authors	99
26	fortios_endpoint_control_forticlient_registration_sync – Configure FortiClient registration synchronization settings in Fortinet’s FortiOS and FortiGate.	101
26.1	Synopsis	101
26.2	Requirements	101
26.3	Parameters	102
26.4	Notes	102
26.5	Examples	102
26.6	Return Values	102
26.7	Status	102
26.8	Authors	102
27	fortios_endpoint_control_profile – Configure FortiClient endpoint control profiles in Fortinet’s FortiOS and FortiGate.	105
27.1	Synopsis	105
27.2	Requirements	105
27.3	Parameters	106
27.4	Notes	106
27.5	Examples	106
27.6	Return Values	108
27.7	Status	108
27.8	Authors	108
28	fortios_endpoint_control_registered_forticlient – Registered FortiClient list in Fortinet’s FortiOS and FortiGate.	111
28.1	Synopsis	111
28.2	Requirements	111
28.3	Parameters	112
28.4	Notes	112
28.5	Examples	112
28.6	Return Values	112
28.7	Status	112
28.8	Authors	112
29	fortios_endpoint_control_settings – Configure endpoint control settings in Fortinet’s FortiOS and FortiGate.	115
29.1	Synopsis	115
29.2	Requirements	115
29.3	Parameters	116
29.4	Notes	116
29.5	Examples	116
29.6	Return Values	116
29.7	Status	116
29.8	Authors	117
30	fortios_extender_controller_extender – Extender controller configuration in Fortinet’s FortiOS and FortiGate.	119
30.1	Synopsis	119
30.2	Requirements	119
30.3	Parameters	120
30.4	Notes	120
30.5	Examples	120
30.6	Return Values	121
30.7	Status	121

30.8	Authors	121
31	fortios_firewall_address – Configure IPv4 addresses in Fortinet’s FortiOS and FortiGate.	123
31.1	Synopsis	123
31.2	Requirements	123
31.3	Parameters	124
31.4	Notes	124
31.5	Examples	124
31.6	Return Values	125
31.7	Status	125
31.8	Authors	125
32	fortios_firewall_address6 – Configure IPv6 firewall addresses in Fortinet’s FortiOS and FortiGate.	127
32.1	Synopsis	127
32.2	Requirements	127
32.3	Parameters	128
32.4	Notes	128
32.5	Examples	128
32.6	Return Values	129
32.7	Status	129
32.8	Authors	129
33	fortios_firewall_address6_template – Configure IPv6 address templates in Fortinet’s FortiOS and FortiGate.	131
33.1	Synopsis	131
33.2	Requirements	131
33.3	Parameters	132
33.4	Notes	132
33.5	Examples	132
33.6	Return Values	132
33.7	Status	132
33.8	Authors	133
34	fortios_firewall_addrgrp – Configure IPv4 address groups in Fortinet’s FortiOS and FortiGate.	135
34.1	Synopsis	135
34.2	Requirements	135
34.3	Parameters	136
34.4	Notes	136
34.5	Examples	136
34.6	Return Values	136
34.7	Status	137
34.8	Authors	137
35	fortios_firewall_addrgrp6 – Configure IPv6 address groups in Fortinet’s FortiOS and FortiGate.	139
35.1	Synopsis	139
35.2	Requirements	139
35.3	Parameters	140
35.4	Notes	140
35.5	Examples	140
35.6	Return Values	140
35.7	Status	141
35.8	Authors	141
36	fortios_firewall_auth_portal – Configure firewall authentication portals in Fortinet’s FortiOS and FortiGate.	143

36.1	Synopsis	143
36.2	Requirements	143
36.3	Parameters	144
36.4	Notes	144
36.5	Examples	144
36.6	Return Values	144
36.7	Status	144
36.8	Authors	144
37	fortios_firewall_central_snat_map – Configure central SNAT policies in Fortinet’s FortiOS and FortiGate.	147
37.1	Synopsis	147
37.2	Requirements	147
37.3	Parameters	148
37.4	Notes	148
37.5	Examples	148
37.6	Return Values	149
37.7	Status	149
37.8	Authors	149
38	fortios_firewall_dnstranslation – Configure DNS translation in Fortinet’s FortiOS and FortiGate.	151
38.1	Synopsis	151
38.2	Requirements	151
38.3	Parameters	152
38.4	Notes	152
38.5	Examples	152
38.6	Return Values	152
38.7	Status	152
38.8	Authors	152
39	fortios_firewall_dos_policy – Configure IPv4 DoS policies in Fortinet’s FortiOS and FortiGate.	155
39.1	Synopsis	155
39.2	Requirements	155
39.3	Parameters	156
39.4	Notes	156
39.5	Examples	156
39.6	Return Values	157
39.7	Status	157
39.8	Authors	157
40	fortios_firewall_dos_policy6 – Configure IPv6 DoS policies in Fortinet’s FortiOS and FortiGate.	159
40.1	Synopsis	159
40.2	Requirements	159
40.3	Parameters	160
40.4	Notes	160
40.5	Examples	160
40.6	Return Values	161
40.7	Status	161
40.8	Authors	161
41	fortios_firewall_identity_based_route – Configure identity based routing in Fortinet’s FortiOS and FortiGate.	163
41.1	Synopsis	163
41.2	Requirements	163
41.3	Parameters	164

41.4	Notes	164
41.5	Examples	164
41.6	Return Values	164
41.7	Status	164
41.8	Authors	165
42	fortios_firewall_interface_policy – Configure IPv4 interface policies in Fortinet’s FortiOS and FortiGate.	167
42.1	Synopsis	167
42.2	Requirements	167
42.3	Parameters	168
42.4	Notes	168
42.5	Examples	168
42.6	Return Values	169
42.7	Status	169
42.8	Authors	169
43	fortios_firewall_interface_policy6 – Configure IPv6 interface policies in Fortinet’s FortiOS and FortiGate.	171
43.1	Synopsis	171
43.2	Requirements	171
43.3	Parameters	172
43.4	Notes	172
43.5	Examples	172
43.6	Return Values	173
43.7	Status	173
43.8	Authors	173
44	fortios_firewall_internet_service – Show Internet Service application in Fortinet’s FortiOS and FortiGate.	175
44.1	Synopsis	175
44.2	Requirements	175
44.3	Parameters	176
44.4	Notes	176
44.5	Examples	176
44.6	Return Values	176
44.7	Status	177
44.8	Authors	177
45	fortios_firewall_internet_service_custom – Configure custom Internet Services in Fortinet’s FortiOS and FortiGate.	179
45.1	Synopsis	179
45.2	Requirements	179
45.3	Parameters	180
45.4	Notes	180
45.5	Examples	180
45.6	Return Values	181
45.7	Status	181
45.8	Authors	181
46	fortios_firewall_internet_service_custom_group – Configure custom Internet Service group in Fortinet’s FortiOS and FortiGate.	183
46.1	Synopsis	183
46.2	Requirements	183
46.3	Parameters	184
46.4	Notes	184

46.5	Examples	184
46.6	Return Values	184
46.7	Status	184
46.8	Authors	184
47	fortios_firewall_internet_service_group – Configure group of Internet Service in Fortinet’s FortiOS and FortiGate.	187
47.1	Synopsis	187
47.2	Requirements	187
47.3	Parameters	188
47.4	Notes	188
47.5	Examples	188
47.6	Return Values	188
47.7	Status	188
47.8	Authors	188
48	fortios_firewall_ip_translation – Configure firewall IP-translation in Fortinet’s FortiOS and FortiGate.	191
48.1	Synopsis	191
48.2	Requirements	191
48.3	Parameters	192
48.4	Notes	192
48.5	Examples	192
48.6	Return Values	192
48.7	Status	192
48.8	Authors	192
49	fortios_firewall_ipmacbinding_setting – Configure IP to MAC binding settings in Fortinet’s FortiOS and FortiGate.	195
49.1	Synopsis	195
49.2	Requirements	195
49.3	Parameters	196
49.4	Notes	196
49.5	Examples	196
49.6	Return Values	196
49.7	Status	196
49.8	Authors	196
50	fortios_firewall_ipmacbinding_table – Configure IP to MAC address pairs in the IP/MAC binding table in Fortinet’s FortiOS and FortiGate.	199
50.1	Synopsis	199
50.2	Requirements	199
50.3	Parameters	200
50.4	Notes	200
50.5	Examples	200
50.6	Return Values	200
50.7	Status	200
50.8	Authors	200
51	fortios_firewall_ippool – Configure IPv4 IP pools in Fortinet’s FortiOS and FortiGate.	203
51.1	Synopsis	203
51.2	Requirements	203
51.3	Parameters	204
51.4	Notes	204
51.5	Examples	204
51.6	Return Values	204

51.7	Status	204
51.8	Authors	205
52	fortios_firewall_ippool6 – Configure IPv6 IP pools in Fortinet’s FortiOS and FortiGate.	207
52.1	Synopsis	207
52.2	Requirements	207
52.3	Parameters	208
52.4	Notes	208
52.5	Examples	208
52.6	Return Values	208
52.7	Status	208
52.8	Authors	208
53	fortios_firewall_ipv6_eh_filter – Configure IPv6 extension header filter in Fortinet’s FortiOS and FortiGate.	211
53.1	Synopsis	211
53.2	Requirements	211
53.3	Parameters	212
53.4	Notes	212
53.5	Examples	212
53.6	Return Values	212
53.7	Status	212
53.8	Authors	212
54	fortios_firewall_ldb_monitor – Configure server load balancing health monitors in Fortinet’s FortiOS and FortiGate.	215
54.1	Synopsis	215
54.2	Requirements	215
54.3	Parameters	216
54.4	Notes	216
54.5	Examples	216
54.6	Return Values	216
54.7	Status	216
54.8	Authors	217
55	fortios_firewall_local_in_policy – Configure user defined IPv4 local-in policies in Fortinet’s FortiOS and FortiGate.	219
55.1	Synopsis	219
55.2	Requirements	219
55.3	Parameters	220
55.4	Notes	220
55.5	Examples	220
55.6	Return Values	220
55.7	Status	221
55.8	Authors	221
56	fortios_firewall_local_in_policy6 – Configure user defined IPv6 local-in policies in Fortinet’s FortiOS and FortiGate.	223
56.1	Synopsis	223
56.2	Requirements	223
56.3	Parameters	224
56.4	Notes	224
56.5	Examples	224
56.6	Return Values	224
56.7	Status	225

56.8	Authors	225
57	fortios_firewall_multicast_address – Configure multicast addresses in Fortinet’s FortiOS and FortiGate.	227
57.1	Synopsis	227
57.2	Requirements	227
57.3	Parameters	228
57.4	Notes	228
57.5	Examples	228
57.6	Return Values	228
57.7	Status	229
57.8	Authors	229
58	fortios_firewall_multicast_address6 – Configure IPv6 multicast address in Fortinet’s FortiOS and FortiGate.	231
58.1	Synopsis	231
58.2	Requirements	231
58.3	Parameters	232
58.4	Notes	232
58.5	Examples	232
58.6	Return Values	232
58.7	Status	232
58.8	Authors	233
59	fortios_firewall_multicast_policy – Configure multicast NAT policies in Fortinet’s FortiOS and FortiGate.	235
59.1	Synopsis	235
59.2	Requirements	235
59.3	Parameters	236
59.4	Notes	236
59.5	Examples	236
59.6	Return Values	236
59.7	Status	237
59.8	Authors	237
60	fortios_firewall_multicast_policy6 – Configure IPv6 multicast NAT policies in Fortinet’s FortiOS and FortiGate.	239
60.1	Synopsis	239
60.2	Requirements	239
60.3	Parameters	240
60.4	Notes	240
60.5	Examples	240
60.6	Return Values	240
60.7	Status	241
60.8	Authors	241
61	fortios_firewall_policy – Configure IPv4 policies in Fortinet’s FortiOS and FortiGate.	243
61.1	Synopsis	243
61.2	Requirements	243
61.3	Parameters	244
61.4	Notes	244
61.5	Examples	244
61.6	Return Values	247
61.7	Status	247
61.8	Authors	247

62	fortios_firewall_policy46 – Configure IPv4 to IPv6 policies in Fortinet’s FortiOS and FortiGate.	249
62.1	Synopsis	249
62.2	Requirements	249
62.3	Parameters	250
62.4	Notes	250
62.5	Examples	250
62.6	Return Values	251
62.7	Status	251
62.8	Authors	251
63	fortios_firewall_policy6 – Configure IPv6 policies in Fortinet’s FortiOS and FortiGate.	253
63.1	Synopsis	253
63.2	Requirements	253
63.3	Parameters	254
63.4	Notes	254
63.5	Examples	254
63.6	Return Values	256
63.7	Status	256
63.8	Authors	256
64	fortios_firewall_policy64 – Configure IPv6 to IPv4 policies in Fortinet’s FortiOS and FortiGate.	259
64.1	Synopsis	259
64.2	Requirements	259
64.3	Parameters	260
64.4	Notes	260
64.5	Examples	260
64.6	Return Values	261
64.7	Status	261
64.8	Authors	261
65	fortios_firewall_profile_group – Configure profile groups in Fortinet’s FortiOS and FortiGate.	263
65.1	Synopsis	263
65.2	Requirements	263
65.3	Parameters	264
65.4	Notes	264
65.5	Examples	264
65.6	Return Values	264
65.7	Status	265
65.8	Authors	265
66	fortios_firewall_profile_protocol_options – Configure protocol options in Fortinet’s FortiOS and FortiGate.	267
66.1	Synopsis	267
66.2	Requirements	267
66.3	Parameters	268
66.4	Notes	268
66.5	Examples	268
66.6	Return Values	270
66.7	Status	270
66.8	Authors	270
67	fortios_firewall_proxy_address – Web proxy address configuration in Fortinet’s FortiOS and FortiGate.	271
67.1	Synopsis	271
67.2	Requirements	271
67.3	Parameters	272

67.4	Notes	272
67.5	Examples	272
67.6	Return Values	273
67.7	Status	273
67.8	Authors	273
68	fortios_firewall_proxy_addrgrp – Web proxy address group configuration in Fortinet’s FortiOS and FortiGate.	275
68.1	Synopsis	275
68.2	Requirements	275
68.3	Parameters	276
68.4	Notes	276
68.5	Examples	276
68.6	Return Values	276
68.7	Status	277
68.8	Authors	277
69	fortios_firewall_proxy_policy – Configure proxy policies in Fortinet’s FortiOS and FortiGate.	279
69.1	Synopsis	279
69.2	Requirements	279
69.3	Parameters	280
69.4	Notes	280
69.5	Examples	280
69.6	Return Values	282
69.7	Status	282
69.8	Authors	282
70	fortios_firewall_schedule_group – Schedule group configuration in Fortinet’s FortiOS and FortiGate.	283
70.1	Synopsis	283
70.2	Requirements	283
70.3	Parameters	284
70.4	Notes	284
70.5	Examples	284
70.6	Return Values	284
70.7	Status	284
70.8	Authors	284
71	fortios_firewall_schedule_onetime – Onetime schedule configuration in Fortinet’s FortiOS and FortiGate.	287
71.1	Synopsis	287
71.2	Requirements	287
71.3	Parameters	288
71.4	Notes	288
71.5	Examples	288
71.6	Return Values	288
71.7	Status	288
71.8	Authors	288
72	fortios_firewall_schedule_recurring – Recurring schedule configuration in Fortinet’s FortiOS and FortiGate.	291
72.1	Synopsis	291
72.2	Requirements	291
72.3	Parameters	292
72.4	Notes	292
72.5	Examples	292

72.6	Return Values	292
72.7	Status	292
72.8	Authors	292
73	fortios_firewall_service_category – Configure service categories in Fortinet’s FortiOS and FortiGate.	295
73.1	Synopsis	295
73.2	Requirements	295
73.3	Parameters	296
73.4	Notes	296
73.5	Examples	296
73.6	Return Values	296
73.7	Status	296
73.8	Authors	296
74	fortios_firewall_service_custom – Configure custom services in Fortinet’s FortiOS and FortiGate.	299
74.1	Synopsis	299
74.2	Requirements	299
74.3	Parameters	300
74.4	Notes	300
74.5	Examples	300
74.6	Return Values	301
74.7	Status	301
74.8	Authors	301
75	fortios_firewall_service_group – Configure service groups in Fortinet’s FortiOS and FortiGate.	303
75.1	Synopsis	303
75.2	Requirements	303
75.3	Parameters	304
75.4	Notes	304
75.5	Examples	304
75.6	Return Values	304
75.7	Status	304
75.8	Authors	304
76	fortios_firewall_shaper_per_ip_shaper – Configure per-IP traffic shaper in Fortinet’s FortiOS and FortiGate.	307
76.1	Synopsis	307
76.2	Requirements	307
76.3	Parameters	308
76.4	Notes	308
76.5	Examples	308
76.6	Return Values	308
76.7	Status	308
76.8	Authors	308
77	fortios_firewall_shaper_traffic_shaper – Configure shared traffic shaper in Fortinet’s FortiOS and FortiGate.	311
77.1	Synopsis	311
77.2	Requirements	311
77.3	Parameters	312
77.4	Notes	312
77.5	Examples	312
77.6	Return Values	312
77.7	Status	312
77.8	Authors	312

78	fortios_firewall_shaping_policy – Configure shaping policies in Fortinet’s FortiOS and FortiGate.	315
78.1	Synopsis	315
78.2	Requirements	315
78.3	Parameters	316
78.4	Notes	316
78.5	Examples	316
78.6	Return Values	317
78.7	Status	317
78.8	Authors	317
79	fortios_firewall_shaping_profile – Configure shaping profiles in Fortinet’s FortiOS and FortiGate.	319
79.1	Synopsis	319
79.2	Requirements	319
79.3	Parameters	320
79.4	Notes	320
79.5	Examples	320
79.6	Return Values	320
79.7	Status	320
79.8	Authors	321
80	fortios_firewall_sniffer – Configure sniffer in Fortinet’s FortiOS and FortiGate.	323
80.1	Synopsis	323
80.2	Requirements	323
80.3	Parameters	324
80.4	Notes	324
80.5	Examples	324
80.6	Return Values	325
80.7	Status	325
80.8	Authors	325
81	fortios_firewall_ssh_host_key – SSH proxy host public keys in Fortinet’s FortiOS and FortiGate.	327
81.1	Synopsis	327
81.2	Requirements	327
81.3	Parameters	328
81.4	Notes	328
81.5	Examples	328
81.6	Return Values	328
81.7	Status	328
81.8	Authors	328
82	fortios_firewall_ssh_local_ca – SSH proxy local CA in Fortinet’s FortiOS and FortiGate.	331
82.1	Synopsis	331
82.2	Requirements	331
82.3	Parameters	332
82.4	Notes	332
82.5	Examples	332
82.6	Return Values	332
82.7	Status	332
82.8	Authors	332
83	fortios_firewall_ssh_local_key – SSH proxy local keys in Fortinet’s FortiOS and FortiGate.	335
83.1	Synopsis	335
83.2	Requirements	335
83.3	Parameters	336
83.4	Notes	336

83.5	Examples	336
83.6	Return Values	336
83.7	Status	336
83.8	Authors	336
84	fortios_firewall_ssh_setting – SSH proxy settings in Fortinet’s FortiOS and FortiGate.	339
84.1	Synopsis	339
84.2	Requirements	339
84.3	Parameters	340
84.4	Notes	340
84.5	Examples	340
84.6	Return Values	340
84.7	Status	340
84.8	Authors	340
85	fortios_firewall_ssl_server – Configure SSL servers in Fortinet’s FortiOS and FortiGate.	343
85.1	Synopsis	343
85.2	Requirements	343
85.3	Parameters	344
85.4	Notes	344
85.5	Examples	344
85.6	Return Values	344
85.7	Status	344
85.8	Authors	345
86	fortios_firewall_ssl_setting – SSL proxy settings in Fortinet’s FortiOS and FortiGate.	347
86.1	Synopsis	347
86.2	Requirements	347
86.3	Parameters	348
86.4	Notes	348
86.5	Examples	348
86.6	Return Values	348
86.7	Status	348
86.8	Authors	349
87	fortios_firewall_ssl_ssh_profile – Configure SSL/SSH protocol options in Fortinet’s FortiOS and FortiGate.	351
87.1	Synopsis	351
87.2	Requirements	351
87.3	Parameters	352
87.4	Notes	352
87.5	Examples	352
87.6	Return Values	354
87.7	Status	354
87.8	Authors	354
88	fortios_firewall_ttl_policy – Configure TTL policies in Fortinet’s FortiOS and FortiGate.	355
88.1	Synopsis	355
88.2	Requirements	355
88.3	Parameters	356
88.4	Notes	356
88.5	Examples	356
88.6	Return Values	356
88.7	Status	357
88.8	Authors	357

89	fortios_firewall_vip – Configure virtual IP for IPv4 in Fortinet’s FortiOS and FortiGate.	359
89.1	Synopsis	359
89.2	Requirements	359
89.3	Parameters	360
89.4	Notes	360
89.5	Examples	360
89.6	Return Values	362
89.7	Status	362
89.8	Authors	362
90	fortios_firewall_vip46 – Configure IPv4 to IPv6 virtual IPs in Fortinet’s FortiOS and FortiGate.	365
90.1	Synopsis	365
90.2	Requirements	365
90.3	Parameters	366
90.4	Notes	366
90.5	Examples	366
90.6	Return Values	367
90.7	Status	367
90.8	Authors	367
91	fortios_firewall_vip6 – Configure virtual IP for IPv6 in Fortinet’s FortiOS and FortiGate.	369
91.1	Synopsis	369
91.2	Requirements	369
91.3	Parameters	370
91.4	Notes	370
91.5	Examples	370
91.6	Return Values	372
91.7	Status	372
91.8	Authors	372
92	fortios_firewall_vip64 – Configure IPv6 to IPv4 virtual IPs in Fortinet’s FortiOS and FortiGate.	373
92.1	Synopsis	373
92.2	Requirements	373
92.3	Parameters	374
92.4	Notes	374
92.5	Examples	374
92.6	Return Values	375
92.7	Status	375
92.8	Authors	375
93	fortios_firewall_vipgrp – Configure IPv4 virtual IP groups in Fortinet’s FortiOS and FortiGate.	377
93.1	Synopsis	377
93.2	Requirements	377
93.3	Parameters	378
93.4	Notes	378
93.5	Examples	378
93.6	Return Values	378
93.7	Status	378
93.8	Authors	378
94	fortios_firewall_vipgrp46 – Configure IPv4 to IPv6 virtual IP groups in Fortinet’s FortiOS and FortiGate.	381
94.1	Synopsis	381
94.2	Requirements	381
94.3	Parameters	382

94.4	Notes	382
94.5	Examples	382
94.6	Return Values	382
94.7	Status	382
94.8	Authors	382
95	fortios_firewall_vipgrp6 – Configure IPv6 virtual IP groups in Fortinet’s FortiOS and FortiGate.	385
95.1	Synopsis	385
95.2	Requirements	385
95.3	Parameters	386
95.4	Notes	386
95.5	Examples	386
95.6	Return Values	386
95.7	Status	386
95.8	Authors	386
96	fortios_firewall_vipgrp64 – Configure IPv6 to IPv4 virtual IP groups in Fortinet’s FortiOS and FortiGate.	389
96.1	Synopsis	389
96.2	Requirements	389
96.3	Parameters	390
96.4	Notes	390
96.5	Examples	390
96.6	Return Values	390
96.7	Status	390
96.8	Authors	390
97	fortios_firewall_wildcard_fqdn_custom – Config global/VDOM Wildcard FQDN address in Fortinet’s FortiOS and FortiGate.	393
97.1	Synopsis	393
97.2	Requirements	393
97.3	Parameters	394
97.4	Notes	394
97.5	Examples	394
97.6	Return Values	394
97.7	Status	394
97.8	Authors	394
98	fortios_firewall_wildcard_fqdn_group – Config global Wildcard FQDN address groups in Fortinet’s FortiOS and FortiGate.	397
98.1	Synopsis	397
98.2	Requirements	397
98.3	Parameters	398
98.4	Notes	398
98.5	Examples	398
98.6	Return Values	398
98.7	Status	398
98.8	Authors	398
99	fortios_ftp_proxy_explicit – Configure explicit FTP proxy settings in Fortinet’s FortiOS and FortiGate.	401
99.1	Synopsis	401
99.2	Requirements	401
99.3	Parameters	402
99.4	Notes	402
99.5	Examples	402

99.6	Return Values	402
99.7	Status	402
99.8	Authors	402
100	fortios_icap_profile – Configure ICAP profiles in Fortinet’s FortiOS and FortiGate.	405
100.1	Synopsis	405
100.2	Requirements	405
100.3	Parameters	406
100.4	Notes	406
100.5	Examples	406
100.6	Return Values	406
100.7	Status	406
100.8	Authors	407
101	fortios_icap_server – Configure ICAP servers in Fortinet’s FortiOS and FortiGate.	409
101.1	Synopsis	409
101.2	Requirements	409
101.3	Parameters	410
101.4	Notes	410
101.5	Examples	410
101.6	Return Values	410
101.7	Status	410
101.8	Authors	410
102	fortios_ips_custom – Configure IPS custom signature in Fortinet’s FortiOS and FortiGate.	413
102.1	Synopsis	413
102.2	Requirements	413
102.3	Parameters	414
102.4	Notes	414
102.5	Examples	414
102.6	Return Values	414
102.7	Status	414
102.8	Authors	415
103	fortios_ips_decoder – Configure IPS decoder in Fortinet’s FortiOS and FortiGate.	417
103.1	Synopsis	417
103.2	Requirements	417
103.3	Parameters	418
103.4	Notes	418
103.5	Examples	418
103.6	Return Values	418
103.7	Status	418
103.8	Authors	418
104	fortios_ips_global – Configure IPS global parameter in Fortinet’s FortiOS and FortiGate.	421
104.1	Synopsis	421
104.2	Requirements	421
104.3	Parameters	422
104.4	Notes	422
104.5	Examples	422
104.6	Return Values	422
104.7	Status	422
104.8	Authors	423
105	fortios_ips_rule – Configure IPS rules in Fortinet’s FortiOS and FortiGate.	425

105.1 Synopsis	425
105.2 Requirements	425
105.3 Parameters	426
105.4 Notes	426
105.5 Examples	426
105.6 Return Values	426
105.7 Status	427
105.8 Authors	427
106fortios_ips_rule_settings – Configure IPS rule setting in Fortinet’s FortiOS and FortiGate.	429
106.1 Synopsis	429
106.2 Requirements	429
106.3 Parameters	430
106.4 Notes	430
106.5 Examples	430
106.6 Return Values	430
106.7 Status	430
106.8 Authors	430
107fortios_ips_sensor – Configure IPS sensor in Fortinet’s FortiOS and FortiGate.	433
107.1 Synopsis	433
107.2 Requirements	433
107.3 Parameters	434
107.4 Notes	434
107.5 Examples	434
107.6 Return Values	435
107.7 Status	435
107.8 Authors	435
108fortios_ips_settings – Configure IPS VDOM parameter in Fortinet’s FortiOS and FortiGate.	437
108.1 Synopsis	437
108.2 Requirements	437
108.3 Parameters	438
108.4 Notes	438
108.5 Examples	438
108.6 Return Values	438
108.7 Status	438
108.8 Authors	438
109fortios_log_custom_field – Configure custom log fields in Fortinet’s FortiOS and FortiGate.	441
109.1 Synopsis	441
109.2 Requirements	441
109.3 Parameters	442
109.4 Notes	442
109.5 Examples	442
109.6 Return Values	442
109.7 Status	442
109.8 Authors	442
110fortios_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.	445
110.1 Synopsis	445
110.2 Requirements	445
110.3 Parameters	446
110.4 Notes	446

110.5 Examples	446
110.6 Return Values	447
110.7 Status	447
110.8 Authors	447
111fortios_log_disk_setting – Settings for local disk logging in Fortinet’s FortiOS and FortiGate.	449
111.1 Synopsis	449
111.2 Requirements	449
111.3 Parameters	450
111.4 Notes	450
111.5 Examples	450
111.6 Return Values	451
111.7 Status	451
111.8 Authors	451
112fortios_log_eventfilter – Configure log event filters in Fortinet’s FortiOS and FortiGate.	453
112.1 Synopsis	453
112.2 Requirements	453
112.3 Parameters	454
112.4 Notes	454
112.5 Examples	454
112.6 Return Values	454
112.7 Status	454
112.8 Authors	455
113fortios_log_fortianalyzer2_filter – Filters for FortiAnalyzer in Fortinet’s FortiOS and FortiGate.	457
113.1 Synopsis	457
113.2 Requirements	457
113.3 Parameters	458
113.4 Notes	458
113.5 Examples	458
113.6 Return Values	458
113.7 Status	458
113.8 Authors	459
114fortios_log_fortianalyzer2_setting – Global FortiAnalyzer settings in Fortinet’s FortiOS and FortiGate.	461
114.1 Synopsis	461
114.2 Requirements	461
114.3 Parameters	462
114.4 Notes	462
114.5 Examples	462
114.6 Return Values	462
114.7 Status	463
114.8 Authors	463
115fortios_log_fortianalyzer3_filter – Filters for FortiAnalyzer in Fortinet’s FortiOS and FortiGate.	465
115.1 Synopsis	465
115.2 Requirements	465
115.3 Parameters	466
115.4 Notes	466
115.5 Examples	466
115.6 Return Values	466
115.7 Status	466
115.8 Authors	467

116	fortios_log_fortianalyzer3_setting – Global FortiAnalyzer settings in Fortinet’s FortiOS and FortiGate.	469
116.1	Synopsis	469
116.2	Requirements	469
116.3	Parameters	470
116.4	Notes	470
116.5	Examples	470
116.6	Return Values	470
116.7	Status	471
116.8	Authors	471
117	fortios_log_fortianalyzer_filter – Filters for FortiAnalyzer in Fortinet’s FortiOS and FortiGate.	473
117.1	Synopsis	473
117.2	Requirements	473
117.3	Parameters	474
117.4	Notes	474
117.5	Examples	474
117.6	Return Values	474
117.7	Status	474
117.8	Authors	475
118	fortios_log_fortianalyzer_override_filter – Override filters for FortiAnalyzer in Fortinet’s FortiOS and FortiGate.	477
118.1	Synopsis	477
118.2	Requirements	477
118.3	Parameters	478
118.4	Notes	478
118.5	Examples	478
118.6	Return Values	478
118.7	Status	478
118.8	Authors	479
119	fortios_log_fortianalyzer_override_setting – Override FortiAnalyzer settings in Fortinet’s FortiOS and FortiGate.	481
119.1	Synopsis	481
119.2	Requirements	481
119.3	Parameters	482
119.4	Notes	482
119.5	Examples	482
119.6	Return Values	482
119.7	Status	483
119.8	Authors	483
120	fortios_log_fortianalyzer_setting – Global FortiAnalyzer settings in Fortinet’s FortiOS and FortiGate.	485
120.1	Synopsis	485
120.2	Requirements	485
120.3	Parameters	486
120.4	Notes	486
120.5	Examples	486
120.6	Return Values	486
120.7	Status	487
120.8	Authors	487
121	fortios_log_fortiguard_filter – Filters for FortiCloud in Fortinet’s FortiOS and FortiGate.	489
121.1	Synopsis	489
121.2	Requirements	489

121.3 Parameters	490
121.4 Notes	490
121.5 Examples	490
121.6 Return Values	490
121.7 Status	490
121.8 Authors	491
122fortios_log_fortiguard_override_filter – Override filters for FortiCloud in Fortinet’s FortiOS and FortiGate.	493
122.1 Synopsis	493
122.2 Requirements	493
122.3 Parameters	494
122.4 Notes	494
122.5 Examples	494
122.6 Return Values	494
122.7 Status	494
122.8 Authors	495
123fortios_log_fortiguard_override_setting – Override global FortiCloud logging settings for this VDOM in Fortinet’s FortiOS and FortiGate.	497
123.1 Synopsis	497
123.2 Requirements	497
123.3 Parameters	498
123.4 Notes	498
123.5 Examples	498
123.6 Return Values	498
123.7 Status	498
123.8 Authors	498
124fortios_log_fortiguard_setting – Configure logging to FortiCloud in Fortinet’s FortiOS and FortiGate.	501
124.1 Synopsis	501
124.2 Requirements	501
124.3 Parameters	502
124.4 Notes	502
124.5 Examples	502
124.6 Return Values	502
124.7 Status	502
124.8 Authors	502
125fortios_log_gui_display – Configure how log messages are displayed on the GUI in Fortinet’s FortiOS and FortiGate.	505
125.1 Synopsis	505
125.2 Requirements	505
125.3 Parameters	506
125.4 Notes	506
125.5 Examples	506
125.6 Return Values	506
125.7 Status	506
125.8 Authors	506
126fortios_log_memory_filter – Filters for memory buffer in Fortinet’s FortiOS and FortiGate.	509
126.1 Synopsis	509
126.2 Requirements	509
126.3 Parameters	510
126.4 Notes	510

126.5 Examples	510
126.6 Return Values	511
126.7 Status	511
126.8 Authors	511
127fortios_log_memory_global_setting – Global settings for memory logging in Fortinet’s FortiOS and FortiGate.	513
127.1 Synopsis	513
127.2 Requirements	513
127.3 Parameters	514
127.4 Notes	514
127.5 Examples	514
127.6 Return Values	514
127.7 Status	514
127.8 Authors	514
128fortios_log_memory_setting – Settings for memory buffer in Fortinet’s FortiOS and FortiGate.	517
128.1 Synopsis	517
128.2 Requirements	517
128.3 Parameters	518
128.4 Notes	518
128.5 Examples	518
128.6 Return Values	518
128.7 Status	518
128.8 Authors	518
129fortios_log_null_device_filter – Filters for null device logging in Fortinet’s FortiOS and FortiGate.	521
129.1 Synopsis	521
129.2 Requirements	521
129.3 Parameters	522
129.4 Notes	522
129.5 Examples	522
129.6 Return Values	522
129.7 Status	522
129.8 Authors	523
130fortios_log_null_device_setting – Settings for null device logging in Fortinet’s FortiOS and FortiGate.	525
130.1 Synopsis	525
130.2 Requirements	525
130.3 Parameters	526
130.4 Notes	526
130.5 Examples	526
130.6 Return Values	526
130.7 Status	526
130.8 Authors	526
131fortios_log_setting – Configure general log settings in Fortinet’s FortiOS and FortiGate.	529
131.1 Synopsis	529
131.2 Requirements	529
131.3 Parameters	530
131.4 Notes	530
131.5 Examples	530
131.6 Return Values	530
131.7 Status	531
131.8 Authors	531

132fortios_log_syslogd2_filter – Filters for remote system server in Fortinet’s FortiOS and FortiGate.	533
132.1 Synopsis	533
132.2 Requirements	533
132.3 Parameters	534
132.4 Notes	534
132.5 Examples	534
132.6 Return Values	534
132.7 Status	534
132.8 Authors	535
133fortios_log_syslogd2_setting – Global settings for remote syslog server in Fortinet’s FortiOS and FortiGate.	537
133.1 Synopsis	537
133.2 Requirements	537
133.3 Parameters	538
133.4 Notes	538
133.5 Examples	538
133.6 Return Values	538
133.7 Status	538
133.8 Authors	539
134fortios_log_syslogd3_filter – Filters for remote system server in Fortinet’s FortiOS and FortiGate.	541
134.1 Synopsis	541
134.2 Requirements	541
134.3 Parameters	542
134.4 Notes	542
134.5 Examples	542
134.6 Return Values	542
134.7 Status	542
134.8 Authors	543
135fortios_log_syslogd3_setting – Global settings for remote syslog server in Fortinet’s FortiOS and FortiGate.	545
135.1 Synopsis	545
135.2 Requirements	545
135.3 Parameters	546
135.4 Notes	546
135.5 Examples	546
135.6 Return Values	546
135.7 Status	546
135.8 Authors	547
136fortios_log_syslogd4_filter – Filters for remote system server in Fortinet’s FortiOS and FortiGate.	549
136.1 Synopsis	549
136.2 Requirements	549
136.3 Parameters	550
136.4 Notes	550
136.5 Examples	550
136.6 Return Values	550
136.7 Status	550
136.8 Authors	551
137fortios_log_syslogd4_setting – Global settings for remote syslog server in Fortinet’s FortiOS and FortiGate.	553
137.1 Synopsis	553

137.2	Requirements	553
137.3	Parameters	554
137.4	Notes	554
137.5	Examples	554
137.6	Return Values	554
137.7	Status	554
137.8	Authors	555
138	fortios_log_syslogd_filter – Filters for remote system server in Fortinet’s FortiOS and FortiGate.	557
138.1	Synopsis	557
138.2	Requirements	557
138.3	Parameters	558
138.4	Notes	558
138.5	Examples	558
138.6	Return Values	558
138.7	Status	558
138.8	Authors	559
139	fortios_log_syslogd_override_filter – Override filters for remote system server in Fortinet’s FortiOS and FortiGate.	561
139.1	Synopsis	561
139.2	Requirements	561
139.3	Parameters	562
139.4	Notes	562
139.5	Examples	562
139.6	Return Values	562
139.7	Status	562
139.8	Authors	563
140	fortios_log_syslogd_override_setting – Override settings for remote syslog server in Fortinet’s FortiOS and FortiGate.	565
140.1	Synopsis	565
140.2	Requirements	565
140.3	Parameters	566
140.4	Notes	566
140.5	Examples	566
140.6	Return Values	566
140.7	Status	566
140.8	Authors	567
141	fortios_log_syslogd_setting – Global settings for remote syslog server in Fortinet’s FortiOS and FortiGate.	569
141.1	Synopsis	569
141.2	Requirements	569
141.3	Parameters	570
141.4	Notes	570
141.5	Examples	570
141.6	Return Values	570
141.7	Status	570
141.8	Authors	571
142	fortios_log_threat_weight – Configure threat weight settings in Fortinet’s FortiOS and FortiGate.	573
142.1	Synopsis	573
142.2	Requirements	573
142.3	Parameters	574

142.4 Notes	574
142.5 Examples	574
142.6 Return Values	575
142.7 Status	575
142.8 Authors	575
143fortios_log_webtrends_filter – Filters for WebTrends in Fortinet’s FortiOS and FortiGate.	577
143.1 Synopsis	577
143.2 Requirements	577
143.3 Parameters	578
143.4 Notes	578
143.5 Examples	578
143.6 Return Values	578
143.7 Status	578
143.8 Authors	579
144fortios_log_webtrends_setting – Settings for WebTrends in Fortinet’s FortiOS and FortiGate.	581
144.1 Synopsis	581
144.2 Requirements	581
144.3 Parameters	582
144.4 Notes	582
144.5 Examples	582
144.6 Return Values	582
144.7 Status	582
144.8 Authors	582
145fortios_registration_forticare – Add a FortiCare license in Fortinet’s FortiOS and FortiGate.	585
145.1 Synopsis	585
145.2 Requirements	585
145.3 Parameters	586
145.4 Notes	586
145.5 Examples	586
145.6 Return Values	586
145.7 Status	586
145.8 Authors	586
146fortios_registration_vdom – Add a VDOM license in Fortinet’s FortiOS and FortiGate.	589
146.1 Synopsis	589
146.2 Requirements	589
146.3 Parameters	590
146.4 Notes	590
146.5 Examples	590
146.6 Return Values	590
146.7 Status	590
146.8 Authors	590
147fortios_report_chart – Report chart widget configuration in Fortinet’s FortiOS and FortiGate.	593
147.1 Synopsis	593
147.2 Requirements	593
147.3 Parameters	594
147.4 Notes	594
147.5 Examples	594
147.6 Return Values	595
147.7 Status	595
147.8 Authors	596

148fortios_report_dataset – Report dataset configuration in Fortinet’s FortiOS and FortiGate.	597
148.1 Synopsis	597
148.2 Requirements	597
148.3 Parameters	598
148.4 Notes	598
148.5 Examples	598
148.6 Return Values	598
148.7 Status	599
148.8 Authors	599
149fortios_report_layout – Report layout configuration in Fortinet’s FortiOS and FortiGate.	601
149.1 Synopsis	601
149.2 Requirements	601
149.3 Parameters	602
149.4 Notes	602
149.5 Examples	602
149.6 Return Values	603
149.7 Status	604
149.8 Authors	604
150fortios_report_setting – Report setting configuration in Fortinet’s FortiOS and FortiGate.	605
150.1 Synopsis	605
150.2 Requirements	605
150.3 Parameters	606
150.4 Notes	606
150.5 Examples	606
150.6 Return Values	606
150.7 Status	606
150.8 Authors	606
151fortios_report_style – Report style configuration in Fortinet’s FortiOS and FortiGate.	609
151.1 Synopsis	609
151.2 Requirements	609
151.3 Parameters	610
151.4 Notes	610
151.5 Examples	610
151.6 Return Values	611
151.7 Status	611
151.8 Authors	611
152fortios_report_theme – Report themes configuratio in Fortinet’s FortiOS and FortiGate.	613
152.1 Synopsis	613
152.2 Requirements	613
152.3 Parameters	614
152.4 Notes	614
152.5 Examples	614
152.6 Return Values	615
152.7 Status	615
152.8 Authors	615
153fortios_router_access_list – Configure access lists in Fortinet’s FortiOS and FortiGate.	617
153.1 Synopsis	617
153.2 Requirements	617
153.3 Parameters	618
153.4 Notes	618

153.5 Examples	618
153.6 Return Values	618
153.7 Status	618
153.8 Authors	619
154fortios_router_access_list6 – Configure IPv6 access lists in Fortinet’s FortiOS and FortiGate.	621
154.1 Synopsis	621
154.2 Requirements	621
154.3 Parameters	622
154.4 Notes	622
154.5 Examples	622
154.6 Return Values	622
154.7 Status	622
154.8 Authors	623
155fortios_router_aspath_list – Configure Autonomous System (AS) path lists in Fortinet’s FortiOS and FortiGate.	625
155.1 Synopsis	625
155.2 Requirements	625
155.3 Parameters	626
155.4 Notes	626
155.5 Examples	626
155.6 Return Values	626
155.7 Status	626
155.8 Authors	626
156fortios_router_auth_path – Configure authentication based routing in Fortinet’s FortiOS and FortiGate.	629
156.1 Synopsis	629
156.2 Requirements	629
156.3 Parameters	630
156.4 Notes	630
156.5 Examples	630
156.6 Return Values	630
156.7 Status	630
156.8 Authors	630
157fortios_router_bfd – Configure BFD in Fortinet’s FortiOS and FortiGate.	633
157.1 Synopsis	633
157.2 Requirements	633
157.3 Parameters	634
157.4 Notes	634
157.5 Examples	634
157.6 Return Values	634
157.7 Status	634
157.8 Authors	634
158fortios_router_bfd6 – Configure IPv6 BFD in Fortinet’s FortiOS and FortiGate.	637
158.1 Synopsis	637
158.2 Requirements	637
158.3 Parameters	638
158.4 Notes	638
158.5 Examples	638
158.6 Return Values	638
158.7 Status	638
158.8 Authors	638

159	fortios_router_bgp – Configure BGP in Fortinet’s FortiOS and FortiGate.	641
159.1	Synopsis	641
159.2	Requirements	641
159.3	Parameters	642
159.4	Notes	642
159.5	Examples	642
159.6	Return Values	647
159.7	Status	647
159.8	Authors	647
160	fortios_router_community_list – Configure community lists in Fortinet’s FortiOS and FortiGate.	649
160.1	Synopsis	649
160.2	Requirements	649
160.3	Parameters	650
160.4	Notes	650
160.5	Examples	650
160.6	Return Values	650
160.7	Status	650
160.8	Authors	650
161	fortios_router_isis – Configure IS-IS in Fortinet’s FortiOS and FortiGate.	653
161.1	Synopsis	653
161.2	Requirements	653
161.3	Parameters	654
161.4	Notes	654
161.5	Examples	654
161.6	Return Values	656
161.7	Status	656
161.8	Authors	656
162	fortios_router_key_chain – Configure key-chain in Fortinet’s FortiOS and FortiGate.	657
162.1	Synopsis	657
162.2	Requirements	657
162.3	Parameters	658
162.4	Notes	658
162.5	Examples	658
162.6	Return Values	658
162.7	Status	658
162.8	Authors	658
163	fortios_router_multicast – Configure router multicast in Fortinet’s FortiOS and FortiGate.	661
163.1	Synopsis	661
163.2	Requirements	661
163.3	Parameters	662
163.4	Notes	662
163.5	Examples	662
163.6	Return Values	663
163.7	Status	663
163.8	Authors	664
164	fortios_router_multicast6 – Configure IPv6 multicast in Fortinet’s FortiOS and FortiGate.	665
164.1	Synopsis	665
164.2	Requirements	665
164.3	Parameters	666
164.4	Notes	666

164.5 Examples	666
164.6 Return Values	666
164.7 Status	666
164.8 Authors	667
165fortios_router_multicast_flow – Configure multicast-flow in Fortinet’s FortiOS and FortiGate.	669
165.1 Synopsis	669
165.2 Requirements	669
165.3 Parameters	670
165.4 Notes	670
165.5 Examples	670
165.6 Return Values	670
165.7 Status	670
165.8 Authors	670
166fortios_router_ospf – Configure OSPF in Fortinet’s FortiOS and FortiGate.	673
166.1 Synopsis	673
166.2 Requirements	673
166.3 Parameters	674
166.4 Notes	674
166.5 Examples	674
166.6 Return Values	676
166.7 Status	676
166.8 Authors	676
167fortios_router_ospf6 – Configure IPv6 OSPF in Fortinet’s FortiOS and FortiGate.	679
167.1 Synopsis	679
167.2 Requirements	679
167.3 Parameters	680
167.4 Notes	680
167.5 Examples	680
167.6 Return Values	681
167.7 Status	681
167.8 Authors	682
168fortios_router_policy – Configure IPv4 routing policies in Fortinet’s FortiOS and FortiGate.	683
168.1 Synopsis	683
168.2 Requirements	683
168.3 Parameters	684
168.4 Notes	684
168.5 Examples	684
168.6 Return Values	685
168.7 Status	685
168.8 Authors	685
169fortios_router_policy6 – Configure IPv6 routing policies in Fortinet’s FortiOS and FortiGate.	687
169.1 Synopsis	687
169.2 Requirements	687
169.3 Parameters	688
169.4 Notes	688
169.5 Examples	688
169.6 Return Values	688
169.7 Status	688
169.8 Authors	689

170fortios_router_prefix_list – Configure IPv4 prefix lists in Fortinet’s FortiOS and FortiGate.	691
170.1 Synopsis	691
170.2 Requirements	691
170.3 Parameters	692
170.4 Notes	692
170.5 Examples	692
170.6 Return Values	692
170.7 Status	692
170.8 Authors	693
171fortios_router_prefix_list6 – Configure IPv6 prefix lists in Fortinet’s FortiOS and FortiGate.	695
171.1 Synopsis	695
171.2 Requirements	695
171.3 Parameters	696
171.4 Notes	696
171.5 Examples	696
171.6 Return Values	696
171.7 Status	696
171.8 Authors	697
172fortios_router_rip – Configure RIP in Fortinet’s FortiOS and FortiGate.	699
172.1 Synopsis	699
172.2 Requirements	699
172.3 Parameters	700
172.4 Notes	700
172.5 Examples	700
172.6 Return Values	701
172.7 Status	701
172.8 Authors	701
173fortios_router_ripng – Configure RIPng in Fortinet’s FortiOS and FortiGate.	703
173.1 Synopsis	703
173.2 Requirements	703
173.3 Parameters	704
173.4 Notes	704
173.5 Examples	704
173.6 Return Values	705
173.7 Status	705
173.8 Authors	705
174fortios_router_route_map – Configure route maps in Fortinet’s FortiOS and FortiGate.	707
174.1 Synopsis	707
174.2 Requirements	707
174.3 Parameters	708
174.4 Notes	708
174.5 Examples	708
174.6 Return Values	709
174.7 Status	709
174.8 Authors	709
175fortios_router_setting – Configure router settings in Fortinet’s FortiOS and FortiGate.	711
175.1 Synopsis	711
175.2 Requirements	711
175.3 Parameters	712
175.4 Notes	712

175.5 Examples	712
175.6 Return Values	712
175.7 Status	712
175.8 Authors	712
176fortios_router_static – Configure IPv4 static routing tables in Fortinet’s FortiOS and FortiGate.	715
176.1 Synopsis	715
176.2 Requirements	715
176.3 Parameters	716
176.4 Notes	716
176.5 Examples	716
176.6 Return Values	717
176.7 Status	717
176.8 Authors	717
177fortios_router_static6 – Configure IPv6 static routing tables in Fortinet’s FortiOS and FortiGate.	719
177.1 Synopsis	719
177.2 Requirements	719
177.3 Parameters	720
177.4 Notes	720
177.5 Examples	720
177.6 Return Values	720
177.7 Status	720
177.8 Authors	721
178fortios_spamfilter_bwl – Configure anti-spam black/white list in Fortinet’s FortiOS and FortiGate.	723
178.1 Synopsis	723
178.2 Requirements	723
178.3 Parameters	724
178.4 Notes	724
178.5 Examples	724
178.6 Return Values	724
178.7 Status	724
178.8 Authors	725
179fortios_spamfilter_bword – Configure AntiSpam banned word list in Fortinet’s FortiOS and FortiGate.	727
179.1 Synopsis	727
179.2 Requirements	727
179.3 Parameters	728
179.4 Notes	728
179.5 Examples	728
179.6 Return Values	728
179.7 Status	728
179.8 Authors	729
180fortios_spamfilter_dnsbl – Configure AntiSpam DNSBL/ORBL in Fortinet’s FortiOS and FortiGate.	731
180.1 Synopsis	731
180.2 Requirements	731
180.3 Parameters	732
180.4 Notes	732
180.5 Examples	732
180.6 Return Values	732
180.7 Status	732
180.8 Authors	733

181	fortios_spamfilter_fortishield – Configure FortiGuard - AntiSpam in Fortinet’s FortiOS and FortiGate.	735
181.1	Synopsis	735
181.2	Requirements	735
181.3	Parameters	736
181.4	Notes	736
181.5	Examples	736
181.6	Return Values	736
181.7	Status	736
181.8	Authors	736
182	fortios_spamfilter_iptrust – Configure AntiSpam IP trust in Fortinet’s FortiOS and FortiGate.	739
182.1	Synopsis	739
182.2	Requirements	739
182.3	Parameters	740
182.4	Notes	740
182.5	Examples	740
182.6	Return Values	740
182.7	Status	740
182.8	Authors	741
183	fortios_spamfilter_mheader – Configure AntiSpam MIME header in Fortinet’s FortiOS and FortiGate.	743
183.1	Synopsis	743
183.2	Requirements	743
183.3	Parameters	744
183.4	Notes	744
183.5	Examples	744
183.6	Return Values	744
183.7	Status	744
183.8	Authors	745
184	fortios_spamfilter_options – Configure AntiSpam options in Fortinet’s FortiOS and FortiGate.	747
184.1	Synopsis	747
184.2	Requirements	747
184.3	Parameters	748
184.4	Notes	748
184.5	Examples	748
184.6	Return Values	748
184.7	Status	748
184.8	Authors	748
185	fortios_spamfilter_profile – Configure AntiSpam profiles in Fortinet’s FortiOS and FortiGate.	751
185.1	Synopsis	751
185.2	Requirements	751
185.3	Parameters	752
185.4	Notes	752
185.5	Examples	752
185.6	Return Values	753
185.7	Status	753
185.8	Authors	753
186	fortios_ssh_filter_profile – SSH filter profile in Fortinet’s FortiOS and FortiGate.	755
186.1	Synopsis	755
186.2	Requirements	755
186.3	Parameters	756
186.4	Notes	756

186.5 Examples	756
186.6 Return Values	756
186.7 Status	756
186.8 Authors	757
187fortios_switch_controller_802_1x_settings – Configure global 802.1X settings in Fortinet’s FortiOS and FortiGate.	759
187.1 Synopsis	759
187.2 Requirements	759
187.3 Parameters	760
187.4 Notes	760
187.5 Examples	760
187.6 Return Values	760
187.7 Status	760
187.8 Authors	760
188fortios_switch_controller_custom_command – Configure the FortiGate switch controller to send custom commands to managed FortiSwitch devices in Fortinet’s FortiOS and FortiGate.	763
188.1 Synopsis	763
188.2 Requirements	763
188.3 Parameters	764
188.4 Notes	764
188.5 Examples	764
188.6 Return Values	764
188.7 Status	764
188.8 Authors	764
189fortios_switch_controller_global – Configure FortiSwitch global settings in Fortinet’s FortiOS and FortiGate.	767
189.1 Synopsis	767
189.2 Requirements	767
189.3 Parameters	768
189.4 Notes	768
189.5 Examples	768
189.6 Return Values	768
189.7 Status	768
189.8 Authors	768
190fortios_switch_controller_igmp_snooping – Configure FortiSwitch IGMP snooping global settings in Fortinet’s FortiOS and FortiGate.	771
190.1 Synopsis	771
190.2 Requirements	771
190.3 Parameters	772
190.4 Notes	772
190.5 Examples	772
190.6 Return Values	772
190.7 Status	772
190.8 Authors	772
191fortios_switch_controller_ldap_profile – Configure FortiSwitch LLDP profiles in Fortinet’s FortiOS and FortiGate.	775
191.1 Synopsis	775
191.2 Requirements	775
191.3 Parameters	776
191.4 Notes	776

191.5 Examples	776
191.6 Return Values	777
191.7 Status	777
191.8 Authors	777
192fortios_switch_controller_lddp_settings – Configure FortiSwitch LLDP settings in Fortinet’s FortiOS and FortiGate.	779
192.1 Synopsis	779
192.2 Requirements	779
192.3 Parameters	780
192.4 Notes	780
192.5 Examples	780
192.6 Return Values	780
192.7 Status	780
192.8 Authors	780
193fortios_switch_controller_mac_sync_settings – Configure global MAC synchronization settings in Fortinet’s FortiOS and FortiGate.	783
193.1 Synopsis	783
193.2 Requirements	783
193.3 Parameters	784
193.4 Notes	784
193.5 Examples	784
193.6 Return Values	784
193.7 Status	784
193.8 Authors	784
194fortios_switch_controller_managed_switch – Configure FortiSwitch devices that are managed by this FortiGate in Fortinet’s FortiOS and FortiGate.	787
194.1 Synopsis	787
194.2 Requirements	787
194.3 Parameters	788
194.4 Notes	788
194.5 Examples	788
194.6 Return Values	791
194.7 Status	791
194.8 Authors	791
195fortios_switch_controller_network_monitor_settings – Configure network monitor settings in Fortinet’s FortiOS and FortiGate.	793
195.1 Synopsis	793
195.2 Requirements	793
195.3 Parameters	794
195.4 Notes	794
195.5 Examples	794
195.6 Return Values	794
195.7 Status	794
195.8 Authors	794
196fortios_switch_controller_qos_dot1p_map – Configure FortiSwitch QoS 802.1p in Fortinet’s FortiOS and FortiGate.	797
196.1 Synopsis	797
196.2 Requirements	797
196.3 Parameters	798
196.4 Notes	798

196.5 Examples	798
196.6 Return Values	798
196.7 Status	798
196.8 Authors	799
197fortios_switch_controller_qos_ip_dscp_map – Configure FortiSwitch QoS IP precedence/DSCP in Fortinet’s FortiOS and FortiGate.	801
197.1 Synopsis	801
197.2 Requirements	801
197.3 Parameters	802
197.4 Notes	802
197.5 Examples	802
197.6 Return Values	802
197.7 Status	802
197.8 Authors	803
198fortios_switch_controller_qos_qos_policy – Configure FortiSwitch QoS policy in Fortinet’s FortiOS and FortiGate.	805
198.1 Synopsis	805
198.2 Requirements	805
198.3 Parameters	806
198.4 Notes	806
198.5 Examples	806
198.6 Return Values	806
198.7 Status	806
198.8 Authors	806
199fortios_switch_controller_qos_queue_policy – Configure FortiSwitch QoS egress queue policy in Fortinet’s FortiOS and FortiGate.	809
199.1 Synopsis	809
199.2 Requirements	809
199.3 Parameters	810
199.4 Notes	810
199.5 Examples	810
199.6 Return Values	810
199.7 Status	810
199.8 Authors	811
200fortios_switch_controller_quarantine – Configure FortiSwitch quarantine support in Fortinet’s FortiOS and FortiGate.	813
200.1 Synopsis	813
200.2 Requirements	813
200.3 Parameters	814
200.4 Notes	814
200.5 Examples	814
200.6 Return Values	814
200.7 Status	814
200.8 Authors	814
201fortios_switch_controller_security_policy_802_1x – Configure 802.1x MAC Authentication Bypass (MAB) policies in Fortinet’s FortiOS and FortiGate.	817
201.1 Synopsis	817
201.2 Requirements	817
201.3 Parameters	818
201.4 Notes	818

201.5 Examples	818
201.6 Return Values	818
201.7 Status	819
201.8 Authors	819
202fortios_switch_controller_security_policy_captive_portal – Names of VLANs that use captive portal authentication in Fortinet’s FortiOS and FortiGate.	821
202.1 Synopsis	821
202.2 Requirements	821
202.3 Parameters	822
202.4 Notes	822
202.5 Examples	822
202.6 Return Values	822
202.7 Status	822
202.8 Authors	822
203fortios_switch_controller_sflow – Configure FortiSwitch sFlow in Fortinet’s FortiOS and FortiGate.	825
203.1 Synopsis	825
203.2 Requirements	825
203.3 Parameters	826
203.4 Notes	826
203.5 Examples	826
203.6 Return Values	826
203.7 Status	826
203.8 Authors	826
204fortios_switch_controller_storm_control – Configure FortiSwitch storm control in Fortinet’s FortiOS and FortiGate.	829
204.1 Synopsis	829
204.2 Requirements	829
204.3 Parameters	830
204.4 Notes	830
204.5 Examples	830
204.6 Return Values	830
204.7 Status	830
204.8 Authors	830
205fortios_switch_controller_stp_settings – Configure FortiSwitch spanning tree protocol (STP) in Fortinet’s FortiOS and FortiGate.	833
205.1 Synopsis	833
205.2 Requirements	833
205.3 Parameters	834
205.4 Notes	834
205.5 Examples	834
205.6 Return Values	834
205.7 Status	834
205.8 Authors	834
206fortios_switch_controller_switch_group – Configure FortiSwitch switch groups in Fortinet’s FortiOS and FortiGate.	837
206.1 Synopsis	837
206.2 Requirements	837
206.3 Parameters	838
206.4 Notes	838
206.5 Examples	838

206.6 Return Values	838
206.7 Status	838
206.8 Authors	838
207fortios_switch_controller_switch_interface_tag – Configure switch object tags in Fortinet’s FortiOS and FortiGate.	841
207.1 Synopsis	841
207.2 Requirements	841
207.3 Parameters	842
207.4 Notes	842
207.5 Examples	842
207.6 Return Values	842
207.7 Status	842
207.8 Authors	842
208fortios_switch_controller_switch_log – Configure FortiSwitch logging (logs are transferred to and inserted into FortiGate event log) in Fortinet’s FortiOS and FortiGate.	845
208.1 Synopsis	845
208.2 Requirements	845
208.3 Parameters	846
208.4 Notes	846
208.5 Examples	846
208.6 Return Values	846
208.7 Status	846
208.8 Authors	846
209fortios_switch_controller_switch_profile – Configure FortiSwitch switch profile in Fortinet’s FortiOS and FortiGate.	849
209.1 Synopsis	849
209.2 Requirements	849
209.3 Parameters	850
209.4 Notes	850
209.5 Examples	850
209.6 Return Values	850
209.7 Status	850
209.8 Authors	850
210fortios_switch_controller_system – Configure system-wide switch controller settings in Fortinet’s FortiOS and FortiGate.	853
210.1 Synopsis	853
210.2 Requirements	853
210.3 Parameters	854
210.4 Notes	854
210.5 Examples	854
210.6 Return Values	854
210.7 Status	854
210.8 Authors	854
211fortios_switch_controller_virtual_port_pool – Configure virtual pool in Fortinet’s FortiOS and FortiGate.	857
211.1 Synopsis	857
211.2 Requirements	857
211.3 Parameters	858
211.4 Notes	858
211.5 Examples	858

211.6 Return Values	858
211.7 Status	858
211.8 Authors	858
212fortios_switch_controller_vlan – Configure VLANs for switch controller in Fortinet’s FortiOS and FortiGate.	861
212.1 Synopsis	861
212.2 Requirements	861
212.3 Parameters	862
212.4 Notes	862
212.5 Examples	862
212.6 Return Values	862
212.7 Status	863
212.8 Authors	863
213fortios_system_3g_modem_custom – 3G MODEM custom in Fortinet’s FortiOS and FortiGate.	865
213.1 Synopsis	865
213.2 Requirements	865
213.3 Parameters	866
213.4 Notes	866
213.5 Examples	866
213.6 Return Values	866
213.7 Status	866
213.8 Authors	866
214fortios_system_accprofile – Configure access profiles for system administrators in Fortinet’s FortiOS and FortiGate.	869
214.1 Synopsis	869
214.2 Requirements	869
214.3 Parameters	870
214.4 Notes	870
214.5 Examples	870
214.6 Return Values	871
214.7 Status	871
214.8 Authors	871
215fortios_system_admin – Configure admin users in Fortinet’s FortiOS and FortiGate.	873
215.1 Synopsis	873
215.2 Requirements	873
215.3 Parameters	874
215.4 Notes	874
215.5 Examples	874
215.6 Return Values	876
215.7 Status	876
215.8 Authors	876
216fortios_system_affinity_interrupt – Configure interrupt affinity in Fortinet’s FortiOS and FortiGate.	877
216.1 Synopsis	877
216.2 Requirements	877
216.3 Parameters	878
216.4 Notes	878
216.5 Examples	878
216.6 Return Values	878
216.7 Status	878
216.8 Authors	878

217	fortios_system_affinity_packet_redistribution – Configure packet redistribution in Fortinet’s FortiOS and FortiGate.	881
217.1	Synopsis	881
217.2	Requirements	881
217.3	Parameters	882
217.4	Notes	882
217.5	Examples	882
217.6	Return Values	882
217.7	Status	882
217.8	Authors	882
218	fortios_system_alarm – Configure alarm in Fortinet’s FortiOS and FortiGate.	885
218.1	Synopsis	885
218.2	Requirements	885
218.3	Parameters	886
218.4	Notes	886
218.5	Examples	886
218.6	Return Values	887
218.7	Status	887
218.8	Authors	887
219	fortios_system_alias – Configure alias command in Fortinet’s FortiOS and FortiGate.	889
219.1	Synopsis	889
219.2	Requirements	889
219.3	Parameters	890
219.4	Notes	890
219.5	Examples	890
219.6	Return Values	890
219.7	Status	890
219.8	Authors	890
220	fortios_system_api_user – Configure API users in Fortinet’s FortiOS and FortiGate.	893
220.1	Synopsis	893
220.2	Requirements	893
220.3	Parameters	894
220.4	Notes	894
220.5	Examples	894
220.6	Return Values	894
220.7	Status	895
220.8	Authors	895
221	fortios_system_arp_table – Configure ARP table in Fortinet’s FortiOS and FortiGate.	897
221.1	Synopsis	897
221.2	Requirements	897
221.3	Parameters	898
221.4	Notes	898
221.5	Examples	898
221.6	Return Values	898
221.7	Status	898
221.8	Authors	898
222	fortios_system_auto_install – Configure USB auto installation in Fortinet’s FortiOS and FortiGate.	901
222.1	Synopsis	901
222.2	Requirements	901
222.3	Parameters	902

222.4 Notes	902
222.5 Examples	902
222.6 Return Values	902
222.7 Status	902
222.8 Authors	902
223fortios_system_auto_script – Configure auto script in Fortinet’s FortiOS and FortiGate.	905
223.1 Synopsis	905
223.2 Requirements	905
223.3 Parameters	906
223.4 Notes	906
223.5 Examples	906
223.6 Return Values	906
223.7 Status	906
223.8 Authors	906
224fortios_system_automation_action – Action for automation stitches in Fortinet’s FortiOS and FortiGate.	909
224.1 Synopsis	909
224.2 Requirements	909
224.3 Parameters	910
224.4 Notes	910
224.5 Examples	910
224.6 Return Values	910
224.7 Status	911
224.8 Authors	911
225fortios_system_automation_destination – Automation destinations in Fortinet’s FortiOS and FortiGate.	913
225.1 Synopsis	913
225.2 Requirements	913
225.3 Parameters	914
225.4 Notes	914
225.5 Examples	914
225.6 Return Values	914
225.7 Status	914
225.8 Authors	914
226fortios_system_automation_stitch – Automation stitches in Fortinet’s FortiOS and FortiGate.	917
226.1 Synopsis	917
226.2 Requirements	917
226.3 Parameters	918
226.4 Notes	918
226.5 Examples	918
226.6 Return Values	918
226.7 Status	918
226.8 Authors	919
227fortios_system_automation_trigger – Trigger for automation stitches in Fortinet’s FortiOS and FortiGate.	921
227.1 Synopsis	921
227.2 Requirements	921
227.3 Parameters	922
227.4 Notes	922
227.5 Examples	922
227.6 Return Values	922
227.7 Status	922

227.8 Authors	923
228fortios_system_autoupdate_push_update – Configure push updates in Fortinet’s FortiOS and FortiGate.	925
228.1 Synopsis	925
228.2 Requirements	925
228.3 Parameters	926
228.4 Notes	926
228.5 Examples	926
228.6 Return Values	926
228.7 Status	926
228.8 Authors	926
229fortios_system_autoupdate_schedule – Configure update schedule in Fortinet’s FortiOS and FortiGate.	929
229.1 Synopsis	929
229.2 Requirements	929
229.3 Parameters	930
229.4 Notes	930
229.5 Examples	930
229.6 Return Values	930
229.7 Status	930
229.8 Authors	930
230fortios_system_autoupdate_tunneling – Configure web proxy tunnelling for the FDN in Fortinet’s FortiOS and FortiGate.	933
230.1 Synopsis	933
230.2 Requirements	933
230.3 Parameters	934
230.4 Notes	934
230.5 Examples	934
230.6 Return Values	934
230.7 Status	934
230.8 Authors	934
231fortios_system_central_management – Configure central management in Fortinet’s FortiOS and FortiGate.	937
231.1 Synopsis	937
231.2 Requirements	937
231.3 Parameters	938
231.4 Notes	938
231.5 Examples	938
231.6 Return Values	939
231.7 Status	939
231.8 Authors	939
232fortios_system_cluster_sync – Configure FortiGate Session Life Support Protocol (FGSP) session synchronization in Fortinet’s FortiOS and FortiGate.	941
232.1 Synopsis	941
232.2 Requirements	941
232.3 Parameters	942
232.4 Notes	942
232.5 Examples	942
232.6 Return Values	943
232.7 Status	943
232.8 Authors	943

233fortios_system_console – Configure console in Fortinet’s FortiOS and FortiGate.	945
233.1 Synopsis	945
233.2 Requirements	945
233.3 Parameters	946
233.4 Notes	946
233.5 Examples	946
233.6 Return Values	946
233.7 Status	946
233.8 Authors	946
234fortios_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.	949
234.1 Synopsis	949
234.2 Requirements	949
234.3 Parameters	950
234.4 Notes	950
234.5 Examples	950
234.6 Return Values	951
234.7 Status	951
234.8 Authors	951
235fortios_system_custom_language – Configure custom languages in Fortinet’s FortiOS and FortiGate.	953
235.1 Synopsis	953
235.2 Requirements	953
235.3 Parameters	954
235.4 Notes	954
235.5 Examples	954
235.6 Return Values	954
235.7 Status	954
235.8 Authors	954
236fortios_system_ddns – Configure DDNS in Fortinet’s FortiOS and FortiGate.	957
236.1 Synopsis	957
236.2 Requirements	957
236.3 Parameters	958
236.4 Notes	958
236.5 Examples	958
236.6 Return Values	958
236.7 Status	959
236.8 Authors	959
237fortios_system_dedicated_mgmt – Configure dedicated management in Fortinet’s FortiOS and FortiGate.	961
237.1 Synopsis	961
237.2 Requirements	961
237.3 Parameters	962
237.4 Notes	962
237.5 Examples	962
237.6 Return Values	962
237.7 Status	962
237.8 Authors	962
238fortios_system_dhcp6_server – Configure DHCPv6 servers in Fortinet’s FortiOS and FortiGate.	965
238.1 Synopsis	965
238.2 Requirements	965

238.3 Parameters	966
238.4 Notes	966
238.5 Examples	966
238.6 Return Values	967
238.7 Status	967
238.8 Authors	967
239fortios_system_dhcp_server – Configure DHCP servers in Fortinet’s FortiOS and FortiGate.	969
239.1 Synopsis	969
239.2 Requirements	969
239.3 Parameters	970
239.4 Notes	970
239.5 Examples	970
239.6 Return Values	971
239.7 Status	971
239.8 Authors	972
240fortios_system_dns – Configure DNS in Fortinet’s FortiOS and FortiGate.	973
240.1 Synopsis	973
240.2 Requirements	973
240.3 Parameters	974
240.4 Notes	974
240.5 Examples	974
240.6 Return Values	974
240.7 Status	974
240.8 Authors	974
241fortios_system_dns_database – Configure DNS databases in Fortinet’s FortiOS and FortiGate.	977
241.1 Synopsis	977
241.2 Requirements	977
241.3 Parameters	978
241.4 Notes	978
241.5 Examples	978
241.6 Return Values	979
241.7 Status	979
241.8 Authors	979
242fortios_system_dns_server – Configure DNS servers in Fortinet’s FortiOS and FortiGate.	981
242.1 Synopsis	981
242.2 Requirements	981
242.3 Parameters	982
242.4 Notes	982
242.5 Examples	982
242.6 Return Values	982
242.7 Status	982
242.8 Authors	982
243fortios_system_dscp_based_priority – Configure DSCP based priority table in Fortinet’s FortiOS and FortiGate.	985
243.1 Synopsis	985
243.2 Requirements	985
243.3 Parameters	986
243.4 Notes	986
243.5 Examples	986
243.6 Return Values	986

243.7 Status	986
243.8 Authors	986
244fortios_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.	989
244.1 Synopsis	989
244.2 Requirements	990
244.3 Parameters	990
244.4 Notes	990
244.5 Examples	990
244.6 Return Values	990
244.7 Status	991
244.8 Authors	991
245fortios_system_external_resource – Configure external resource in Fortinet’s FortiOS and FortiGate.	993
245.1 Synopsis	993
245.2 Requirements	993
245.3 Parameters	994
245.4 Notes	994
245.5 Examples	994
245.6 Return Values	994
245.7 Status	994
245.8 Authors	994
246fortios_system_fips_cc – Configure FIPS-CC mode in Fortinet’s FortiOS and FortiGate.	997
246.1 Synopsis	997
246.2 Requirements	997
246.3 Parameters	998
246.4 Notes	998
246.5 Examples	998
246.6 Return Values	998
246.7 Status	998
246.8 Authors	998
247fortios_system_fm – Configure FM in Fortinet’s FortiOS and FortiGate.	1001
247.1 Synopsis	1001
247.2 Requirements	1001
247.3 Parameters	1002
247.4 Notes	1002
247.5 Examples	1002
247.6 Return Values	1002
247.7 Status	1002
247.8 Authors	1002
248fortios_system_fortiguard – Configure FortiGuard services in Fortinet’s FortiOS and FortiGate.	1005
248.1 Synopsis	1005
248.2 Requirements	1005
248.3 Parameters	1006
248.4 Notes	1006
248.5 Examples	1006
248.6 Return Values	1007
248.7 Status	1007
248.8 Authors	1007

249	fortios_system_fortimanager – Configure FortiManager in Fortinet’s FortiOS and FortiGate.	1009
249.1	Synopsis	1009
249.2	Requirements	1009
249.3	Parameters	1010
249.4	Notes	1010
249.5	Examples	1010
249.6	Return Values	1010
249.7	Status	1010
249.8	Authors	1010
250	fortios_system_fortisandbox – Configure FortiSandbox in Fortinet’s FortiOS and FortiGate.	1013
250.1	Synopsis	1013
250.2	Requirements	1013
250.3	Parameters	1014
250.4	Notes	1014
250.5	Examples	1014
250.6	Return Values	1014
250.7	Status	1014
250.8	Authors	1014
251	fortios_system_fsso_polling – Configure Fortinet Single Sign On (FSSO) server in Fortinet’s FortiOS and FortiGate.	1017
251.1	Synopsis	1017
251.2	Requirements	1017
251.3	Parameters	1018
251.4	Notes	1018
251.5	Examples	1018
251.6	Return Values	1018
251.7	Status	1018
251.8	Authors	1018
252	fortios_system_ftm_push – Configure FortiToken Mobile push services in Fortinet’s FortiOS and FortiGate.	1021
252.1	Synopsis	1021
252.2	Requirements	1021
252.3	Parameters	1022
252.4	Notes	1022
252.5	Examples	1022
252.6	Return Values	1022
252.7	Status	1022
252.8	Authors	1022
253	fortios_system_geoip_override – Configure geographical location mapping for IP address(es) to override mappings from FortiGuard in Fortinet’s FortiOS and FortiGate.	1025
253.1	Synopsis	1025
253.2	Requirements	1025
253.3	Parameters	1026
253.4	Notes	1026
253.5	Examples	1026
253.6	Return Values	1026
253.7	Status	1026
253.8	Authors	1027
254	fortios_system_global – Configure global attributes in Fortinet’s FortiOS and FortiGate.	1029
254.1	Synopsis	1029

254.2 Requirements	1029
254.3 Parameters	1030
254.4 Notes	1030
254.5 Examples	1030
254.6 Return Values	1033
254.7 Status	1033
254.8 Authors	1033
255fortios_system_gre_tunnel – Configure GRE tunnel in Fortinet’s FortiOS and FortiGate.	1035
255.1 Synopsis	1035
255.2 Requirements	1035
255.3 Parameters	1036
255.4 Notes	1036
255.5 Examples	1036
255.6 Return Values	1036
255.7 Status	1037
255.8 Authors	1037
256fortios_system_ha – Configure HA in Fortinet’s FortiOS and FortiGate.	1039
256.1 Synopsis	1039
256.2 Requirements	1039
256.3 Parameters	1040
256.4 Notes	1040
256.5 Examples	1040
256.6 Return Values	1042
256.7 Status	1042
256.8 Authors	1042
257fortios_system_ha_monitor – Configure HA monitor in Fortinet’s FortiOS and FortiGate.	1043
257.1 Synopsis	1043
257.2 Requirements	1043
257.3 Parameters	1044
257.4 Notes	1044
257.5 Examples	1044
257.6 Return Values	1044
257.7 Status	1044
257.8 Authors	1044
258fortios_system_interface – Configure interfaces in Fortinet’s FortiOS and FortiGate.	1047
258.1 Synopsis	1047
258.2 Requirements	1047
258.3 Parameters	1048
258.4 Notes	1048
258.5 Examples	1048
258.6 Return Values	1053
258.7 Status	1053
258.8 Authors	1053
259fortios_system_ipip_tunnel – Configure IP in IP Tunneling in Fortinet’s FortiOS and FortiGate.	1055
259.1 Synopsis	1055
259.2 Requirements	1055
259.3 Parameters	1056
259.4 Notes	1056
259.5 Examples	1056
259.6 Return Values	1056

259.7 Status	1056
259.8 Authors	1056
260fortios_system_ips_urlfilter_dns – Configure IPS URL filter DNS servers in Fortinet’s FortiOS and FortiGate.	1059
260.1 Synopsis	1059
260.2 Requirements	1059
260.3 Parameters	1060
260.4 Notes	1060
260.5 Examples	1060
260.6 Return Values	1060
260.7 Status	1060
260.8 Authors	1060
261fortios_system_ips_urlfilter_dns6 – Configure IPS URL filter IPv6 DNS servers in Fortinet’s FortiOS and FortiGate.	1063
261.1 Synopsis	1063
261.2 Requirements	1063
261.3 Parameters	1064
261.4 Notes	1064
261.5 Examples	1064
261.6 Return Values	1064
261.7 Status	1064
261.8 Authors	1064
262fortios_system_ipv6_neighbor_cache – Configure IPv6 neighbor cache table in Fortinet’s FortiOS and FortiGate.	1067
262.1 Synopsis	1067
262.2 Requirements	1067
262.3 Parameters	1068
262.4 Notes	1068
262.5 Examples	1068
262.6 Return Values	1068
262.7 Status	1068
262.8 Authors	1068
263fortios_system_ipv6_tunnel – Configure IPv6/IPv4 in IPv6 tunnel in Fortinet’s FortiOS and FortiGate.	1071
263.1 Synopsis	1071
263.2 Requirements	1071
263.3 Parameters	1072
263.4 Notes	1072
263.5 Examples	1072
263.6 Return Values	1072
263.7 Status	1072
263.8 Authors	1072
264fortios_system_link_monitor – Configure Link Health Monitor in Fortinet’s FortiOS and FortiGate.	1075
264.1 Synopsis	1075
264.2 Requirements	1075
264.3 Parameters	1076
264.4 Notes	1076
264.5 Examples	1076
264.6 Return Values	1077
264.7 Status	1077
264.8 Authors	1077

265	fortios_system_lte_modem – Configure USB LTE/WIMAX devices in Fortinet’s FortiOS and FortiGate.	1079
265.1	Synopsis	1079
265.2	Requirements	1079
265.3	Parameters	1080
265.4	Notes	1080
265.5	Examples	1080
265.6	Return Values	1080
265.7	Status	1080
265.8	Authors	1081
266	fortios_system_mac_address_table – Configure MAC address tables in Fortinet’s FortiOS and FortiGate.	1083
266.1	Synopsis	1083
266.2	Requirements	1083
266.3	Parameters	1084
266.4	Notes	1084
266.5	Examples	1084
266.6	Return Values	1084
266.7	Status	1084
266.8	Authors	1084
267	fortios_system_management_tunnel – Management tunnel configuration in Fortinet’s FortiOS and FortiGate.	1087
267.1	Synopsis	1087
267.2	Requirements	1087
267.3	Parameters	1088
267.4	Notes	1088
267.5	Examples	1088
267.6	Return Values	1088
267.7	Status	1088
267.8	Authors	1088
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.	1091
268.1	Synopsis	1091
268.2	Requirements	1091
268.3	Parameters	1092
268.4	Notes	1092
268.5	Examples	1092
268.6	Return Values	1093
268.7	Status	1093
268.8	Authors	1093
269	fortios_system_modem – Configure MODEM in Fortinet’s FortiOS and FortiGate.	1095
269.1	Synopsis	1095
269.2	Requirements	1095
269.3	Parameters	1096
269.4	Notes	1096
269.5	Examples	1096
269.6	Return Values	1097
269.7	Status	1097
269.8	Authors	1097
270	fortios_system_nat64 – Configure NAT64 in Fortinet’s FortiOS and FortiGate.	1099
270.1	Synopsis	1099

270.2 Requirements	1099
270.3 Parameters	1100
270.4 Notes	1100
270.5 Examples	1100
270.6 Return Values	1100
270.7 Status	1100
270.8 Authors	1100
271fortios_system_netflow – Configure NetFlow in Fortinet’s FortiOS and FortiGate.	1103
271.1 Synopsis	1103
271.2 Requirements	1103
271.3 Parameters	1104
271.4 Notes	1104
271.5 Examples	1104
271.6 Return Values	1104
271.7 Status	1104
271.8 Authors	1104
272fortios_system_network_visibility – Configure network visibility settings in Fortinet’s FortiOS and FortiGate.	1107
272.1 Synopsis	1107
272.2 Requirements	1107
272.3 Parameters	1108
272.4 Notes	1108
272.5 Examples	1108
272.6 Return Values	1108
272.7 Status	1108
272.8 Authors	1108
273fortios_system_ntp – Configure system NTP information in Fortinet’s FortiOS and FortiGate.	1111
273.1 Synopsis	1111
273.2 Requirements	1111
273.3 Parameters	1112
273.4 Notes	1112
273.5 Examples	1112
273.6 Return Values	1112
273.7 Status	1113
273.8 Authors	1113
274fortios_system_object_tagging – Configure object tagging in Fortinet’s FortiOS and FortiGate.	1115
274.1 Synopsis	1115
274.2 Requirements	1115
274.3 Parameters	1116
274.4 Notes	1116
274.5 Examples	1116
274.6 Return Values	1116
274.7 Status	1116
274.8 Authors	1117
275fortios_system_password_policy – Configure password policy for locally defined administrator passwords and IPsec VPN pre-shared keys in Fortinet’s FortiOS and FortiGate.	1119
275.1 Synopsis	1119
275.2 Requirements	1119
275.3 Parameters	1120
275.4 Notes	1120

275.5 Examples	1120
275.6 Return Values	1120
275.7 Status	1120
275.8 Authors	1121
276fortios_system_password_policy_guest_admin – Configure the password policy for guest administrators in Fortinet’s FortiOS and FortiGate.	1123
276.1 Synopsis	1123
276.2 Requirements	1123
276.3 Parameters	1124
276.4 Notes	1124
276.5 Examples	1124
276.6 Return Values	1124
276.7 Status	1124
276.8 Authors	1125
277fortios_system_physical_switch – Configure physical switches in Fortinet’s FortiOS and FortiGate.	1127
277.1 Synopsis	1127
277.2 Requirements	1127
277.3 Parameters	1128
277.4 Notes	1128
277.5 Examples	1128
277.6 Return Values	1128
277.7 Status	1128
277.8 Authors	1128
278fortios_system_pppoe_interface – Configure the PPPoE interfaces in Fortinet’s FortiOS and FortiGate	1131
278.1 Synopsis	1131
278.2 Requirements	1131
278.3 Parameters	1132
278.4 Notes	1132
278.5 Examples	1132
278.6 Return Values	1132
278.7 Status	1133
278.8 Authors	1133
279fortios_system_probe_response – Configure system probe response in Fortinet’s FortiOS and FortiGate	1135
279.1 Synopsis	1135
279.2 Requirements	1135
279.3 Parameters	1136
279.4 Notes	1136
279.5 Examples	1136
279.6 Return Values	1136
279.7 Status	1136
279.8 Authors	1136
280fortios_system_proxy_arp – Configure proxy-ARP in Fortinet’s FortiOS and FortiGate.	1139
280.1 Synopsis	1139
280.2 Requirements	1139
280.3 Parameters	1140
280.4 Notes	1140
280.5 Examples	1140
280.6 Return Values	1140
280.7 Status	1140
280.8 Authors	1140

281	fortios_system_replacemsg_admin – Replacement messages in Fortinet’s FortiOS and FortiGate.	1143
281.1	Synopsis	1143
281.2	Requirements	1143
281.3	Parameters	1144
281.4	Notes	1144
281.5	Examples	1144
281.6	Return Values	1144
281.7	Status	1144
281.8	Authors	1144
282	fortios_system_replacemsg_alertmail – Replacement messages in Fortinet’s FortiOS and FortiGate.	1147
282.1	Synopsis	1147
282.2	Requirements	1147
282.3	Parameters	1148
282.4	Notes	1148
282.5	Examples	1148
282.6	Return Values	1148
282.7	Status	1148
282.8	Authors	1148
283	fortios_system_replacemsg_auth – Replacement messages in Fortinet’s FortiOS and FortiGate.	1151
283.1	Synopsis	1151
283.2	Requirements	1151
283.3	Parameters	1152
283.4	Notes	1152
283.5	Examples	1152
283.6	Return Values	1152
283.7	Status	1152
283.8	Authors	1152
284	fortios_system_replacemsg_device_detection_portal – Replacement messages in Fortinet’s FortiOS and FortiGate.	1155
284.1	Synopsis	1155
284.2	Requirements	1155
284.3	Parameters	1156
284.4	Notes	1156
284.5	Examples	1156
284.6	Return Values	1156
284.7	Status	1156
284.8	Authors	1156
285	fortios_system_replacemsg_ec – Replacement messages in Fortinet’s FortiOS and FortiGate.	1159
285.1	Synopsis	1159
285.2	Requirements	1159
285.3	Parameters	1160
285.4	Notes	1160
285.5	Examples	1160
285.6	Return Values	1160
285.7	Status	1160
285.8	Authors	1160
286	fortios_system_replacemsg_fortiguard_wf – Replacement messages in Fortinet’s FortiOS and FortiGate.	1163
286.1	Synopsis	1163
286.2	Requirements	1163
286.3	Parameters	1164

286.4 Notes	1164
286.5 Examples	1164
286.6 Return Values	1164
286.7 Status	1164
286.8 Authors	1164
287fortios_system_replacemsg_ftp – Replacement messages in Fortinet’s FortiOS and FortiGate.	1167
287.1 Synopsis	1167
287.2 Requirements	1167
287.3 Parameters	1168
287.4 Notes	1168
287.5 Examples	1168
287.6 Return Values	1168
287.7 Status	1168
287.8 Authors	1168
288fortios_system_replacemsg_group – Configure replacement message groups in Fortinet’s FortiOS and FortiGate.	1171
288.1 Synopsis	1171
288.2 Requirements	1171
288.3 Parameters	1172
288.4 Notes	1172
288.5 Examples	1172
288.6 Return Values	1174
288.7 Status	1174
288.8 Authors	1174
289fortios_system_replacemsg_http – Replacement messages in Fortinet’s FortiOS and FortiGate.	1177
289.1 Synopsis	1177
289.2 Requirements	1177
289.3 Parameters	1178
289.4 Notes	1178
289.5 Examples	1178
289.6 Return Values	1178
289.7 Status	1178
289.8 Authors	1178
290fortios_system_replacemsg_icap – Replacement messages in Fortinet’s FortiOS and FortiGate.	1181
290.1 Synopsis	1181
290.2 Requirements	1181
290.3 Parameters	1182
290.4 Notes	1182
290.5 Examples	1182
290.6 Return Values	1182
290.7 Status	1182
290.8 Authors	1182
291fortios_system_replacemsg_image – Configure replacement message images in Fortinet’s FortiOS and FortiGate.	1185
291.1 Synopsis	1185
291.2 Requirements	1185
291.3 Parameters	1186
291.4 Notes	1186
291.5 Examples	1186
291.6 Return Values	1186

291.7 Status	1186
291.8 Authors	1186
292fortios_system_replacemsg_mail – Replacement messages in Fortinet’s FortiOS and FortiGate.	1189
292.1 Synopsis	1189
292.2 Requirements	1189
292.3 Parameters	1190
292.4 Notes	1190
292.5 Examples	1190
292.6 Return Values	1190
292.7 Status	1190
292.8 Authors	1190
293fortios_system_replacemsg_nac_quar – Replacement messages in Fortinet’s FortiOS and FortiGate.	1193
293.1 Synopsis	1193
293.2 Requirements	1193
293.3 Parameters	1194
293.4 Notes	1194
293.5 Examples	1194
293.6 Return Values	1194
293.7 Status	1194
293.8 Authors	1194
294fortios_system_replacemsg_nntp – Replacement messages in Fortinet’s FortiOS and FortiGate.	1197
294.1 Synopsis	1197
294.2 Requirements	1197
294.3 Parameters	1198
294.4 Notes	1198
294.5 Examples	1198
294.6 Return Values	1198
294.7 Status	1198
294.8 Authors	1198
295fortios_system_replacemsg_spam – Replacement messages in Fortinet’s FortiOS and FortiGate.	1201
295.1 Synopsis	1201
295.2 Requirements	1201
295.3 Parameters	1202
295.4 Notes	1202
295.5 Examples	1202
295.6 Return Values	1202
295.7 Status	1202
295.8 Authors	1202
296fortios_system_replacemsg_sslvpn – Replacement messages in Fortinet’s FortiOS and FortiGate.	1205
296.1 Synopsis	1205
296.2 Requirements	1205
296.3 Parameters	1206
296.4 Notes	1206
296.5 Examples	1206
296.6 Return Values	1206
296.7 Status	1206
296.8 Authors	1206
297fortios_system_replacemsg_traffic_quota – Replacement messages in Fortinet’s FortiOS and FortiGate.	1209
297.1 Synopsis	1209

297.2	Requirements	1209
297.3	Parameters	1210
297.4	Notes	1210
297.5	Examples	1210
297.6	Return Values	1210
297.7	Status	1210
297.8	Authors	1210
298	fortios_system_replacemsg_utm – Replacement messages in Fortinet’s FortiOS and FortiGate.	1213
298.1	Synopsis	1213
298.2	Requirements	1213
298.3	Parameters	1214
298.4	Notes	1214
298.5	Examples	1214
298.6	Return Values	1214
298.7	Status	1214
298.8	Authors	1214
299	fortios_system_replacemsg_webproxy – Replacement messages in Fortinet’s FortiOS and FortiGate.	1217
299.1	Synopsis	1217
299.2	Requirements	1217
299.3	Parameters	1218
299.4	Notes	1218
299.5	Examples	1218
299.6	Return Values	1218
299.7	Status	1218
299.8	Authors	1218
300	fortios_system_resource_limits – Configure resource limits in Fortinet’s FortiOS and FortiGate.	1221
300.1	Synopsis	1221
300.2	Requirements	1221
300.3	Parameters	1222
300.4	Notes	1222
300.5	Examples	1222
300.6	Return Values	1222
300.7	Status	1223
300.8	Authors	1223
301	fortios_system_sdn_connector – Configure connection to SDN Connector in Fortinet’s FortiOS and FortiGate.	1225
301.1	Synopsis	1225
301.2	Requirements	1225
301.3	Parameters	1226
301.4	Notes	1226
301.5	Examples	1226
301.6	Return Values	1227
301.7	Status	1227
301.8	Authors	1227
302	fortios_system_session_helper – Configure session helper in Fortinet’s FortiOS and FortiGate.	1229
302.1	Synopsis	1229
302.2	Requirements	1229
302.3	Parameters	1230
302.4	Notes	1230
302.5	Examples	1230

302.6 Return Values	1230
302.7 Status	1230
302.8 Authors	1230
303fortios_system_session_ttl – Configure global session TTL timers for this FortiGate in Fortinet’s FortiOS and FortiGate.	1233
303.1 Synopsis	1233
303.2 Requirements	1233
303.3 Parameters	1234
303.4 Notes	1234
303.5 Examples	1234
303.6 Return Values	1234
303.7 Status	1234
303.8 Authors	1234
304fortios_system_settings – Configure VDOM settings in Fortinet’s FortiOS and FortiGate.	1237
304.1 Synopsis	1237
304.2 Requirements	1237
304.3 Parameters	1238
304.4 Notes	1238
304.5 Examples	1238
304.6 Return Values	1240
304.7 Status	1240
304.8 Authors	1240
305fortios_system_sflow – Configure sFlow in Fortinet’s FortiOS and FortiGate.	1243
305.1 Synopsis	1243
305.2 Requirements	1243
305.3 Parameters	1244
305.4 Notes	1244
305.5 Examples	1244
305.6 Return Values	1244
305.7 Status	1244
305.8 Authors	1244
306fortios_system_sit_tunnel – Configure IPv6 tunnel over IPv4 in Fortinet’s FortiOS and FortiGate.	1247
306.1 Synopsis	1247
306.2 Requirements	1247
306.3 Parameters	1248
306.4 Notes	1248
306.5 Examples	1248
306.6 Return Values	1248
306.7 Status	1248
306.8 Authors	1248
307fortios_system_sms_server – Configure SMS server for sending SMS messages to support user authentication in Fortinet’s FortiOS and FortiGate.	1251
307.1 Synopsis	1251
307.2 Requirements	1251
307.3 Parameters	1252
307.4 Notes	1252
307.5 Examples	1252
307.6 Return Values	1252
307.7 Status	1252
307.8 Authors	1252

308fortios_system_snmp_community – SNMP community configuration in Fortinet’s FortiOS and FortiGate.	1255
308.1 Synopsis	1255
308.2 Requirements	1255
308.3 Parameters	1256
308.4 Notes	1256
308.5 Examples	1256
308.6 Return Values	1257
308.7 Status	1257
308.8 Authors	1257
309fortios_system_snmp_sysinfo – SNMP system info configuration in Fortinet’s FortiOS and FortiGate.	1259
309.1 Synopsis	1259
309.2 Requirements	1259
309.3 Parameters	1260
309.4 Notes	1260
309.5 Examples	1260
309.6 Return Values	1260
309.7 Status	1260
309.8 Authors	1260
310fortios_system_snmp_user – SNMP user configuration in Fortinet’s FortiOS and FortiGate.	1263
310.1 Synopsis	1263
310.2 Requirements	1263
310.3 Parameters	1264
310.4 Notes	1264
310.5 Examples	1264
310.6 Return Values	1264
310.7 Status	1265
310.8 Authors	1265
311fortios_system_storage – Configure logical storage in Fortinet’s FortiOS and FortiGate.	1267
311.1 Synopsis	1267
311.2 Requirements	1267
311.3 Parameters	1268
311.4 Notes	1268
311.5 Examples	1268
311.6 Return Values	1268
311.7 Status	1268
311.8 Authors	1269
312fortios_system_stp – Configure Spanning Tree Protocol (STP) in Fortinet’s FortiOS and FortiGate.	1271
312.1 Synopsis	1271
312.2 Requirements	1271
312.3 Parameters	1272
312.4 Notes	1272
312.5 Examples	1272
312.6 Return Values	1272
312.7 Status	1272
312.8 Authors	1272
313fortios_system_switch_interface – Configure software switch interfaces by grouping physical and WiFi interfaces in Fortinet’s FortiOS and FortiGate.	1275
313.1 Synopsis	1275
313.2 Requirements	1275

313.3 Parameters	1276
313.4 Notes	1276
313.5 Examples	1276
313.6 Return Values	1276
313.7 Status	1276
313.8 Authors	1277
314fortios_system_tos_based_priority – Configure Type of Service (ToS) based priority table to set network traffic priorities in Fortinet’s FortiOS and FortiGate.	1279
314.1 Synopsis	1279
314.2 Requirements	1279
314.3 Parameters	1280
314.4 Notes	1280
314.5 Examples	1280
314.6 Return Values	1280
314.7 Status	1280
314.8 Authors	1280
315fortios_system_vdom – Configure virtual domain in Fortinet’s FortiOS and FortiGate.	1283
315.1 Synopsis	1283
315.2 Requirements	1283
315.3 Parameters	1284
315.4 Notes	1284
315.5 Examples	1284
315.6 Return Values	1284
315.7 Status	1284
315.8 Authors	1284
316fortios_system_vdom_dns – Configure DNS servers for a non-management VDOM in Fortinet’s FortiOS and FortiGate.	1287
316.1 Synopsis	1287
316.2 Requirements	1287
316.3 Parameters	1288
316.4 Notes	1288
316.5 Examples	1288
316.6 Return Values	1288
316.7 Status	1288
316.8 Authors	1288
317fortios_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.	1291
317.1 Synopsis	1291
317.2 Requirements	1291
317.3 Parameters	1292
317.4 Notes	1292
317.5 Examples	1292
317.6 Return Values	1292
317.7 Status	1292
317.8 Authors	1293
318fortios_system_vdom_link – Configure VDOM links in Fortinet’s FortiOS and FortiGate.	1295
318.1 Synopsis	1295
318.2 Requirements	1295
318.3 Parameters	1296
318.4 Notes	1296

318.5 Examples	1296
318.6 Return Values	1296
318.7 Status	1296
318.8 Authors	1296
319fortios_system_vdom_netflow – Configure NetFlow per VDOM in Fortinet’s FortiOS and FortiGate.	1299
319.1 Synopsis	1299
319.2 Requirements	1299
319.3 Parameters	1300
319.4 Notes	1300
319.5 Examples	1300
319.6 Return Values	1300
319.7 Status	1300
319.8 Authors	1300
320fortios_system_vdom_property – Configure VDOM property in Fortinet’s FortiOS and FortiGate.	1303
320.1 Synopsis	1303
320.2 Requirements	1303
320.3 Parameters	1304
320.4 Notes	1304
320.5 Examples	1304
320.6 Return Values	1305
320.7 Status	1305
320.8 Authors	1305
321fortios_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.	1307
321.1 Synopsis	1307
321.2 Requirements	1307
321.3 Parameters	1308
321.4 Notes	1308
321.5 Examples	1308
321.6 Return Values	1308
321.7 Status	1308
321.8 Authors	1308
322fortios_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.	1311
322.1 Synopsis	1311
322.2 Requirements	1312
322.3 Parameters	1312
322.4 Notes	1312
322.5 Examples	1312
322.6 Return Values	1312
322.7 Status	1312
322.8 Authors	1313
323fortios_system_virtual_switch – Configure virtual hardware switch interfaces in Fortinet’s FortiOS and FortiGate.	1315
323.1 Synopsis	1315
323.2 Requirements	1315
323.3 Parameters	1316
323.4 Notes	1316
323.5 Examples	1316

323.6 Return Values	1316
323.7 Status	1316
323.8 Authors	1317
324fortios_system_virtual_wan_link – Configure redundant internet connections using SD-WAN (formerly virtual WAN link) in Fortinet’s FortiOS and FortiGate.	1319
324.1 Synopsis	1319
324.2 Requirements	1319
324.3 Parameters	1320
324.4 Notes	1320
324.5 Examples	1320
324.6 Return Values	1323
324.7 Status	1323
324.8 Authors	1323
325fortios_system_virtual_wire_pair – Configure virtual wire pairs in Fortinet’s FortiOS and FortiGate.	1325
325.1 Synopsis	1325
325.2 Requirements	1325
325.3 Parameters	1326
325.4 Notes	1326
325.5 Examples	1326
325.6 Return Values	1326
325.7 Status	1326
325.8 Authors	1326
326fortios_system_vmlicense – Update VM license using uploaded file. Reboots immediately if successful in Fortinet’s FortiOS and FortiGate.	1329
326.1 Synopsis	1329
326.2 Requirements	1329
326.3 Parameters	1330
326.4 Notes	1330
326.5 Examples	1330
326.6 Return Values	1330
326.7 Status	1330
326.8 Authors	1330
327fortios_system_vxlan – Configure VXLAN devices in Fortinet’s FortiOS and FortiGate.	1333
327.1 Synopsis	1333
327.2 Requirements	1333
327.3 Parameters	1334
327.4 Notes	1334
327.5 Examples	1334
327.6 Return Values	1334
327.7 Status	1334
327.8 Authors	1335
328fortios_system_wccp – Configure WCCP in Fortinet’s FortiOS and FortiGate.	1337
328.1 Synopsis	1337
328.2 Requirements	1337
328.3 Parameters	1338
328.4 Notes	1338
328.5 Examples	1338
328.6 Return Values	1339
328.7 Status	1339
328.8 Authors	1339

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.	1341
329.1	Synopsis	1341
329.2	Requirements	1341
329.3	Parameters	1342
329.4	Notes	1342
329.5	Examples	1342
329.6	Return Values	1342
329.7	Status	1343
329.8	Authors	1343
330	fortios_user_adgrp – Configure FSSO groups in Fortinet’s FortiOS and FortiGate.	1345
330.1	Synopsis	1345
330.2	Requirements	1345
330.3	Parameters	1346
330.4	Notes	1346
330.5	Examples	1346
330.6	Return Values	1346
330.7	Status	1346
330.8	Authors	1346
331	fortios_user_device – Configure devices in Fortinet’s FortiOS and FortiGate.	1349
331.1	Synopsis	1349
331.2	Requirements	1349
331.3	Parameters	1350
331.4	Notes	1350
331.5	Examples	1350
331.6	Return Values	1350
331.7	Status	1351
331.8	Authors	1351
332	fortios_user_device_access_list – Configure device access control lists in Fortinet’s FortiOS and FortiGate.	1353
332.1	Synopsis	1353
332.2	Requirements	1353
332.3	Parameters	1354
332.4	Notes	1354
332.5	Examples	1354
332.6	Return Values	1354
332.7	Status	1354
332.8	Authors	1354
333	fortios_user_device_category – Configure device categories in Fortinet’s FortiOS and FortiGate.	1357
333.1	Synopsis	1357
333.2	Requirements	1357
333.3	Parameters	1358
333.4	Notes	1358
333.5	Examples	1358
333.6	Return Values	1358
333.7	Status	1358
333.8	Authors	1358
334	fortios_user_device_group – Configure device groups in Fortinet’s FortiOS and FortiGate.	1361
334.1	Synopsis	1361

334.2 Requirements	1361
334.3 Parameters	1362
334.4 Notes	1362
334.5 Examples	1362
334.6 Return Values	1362
334.7 Status	1362
334.8 Authors	1363
335fortios_user_domain_controller – Configure domain controller entries in Fortinet’s FortiOS and FortiGate.	1365
335.1 Synopsis	1365
335.2 Requirements	1365
335.3 Parameters	1366
335.4 Notes	1366
335.5 Examples	1366
335.6 Return Values	1366
335.7 Status	1366
335.8 Authors	1366
336fortios_user_fortitoken – Configure FortiToken in Fortinet’s FortiOS and FortiGate.	1369
336.1 Synopsis	1369
336.2 Requirements	1369
336.3 Parameters	1370
336.4 Notes	1370
336.5 Examples	1370
336.6 Return Values	1370
336.7 Status	1370
336.8 Authors	1371
337fortios_user_fsso – Configure Fortinet Single Sign On (FSSO) agents in Fortinet’s FortiOS and FortiGate.	1373
337.1 Synopsis	1373
337.2 Requirements	1373
337.3 Parameters	1374
337.4 Notes	1374
337.5 Examples	1374
337.6 Return Values	1374
337.7 Status	1375
337.8 Authors	1375
338fortios_user_fsso_polling – Configure FSSO active directory servers for polling mode in Fortinet’s FortiOS and FortiGate.	1377
338.1 Synopsis	1377
338.2 Requirements	1377
338.3 Parameters	1378
338.4 Notes	1378
338.5 Examples	1378
338.6 Return Values	1378
338.7 Status	1378
338.8 Authors	1379
339fortios_user_group – Configure user groups in Fortinet’s FortiOS and FortiGate.	1381
339.1 Synopsis	1381
339.2 Requirements	1381
339.3 Parameters	1382

339.4 Notes	1382
339.5 Examples	1382
339.6 Return Values	1383
339.7 Status	1383
339.8 Authors	1383
340fortios_user_krb_keytab – Configure Kerberos keytab entries in Fortinet’s FortiOS and FortiGate.	1385
340.1 Synopsis	1385
340.2 Requirements	1385
340.3 Parameters	1386
340.4 Notes	1386
340.5 Examples	1386
340.6 Return Values	1386
340.7 Status	1386
340.8 Authors	1386
341fortios_user_ldap – Configure LDAP server entries in Fortinet’s FortiOS and FortiGate.	1389
341.1 Synopsis	1389
341.2 Requirements	1389
341.3 Parameters	1390
341.4 Notes	1390
341.5 Examples	1390
341.6 Return Values	1391
341.7 Status	1391
341.8 Authors	1391
342fortios_user_local – Configure local users in Fortinet’s FortiOS and FortiGate.	1393
342.1 Synopsis	1393
342.2 Requirements	1393
342.3 Parameters	1394
342.4 Notes	1394
342.5 Examples	1394
342.6 Return Values	1395
342.7 Status	1395
342.8 Authors	1395
343fortios_user_password_policy – Configure user password policy in Fortinet’s FortiOS and FortiGate.	1397
343.1 Synopsis	1397
343.2 Requirements	1397
343.3 Parameters	1398
343.4 Notes	1398
343.5 Examples	1398
343.6 Return Values	1398
343.7 Status	1398
343.8 Authors	1398
344fortios_user_peer – Configure peer users in Fortinet’s FortiOS and FortiGate.	1401
344.1 Synopsis	1401
344.2 Requirements	1401
344.3 Parameters	1402
344.4 Notes	1402
344.5 Examples	1402
344.6 Return Values	1402
344.7 Status	1402
344.8 Authors	1403

345fortios_user_peergroup – Configure peer groups in Fortinet’s FortiOS and FortiGate.	1405
345.1 Synopsis	1405
345.2 Requirements	1405
345.3 Parameters	1406
345.4 Notes	1406
345.5 Examples	1406
345.6 Return Values	1406
345.7 Status	1406
345.8 Authors	1406
346fortios_user_pop3 – POP3 server entry configuration in Fortinet’s FortiOS and FortiGate.	1409
346.1 Synopsis	1409
346.2 Requirements	1409
346.3 Parameters	1410
346.4 Notes	1410
346.5 Examples	1410
346.6 Return Values	1410
346.7 Status	1410
346.8 Authors	1410
347fortios_user_quarantine – Configure quarantine support in Fortinet’s FortiOS and FortiGate.	1413
347.1 Synopsis	1413
347.2 Requirements	1413
347.3 Parameters	1414
347.4 Notes	1414
347.5 Examples	1414
347.6 Return Values	1414
347.7 Status	1414
347.8 Authors	1414
348fortios_user_radius – Configure RADIUS server entries in Fortinet’s FortiOS and FortiGate.	1417
348.1 Synopsis	1417
348.2 Requirements	1417
348.3 Parameters	1418
348.4 Notes	1418
348.5 Examples	1418
348.6 Return Values	1419
348.7 Status	1419
348.8 Authors	1419
349fortios_user_security_exempt_list – Configure security exemption list in Fortinet’s FortiOS and FortiGate.	1421
349.1 Synopsis	1421
349.2 Requirements	1421
349.3 Parameters	1422
349.4 Notes	1422
349.5 Examples	1422
349.6 Return Values	1423
349.7 Status	1423
349.8 Authors	1423
350fortios_user_setting – Configure user authentication setting in Fortinet’s FortiOS and FortiGate.	1425
350.1 Synopsis	1425
350.2 Requirements	1425
350.3 Parameters	1426

350.4 Notes	1426
350.5 Examples	1426
350.6 Return Values	1426
350.7 Status	1427
350.8 Authors	1427
351fortios_user_tacacsplus – Configure TACACS+ server entries in Fortinet’s FortiOS and FortiGate.	1429
351.1 Synopsis	1429
351.2 Requirements	1429
351.3 Parameters	1430
351.4 Notes	1430
351.5 Examples	1430
351.6 Return Values	1430
351.7 Status	1430
351.8 Authors	1431
352fortios_voip_profile – Configure VoIP profiles in Fortinet’s FortiOS and FortiGate.	1433
352.1 Synopsis	1433
352.2 Requirements	1433
352.3 Parameters	1434
352.4 Notes	1434
352.5 Examples	1434
352.6 Return Values	1436
352.7 Status	1436
352.8 Authors	1436
353fortios_vpn_certificate_ca – CA certificate in Fortinet’s FortiOS and FortiGate.	1439
353.1 Synopsis	1439
353.2 Requirements	1439
353.3 Parameters	1440
353.4 Notes	1440
353.5 Examples	1440
353.6 Return Values	1440
353.7 Status	1440
353.8 Authors	1441
354fortios_vpn_certificate_crl – Certificate Revocation List as a PEM file in Fortinet’s FortiOS and FortiGate.	1443
354.1 Synopsis	1443
354.2 Requirements	1443
354.3 Parameters	1444
354.4 Notes	1444
354.5 Examples	1444
354.6 Return Values	1444
354.7 Status	1444
354.8 Authors	1445
355fortios_vpn_certificate_local – Local keys and certificates in Fortinet’s FortiOS and FortiGate.	1447
355.1 Synopsis	1447
355.2 Requirements	1447
355.3 Parameters	1448
355.4 Notes	1448
355.5 Examples	1448
355.6 Return Values	1449
355.7 Status	1449

355.8 Authors	1449
356fortios_vpn_certificate_ocsp_server – OCSP server configuration in Fortinet’s FortiOS and FortiGate.	1451
356.1 Synopsis	1451
356.2 Requirements	1451
356.3 Parameters	1452
356.4 Notes	1452
356.5 Examples	1452
356.6 Return Values	1452
356.7 Status	1452
356.8 Authors	1453
357fortios_vpn_certificate_remote – Remote certificate as a PEM file in Fortinet’s FortiOS and FortiGate.	1455
357.1 Synopsis	1455
357.2 Requirements	1455
357.3 Parameters	1456
357.4 Notes	1456
357.5 Examples	1456
357.6 Return Values	1456
357.7 Status	1456
357.8 Authors	1456
358fortios_vpn_certificate_setting – VPN certificate setting in Fortinet’s FortiOS and FortiGate.	1459
358.1 Synopsis	1459
358.2 Requirements	1459
358.3 Parameters	1460
358.4 Notes	1460
358.5 Examples	1460
358.6 Return Values	1460
358.7 Status	1461
358.8 Authors	1461
359fortios_vpn_ipsec_concentrator – Concentrator configuration in Fortinet’s FortiOS and FortiGate.	1463
359.1 Synopsis	1463
359.2 Requirements	1463
359.3 Parameters	1464
359.4 Notes	1464
359.5 Examples	1464
359.6 Return Values	1464
359.7 Status	1464
359.8 Authors	1464
360fortios_vpn_ipsec_forticlient – Configure FortiClient policy realm in Fortinet’s FortiOS and FortiGate.	1467
360.1 Synopsis	1467
360.2 Requirements	1467
360.3 Parameters	1468
360.4 Notes	1468
360.5 Examples	1468
360.6 Return Values	1468
360.7 Status	1468
360.8 Authors	1468
361fortios_vpn_ipsec_manualkey – Configure IPsec manual keys in Fortinet’s FortiOS and FortiGate.	1471
361.1 Synopsis	1471
361.2 Requirements	1471

361.3 Parameters	1472
361.4 Notes	1472
361.5 Examples	1472
361.6 Return Values	1472
361.7 Status	1472
361.8 Authors	1473
362fortios_vpn_ipsec_manualkey_interface – Configure IPsec manual keys in Fortinet’s FortiOS and FortiGate.	1475
362.1 Synopsis	1475
362.2 Requirements	1475
362.3 Parameters	1476
362.4 Notes	1476
362.5 Examples	1476
362.6 Return Values	1476
362.7 Status	1477
362.8 Authors	1477
363fortios_vpn_ipsec_phase1 – Configure VPN remote gateway in Fortinet’s FortiOS and FortiGate.	1479
363.1 Synopsis	1479
363.2 Requirements	1479
363.3 Parameters	1480
363.4 Notes	1480
363.5 Examples	1480
363.6 Return Values	1482
363.7 Status	1482
363.8 Authors	1482
364fortios_vpn_ipsec_phase1_interface – Configure VPN remote gateway in Fortinet’s FortiOS and FortiGate.	1485
364.1 Synopsis	1485
364.2 Requirements	1485
364.3 Parameters	1486
364.4 Notes	1486
364.5 Examples	1486
364.6 Return Values	1489
364.7 Status	1489
364.8 Authors	1489
365fortios_vpn_ipsec_phase2 – Configure VPN autokey tunnel in Fortinet’s FortiOS and FortiGate.	1491
365.1 Synopsis	1491
365.2 Requirements	1491
365.3 Parameters	1492
365.4 Notes	1492
365.5 Examples	1492
365.6 Return Values	1493
365.7 Status	1493
365.8 Authors	1493
366fortios_vpn_ipsec_phase2_interface – Configure VPN autokey tunnel in Fortinet’s FortiOS and FortiGate.	1495
366.1 Synopsis	1495
366.2 Requirements	1495
366.3 Parameters	1496
366.4 Notes	1496

366.5 Examples	1496
366.6 Return Values	1497
366.7 Status	1497
366.8 Authors	1497
367fortios_vpn_l2tp – Configure L2TP in Fortinet’s FortiOS and FortiGate.	1499
367.1 Synopsis	1499
367.2 Requirements	1499
367.3 Parameters	1500
367.4 Notes	1500
367.5 Examples	1500
367.6 Return Values	1500
367.7 Status	1500
367.8 Authors	1500
368fortios_vpn_ocvpn – Configure One-Click VPN settings in Fortinet’s FortiOS and FortiGate.	1503
368.1 Synopsis	1503
368.2 Requirements	1503
368.3 Parameters	1504
368.4 Notes	1504
368.5 Examples	1504
368.6 Return Values	1504
368.7 Status	1504
368.8 Authors	1504
369fortios_vpn_pptp – Configure PPTP in Fortinet’s FortiOS and FortiGate.	1507
369.1 Synopsis	1507
369.2 Requirements	1507
369.3 Parameters	1508
369.4 Notes	1508
369.5 Examples	1508
369.6 Return Values	1508
369.7 Status	1508
369.8 Authors	1508
370fortios_vpn_ssl_settings – Configure SSL VPN in Fortinet’s FortiOS and FortiGate.	1511
370.1 Synopsis	1511
370.2 Requirements	1511
370.3 Parameters	1512
370.4 Notes	1512
370.5 Examples	1512
370.6 Return Values	1514
370.7 Status	1514
370.8 Authors	1514
371fortios_vpn_ssl_web_host_check_software – SSL-VPN host check software in Fortinet’s FortiOS and FortiGate.	1515
371.1 Synopsis	1515
371.2 Requirements	1515
371.3 Parameters	1516
371.4 Notes	1516
371.5 Examples	1516
371.6 Return Values	1516
371.7 Status	1517
371.8 Authors	1517

372fortios_vpn_ssl_web_portal – Portal in Fortinet’s FortiOS and FortiGate.	1519
372.1 Synopsis	1519
372.2 Requirements	1519
372.3 Parameters	1520
372.4 Notes	1520
372.5 Examples	1520
372.6 Return Values	1522
372.7 Status	1522
372.8 Authors	1522
373fortios_vpn_ssl_web_realm – Realm in Fortinet’s FortiOS and FortiGate.	1525
373.1 Synopsis	1525
373.2 Requirements	1525
373.3 Parameters	1526
373.4 Notes	1526
373.5 Examples	1526
373.6 Return Values	1526
373.7 Status	1526
373.8 Authors	1526
374fortios_vpn_ssl_web_user_bookmark – Configure SSL VPN user bookmark in Fortinet’s FortiOS and FortiGate.	1529
374.1 Synopsis	1529
374.2 Requirements	1529
374.3 Parameters	1530
374.4 Notes	1530
374.5 Examples	1530
374.6 Return Values	1531
374.7 Status	1531
374.8 Authors	1531
375fortios_vpn_ssl_web_user_group_bookmark – Configure SSL VPN user group bookmark in Fortinet’s FortiOS and FortiGate.	1533
375.1 Synopsis	1533
375.2 Requirements	1533
375.3 Parameters	1534
375.4 Notes	1534
375.5 Examples	1534
375.6 Return Values	1535
375.7 Status	1535
375.8 Authors	1535
376fortios_waf_main_class – Hidden table for datasource in Fortinet’s FortiOS and FortiGate.	1537
376.1 Synopsis	1537
376.2 Requirements	1537
376.3 Parameters	1538
376.4 Notes	1538
376.5 Examples	1538
376.6 Return Values	1538
376.7 Status	1538
376.8 Authors	1538
377fortios_waf_profile – Web application firewall configuration in Fortinet’s FortiOS and FortiGate.	1541
377.1 Synopsis	1541
377.2 Requirements	1541

377.3 Parameters	1542
377.4 Notes	1542
377.5 Examples	1542
377.6 Return Values	1545
377.7 Status	1545
377.8 Authors	1545
378fortios_waf_signature – Hidden table for datasource in Fortinet’s FortiOS and FortiGate.	1547
378.1 Synopsis	1547
378.2 Requirements	1547
378.3 Parameters	1548
378.4 Notes	1548
378.5 Examples	1548
378.6 Return Values	1548
378.7 Status	1548
378.8 Authors	1548
379fortios_waf_sub_class – Hidden table for datasource in Fortinet’s FortiOS and FortiGate.	1551
379.1 Synopsis	1551
379.2 Requirements	1551
379.3 Parameters	1552
379.4 Notes	1552
379.5 Examples	1552
379.6 Return Values	1552
379.7 Status	1552
379.8 Authors	1552
380fortios_wanopt_auth_group – Configure WAN optimization authentication groups in Fortinet’s FortiOS and FortiGate.	1555
380.1 Synopsis	1555
380.2 Requirements	1555
380.3 Parameters	1556
380.4 Notes	1556
380.5 Examples	1556
380.6 Return Values	1556
380.7 Status	1556
380.8 Authors	1556
381fortios_wanopt_cache_service – Designate cache-service for wan-optimization and webcache in Fortinet’s FortiOS and FortiGate.	1559
381.1 Synopsis	1559
381.2 Requirements	1559
381.3 Parameters	1560
381.4 Notes	1560
381.5 Examples	1560
381.6 Return Values	1560
381.7 Status	1561
381.8 Authors	1561
382fortios_wanopt_content_delivery_network_rule – Configure WAN optimization content delivery network rules in Fortinet’s FortiOS and FortiGate.	1563
382.1 Synopsis	1563
382.2 Requirements	1563
382.3 Parameters	1564
382.4 Notes	1564

382.5 Examples	1564
382.6 Return Values	1565
382.7 Status	1565
382.8 Authors	1565
383fortios_wanopt_peer – Configure WAN optimization peers in Fortinet’s FortiOS and FortiGate.	1567
383.1 Synopsis	1567
383.2 Requirements	1567
383.3 Parameters	1568
383.4 Notes	1568
383.5 Examples	1568
383.6 Return Values	1568
383.7 Status	1568
383.8 Authors	1568
384fortios_wanopt_profile – Configure WAN optimization profiles in Fortinet’s FortiOS and FortiGate.	1571
384.1 Synopsis	1571
384.2 Requirements	1571
384.3 Parameters	1572
384.4 Notes	1572
384.5 Examples	1572
384.6 Return Values	1573
384.7 Status	1573
384.8 Authors	1573
385fortios_wanopt_remote_storage – Configure a remote cache device as Web cache storage in Fortinet’s FortiOS and FortiGate.	1575
385.1 Synopsis	1575
385.2 Requirements	1575
385.3 Parameters	1576
385.4 Notes	1576
385.5 Examples	1576
385.6 Return Values	1576
385.7 Status	1576
385.8 Authors	1576
386fortios_wanopt_settings – Configure WAN optimization settings in Fortinet’s FortiOS and FortiGate.	1579
386.1 Synopsis	1579
386.2 Requirements	1579
386.3 Parameters	1580
386.4 Notes	1580
386.5 Examples	1580
386.6 Return Values	1580
386.7 Status	1580
386.8 Authors	1580
387fortios_wanopt_webcache – Configure global Web cache settings in Fortinet’s FortiOS and FortiGate.	1583
387.1 Synopsis	1583
387.2 Requirements	1583
387.3 Parameters	1584
387.4 Notes	1584
387.5 Examples	1584
387.6 Return Values	1584
387.7 Status	1585
387.8 Authors	1585

388	fortios_web_proxy_debug_url – Configure debug URL addresses in Fortinet’s FortiOS and FortiGate.	1587
388.1	Synopsis	1587
388.2	Requirements	1587
388.3	Parameters	1588
388.4	Notes	1588
388.5	Examples	1588
388.6	Return Values	1588
388.7	Status	1588
388.8	Authors	1588
389	fortios_web_proxy_explicit – Configure explicit Web proxy settings in Fortinet’s FortiOS and FortiGate.	1591
389.1	Synopsis	1591
389.2	Requirements	1591
389.3	Parameters	1592
389.4	Notes	1592
389.5	Examples	1592
389.6	Return Values	1593
389.7	Status	1593
389.8	Authors	1593
390	fortios_web_proxy_forward_server – Configure forward-server addresses in Fortinet’s FortiOS and FortiGate.	1595
390.1	Synopsis	1595
390.2	Requirements	1595
390.3	Parameters	1596
390.4	Notes	1596
390.5	Examples	1596
390.6	Return Values	1596
390.7	Status	1596
390.8	Authors	1597
391	fortios_web_proxy_forward_server_group – Configure a forward server group consisting of multiple forward servers. Supports failover and load balancing in Fortinet’s FortiOS and FortiGate.	1599
391.1	Synopsis	1599
391.2	Requirements	1599
391.3	Parameters	1600
391.4	Notes	1600
391.5	Examples	1600
391.6	Return Values	1600
391.7	Status	1600
391.8	Authors	1601
392	fortios_web_proxy_global – Configure Web proxy global settings in Fortinet’s FortiOS and FortiGate.	1603
392.1	Synopsis	1603
392.2	Requirements	1603
392.3	Parameters	1604
392.4	Notes	1604
392.5	Examples	1604
392.6	Return Values	1604
392.7	Status	1605
392.8	Authors	1605
393	fortios_web_proxy_profile – Configure web proxy profiles in Fortinet’s FortiOS and FortiGate.	1607
393.1	Synopsis	1607
393.2	Requirements	1607

393.3 Parameters	1608
393.4 Notes	1608
393.5 Examples	1608
393.6 Return Values	1608
393.7 Status	1609
393.8 Authors	1609
394fortios_web_proxy_url_match – Exempt URLs from web proxy forwarding and caching in Fortinet’s FortiOS and FortiGate.	1611
394.1 Synopsis	1611
394.2 Requirements	1611
394.3 Parameters	1612
394.4 Notes	1612
394.5 Examples	1612
394.6 Return Values	1612
394.7 Status	1612
394.8 Authors	1612
395fortios_web_proxy_wisp – Configure Wireless Internet service provider (WISP) servers in Fortinet’s FortiOS and FortiGate.	1615
395.1 Synopsis	1615
395.2 Requirements	1615
395.3 Parameters	1616
395.4 Notes	1616
395.5 Examples	1616
395.6 Return Values	1616
395.7 Status	1616
395.8 Authors	1616
396fortios_webfilter_content – Configure Web filter banned word table in Fortinet’s FortiOS and FortiGate	1619
396.1 Synopsis	1619
396.2 Requirements	1619
396.3 Parameters	1620
396.4 Notes	1620
396.5 Examples	1620
396.6 Return Values	1620
396.7 Status	1620
396.8 Authors	1621
397fortios_webfilter_content_header – Configure content types used by Web filter in Fortinet’s FortiOS and FortiGate.	1623
397.1 Synopsis	1623
397.2 Requirements	1623
397.3 Parameters	1624
397.4 Notes	1624
397.5 Examples	1624
397.6 Return Values	1624
397.7 Status	1624
397.8 Authors	1624
398fortios_webfilter_fortiguard – Configure FortiGuard Web Filter service in Fortinet’s FortiOS and FortiGate.	1627
398.1 Synopsis	1627
398.2 Requirements	1627
398.3 Parameters	1628

398.4 Notes	1628
398.5 Examples	1628
398.6 Return Values	1628
398.7 Status	1628
398.8 Authors	1629
399fortios_webfilter_ftgd_local_cat – Configure FortiGuard Web Filter local categories in Fortinet’s FortiOS and FortiGate.	1631
399.1 Synopsis	1631
399.2 Requirements	1631
399.3 Parameters	1632
399.4 Notes	1632
399.5 Examples	1632
399.6 Return Values	1632
399.7 Status	1632
399.8 Authors	1632
400fortios_webfilter_ftgd_local_rating – Configure local FortiGuard Web Filter local ratings in Fortinet’s FortiOS and FortiGate.	1635
400.1 Synopsis	1635
400.2 Requirements	1635
400.3 Parameters	1636
400.4 Notes	1636
400.5 Examples	1636
400.6 Return Values	1636
400.7 Status	1636
400.8 Authors	1636
401fortios_webfilter_ips_urlfilter_cache_setting – Configure IPS URL filter cache settings in Fortinet’s FortiOS and FortiGate.	1639
401.1 Synopsis	1639
401.2 Requirements	1639
401.3 Parameters	1640
401.4 Notes	1640
401.5 Examples	1640
401.6 Return Values	1640
401.7 Status	1640
401.8 Authors	1640
402fortios_webfilter_ips_urlfilter_setting – Configure IPS URL filter settings in Fortinet’s FortiOS and FortiGate.	1643
402.1 Synopsis	1643
402.2 Requirements	1643
402.3 Parameters	1644
402.4 Notes	1644
402.5 Examples	1644
402.6 Return Values	1644
402.7 Status	1644
402.8 Authors	1644
403fortios_webfilter_ips_urlfilter_setting6 – Configure IPS URL filter settings for IPv6 in Fortinet’s FortiOS and FortiGate.	1647
403.1 Synopsis	1647
403.2 Requirements	1647
403.3 Parameters	1648

403.4 Notes	1648
403.5 Examples	1648
403.6 Return Values	1648
403.7 Status	1648
403.8 Authors	1648
404fortios_webfilter_override – Configure FortiGuard Web Filter administrative overrides in Fortinet’s FortiOS and FortiGate.	1651
404.1 Synopsis	1651
404.2 Requirements	1651
404.3 Parameters	1652
404.4 Notes	1652
404.5 Examples	1652
404.6 Return Values	1652
404.7 Status	1652
404.8 Authors	1653
405fortios_webfilter_profile – Configure Web filter profiles in Fortinet’s FortiOS and FortiGate.	1655
405.1 Synopsis	1655
405.2 Requirements	1655
405.3 Parameters	1656
405.4 Notes	1656
405.5 Examples	1656
405.6 Return Values	1658
405.7 Status	1658
405.8 Authors	1658
406fortios_webfilter_search_engine – Configure web filter search engines in Fortinet’s FortiOS and FortiGate.	1659
406.1 Synopsis	1659
406.2 Requirements	1659
406.3 Parameters	1660
406.4 Notes	1660
406.5 Examples	1660
406.6 Return Values	1660
406.7 Status	1660
406.8 Authors	1660
407fortios_webfilter_urlfilter – Configure URL filter lists in Fortinet’s FortiOS and FortiGate.	1663
407.1 Synopsis	1663
407.2 Requirements	1663
407.3 Parameters	1664
407.4 Notes	1664
407.5 Examples	1664
407.6 Return Values	1664
407.7 Status	1665
407.8 Authors	1665
408fortios_wireless_controller_ap_status – Configure access point status (rogue accepted suppressed) in Fortinet’s FortiOS and FortiGate.	1667
408.1 Synopsis	1667
408.2 Requirements	1667
408.3 Parameters	1668
408.4 Notes	1668
408.5 Examples	1668

408.6 Return Values	1668
408.7 Status	1668
408.8 Authors	1668
409fortios_wireless_controller_ble_profile – Configure Bluetooth Low Energy profile in Fortinet’s FortiOS and FortiGate.	1671
409.1 Synopsis	1671
409.2 Requirements	1671
409.3 Parameters	1672
409.4 Notes	1672
409.5 Examples	1672
409.6 Return Values	1672
409.7 Status	1672
409.8 Authors	1673
410fortios_wireless_controller_bonjour_profile – Configure Bonjour profiles. Bonjour is Apple’s zero configuration networking protocol. Bonjour profiles allow APs and FortiAPs to connect to networks using Bonjour in Fortinet’s FortiOS and FortiGate.	1675
410.1 Synopsis	1675
410.2 Requirements	1676
410.3 Parameters	1676
410.4 Notes	1676
410.5 Examples	1676
410.6 Return Values	1676
410.7 Status	1677
410.8 Authors	1677
411fortios_wireless_controller_global – Configure wireless controller global settings in Fortinet’s FortiOS and FortiGate.	1679
411.1 Synopsis	1679
411.2 Requirements	1679
411.3 Parameters	1680
411.4 Notes	1680
411.5 Examples	1680
411.6 Return Values	1680
411.7 Status	1681
411.8 Authors	1681
412fortios_wireless_controller_hotspot20_anqp_3gpp_cellular – Configure 3GPP public land mobile network (PLMN) in Fortinet’s FortiOS and FortiGate.	1683
412.1 Synopsis	1683
412.2 Requirements	1683
412.3 Parameters	1684
412.4 Notes	1684
412.5 Examples	1684
412.6 Return Values	1684
412.7 Status	1684
412.8 Authors	1685
413fortios_wireless_controller_hotspot20_anqp_ip_address_type – Configure IP address type availability in Fortinet’s FortiOS and FortiGate.	1687
413.1 Synopsis	1687
413.2 Requirements	1687
413.3 Parameters	1688
413.4 Notes	1688

413.5 Examples	1688
413.6 Return Values	1688
413.7 Status	1688
413.8 Authors	1688
414fortios_wireless_controller_hotspot20_anqp_nai_realm – Configure network access identifier (NAI) realm in Fortinet’s FortiOS and FortiGate.	1691
414.1 Synopsis	1691
414.2 Requirements	1691
414.3 Parameters	1692
414.4 Notes	1692
414.5 Examples	1692
414.6 Return Values	1692
414.7 Status	1693
414.8 Authors	1693
415fortios_wireless_controller_hotspot20_anqp_network_auth_type – Configure network authentication type in Fortinet’s FortiOS and FortiGate.	1695
415.1 Synopsis	1695
415.2 Requirements	1695
415.3 Parameters	1696
415.4 Notes	1696
415.5 Examples	1696
415.6 Return Values	1696
415.7 Status	1696
415.8 Authors	1696
416fortios_wireless_controller_hotspot20_anqp_roaming_consortium – Configure roaming consortium in Fortinet’s FortiOS and FortiGate.	1699
416.1 Synopsis	1699
416.2 Requirements	1699
416.3 Parameters	1700
416.4 Notes	1700
416.5 Examples	1700
416.6 Return Values	1700
416.7 Status	1700
416.8 Authors	1700
417fortios_wireless_controller_hotspot20_anqp_venue_name – Configure venue name duple in Fortinet’s FortiOS and FortiGate.	1703
417.1 Synopsis	1703
417.2 Requirements	1703
417.3 Parameters	1704
417.4 Notes	1704
417.5 Examples	1704
417.6 Return Values	1704
417.7 Status	1704
417.8 Authors	1704
418fortios_wireless_controller_hotspot20_h2qp_conn_capability – Configure connection capability in Fortinet’s FortiOS and FortiGate.	1707
418.1 Synopsis	1707
418.2 Requirements	1707
418.3 Parameters	1708
418.4 Notes	1708

418.5 Examples	1708
418.6 Return Values	1708
418.7 Status	1708
418.8 Authors	1709
419fortios_wireless_controller_hotspot20_h2qp_operator_name – Configure operator friendly name in Fortinet’s FortiOS and FortiGate.	1711
419.1 Synopsis	1711
419.2 Requirements	1711
419.3 Parameters	1712
419.4 Notes	1712
419.5 Examples	1712
419.6 Return Values	1712
419.7 Status	1712
419.8 Authors	1712
420fortios_wireless_controller_hotspot20_h2qp_osu_provider – Configure online sign up (OSU) provider list in Fortinet’s FortiOS and FortiGate.	1715
420.1 Synopsis	1715
420.2 Requirements	1715
420.3 Parameters	1716
420.4 Notes	1716
420.5 Examples	1716
420.6 Return Values	1716
420.7 Status	1717
420.8 Authors	1717
421fortios_wireless_controller_hotspot20_h2qp_wan_metric – Configure WAN metrics in Fortinet’s FortiOS and FortiGate.	1719
421.1 Synopsis	1719
421.2 Requirements	1719
421.3 Parameters	1720
421.4 Notes	1720
421.5 Examples	1720
421.6 Return Values	1720
421.7 Status	1720
421.8 Authors	1721
422fortios_wireless_controller_hotspot20_hs_profile – Configure hotspot profile in Fortinet’s FortiOS and FortiGate.	1723
422.1 Synopsis	1723
422.2 Requirements	1723
422.3 Parameters	1724
422.4 Notes	1724
422.5 Examples	1724
422.6 Return Values	1725
422.7 Status	1725
422.8 Authors	1725
423fortios_wireless_controller_hotspot20_icon – Configure OSU provider icon in Fortinet’s FortiOS and FortiGate.	1727
423.1 Synopsis	1727
423.2 Requirements	1727
423.3 Parameters	1728
423.4 Notes	1728

423.5 Examples	1728
423.6 Return Values	1728
423.7 Status	1728
423.8 Authors	1729
424fortios_wireless_controller_hotspot20_qos_map – Configure QoS map set in Fortinet’s FortiOS and FortiGate.	1731
424.1 Synopsis	1731
424.2 Requirements	1731
424.3 Parameters	1732
424.4 Notes	1732
424.5 Examples	1732
424.6 Return Values	1732
424.7 Status	1732
424.8 Authors	1733
425fortios_wireless_controller_inter_controller – Configure inter wireless controller operation in Fortinet’s FortiOS and FortiGate.	1735
425.1 Synopsis	1735
425.2 Requirements	1735
425.3 Parameters	1736
425.4 Notes	1736
425.5 Examples	1736
425.6 Return Values	1736
425.7 Status	1736
425.8 Authors	1737
426fortios_wireless_controller_qos_profile – Configure WiFi quality of service (QoS) profiles in Fortinet’s FortiOS and FortiGate.	1739
426.1 Synopsis	1739
426.2 Requirements	1739
426.3 Parameters	1740
426.4 Notes	1740
426.5 Examples	1740
426.6 Return Values	1741
426.7 Status	1741
426.8 Authors	1741
427fortios_wireless_controller_setting – VDOM wireless controller configuration in Fortinet’s FortiOS and FortiGate.	1743
427.1 Synopsis	1743
427.2 Requirements	1743
427.3 Parameters	1744
427.4 Notes	1744
427.5 Examples	1744
427.6 Return Values	1744
427.7 Status	1744
427.8 Authors	1744
428fortios_wireless_controller_timers – Configure CAPWAP timers in Fortinet’s FortiOS and FortiGate.	1747
428.1 Synopsis	1747
428.2 Requirements	1747
428.3 Parameters	1748
428.4 Notes	1748
428.5 Examples	1748

428.6 Return Values	1748
428.7 Status	1749
428.8 Authors	1749
429fortios_wireless_controller_utm_profile – Configure UTM (Unified Threat Management) profile in Fortinet’s FortiOS and FortiGate.	1751
429.1 Synopsis	1751
429.2 Requirements	1751
429.3 Parameters	1752
429.4 Notes	1752
429.5 Examples	1752
429.6 Return Values	1752
429.7 Status	1752
429.8 Authors	1752
430fortios_wireless_controller_vap – Configure Virtual Access Points (VAPs) in Fortinet’s FortiOS and FortiGate.	1755
430.1 Synopsis	1755
430.2 Requirements	1755
430.3 Parameters	1756
430.4 Notes	1756
430.5 Examples	1756
430.6 Return Values	1758
430.7 Status	1758
430.8 Authors	1758
431fortios_wireless_controller_vap_group – Configure virtual Access Point (VAP) groups in Fortinet’s FortiOS and FortiGate.	1761
431.1 Synopsis	1761
431.2 Requirements	1761
431.3 Parameters	1762
431.4 Notes	1762
431.5 Examples	1762
431.6 Return Values	1762
431.7 Status	1762
431.8 Authors	1762
432fortios_wireless_controller_wids_profile – Configure wireless intrusion detection system (WIDS) profiles in Fortinet’s FortiOS and FortiGate.	1765
432.1 Synopsis	1765
432.2 Requirements	1765
432.3 Parameters	1766
432.4 Notes	1766
432.5 Examples	1766
432.6 Return Values	1767
432.7 Status	1767
432.8 Authors	1767
433fortios_wireless_controller_wtp – Configure Wireless Termination Points (WTPs), that is, FortiAPs or APs to be managed by FortiGate in Fortinet’s FortiOS and FortiGate.	1769
433.1 Synopsis	1769
433.2 Requirements	1769
433.3 Parameters	1770
433.4 Notes	1770
433.5 Examples	1770

433.6 Return Values	1772
433.7 Status	1772
433.8 Authors	1772
434fortios_wireless_controller_wtp_group – Configure WTP groups in Fortinet’s FortiOS and FortiGate.	1773
434.1 Synopsis	1773
434.2 Requirements	1773
434.3 Parameters	1774
434.4 Notes	1774
434.5 Examples	1774
434.6 Return Values	1774
434.7 Status	1774
434.8 Authors	1774
435fortios_wireless_controller_wtp_profile – Configure WTP profiles or FortiAP profiles that define radio settings for manageable FortiAP platforms in Fortinet’s FortiOS and FortiGate.	1777
435.1 Synopsis	1777
435.2 Requirements	1777
435.3 Parameters	1778
435.4 Notes	1778
435.5 Examples	1778
435.6 Return Values	1781
435.7 Status	1781
435.8 Authors	1782
436Indices and tables	1783

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*

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

1.2 Requirements

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

- ansible>=2.9.0

1.3 Parameters

1.4 Notes

Note:

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

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>"
      notification_interval: "30"
```

(continues on next page)

(continued from previous page)

```
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"
```

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:

1.7 Status

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

1.8 Authors

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

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

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*

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

2.2 Requirements

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

- ansible>=2.9.0

2.3 Parameters

2.4 Notes

Note:

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

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"
```

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:

2.7 Status

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

2.8 Authors

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

- Nicolas Thomas (@thomnico)

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

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*

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

3.2 Requirements

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

- ansible>=2.9.0

3.3 Parameters

3.4 Notes

Note:

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

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"
    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:
```

(continues on next page)

(continued from previous page)

```

    archive_block: "encrypted"
    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:

```

(continues on next page)

(continued from previous page)

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

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:

3.7 Status

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

3.8 Authors

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

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

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*

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

4.2 Requirements

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

- ansible>=2.9.0

4.3 Parameters

4.4 Notes

Note:

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

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"
```

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:

4.7 Status

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

4.8 Authors

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

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

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*

5.1 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

5.2 Requirements

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

- ansible>=2.9.0

5.3 Parameters

5.4 Notes

Note:

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

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"
```

5.6 Return Values

Common return values are documented: https://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 Status

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

5.8 Authors

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

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

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

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*

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

6.2 Requirements

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

- ansible>=2.9.0

6.3 Parameters

6.4 Notes

Note:

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

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"
    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>"
```

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:

6.7 Status

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

6.8 Authors

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

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

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*

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

7.2 Requirements

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

- ansible>=2.9.0

7.3 Parameters

7.4 Notes

Note:

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

7.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Configure firewall application groups.
      fortios_application_group:
        vdom: "{{ vdom }}"
        state: "present"
        application_group:
          application:
            -
              id: "4"
            category:
            -
              id: "6"
          comment: "Comment"
          name: "default_name_8"
          type: "application"
```

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:

7.7 Status

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

7.8 Authors

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

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

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*

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

8.2 Requirements

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

- ansible>=2.9.0

8.3 Parameters

8.4 Notes

Note:

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

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:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

(continues on next page)

(continued from previous page)

```

    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"

```

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:

8.7 Status

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

8.8 Authors

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

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

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*

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

9.2 Requirements

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

- ansible>=2.9.0

9.3 Parameters

9.4 Notes

Note:

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

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"
    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"
```

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:

9.7 Status

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

9.8 Authors

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

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

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*

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

10.2 Requirements

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

- ansible>=2.9.0

10.3 Parameters

10.4 Notes

Note:

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

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"
        application_rule_settings:
          id: "3"
```

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:

10.7 Status

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

10.8 Authors

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

- Nicolas Thomas (@thomnico)

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

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*

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

11.2 Requirements

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

- ansible>=2.9.0

11.3 Parameters

11.4 Notes

Note:

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

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"
    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"
```

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:

11.7 Status

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

11.8 Authors

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

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

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*

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

12.2 Requirements

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

- ansible>=2.9.0

12.3 Parameters

12.4 Notes

Note:

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

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"
    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.datasources.name user.radius.name_
↪user.tacacs+.name user.ldap.name user.group.name)"
```

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:

12.7 Status

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

12.8 Authors

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

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

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*

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

13.2 Requirements

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

- ansible>=2.9.0

13.3 Parameters

13.4 Notes

Note:

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

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) "
```

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:

13.7 Status

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

13.8 Authors

- Link Zheng (@chillancezen)

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

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

`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*

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

14.2 Requirements

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

- `ansible>=2.9.0`

14.3 Parameters

14.4 Notes

Note:

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

14.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
  - name: CA certificate.
    fortios_certificate_ca:
      vdom: "{{ vdom }}"
      state: "present"
      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"
```

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:

14.7 Status

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

14.8 Authors

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

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

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*

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

15.2 Requirements

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

- ansible>=2.9.0

15.3 Parameters

15.4 Notes

Note:

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

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:
    vdom: "{{ vdom }}"
    state: "present"
    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)"
```

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:

15.7 Status

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

15.8 Authors

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

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

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*

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

16.2 Requirements

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

- ansible>=2.9.0

16.3 Parameters

16.4 Notes

Note:

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

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:
    vdom: "{{ vdom }}"
    state: "present"
    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>"
```

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:

16.7 Status

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

16.8 Authors

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

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

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*

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

17.2 Requirements

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

- ansible>=2.9.0

17.3 Parameters

17.4 Notes

Note:

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

17.5 Examples

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

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:

17.7 Status

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

17.8 Authors

- Link Zheng (@chillancezen)

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

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

`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*

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

18.2 Requirements

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

- ansible>=2.9.0

18.3 Parameters

18.4 Notes

Note:

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

18.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Create a DLP fingerprint database by allowing the FortiGate to access a
      ↪file server containing files from which to create fingerprints.
      fortios_dlp_fp_doc_source:
        vdom: "{{ vdom }}"
        state: "present"
        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"
```

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:

18.7 Status

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

18.8 Authors

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

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

`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*

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

19.2 Requirements

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

- ansible>=2.9.0

19.3 Parameters

19.4 Notes

Note:

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

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"
        dlp_fp_sensitivity:
          name: "default_name_3"
```

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:

19.7 Status

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

19.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

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

20.2 Requirements

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

- ansible>=2.9.0

20.3 Parameters

20.4 Notes

Note:

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

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:
    vdom: "{{ vdom }}"
    state: "present"
    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>"
```

(continues on next page)

(continued from previous page)

```
replacemsg_group: "<your_own_value> (source system.replacemsg-group.name) "  
summary_proto: "smtp"
```

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:

20.7 Status

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

20.8 Authors

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

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

`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*

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

21.2 Requirements

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

- `ansible>=2.9.0`

21.3 Parameters

21.4 Notes

Note:

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

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) "
```

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:

21.7 Status

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

21.8 Authors

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

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

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

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*

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

22.2 Requirements

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

- ansible>=2.9.0

22.3 Parameters

22.4 Notes

Note:

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

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:
        vdom: "{{ vdom }}"
        state: "present"
        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"
```

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:

22.7 Status

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

22.8 Authors

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

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

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*

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

23.2 Requirements

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

- ansible>=2.9.0

23.3 Parameters

23.4 Notes

Note:

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

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"
    dnsfilter_profile:
      block_action: "block"
      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"
```


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:

23.7 Status

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

23.8 Authors

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

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

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*

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

24.2 Requirements

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

- ansible>=2.9.0

24.3 Parameters

24.4 Notes

Note:

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

24.5 Examples

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

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:

24.7 Status

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

24.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

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

25.2 Requirements

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

- ansible>=2.9.0

25.3 Parameters

25.4 Notes

Note:

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

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 }}"
        state: "present"
        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"
```

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:

25.7 Status

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

25.8 Authors

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

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

`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*

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

26.2 Requirements

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

- ansible>=2.9.0

26.3 Parameters

26.4 Notes

Note:

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

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"
        endpoint_control_forticlient_registration_sync:
          peer_ip: "<your_own_value>"
          peer_name: "<your_own_value>"
```

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:

26.7 Status

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

26.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

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

27.2 Requirements

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

- ansible>=2.9.0

27.3 Parameters

27.4 Notes

Note:

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

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"
        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)"
        forticlient_ios_settings:
          client_vpn_provisioning: "enable"
          client_vpn_settings:
            -
              auth_method: "psk"
              name: "default_name_25"
```

(continues on next page)

(continued from previous page)

```

    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>"
          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>"

```

(continues on next page)

(continued from previous page)

```

        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) "

```

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:

27.7 Status

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

27.8 Authors

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

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

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

`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*

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

28.2 Requirements

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

- `ansible>=2.9.0`

28.3 Parameters

28.4 Notes

Note:

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

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"
        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>"
```

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:

28.7 Status

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

28.8 Authors

- Link Zheng (@chillancezen)

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

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

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*

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

29.2 Requirements

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

- ansible>=2.9.0

29.3 Parameters

29.4 Notes

Note:

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

29.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure endpoint control settings.
  fortios_endpoint_control_settings:
    vdom: "{{ vdom }}"
    endpoint_control_settings:
      download_custom_link: "<your_own_value>"
      download_location: "fortiguard"
      forticlient_avdb_update_interval: "5"
      forticlient_dereg_unsupported_client: "enable"
      forticlient_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"
```

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:

29.7 Status

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

29.8 Authors

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

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

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*

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

30.2 Requirements

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

- `ansible>=2.9.0`

30.3 Parameters

30.4 Notes

Note:

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

30.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Extender controller configuration.
  fortios_extender_controller_extender:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

(continues on next page)

(continued from previous page)

```
redial: "none"
redundant_intf: "<your_own_value>"
roaming: "enable"
role: "none"
secondary_ha: "<your_own_value>"
sim_pin: "<your_own_value>"
vdom: "36"
wimax_auth_protocol: "tls"
wimax_carrier: "<your_own_value>"
wimax_realm: "<your_own_value>"
```

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:

30.7 Status

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

30.8 Authors

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

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

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*

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

31.2 Requirements

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

- ansible>=2.9.0

31.3 Parameters

31.4 Notes

Note:

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

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"
    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"
```

(continues on next page)

(continued from previous page)

```
tags:
  -
    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>"
```

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:

31.7 Status

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

31.8 Authors

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

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

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*

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

32.2 Requirements

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

- ansible>=2.9.0

32.3 Parameters

32.4 Notes

Note:

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

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"
    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>"
      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)"
```

(continues on next page)

(continued from previous page)

```
template: "<your_own_value> (source firewall.address6-template.name) "  
type: "ipprefix"  
uuid: "<your_own_value>"  
visibility: "enable"
```

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:

32.7 Status

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

32.8 Authors

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

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

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*

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

33.2 Requirements

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

- ansible>=2.9.0

33.3 Parameters

33.4 Notes

Note:

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

33.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Configure IPv6 address templates.
  fortios_firewall_address6_template:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

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:

33.7 Status

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

33.8 Authors

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

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

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*

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

34.2 Requirements

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

- ansible>=2.9.0

34.3 Parameters

34.4 Notes

Note:

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

34.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure IPv4 address groups.
  fortios_firewall_addrgrp:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

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:

34.7 Status

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

34.8 Authors

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

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

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*

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

35.2 Requirements

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

- ansible>=2.9.0

35.3 Parameters

35.4 Notes

Note:

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

35.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Configure IPv6 address groups.
  fortios_firewall_addrgrp6:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

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:

35.7 Status

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

35.8 Authors

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

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

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*

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

36.2 Requirements

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

- ansible>=2.9.0

36.3 Parameters

36.4 Notes

Note:

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

36.5 Examples

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

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:

36.7 Status

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

36.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

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

37.2 Requirements

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

- ansible>=2.9.0

37.3 Parameters

37.4 Notes

Note:

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

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"
    firewall_central_snat_map:
      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"
```

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:

37.7 Status

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

37.8 Authors

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

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

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*

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

38.2 Requirements

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

- ansible>=2.9.0

38.3 Parameters

38.4 Notes

Note:

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

38.5 Examples

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

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:

38.7 Status

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

38.8 Authors

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

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

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

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*

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

39.2 Requirements

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

- ansible>=2.9.0

39.3 Parameters

39.4 Notes

Note:

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

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"
    firewall_dos_policy:
      anomaly:
        -
          action: "pass"
          log: "enable"
          name: "default_name_6"
          quarantine: "none"
          quarantine_expiry: "<your_own_value>"
          quarantine_log: "disable"
          status: "disable"
          threshold: "11"
          threshold(default): "12"
        comments: "<your_own_value>"
        dstaddr:
          -
            name: "default_name_15 (source firewall.address.name firewall.addrgrp.
↪name) "
            interface: "<your_own_value> (source system.zone.name system.interface.name) "
            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"
```

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:

39.7 Status

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

39.8 Authors

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

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

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*

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

40.2 Requirements

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

- ansible>=2.9.0

40.3 Parameters

40.4 Notes

Note:

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

40.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Configure IPv6 DoS policies.
  fortios_firewall_dos_policy6:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

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:

40.7 Status

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

40.8 Authors

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

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

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*

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

41.2 Requirements

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

- ansible>=2.9.0

41.3 Parameters

41.4 Notes

Note:

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

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"
    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"
```

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:

41.7 Status

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

41.8 Authors

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

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

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*

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

42.2 Requirements

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

- ansible>=2.9.0

42.3 Parameters

42.4 Notes

Note:

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

42.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Configure IPv4 interface policies.
  fortios_firewall_interface_policy:
    vdom: "{{ vdom }}"
    state: "present"
    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:
```

(continues on next page)

(continued from previous page)

```
-
  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"
```

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:

42.7 Status

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

42.8 Authors

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

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

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*

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

43.2 Requirements

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

- ansible>=2.9.0

43.3 Parameters

43.4 Notes

Note:

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

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"
    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"
```

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:

43.7 Status

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

43.8 Authors

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

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

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*

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

44.2 Requirements

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

- ansible>=2.9.0

44.3 Parameters

44.4 Notes

Note:

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

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

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:

44.7 Status

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

44.8 Authors

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

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

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*

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

45.2 Requirements

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

- ansible>=2.9.0

45.3 Parameters

45.4 Notes

Note:

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

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"
    firewall_internet_service_custom:
      comment: "Comment."
      disable_entry:
        -
          id: "5"
          ip_range:
            -
              end_ip: "<your_own_value>"
              id: "8"
              start_ip: "<your_own_value>"
            port: "10"
            protocol: "11"
          entry:
            -
              dst:
                -
                  name: "default_name_14 (source firewall.address.name firewall.addrgrp.
↪name) "
              id: "15"
              port_range:
                -
                  end_port: "17"
                  id: "18"
                  start_port: "19"
                protocol: "20"
              master_service_id: "21 (source firewall.internet-service.id) "
              name: "default_name_22"
```

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:

45.7 Status

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

45.8 Authors

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

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

`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*

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

46.2 Requirements

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

- `ansible>=2.9.0`

46.3 Parameters

46.4 Notes

Note:

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

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

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:

46.7 Status

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

46.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

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

47.2 Requirements

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

- ansible>=2.9.0

47.3 Parameters

47.4 Notes

Note:

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

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"
    firewall_internet_service_group:
      comment: "Comment."
      member:
        -
          id: "5 (source firewall.internet-service.id)"
          name: "default_name_6"
```

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:

47.7 Status

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

47.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

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

48.2 Requirements

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

- ansible>=2.9.0

48.3 Parameters

48.4 Notes

Note:

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

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"
    firewall_ip_translation:
      endip: "<your_own_value>"
      map_startip: "<your_own_value>"
      startip: "<your_own_value>"
      transid: "6"
      type: "SCTP"
```

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:

48.7 Status

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

48.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

`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*

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

49.2 Requirements

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

- `ansible>=2.9.0`

49.3 Parameters

49.4 Notes

Note:

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

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"
```

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:

49.7 Status

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

49.8 Authors

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

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

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

`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*

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

50.2 Requirements

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

- `ansible>=2.9.0`

50.3 Parameters

50.4 Notes

Note:

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

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:
        vdom: "{{ vdom }}"
        state: "present"
        firewall_ipmacbinding_table:
          ip: "<your_own_value>"
          mac: "<your_own_value>"
          name: "default_name_5"
          seq_num: "6"
          status: "enable"
```

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:

50.7 Status

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

50.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

51.1 Synopsis

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

51.2 Requirements

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

- ansible>=2.9.0

51.3 Parameters

51.4 Notes

Note:

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

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"
    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>"
      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"
```

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:

51.7 Status

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

51.8 Authors

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

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

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*

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

52.2 Requirements

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

- ansible>=2.9.0

52.3 Parameters

52.4 Notes

Note:

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

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"
        firewall_ippool6:
          comments: "<your_own_value>"
          endip: "<your_own_value>"
          name: "default_name_5"
          startip: "<your_own_value>"
```

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:

52.7 Status

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

52.8 Authors

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

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

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

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*

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

53.2 Requirements

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

- ansible>=2.9.0

53.3 Parameters

53.4 Notes

Note:

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

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"
```

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:

53.7 Status

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

53.8 Authors

- Link Zheng (@chillancezen)

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

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

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*

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

54.2 Requirements

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

- ansible>=2.9.0

54.3 Parameters

54.4 Notes

Note:

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

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"
    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"
```

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:

54.7 Status

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

54.8 Authors

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

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

`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*

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

55.2 Requirements

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

- `ansible>=2.9.0`

55.3 Parameters

55.4 Notes

Note:

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

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"
    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"
```

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:

55.7 Status

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

55.8 Authors

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

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

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*

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

56.2 Requirements

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

- ansible>=2.9.0

56.3 Parameters

56.4 Notes

Note:

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

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"
        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"
```

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:

56.7 Status

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

56.8 Authors

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

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

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*

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

57.2 Requirements

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

- ansible>=2.9.0

57.3 Parameters

57.4 Notes

Note:

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

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"
    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"
```

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:

57.7 Status

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

57.8 Authors

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

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

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*

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

58.2 Requirements

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

- ansible>=2.9.0

58.3 Parameters

58.4 Notes

Note:

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

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"
    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"
```

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:

58.7 Status

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

58.8 Authors

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

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

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*

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

59.2 Requirements

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

- ansible>=2.9.0

59.3 Parameters

59.4 Notes

Note:

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

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"
    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"
```

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:

59.7 Status

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

59.8 Authors

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

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

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*

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

60.2 Requirements

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

- ansible>=2.9.0

60.3 Parameters

60.4 Notes

Note:

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

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"
    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"
```

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:

60.7 Status

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

60.8 Authors

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

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

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*

61.1 Synopsis

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

61.2 Requirements

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

- ansible>=2.9.0

61.3 Parameters

61.4 Notes

Note:

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

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"
    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)"
```

(continues on next page)

(continued from previous page)

```

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:
-
  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"

```

(continues on next page)

(continued from previous page)

```

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"
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"

```

(continues on next page)

(continued from previous page)

```

    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:
      -
        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) "
    vpngateway: "<your_own_value> (source vpn.ipsec.phasel.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) "
    wssso: "enable"

```

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:

61.7 Status

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

61.8 Authors

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

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

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

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*

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

62.2 Requirements

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

- ansible>=2.9.0

62.3 Parameters

62.4 Notes

Note:

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

62.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Configure IPv4 to IPv6 policies.
  fortios_firewall_policy46:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

(continues on next page)

(continued from previous page)

```
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>"
```

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:

62.7 Status

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

62.8 Authors

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

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

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*

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

63.2 Requirements

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

- ansible>=2.9.0

63.3 Parameters

63.4 Notes

Note:

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

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"
    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"
```

(continues on next page)

(continued from previous page)

```

dscp_value: "<your_own_value>"
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:
-

```

(continues on next page)

(continued from previous page)

```

        name: "default_name_68 (source system.zone.name system.interface.name) "
        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) "

```

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:

63.7 Status

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

63.8 Authors

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

- Nicolas Thomas (@thomnico)

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

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*

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

64.2 Requirements

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

- ansible>=2.9.0

64.3 Parameters

64.4 Notes

Note:

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

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"
    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)"
```

(continues on next page)

(continued from previous page)

```

    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>"

```

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:

64.7 Status

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

64.8 Authors

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

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

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*

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

65.2 Requirements

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

- ansible>=2.9.0

65.3 Parameters

65.4 Notes

Note:

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

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"
    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) "
```

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:

65.7 Status

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

65.8 Authors

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

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

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*

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

66.2 Requirements

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

- ansible>=2.9.0

66.3 Parameters

66.4 Notes

Note:

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

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"
    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: "jiso0201"
```

(continues on next page)

(continued from previous page)

```

    range_block: "disable"
    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"

```

(continues on next page)

(continued from previous page)

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

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:

66.7 Status

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

66.8 Authors

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

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

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*

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

67.2 Requirements

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

- ansible>=2.9.0

67.3 Parameters

67.4 Notes

Note:

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

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"
    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"
          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:
```

(continues on next page)

(continued from previous page)

```
-
  name: "default_name_26 (source system.object-tagging.tags.name) "
  type: "host-regex"
  ua: "chrome"
  uuid: "<your_own_value>"
  visibility: "enable"
```

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:

67.7 Status

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

67.8 Authors

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

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

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*

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

68.2 Requirements

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

- ansible>=2.9.0

68.3 Parameters

68.4 Notes

Note:

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

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:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

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:

68.7 Status

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

68.8 Authors

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

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

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*

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

69.2 Requirements

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

- ansible>=2.9.0

69.3 Parameters

69.4 Notes

Note:

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

69.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Configure proxy policies.
  fortios_firewall_proxy_policy:
    vdom: "{{ vdom }}"
    state: "present"
    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) "
```

(continues on next page)

(continued from previous page)

```

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"
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)"

```

(continues on next page)

(continued from previous page)

```
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) "
```

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:

69.7 Status

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

69.8 Authors

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

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

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*

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

70.2 Requirements

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

- ansible>=2.9.0

70.3 Parameters

70.4 Notes

Note:

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

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"
    firewall_schedule_group:
      color: "3"
      member:
        -
          name: "default_name_5 (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name)"
          name: "default_name_6"
```

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:

70.7 Status

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

70.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

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

71.2 Requirements

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

- ansible>=2.9.0

71.3 Parameters

71.4 Notes

Note:

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

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"
    firewall_schedule_onetime:
      color: "3"
      end: "<your_own_value>"
      expiration_days: "5"
      name: "default_name_6"
      start: "<your_own_value>"
```

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:

71.7 Status

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

71.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

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

72.2 Requirements

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

- ansible>=2.9.0

72.3 Parameters

72.4 Notes

Note:

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

72.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Recurring schedule configuration.
  fortios_firewall_schedule_recurring:
    vdom: "{{ vdom }}"
    state: "present"
    firewall_schedule_recurring:
      color: "3"
      day: "sunday"
      end: "<your_own_value>"
      name: "default_name_6"
      start: "<your_own_value>"
```

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:

72.7 Status

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

72.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

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

73.2 Requirements

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

- ansible>=2.9.0

73.3 Parameters

73.4 Notes

Note:

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

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"
        firewall_service_category:
          comment: "Comment."
          name: "default_name_4"
```

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:

73.7 Status

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

73.8 Authors

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

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

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

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*

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

74.2 Requirements

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

- ansible>=2.9.0

74.3 Parameters

74.4 Notes

Note:

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

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"
    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"
              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"
```

(continues on next page)

(continued from previous page)

```
udp_portrange: "<your_own_value>"
visibility: "enable"
```

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:

74.7 Status

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

74.8 Authors

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

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

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*

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

75.2 Requirements

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

- ansible>=2.9.0

75.3 Parameters

75.4 Notes

Note:

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

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 }}"
    state: "present"
    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"
```

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:

75.7 Status

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

75.8 Authors

- Link Zheng (@chillancezen)

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

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

`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*

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

76.2 Requirements

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

- `ansible>=2.9.0`

76.3 Parameters

76.4 Notes

Note:

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

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"
    firewall_shaper_per_ip_shaper:
      bandwidth_unit: "kbps"
      diffserv_forward: "enable"
      diffserv_reverse: "enable"
      diffservcode_forward: "<your_own_value>"
      diffservcode_rev: "<your_own_value>"
      max_bandwidth: "8"
      max_concurrent_session: "9"
      name: "default_name_10"
```

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:

76.7 Status

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

76.8 Authors

- Link Zheng (@chillancezen)

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

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

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*

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

77.2 Requirements

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

- ansible>=2.9.0

77.3 Parameters

77.4 Notes

Note:

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

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"
    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"
```

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:

77.7 Status

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

77.8 Authors

- Link Zheng (@chillancezen)

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

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

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*

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

78.2 Requirements

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

- ansible>=2.9.0

78.3 Parameters

78.4 Notes

Note:

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

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"
    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) "
```

(continues on next page)

(continued from previous page)

```

internet_service_id:
-
  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)"

```

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:

78.7 Status

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

78.8 Authors

- Link Zheng (@chillancezen)

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

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

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*

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

79.2 Requirements

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

- ansible>=2.9.0

79.3 Parameters

79.4 Notes

Note:

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

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"
    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"
```

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:

79.7 Status

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

79.8 Authors

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

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

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*

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

80.2 Requirements

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

- ansible>=2.9.0

80.3 Parameters

80.4 Notes

Note:

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

80.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Configure sniffer.
  fortios_firewall_sniffer:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

(continues on next page)

(continued from previous page)

```
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"
```

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:

80.7 Status

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

80.8 Authors

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

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

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*

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

81.2 Requirements

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

- ansible>=2.9.0

81.3 Parameters

81.4 Notes

Note:

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

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"
    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"
```

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:

81.7 Status

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

81.8 Authors

- Link Zheng (@chillancezen)

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

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

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*

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

82.2 Requirements

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

- ansible>=2.9.0

82.3 Parameters

82.4 Notes

Note:

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

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"
    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"
```

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:

82.7 Status

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

82.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

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

83.2 Requirements

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

- ansible>=2.9.0

83.3 Parameters

83.4 Notes

Note:

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

83.5 Examples

```
- hosts: fortigates
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 keys.
  fortios_firewall_ssh_local_key:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

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:

83.7 Status

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

83.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

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

84.2 Requirements

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

- ansible>=2.9.0

84.3 Parameters

84.4 Notes

Note:

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

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"
      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) "
```

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:

84.7 Status

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

84.8 Authors

- Link Zheng (@chillancezen)

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

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

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*

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

85.2 Requirements

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

- ansible>=2.9.0

85.3 Parameters

85.4 Notes

Note:

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

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"
    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"
      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"
```

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:

85.7 Status

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

85.8 Authors

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

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

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*

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

86.2 Requirements

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

- ansible>=2.9.0

86.3 Parameters

86.4 Notes

Note:

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

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"
```

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:

86.7 Status

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

86.8 Authors

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

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

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*

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

87.2 Requirements

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

- ansible>=2.9.0

87.3 Parameters

87.4 Notes

Note:

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

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"
    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"
        unsupported_ssl: "bypass"
        untrusted_cert: "allow"
      mapi_over_https: "enable"
      name: "default_name_27"
      pop3s:
        allow_invalid_server_cert: "enable"
```

(continues on next page)

(continued from previous page)

```

        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"
                    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"

```

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:

87.7 Status

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

87.8 Authors

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

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

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*

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

88.2 Requirements

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

- ansible>=2.9.0

88.3 Parameters

88.4 Notes

Note:

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

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"
    firewall_ttl_policy:
      action: "accept"
      id: "4"
      schedule: "<your_own_value> (source firewall.schedule.onetime.name firewall.
↪schedule.recurring.name firewall.schedule.group.name) "
      service:
        -
          name: "default_name_7 (source firewall.service.custom.name firewall.
↪service.group.name) "
          srcaddr:
            -
              name: "default_name_9 (source firewall.address.name firewall.addrgrp.name)
↪"
          srcintf: "<your_own_value> (source system.zone.name system.interface.name) "
          status: "enable"
          ttl: "<your_own_value>"
```

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:

88.7 Status

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

88.8 Authors

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

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

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*

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

89.2 Requirements

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

- ansible>=2.9.0

89.3 Parameters

89.4 Notes

Note:

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

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"
    firewall_vip:
      arp_reply: "disable"
      color: "4"
      comment: "Comment."
      dns_mapping_ttl: "6"
      extaddr:
        -
          name: "default_name_8 (source firewall.address.name firewall.addrgrp.name)

      extintf: "<your_own_value> (source system.interface.name)"
      extip: "<your_own_value>"
      extport: "<your_own_value>"
      gratuitous_arp_interval: "12"
      http_cookie_age: "13"
      http_cookie_domain: "<your_own_value>"
      http_cookie_domain_from_host: "disable"
      http_cookie_generation: "16"
      http_cookie_path: "<your_own_value>"
      http_cookie_share: "disable"
      http_ip_header: "enable"
      http_ip_header_name: "<your_own_value>"
      http_multiplex: "enable"
      https_cookie_secure: "disable"
      id: "23"
      ldb_method: "static"
      mapped_addr: "<your_own_value> (source firewall.address.name)"
      mappedip:
        -
```

(continues on next page)

(continued from previous page)

```

    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"
        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)"

```

(continues on next page)

(continued from previous page)

```
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"
```

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:

89.7 Status

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

89.8 Authors

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

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

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*

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

90.2 Requirements

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

- ansible>=2.9.0

90.3 Parameters

90.4 Notes

Note:

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

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"
    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"
```

(continues on next page)

(continued from previous page)

```
server_type: "http"
src_filter:
  -
    range: "<your_own_value>"
type: "static-nat"
uuid: "<your_own_value>"
```

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:

90.7 Status

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

90.8 Authors

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

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

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*

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

91.2 Requirements

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

- ansible>=2.9.0

91.3 Parameters

91.4 Notes

Note:

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

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"
    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:
        -
          name: "default_name_24 (source firewall.ldb-monitor.name)"
          name: "default_name_25"
          outlook_web_access: "disable"
          persistence: "none"
          portforward: "disable"
```

(continues on next page)

(continued from previous page)

```

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:
-
    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"

```

(continues on next page)

(continued from previous page)

```
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"
```

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:

91.7 Status

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

91.8 Authors

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

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

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*

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

92.2 Requirements

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

- ansible>=2.9.0

92.3 Parameters

92.4 Notes

Note:

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

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"
    firewall_vip64:
      arp_reply: "disable"
      color: "4"
      comment: "Comment."
      extip: "<your_own_value>"
      extport: "<your_own_value>"
      id: "8"
      ldb_method: "static"
      mappedip: "<your_own_value>"
      mappedport: "<your_own_value>"
      monitor:
        -
          name: "default_name_13 (source firewall.ldb-monitor.name)"
          name: "default_name_14"
          portforward: "disable"
          protocol: "tcp"
          realservers:
            -
              client_ip: "<your_own_value>"
              healthcheck: "disable"
              holddown_interval: "20"
              id: "21"
              ip: "<your_own_value>"
              max_connections: "23"
              monitor: "<your_own_value> (source firewall.ldb-monitor.name)"
              port: "25"
              status: "active"
              weight: "27"
```

(continues on next page)

(continued from previous page)

```
server_type: "http"
src_filter:
  -
    range: "<your_own_value>"
type: "static-nat"
uuid: "<your_own_value>"
```

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:

92.7 Status

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

92.8 Authors

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

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

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*

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

93.2 Requirements

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

- ansible>=2.9.0

93.3 Parameters

93.4 Notes

Note:

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

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"
    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>"
```

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:

93.7 Status

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

93.8 Authors

- Link Zheng (@chillancezen)

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

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

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*

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

94.2 Requirements

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

- ansible>=2.9.0

94.3 Parameters

94.4 Notes

Note:

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

94.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Configure IPv4 to IPv6 virtual IP groups.
  fortios_firewall_vipgrp46:
    vdom: "{{ vdom }}"
    state: "present"
    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>"
```

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:

94.7 Status

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

94.8 Authors

- Link Zheng (@chillancezen)

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

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

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*

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

95.2 Requirements

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

- ansible>=2.9.0

95.3 Parameters

95.4 Notes

Note:

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

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 }}"
        state: "present"
        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>"
```

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:

95.7 Status

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

95.8 Authors

- Link Zheng (@chillancezen)

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

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

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*

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

96.2 Requirements

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

- ansible>=2.9.0

96.3 Parameters

96.4 Notes

Note:

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

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"
    firewall_vipgrp64:
      color: "3"
      comments: "<your_own_value>"
      member:
        -
          name: "default_name_6 (source firewall.vip64.name)"
      name: "default_name_7"
      uuid: "<your_own_value>"
```

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:

96.7 Status

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

96.8 Authors

- Link Zheng (@chillancezen)

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

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

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*

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

97.2 Requirements

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

- ansible>=2.9.0

97.3 Parameters

97.4 Notes

Note:

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

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"
        firewall_wildcard_fqdn_custom:
          color: "3"
          comment: "Comment."
          name: "default_name_5"
          uuid: "<your_own_value>"
          visibility: "enable"
          wildcard_fqdn: "<your_own_value>"
```

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:

97.7 Status

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

97.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

`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*

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

98.2 Requirements

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

- `ansible>=2.9.0`

98.3 Parameters

98.4 Notes

Note:

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

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"
    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"
```

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:

98.7 Status

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

98.8 Authors

- Link Zheng (@chillancezen)

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

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

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*

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

99.2 Requirements

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

- ansible>=2.9.0

99.3 Parameters

99.4 Notes

Note:

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

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"
```

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:

99.7 Status

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

99.8 Authors

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

- Jie Xue (@JieX19)
- Miguel 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 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*

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

100.2 Requirements

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

- ansible>=2.9.0

100.3 Parameters

100.4 Notes

Note:

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

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:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

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:

100.7 Status

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

100.8 Authors

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

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

101.2 Requirements

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

- ansible>=2.9.0

101.3 Parameters

101.4 Notes

Note:

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

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 }}"
    state: "present"
    icap_server:
      ip_address: "<your_own_value>"
      ip_version: "4"
      ip6_address: "<your_own_value>"
      max_connections: "6"
      name: "default_name_7"
      port: "8"
```

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:

101.7 Status

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

101.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

102.2 Requirements

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

- ansible>=2.9.0

102.3 Parameters

102.4 Notes

Note:

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

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"
    ips_custom:
      action: "pass"
      application: "<your_own_value>"
      comment: "Comment."
      location: "<your_own_value>"
      log: "disable"
      log_packet: "disable"
      os: "<your_own_value>"
      protocol: "<your_own_value>"
      rule_id: "11"
      severity: "<your_own_value>"
      sig_name: "<your_own_value>"
      signature: "<your_own_value>"
      status: "disable"
      tag: "<your_own_value>"
```

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:

102.7 Status

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

102.8 Authors

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

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

103.2 Requirements

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

- ansible>=2.9.0

103.3 Parameters

103.4 Notes

Note:

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

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"
        ips_decoder:
          name: "default_name_3"
          parameter:
            -
              name: "default_name_5"
              value: "<your_own_value>"
```

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:

103.7 Status

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

103.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

104.2 Requirements

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

- ansible>=2.9.0

104.3 Parameters

104.4 Notes

Note:

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

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"
```

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:

104.7 Status

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

104.8 Authors

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

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

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*

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

105.2 Requirements

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

- ansible>=2.9.0

105.3 Parameters

105.4 Notes

Note:

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

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"
    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"
```

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:

105.7 Status

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

105.8 Authors

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

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

106.2 Requirements

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

- ansible>=2.9.0

106.3 Parameters

106.4 Notes

Note:

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

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"
        ips_rule_settings:
          id: "3"
```

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:

106.7 Status

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

106.8 Authors

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

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

107.2 Requirements

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

- ansible>=2.9.0

107.3 Parameters

107.4 Notes

Note:

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

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"
    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:
            -
```

(continues on next page)

(continued from previous page)

```

        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"
        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) "

```

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:

107.7 Status

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

107.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

108.2 Requirements

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

- ansible>=2.9.0

108.3 Parameters

108.4 Notes

Note:

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

108.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Configure IPS VDOM parameter.
      fortios_ips_settings:
        vdom: "{{ vdom }}"
        ips_settings:
          ips_packet_quota: "3"
          packet_log_history: "4"
          packet_log_memory: "5"
          packet_log_post_attack: "6"
```

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:

108.7 Status

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

108.8 Authors

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

- Miguel 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 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*

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

109.2 Requirements

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

- ansible>=2.9.0

109.3 Parameters

109.4 Notes

Note:

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

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"
        log_custom_field:
          id: "3"
          name: "default_name_4"
          value: "<your_own_value>"
```

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:

109.7 Status

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

109.8 Authors

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

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

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

`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*

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

110.2 Requirements

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

- ansible>=2.9.0

110.3 Parameters

110.4 Notes

Note:

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

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"
        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"
```

(continues on next page)

(continued from previous page)

```
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"
```

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:

110.7 Status

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

110.8 Authors

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

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

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*

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

111.2 Requirements

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

- ansible>=2.9.0

111.3 Parameters

111.4 Notes

Note:

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

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:
    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"
      uploadaddr: "<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>"
```


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:

111.7 Status

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

111.8 Authors

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

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

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*

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

112.2 Requirements

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

- ansible>=2.9.0

112.3 Parameters

112.4 Notes

Note:

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

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"
```

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:

112.7 Status

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

112.8 Authors

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

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

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*

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

113.2 Requirements

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

- ansible>=2.9.0

113.3 Parameters

113.4 Notes

Note:

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

113.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Filters for FortiAnalyzer.
  fortios_log_fortianalyzer2_filter:
    vdom: "{{ vdom }}"
    log_fortianalyzer2_filter:
      anomaly: "enable"
      dlp_archive: "enable"
      dns: "enable"
      filter: "<your_own_value>"
      filter_type: "include"
      forward_traffic: "enable"
      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"
```

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:

113.7 Status

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

113.8 Authors

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

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

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*

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

114.2 Requirements

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

- ansible>=2.9.0

114.3 Parameters

114.4 Notes

Note:

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

114.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Global FortiAnalyzer settings.
  fortios_log_fortianalyzer2_setting:
    vdom: "{{ vdom }}"
    log_fortianalyzer2_setting:
      __change_ip: "3"
      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>"
```

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:

114.7 Status

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

114.8 Authors

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

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

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*

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

115.2 Requirements

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

- ansible>=2.9.0

115.3 Parameters

115.4 Notes

Note:

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

115.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Filters for FortiAnalyzer.
  fortios_log_fortianalyzer3_filter:
    vdom: "{{ vdom }}"
    log_fortianalyzer3_filter:
      anomaly: "enable"
      dlp_archive: "enable"
      dns: "enable"
      filter: "<your_own_value>"
      filter_type: "include"
      forward_traffic: "enable"
      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"
```

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:

115.7 Status

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

115.8 Authors

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

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

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*

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

116.2 Requirements

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

- ansible>=2.9.0

116.3 Parameters

116.4 Notes

Note:

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

116.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Global FortiAnalyzer settings.
  fortios_log_fortianalyzer3_setting:
    vdom: "{{ vdom }}"
    log_fortianalyzer3_setting:
      __change_ip: "3"
      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>"
```

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:

116.7 Status

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

116.8 Authors

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

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

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*

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

117.2 Requirements

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

- ansible>=2.9.0

117.3 Parameters

117.4 Notes

Note:

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

117.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Filters for FortiAnalyzer.
  fortios_log_fortianalyzer_filter:
    vdom: "{{ vdom }}"
    log_fortianalyzer_filter:
      anomaly: "enable"
      dlp_archive: "enable"
      dns: "enable"
      filter: "<your_own_value>"
      filter_type: "include"
      forward_traffic: "enable"
      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"
```

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:

117.7 Status

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

117.8 Authors

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

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

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*

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

118.2 Requirements

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

- ansible>=2.9.0

118.3 Parameters

118.4 Notes

Note:

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

118.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Override filters for FortiAnalyzer.
  fortios_log_fortianalyzer_override_filter:
    vdom: "{{ vdom }}"
    log_fortianalyzer_override_filter:
      anomaly: "enable"
      dlp_archive: "enable"
      dns: "enable"
      filter: "<your_own_value>"
      filter_type: "include"
      forward_traffic: "enable"
      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"
```

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:

118.7 Status

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

118.8 Authors

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

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

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*

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

119.2 Requirements

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

- ansible>=2.9.0

119.3 Parameters

119.4 Notes

Note:

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

119.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Override FortiAnalyzer settings.
  fortios_log_fortianalyzer_override_setting:
    vdom: "{{ vdom }}"
  log_fortianalyzer_override_setting:
    __change_ip: "3"
    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"
```

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:

119.7 Status

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

119.8 Authors

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

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

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*

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

120.2 Requirements

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

- ansible>=2.9.0

120.3 Parameters

120.4 Notes

Note:

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

120.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Global FortiAnalyzer settings.
  fortios_log_fortianalyzer_setting:
    vdom: "{{ vdom }}"
    log_fortianalyzer_setting:
      __change_ip: "3"
      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>"
```

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:

120.7 Status

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

120.8 Authors

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

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

121.2 Requirements

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

- ansible>=2.9.0

121.3 Parameters

121.4 Notes

Note:

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

121.5 Examples

```
- hosts: fortigates
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 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"
```

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:

121.7 Status

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

121.8 Authors

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

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

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*

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

122.2 Requirements

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

- ansible>=2.9.0

122.3 Parameters

122.4 Notes

Note:

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

122.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Override filters for FortiCloud.
  fortios_log_fortiguard_override_filter:
    vdom: "{{ vdom }}"
    log_fortiguard_override_filter:
      anomaly: "enable"
      dlp_archive: "enable"
      dns: "enable"
      filter: "<your_own_value>"
      filter_type: "include"
      forward_traffic: "enable"
      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"
```

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:

122.7 Status

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

122.8 Authors

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

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

`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*

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

123.2 Requirements

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

- `ansible>=2.9.0`

123.3 Parameters

123.4 Notes

Note:

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

123.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Override global FortiCloud logging settings for this VDOM.
      fortios_log_fortiguard_override_setting:
        vdom: "{{ vdom }}"
        log_fortiguard_override_setting:
          override: "enable"
          status: "enable"
          upload_day: "<your_own_value>"
          upload_interval: "daily"
          upload_option: "store-and-upload"
          upload_time: "<your_own_value>"
```

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:

123.7 Status

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

123.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

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

124.2 Requirements

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

- ansible>=2.9.0

124.3 Parameters

124.4 Notes

Note:

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

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"
          status: "enable"
          upload_day: "<your_own_value>"
          upload_interval: "daily"
          upload_option: "store-and-upload"
          upload_time: "<your_own_value>"
```

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:

124.7 Status

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

124.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

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

125.2 Requirements

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

- ansible>=2.9.0

125.3 Parameters

125.4 Notes

Note:

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

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"
```

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:

125.7 Status

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

125.8 Authors

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

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

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

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*

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

126.2 Requirements

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

- ansible>=2.9.0

126.3 Parameters

126.4 Notes

Note:

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

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"
```

(continues on next page)

(continued from previous page)

```
vip_ssl: "enable"  
voip: "enable"  
wan_opt: "enable"  
wireless_activity: "enable"
```

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:

126.7 Status

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

126.8 Authors

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

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

`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*

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

127.2 Requirements

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

- `ansible>=2.9.0`

127.3 Parameters

127.4 Notes

Note:

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

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"
```

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:

127.7 Status

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

127.8 Authors

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

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

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

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*

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

128.2 Requirements

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

- ansible>=2.9.0

128.3 Parameters

128.4 Notes

Note:

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

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"
```

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:

128.7 Status

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

128.8 Authors

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

- Nicolas Thomas (@thomnico)

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

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*

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

129.2 Requirements

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

- `ansible>=2.9.0`

129.3 Parameters

129.4 Notes

Note:

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

129.5 Examples

```
- hosts: fortigates
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 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"
```

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:

129.7 Status

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

129.8 Authors

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

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

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*

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

130.2 Requirements

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

- ansible>=2.9.0

130.3 Parameters

130.4 Notes

Note:

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

130.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Settings for null device logging.
      fortios_log_null_device_setting:
        vdom: "{{ vdom }}"
        log_null_device_setting:
          status: "enable"
```

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:

130.7 Status

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

130.8 Authors

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

- Nicolas Thomas (@thomnico)

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

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*

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

131.2 Requirements

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

- ansible>=2.9.0

131.3 Parameters

131.4 Notes

Note:

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

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"
      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"
```

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:

131.7 Status

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

131.8 Authors

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

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

`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*

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

132.2 Requirements

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

- `ansible>=2.9.0`

132.3 Parameters

132.4 Notes

Note:

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

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"
      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"
```

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:

132.7 Status

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

132.8 Authors

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

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

`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*

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

133.2 Requirements

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

- `ansible>=2.9.0`

133.3 Parameters

133.4 Notes

Note:

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

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"
            format: "default"
            mode: "udp"
            port: "12"
            server: "192.168.100.40"
            source_ip: "84.230.14.43"
            status: "enable"
```

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:

133.7 Status

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

133.8 Authors

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

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

`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*

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

134.2 Requirements

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

- `ansible>=2.9.0`

134.3 Parameters

134.4 Notes

Note:

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

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"
      sniffer_traffic: "enable"
      ssh: "enable"
      voip: "enable"
```

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:

134.7 Status

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

134.8 Authors

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

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

`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*

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

135.2 Requirements

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

- `ansible>=2.9.0`

135.3 Parameters

135.4 Notes

Note:

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

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"
```

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:

135.7 Status

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

135.8 Authors

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

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

`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*

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

136.2 Requirements

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

- `ansible>=2.9.0`

136.3 Parameters

136.4 Notes

Note:

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

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"
```

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:

136.7 Status

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

136.8 Authors

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

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

137.2 Requirements

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

- `ansible>=2.9.0`

137.3 Parameters

137.4 Notes

Note:

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

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"
```

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:

137.7 Status

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

137.8 Authors

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

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

138.2 Requirements

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

- `ansible>=2.9.0`

138.3 Parameters

138.4 Notes

Note:

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

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"
```

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:

138.7 Status

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

138.8 Authors

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

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

`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*

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

139.2 Requirements

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

- `ansible>=2.9.0`

139.3 Parameters

139.4 Notes

Note:

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

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"
```

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:

139.7 Status

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

139.8 Authors

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

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

`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*

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

140.2 Requirements

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

- `ansible>=2.9.0`

140.3 Parameters

140.4 Notes

Note:

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

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"
```

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:

140.7 Status

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

140.8 Authors

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

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

`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*

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

141.2 Requirements

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

- `ansible>=2.9.0`

141.3 Parameters

141.4 Notes

Note:

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

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"
```

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:

141.7 Status

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

141.8 Authors

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

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

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*

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

142.2 Requirements

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

- ansible>=2.9.0

142.3 Parameters

142.4 Notes

Note:

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

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:
```

(continues on next page)

(continued from previous page)

```
-  
  category: "29"  
  id: "30"  
  level: "disable"
```

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:

142.7 Status

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

142.8 Authors

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

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

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*

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

143.2 Requirements

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

- ansible>=2.9.0

143.3 Parameters

143.4 Notes

Note:

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

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"
```

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:

143.7 Status

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

143.8 Authors

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

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

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*

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

144.2 Requirements

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

- ansible>=2.9.0

144.3 Parameters

144.4 Notes

Note:

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

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"
```

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:

144.7 Status

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

144.8 Authors

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

- Nicolas Thomas (@thomnico)

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

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*

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

145.2 Requirements

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

- ansible>=2.9.0

145.3 Parameters

145.4 Notes

Note:

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

145.5 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 FortiCare license.
    fortios_registration_forticare:
      vdom: "{{ vdom }}"
      registration_forticare:
        registration_code: "<your_own_value>"
```

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:

145.7 Status

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

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.

`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*

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

146.2 Requirements

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

- `ansible>=2.9.0`

146.3 Parameters

146.4 Notes

Note:

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

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>"
```

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:

146.7 Status

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

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.

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*

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

147.2 Requirements

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

- ansible>=2.9.0

147.3 Parameters

147.4 Notes

Note:

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

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"
    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:
        -
```

(continues on next page)

(continued from previous page)

```

    chart_name: "<your_own_value>"
    id: "28"
    status: "enable"
  favorite: "no"
  graph_type: "none"
  legend: "enable"
  legend_font_size: "33"
  name: "default_name_34"
  period: "last24h"
  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>"

```

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:

147.7 Status

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

147.8 Authors

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

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

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*

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

148.2 Requirements

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

- ansible>=2.9.0

148.3 Parameters

148.4 Notes

Note:

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

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"
    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>"
```

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:

148.7 Status

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

148.8 Authors

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

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

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*

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

149.2 Requirements

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

- ansible>=2.9.0

149.3 Parameters

149.4 Notes

Note:

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

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"
    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>"
```

(continues on next page)

(continued from previous page)

```

    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"
  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>"

```

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:

149.7 Status

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

149.8 Authors

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

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

150.2 Requirements

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

- ansible>=2.9.0

150.3 Parameters

150.4 Notes

Note:

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

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"
```

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:

150.7 Status

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

150.8 Authors

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

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

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

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*

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

151.2 Requirements

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

- ansible>=2.9.0

151.3 Parameters

151.4 Notes

Note:

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

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:
    vdom: "{{ vdom }}"
    state: "present"
    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>"
```


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:

151.7 Status

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

151.8 Authors

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

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

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*

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

152.2 Requirements

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

- ansible>=2.9.0

152.3 Parameters

152.4 Notes

Note:

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

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"
    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>"
```

(continues on next page)

(continued from previous page)

```
toc_heading3_style: "<your_own_value>"
toc_heading4_style: "<your_own_value>"
toc_title_style: "<your_own_value>"
```

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:

152.7 Status

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

152.8 Authors

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

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

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*

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

153.2 Requirements

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

- ansible>=2.9.0

153.3 Parameters

153.4 Notes

Note:

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

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"
    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>"
```

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:

153.7 Status

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

153.8 Authors

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

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

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*

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

154.2 Requirements

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

- ansible>=2.9.0

154.3 Parameters

154.4 Notes

Note:

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

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"
    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>"
```

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:

154.7 Status

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

154.8 Authors

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

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

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*

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

155.2 Requirements

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

- ansible>=2.9.0

155.3 Parameters

155.4 Notes

Note:

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

155.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Configure Autonomous System (AS) path lists.
      fortios_router_aspath_list:
        vdom: "{{ vdom }}"
        state: "present"
        router_aspath_list:
          name: "default_name_3"
          rule:
            -
              action: "deny"
              id: "6"
              regexp: "<your_own_value>"
```

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:

155.7 Status

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

155.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

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

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

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*

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

156.2 Requirements

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

- ansible>=2.9.0

156.3 Parameters

156.4 Notes

Note:

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

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 }}"
    state: "present"
    router_auth_path:
      device: "<your_own_value> (source system.interface.name) "
      gateway: "<your_own_value>"
      name: "default_name_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:

156.7 Status

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

156.8 Authors

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

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

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

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*

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

157.2 Requirements

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

- ansible>=2.9.0

157.3 Parameters

157.4 Notes

Note:

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

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>"
```

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:

157.7 Status

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

157.8 Authors

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

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

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

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*

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

158.2 Requirements

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

- ansible>=2.9.0

158.3 Parameters

158.4 Notes

Note:

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

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>"
```

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:

158.7 Status

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

158.8 Authors

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

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

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

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*

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

159.2 Requirements

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

- ansible>=2.9.0

159.3 Parameters

159.4 Notes

Note:

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

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"
```

(continues on next page)

(continued from previous page)

```

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"
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) "

(continues on next page)

(continued from previous page)

```

↪name) "
    default_originate_routemap6: "<your_own_value> (source router.route-map.
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)"
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"

```

(continues on next page)

(continued from previous page)

```

    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"
    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"

```

(continues on next page)

(continued from previous page)

```

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"
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:

```

(continues on next page)

(continued from previous page)

```
-  
  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"
```

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:

159.7 Status

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

159.8 Authors

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

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

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*

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

160.2 Requirements

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

- ansible>=2.9.0

160.3 Parameters

160.4 Notes

Note:

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

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"
    router_community_list:
      name: "default_name_3"
      rule:
        -
          action: "deny"
          id: "6"
          match: "<your_own_value>"
          regexp: "<your_own_value>"
      type: "standard"
```

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:

160.7 Status

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

160.8 Authors

- Link Zheng (@chillancezen)

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

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

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*

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

161.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

161.3 Parameters

161.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

(continues on next page)

(continued from previous page)

```

    csnp_interval_11: "30"
    csnp_interval_12: "31"
    hello_interval_11: "32"
    hello_interval_12: "33"
    hello_multiplier_11: "34"
    hello_multiplier_12: "35"
    hello_padding: "enable"
    lsp_interval: "37"
    lsp_retransmit_interval: "38"
    mesh_group: "enable"
    mesh_group_id: "40"
    metric_11: "41"
    metric_12: "42"
    name: "default_name_43 (source system.interface.name)"
    network_type: "broadcast"
    priority_11: "45"
    priority_12: "46"
    status: "enable"
    status6: "enable"
    wide_metric_11: "49"
    wide_metric_12: "50"
isis_net:
-
    id: "52"
    net: "<your_own_value>"
lsp_gen_interval_11: "54"
lsp_gen_interval_12: "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_11: "enable"
redistribute_11_list: "<your_own_value> (source router.access-list.name)"
redistribute_12: "enable"
redistribute_12_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_11: "enable"
redistribute6_11_list: "<your_own_value> (source router.access-list6.name)"
redistribute6_12: "enable"
redistribute6_12_list: "<your_own_value> (source router.access-list6.name)"

```

(continues on next page)

(continued from previous page)

```
spf_interval_exp_l1: "<your_own_value>"
spf_interval_exp_l2: "<your_own_value>"
summary_address:
-
  id: "87"
  level: "level-1-2"
  prefix: "<your_own_value>"
summary_address6:
-
  id: "91"
  level: "level-1-2"
  prefix6: "<your_own_value>"
```

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:

161.7 Status

- This module is not guaranteed to have a backwards compatible interface.

161.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

162.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

162.3 Parameters

162.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        router_key_chain:
          key:
            -
              accept_lifetime: "<your_own_value>"
              id: "5"
              key_string: "<your_own_value>"
              send_lifetime: "<your_own_value>"
          name: "default_name_8"
```

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:

162.7 Status

- This module is not guaranteed to have a backwards compatible interface.

162.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

163.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

163.3 Parameters

163.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
            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"
```

(continues on next page)

(continued from previous page)

```

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_suppression: "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"

```

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:

163.7 Status

- This module is not guaranteed to have a backwards compatible interface.

163.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

164.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

164.3 Parameters

164.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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>"
```

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:

164.7 Status

- This module is not guaranteed to have a backwards compatible interface.

164.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

165.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

165.3 Parameters

165.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    router_multicast_flow:
      comments: "<your_own_value>"
      flows:
        -
          group_addr: "<your_own_value>"
          id: "6"
          source_addr: "<your_own_value>"
    name: "default_name_8"
```

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:

165.7 Status

- This module is not guaranteed to have a backwards compatible interface.

165.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

166.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

166.3 Parameters

166.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
```

(continues on next page)

(continued from previous page)

```

-
    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"
  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)"

```

(continues on next page)

(continued from previous page)

```
    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:
    -
      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"
```

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:

166.7 Status

- This module is not guaranteed to have a backwards compatible interface.

166.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel 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 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*

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

167.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

167.3 Parameters

167.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

167.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure IPv6 OSPF.
  fortios_router_ospf6:
    vdom: "{{ vdom }}"
    router_ospf6:
      abr_type: "cisco"
      area:
        -
          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"
```

(continues on next page)

(continued from previous page)

```

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"
        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"

```

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:

167.7 Status

- This module is not guaranteed to have a backwards compatible interface.

167.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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 data-sources before usage. Tested with FOS v6.0.0

168.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

168.3 Parameters

168.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

168.5 Examples

```
- hosts: fortigates
collections:
  - 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 routing policies.
  fortios_router_policy:
    vdom: "{{ vdom }}"
    state: "present"
    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)"
```

(continues on next page)

(continued from previous page)

```
start_port: "23"
start_source_port: "24"
status: "enable"
tos: "<your_own_value>"
tos_mask: "<your_own_value>"
```

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:

168.7 Status

- This module is not guaranteed to have a backwards compatible interface.

168.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

169.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

169.3 Parameters

169.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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>"
```

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:

169.7 Status

- This module is not guaranteed to have a backwards compatible interface.

169.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

170.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

170.3 Parameters

170.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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>"
```

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:

170.7 Status

- This module is not guaranteed to have a backwards compatible interface.

170.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

171.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

171.3 Parameters

171.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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>"
```

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:

171.7 Status

- This module is not guaranteed to have a backwards compatible interface.

171.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

172.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

172.3 Parameters

172.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

172.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure RIP.
  fortios_router_rip:
    vdom: "{{ vdom }}"
    router_rip:
      default_information_originate: "enable"
      default_metric: "4"
      distance:
        -
          access_list: "<your_own_value> (source router.access-list.name)"
          distance: "7"
          id: "8"
          prefix: "<your_own_value>"
      distribute_list:
        -
          direction: "in"
          id: "12"
          interface: "<your_own_value> (source system.interface.name)"
          listname: "<your_own_value> (source router.access-list.name router.prefix-
↪list.name)"
          status: "enable"
      garbage_timer: "16"
      interface:
        -
          auth_keychain: "<your_own_value> (source router.key-chain.name)"
          auth_mode: "none"
          auth_string: "<your_own_value>"
          flags: "21"
          name: "default_name_22 (source system.interface.name)"
          receive_version: "1"
          send_version: "1"
          send_version2_broadcast: "disable"
          split_horizon: "poisoned"
```

(continues on next page)

(continued from previous page)

```

    split_horizon_status: "enable"
max_out_metric: "28"
neighbor:
-
    id: "30"
    ip: "<your_own_value>"
network:
-
    id: "33"
    prefix: "<your_own_value>"
offset_list:
-
    access_list: "<your_own_value> (source router.access-list.name) "
    direction: "in"
    id: "38"
    interface: "<your_own_value> (source system.interface.name) "
    offset: "40"
    status: "enable"
passive_interface:
-
    name: "default_name_43 (source system.interface.name) "
recv_buffer_size: "44"
redistribute:
-
    metric: "46"
    name: "default_name_47"
    routemap: "<your_own_value> (source router.route-map.name) "
    status: "enable"
timeout_timer: "50"
update_timer: "51"
version: "1"

```

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:

172.7 Status

- This module is not guaranteed to have a backwards compatible interface.

172.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

173.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

173.3 Parameters

173.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
          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"
```

(continues on next page)

(continued from previous page)

```

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"

```

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:

173.7 Status

- This module is not guaranteed to have a backwards compatible interface.

173.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

174.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

174.3 Parameters

174.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        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:
                -
```

(continues on next page)

(continued from previous page)

```

        as: "<your_own_value>"
    set_aspath_action: "prepend"
    set_atomic_aggregate: "enable"
    set_community:
    -
        community: "<your_own_value>"
    set_community_additive: "enable"
    set_community_delete: "<your_own_value> (source router.community-list.
↪name) "
    set_dampening_max_suppress: "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"

```

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:

174.7 Status

- This module is not guaranteed to have a backwards compatible interface.

174.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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 data-sources before usage. Tested with FOS v6.0.0

175.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

175.3 Parameters

175.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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)"
```

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:

175.7 Status

- This module is not guaranteed to have a backwards compatible interface.

175.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

176.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

176.3 Parameters

176.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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 }}"
        state: "present"
        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"
```

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:

176.7 Status

- This module is not guaranteed to have a backwards compatible interface.

176.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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 data-sources before usage. Tested with FOS v6.0.0

177.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

177.3 Parameters

177.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

177.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure IPv6 static routing tables.
  fortios_router_static6:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

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:

177.7 Status

- This module is not guaranteed to have a backwards compatible interface.

177.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

178.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

178.3 Parameters

178.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

178.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure anti-spam black/white list.
  fortios_spamfilter_bwl:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

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:

178.7 Status

- This module is not guaranteed to have a backwards compatible interface.

178.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

179.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

179.3 Parameters

179.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

179.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure AntiSpam banned word list.
  fortios_spamfilter_bword:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

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:

179.7 Status

- This module is not guaranteed to have a backwards compatible interface.

179.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

180.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

180.3 Parameters

180.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

180.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Configure AntiSpam DNSBL/ORBL.
      fortios_spamfilter_dnsbl:
        vdom: "{{ vdom }}"
        state: "present"
        spamfilter_dnsbl:
          comment: "Optional comments."
          entries:
            -
              action: "reject"
              id: "6"
              server: "192.168.100.40"
              status: "enable"
            id: "9"
            name: "default_name_10"
```

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:

180.7 Status

- This module is not guaranteed to have a backwards compatible interface.

180.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

fortios_spamfilter_fortishield – Configure FortiGuard - AntiSpam in Fortinet's FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

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

181.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

181.3 Parameters

181.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
        vdom: "{{ vdom }}"
        spamfilter_fortishield:
          spam_submit_force: "enable"
          spam_submit_srv: "<your_own_value>"
          spam_submit_txt2htm: "enable"
```

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:

181.7 Status

- This module is not guaranteed to have a backwards compatible interface.

181.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel 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 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*

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

182.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

182.3 Parameters

182.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

182.7 Status

- This module is not guaranteed to have a backwards compatible interface.

182.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

183.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

183.3 Parameters

183.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

183.7 Status

- This module is not guaranteed to have a backwards compatible interface.

183.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

184.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

184.3 Parameters

184.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

184.7 Status

- This module is not guaranteed to have a backwards compatible interface.

184.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

185.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

185.3 Parameters

185.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

185.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure AntiSpam profiles.
  fortios_spamfilter_profile:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

(continues on next page)

(continued from previous page)

```
    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"
```

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:

185.7 Status

- This module is not guaranteed to have a backwards compatible interface.

185.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

186.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

186.3 Parameters

186.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

186.7 Status

- This module is not guaranteed to have a backwards compatible interface.

186.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

187.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

187.3 Parameters

187.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

187.7 Status

- This module is not guaranteed to have a backwards compatible interface.

187.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

188.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

188.3 Parameters

188.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      switch_controller_custom_command:
        command: "<your_own_value>"
        command_name: "<your_own_value>"
        description: "<your_own_value>"
```

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:

188.7 Status

- This module is not guaranteed to have a backwards compatible interface.

188.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

189.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

189.3 Parameters

189.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

189.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Configure FortiSwitch global settings.
      fortios_switch_controller_global:
        vdom: "{{ vdom }}"
        switch_controller_global:
          allow_multiple_interfaces: "enable"
          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"
```

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:

189.7 Status

- This module is not guaranteed to have a backwards compatible interface.

189.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

190.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

190.3 Parameters

190.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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 }}"
        switch_controller_igmp_snooping:
          aging_time: "3"
          flood_unknown_multicast: "enable"
```

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:

190.7 Status

- This module is not guaranteed to have a backwards compatible interface.

190.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 191

fortios_switch_controller_lddp_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*

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

191.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

191.3 Parameters

191.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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:
      -
        dscp: "15"
        name: "default_name_16"
        priority: "17"
        status: "disable"
        vlan: "19"
    med_tlvs: "inventory-management"
    name: "default_name_21"
```

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:

191.7 Status

- This module is not guaranteed to have a backwards compatible interface.

191.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

192.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

192.3 Parameters

192.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

192.7 Status

- This module is not guaranteed to have a backwards compatible interface.

192.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

193.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

193.3 Parameters

193.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

193.7 Status

- This module is not guaranteed to have a backwards compatible interface.

193.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

194.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

194.3 Parameters

194.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        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"
```

(continues on next page)

(continued from previous page)

```

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>"
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"

```

(continues on next page)

(continued from previous page)

```

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
    .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>"

```

(continues on next page)

(continued from previous page)

```
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"
```

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:

194.7 Status

- This module is not guaranteed to have a backwards compatible interface.

194.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

195.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

195.3 Parameters

195.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

195.7 Status

- This module is not guaranteed to have a backwards compatible interface.

195.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

196.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

196.3 Parameters

196.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

196.7 Status

- This module is not guaranteed to have a backwards compatible interface.

196.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

197.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

197.3 Parameters

197.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

197.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Configure FortiSwitch QoS IP precedence/DSCP.
      fortios_switch_controller_qos_ip_dscp_map:
        vdom: "{{ vdom }}"
        state: "present"
        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"
```

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:

197.7 Status

- This module is not guaranteed to have a backwards compatible interface.

197.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

198.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

198.3 Parameters

198.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
    vdom: "{{ vdom }}"
    state: "present"
    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) "
```

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:

198.7 Status

- This module is not guaranteed to have a backwards compatible interface.

198.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

199.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

199.3 Parameters

199.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    switch_controller_qos_queue_policy:
      cos_queue:
        -
          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"
```

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:

199.7 Status

- This module is not guaranteed to have a backwards compatible interface.

199.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

200.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

200.3 Parameters

200.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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>"
```

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:

200.7 Status

- This module is not guaranteed to have a backwards compatible interface.

200.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

201.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

201.3 Parameters

201.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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) "
```

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:

201.7 Status

- This module is not guaranteed to have a backwards compatible interface.

201.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

202.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

202.3 Parameters

202.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        switch_controller_security_policy_captive_portal:
          name: "default_name_3"
          policy_type: "captive-portal"
          vlan: "<your_own_value> (source system.interface.name) "
```

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:

202.7 Status

- This module is not guaranteed to have a backwards compatible interface.

202.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

203.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

203.3 Parameters

203.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

203.7 Status

- This module is not guaranteed to have a backwards compatible interface.

203.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

204.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

204.3 Parameters

204.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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 }}"
    switch_controller_storm_control:
      broadcast: "enable"
      rate: "4"
      unknown_multicast: "enable"
      unknown_unicast: "enable"
```

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:

204.7 Status

- This module is not guaranteed to have a backwards compatible interface.

204.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

205.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

205.3 Parameters

205.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

205.7 Status

- This module is not guaranteed to have a backwards compatible interface.

205.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

206.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

206.3 Parameters

206.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    switch_controller_switch_group:
      description: "<your_own_value>"
      members:
        -
          name: "default_name_5 (source switch-controller.managed-switch.switch-id)"
          name: "default_name_6"
```

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:

206.7 Status

- This module is not guaranteed to have a backwards compatible interface.

206.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

207.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

207.3 Parameters

207.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        switch_controller_switch_interface_tag:
          name: "default_name_3"
```

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:

207.7 Status

- This module is not guaranteed to have a backwards compatible interface.

207.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

208.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

208.3 Parameters

208.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

208.7 Status

- This module is not guaranteed to have a backwards compatible interface.

208.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

209.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

209.3 Parameters

209.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
        vdom: "{{ vdom }}"
        state: "present"
        switch_controller_switch_profile:
          login_passwd: "<your_own_value>"
          login_passwd_override: "enable"
          name: "default_name_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:

209.7 Status

- This module is not guaranteed to have a backwards compatible interface.

209.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

210.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

210.3 Parameters

210.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

210.7 Status

- This module is not guaranteed to have a backwards compatible interface.

210.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 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*

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

211.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

211.3 Parameters

211.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    switch_controller_virtual_port_pool:
      description: "<your_own_value>"
      name: "default_name_4"
```

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:

211.7 Status

- This module is not guaranteed to have a backwards compatible interface.

211.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

212.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

212.3 Parameters

212.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

212.7 Status

- This module is not guaranteed to have a backwards compatible interface.

212.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

213.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

213.3 Parameters

213.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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>"
```

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:

213.7 Status

- This module is not guaranteed to have a backwards compatible interface.

213.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

214.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

214.3 Parameters

214.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

214.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure access profiles for system administrators.
  fortios_system_accprofile:
    vdom: "{{ vdom }}"
    state: "present"
    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:
```

(continues on next page)

(continued from previous page)

```
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"
```

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:

214.7 Status

- This module is not guaranteed to have a backwards compatible interface.

214.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

215.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

215.3 Parameters

215.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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:
            -
              fabric_device: "<your_own_value>"
              filters:
                -
                  id: "23"
                  key: "<your_own_value>"
                  value: "<your_own_value>"
```

(continues on next page)

(continued from previous page)

```

    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) "
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>"

```

(continues on next page)

(continued from previous page)

```
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"
```

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:

215.7 Status

- This module is not guaranteed to have a backwards compatible interface.

215.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

216.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

216.3 Parameters

216.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
    vdom: "{{ vdom }}"
    state: "present"
    system_affinity_interrupt:
      affinity_cpumask: "<your_own_value>"
      id: "4"
      interrupt: "<your_own_value>"
```

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:

216.7 Status

- This module is not guaranteed to have a backwards compatible interface.

216.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel 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 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*

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

217.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

217.3 Parameters

217.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
  system_affinity_packet_redistribution:
    affinity_cpumask: "<your_own_value>"
    id: "4"
    interface: "<your_own_value> (source system.interface.name)"
    rxqid: "6"
```

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:

217.7 Status

- This module is not guaranteed to have a backwards compatible interface.

217.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel 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 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*

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

218.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

218.3 Parameters

218.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
              user_auth_lockout_threshold: "24"
        status: "enable"
```

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:

218.7 Status

- This module is not guaranteed to have a backwards compatible interface.

218.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

219.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

219.3 Parameters

219.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      system_alias:
        command: "<your_own_value>"
        name: "default_name_4"
```

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:

219.7 Status

- This module is not guaranteed to have a backwards compatible interface.

219.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

220.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

220.3 Parameters

220.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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)"
```

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:

220.7 Status

- This module is not guaranteed to have a backwards compatible interface.

220.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

221.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

221.3 Parameters

221.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_arp_table:
      id: "3"
      interface: "<your_own_value> (source system.interface.name)"
      ip: "<your_own_value>"
      mac: "<your_own_value>"
```

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:

221.7 Status

- This module is not guaranteed to have a backwards compatible interface.

221.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

222.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

222.3 Parameters

222.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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>"
```

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:

222.7 Status

- This module is not guaranteed to have a backwards compatible interface.

222.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

223.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

223.3 Parameters

223.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
      vdom: "{{ vdom }}"
      state: "present"
      system_auto_script:
        interval: "3"
        name: "default_name_4"
        output_size: "5"
        repeat: "6"
        script: "<your_own_value>"
        start: "manual"
```

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:

223.7 Status

- This module is not guaranteed to have a backwards compatible interface.

223.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

224.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

224.3 Parameters

224.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_automation_action:
      action_type: "email"
      aws_api_id: "<your_own_value>"
      aws_api_key: "<your_own_value>"
      aws_api_path: "<your_own_value>"
      aws_api_stage: "<your_own_value>"
      aws_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>"
```

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:

224.7 Status

- This module is not guaranteed to have a backwards compatible interface.

224.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

225.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

225.3 Parameters

225.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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 }}"
    state: "present"
    system_automation_destination:
      destination:
        -
          name: "default_name_4"
          ha_group_id: "5"
          name: "default_name_6"
          type: "fortigate"
```

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:

225.7 Status

- This module is not guaranteed to have a backwards compatible interface.

225.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

226.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

226.3 Parameters

226.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_automation_stitch:
      action:
        -
          name: "default_name_4 (source system.automation-action.name) "
        destination:
          -
            name: "default_name_6 (source system.automation-destination.name) "
          name: "default_name_7"
          status: "enable"
          trigger: "<your_own_value> (source system.automation-trigger.name) "
```

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:

226.7 Status

- This module is not guaranteed to have a backwards compatible interface.

226.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

227.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

227.3 Parameters

227.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

227.7 Status

- This module is not guaranteed to have a backwards compatible interface.

227.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

228.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

228.3 Parameters

228.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

228.7 Status

- This module is not guaranteed to have a backwards compatible interface.

228.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

229.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

229.3 Parameters

229.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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>"
```

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:

229.7 Status

- This module is not guaranteed to have a backwards compatible interface.

229.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

230.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

230.3 Parameters

230.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
        vdom: "{{ vdom }}"
        system_autoupdate_tunneling:
          address: "<your_own_value>"
          password: "<your_own_value>"
          port: "5"
          status: "enable"
          username: "<your_own_value>"
```

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:

230.7 Status

- This module is not guaranteed to have a backwards compatible interface.

230.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

231.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

231.3 Parameters

231.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      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) "
```


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:

231.7 Status

- This module is not guaranteed to have a backwards compatible interface.

231.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

232.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

232.3 Parameters

232.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      system_cluster_sync:
        down_intf_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:
```

(continues on next page)

(continued from previous page)

```
-  
  name: "default_name_23 (source system.vdom.name) "
```

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:

232.7 Status

- This module is not guaranteed to have a backwards compatible interface.

232.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

233.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

233.3 Parameters

233.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

233.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
  - name: Configure console.
    fortios_system_console:
      vdom: "{{ vdom }}"
      system_console:
        baudrate: "9600"
        login: "enable"
        mode: "batch"
        output: "standard"
```

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:

233.7 Status

- This module is not guaranteed to have a backwards compatible interface.

233.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

234.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

234.3 Parameters

234.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
          -
            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"
```

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:

234.7 Status

- This module is not guaranteed to have a backwards compatible interface.

234.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

235.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

235.3 Parameters

235.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
    vdom: "{{ vdom }}"
    state: "present"
    system_custom_language:
      comments: "<your_own_value>"
      filename: "<your_own_value>"
      name: "default_name_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:

235.7 Status

- This module is not guaranteed to have a backwards compatible interface.

235.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

236.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

236.3 Parameters

236.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        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"
          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"
```

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:

236.7 Status

- This module is not guaranteed to have a backwards compatible interface.

236.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

237.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

237.3 Parameters

237.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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>"
      interface: "<your_own_value> (source system.interface.name)"
      status: "enable"
```

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:

237.7 Status

- This module is not guaranteed to have a backwards compatible interface.

237.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

238.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

238.3 Parameters

238.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
          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"
```

(continues on next page)

(continued from previous page)

```
subnet: "<your_own_value>"
upstream_interface: "<your_own_value> (source system.interface.name) "
```

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:

238.7 Status

- This module is not guaranteed to have a backwards compatible interface.

238.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

239.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

239.3 Parameters

239.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_dhcp_server:
      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:
```

(continues on next page)

(continued from previous page)

```

-
    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:
-
    tftp_server: "<your_own_value>"
    timezone: "01"
    timezone_option: "disable"
    vci_match: "disable"
    vci_string:
-
    vci_string: "<your_own_value>"
    wifi_acl: "<your_own_value>"
    wifi_ac2: "<your_own_value>"
    wifi_ac3: "<your_own_value>"
    wins_server1: "<your_own_value>"
    wins_server2: "<your_own_value>"

```

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:

239.7 Status

- This module is not guaranteed to have a backwards compatible interface.

239.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

240.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

240.3 Parameters

240.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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>"
      ip6_secondary: "<your_own_value>"
      primary: "<your_own_value>"
      secondary: "<your_own_value>"
      source_ip: "84.230.14.43"
```

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:

240.7 Status

- This module is not guaranteed to have a backwards compatible interface.

240.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

241.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

241.3 Parameters

241.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_dns_database:
      allow_transfer: "<your_own_value>"
      authoritative: "enable"
      contact: "<your_own_value>"
      dns_entry:
        -
          canonical_name: "<your_own_value>"
          hostname: "myhostname"
          id: "9"
          ip: "<your_own_value>"
          ipv6: "<your_own_value>"
          preference: "12"
          status: "enable"
          ttl: "14"
          type: "A"
      domain: "<your_own_value>"
      forwarder: "<your_own_value>"
      ip_master: "<your_own_value>"
      name: "default_name_19"
      primary_name: "<your_own_value>"
      source_ip: "84.230.14.43"
      status: "enable"
      ttl: "23"
      type: "master"
      view: "shadow"
```


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:

241.7 Status

- This module is not guaranteed to have a backwards compatible interface.

241.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

242.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

242.3 Parameters

242.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_dns_server:
      dnsfilter_profile: "<your_own_value> (source dnsfilter.profile.name)"
      mode: "recursive"
      name: "default_name_5 (source system.interface.name)"
```

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:

242.7 Status

- This module is not guaranteed to have a backwards compatible interface.

242.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

243.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

243.3 Parameters

243.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_dscp_based_priority:
      ds: "3"
      id: "4"
      priority: "low"
```

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:

243.7 Status

- This module is not guaranteed to have a backwards compatible interface.

243.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

244.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

244.3 Parameters

244.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

244.7 Status

- This module is not guaranteed to have a backwards compatible interface.

244.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

245.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

245.3 Parameters

245.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

245.7 Status

- This module is not guaranteed to have a backwards compatible interface.

245.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

246.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

246.3 Parameters

246.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

246.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure FIPS-CC mode.
  fortios_system_fips_cc:
    vdom: "{{ vdom }}"
    system_fips_cc:
      entropy_token: "enable"
      key_generation_self_test: "enable"
      self_test_period: "5"
      status: "enable"
```

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:

246.7 Status

- This module is not guaranteed to have a backwards compatible interface.

246.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

247.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

247.3 Parameters

247.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      status: "enable"
      vdom: "<your_own_value> (source system.vdom.name)"
```

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:

247.7 Status

- This module is not guaranteed to have a backwards compatible interface.

247.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

248.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

248.3 Parameters

248.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      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"
```

(continues on next page)

(continued from previous page)

```
webfilter_license: "31"  
webfilter_timeout: "32"
```

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:

248.7 Status

- This module is not guaranteed to have a backwards compatible interface.

248.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

249.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

249.3 Parameters

249.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      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)"
```

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:

249.7 Status

- This module is not guaranteed to have a backwards compatible interface.

249.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

250.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

250.3 Parameters

250.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

250.7 Status

- This module is not guaranteed to have a backwards compatible interface.

250.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

251.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

251.3 Parameters

251.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

251.7 Status

- This module is not guaranteed to have a backwards compatible interface.

251.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

252.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

252.3 Parameters

252.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

252.7 Status

- This module is not guaranteed to have a backwards compatible interface.

252.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

253.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

253.3 Parameters

253.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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.
    fortios_system_geoip_override:
      vdom: "{{ vdom }}"
      state: "present"
      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"
```

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:

253.7 Status

- This module is not guaranteed to have a backwards compatible interface.

253.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

254.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

254.3 Parameters

254.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      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"
```

(continues on next page)

(continued from previous page)

```

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"
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"

```

(continues on next page)

(continued from previous page)

```
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"
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"
```

(continues on next page)

(continued from previous page)

```

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"

```

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:

254.7 Status

- This module is not guaranteed to have a backwards compatible interface.

254.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

255.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

255.3 Parameters

255.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

255.7 Status

- This module is not guaranteed to have a backwards compatible interface.

255.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

256.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

256.3 Parameters

256.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

(continues on next page)

(continued from previous page)

```

key: "<your_own_value>"
l2ep_eth_type: "<your_own_value>"
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>"

```

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:

256.7 Status

- This module is not guaranteed to have a backwards compatible interface.

256.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

257.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

257.3 Parameters

257.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

257.7 Status

- This module is not guaranteed to have a backwards compatible interface.

257.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

258.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

258.3 Parameters

258.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

(continues on next page)

(continued from previous page)

```

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"
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>"

```

(continues on next page)

(continued from previous page)

```

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"
    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"

```

(continues on next page)

(continued from previous page)

```

        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"
    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"

```

(continues on next page)

(continued from previous page)

```

    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"
        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:
    -

```

(continues on next page)

(continued from previous page)

```

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"
    vrdest: "<your_own_value>"
    vrdest_priority: "256"
    vrgrp: "257"
    vrid: "258"
    vrip: "<your_own_value>"
vrrp_virtual_mac: "enable"
wccp: "enable"
weight: "262"
wins_ip: "<your_own_value>"

```

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:

258.7 Status

- This module is not guaranteed to have a backwards compatible interface.

258.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

259.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

259.3 Parameters

259.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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>"
```

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:

259.7 Status

- This module is not guaranteed to have a backwards compatible interface.

259.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

260.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

260.3 Parameters

260.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_ips_urlfilter_dns:
      address: "<your_own_value>"
      ipv6_capability: "enable"
      status: "enable"
```

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:

260.7 Status

- This module is not guaranteed to have a backwards compatible interface.

260.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

261.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

261.3 Parameters

261.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_ips_urlfilter_dns6:
      address6: "<your_own_value>"
      status: "enable"
```

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:

261.7 Status

- This module is not guaranteed to have a backwards compatible interface.

261.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

262.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

262.3 Parameters

262.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
    vdom: "{{ vdom }}"
    state: "present"
    system_ipv6_neighbor_cache:
      id: "3"
      interface: "<your_own_value> (source system.interface.name)"
      ipv6: "<your_own_value>"
      mac: "<your_own_value>"
```

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:

262.7 Status

- This module is not guaranteed to have a backwards compatible interface.

262.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

263.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

263.3 Parameters

263.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_ipv6_tunnel:
      destination: "<your_own_value>"
      interface: "<your_own_value> (source system.interface.name)"
      name: "default_name_5"
      source: "<your_own_value>"
```

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:

263.7 Status

- This module is not guaranteed to have a backwards compatible interface.

263.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

264.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

264.3 Parameters

264.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        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)"
              status: "enable"
              update_cascade_interface: "enable"
              update_static_route: "enable"
```

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:

264.7 Status

- This module is not guaranteed to have a backwards compatible interface.

264.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

265.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

265.3 Parameters

265.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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>"
```

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:

265.7 Status

- This module is not guaranteed to have a backwards compatible interface.

265.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

266.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

266.3 Parameters

266.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_mac_address_table:
      interface: "<your_own_value> (source system.interface.name)"
      mac: "<your_own_value>"
      reply_substitute: "<your_own_value>"
```

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:

266.7 Status

- This module is not guaranteed to have a backwards compatible interface.

266.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

267.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

267.3 Parameters

267.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

267.7 Status

- This module is not guaranteed to have a backwards compatible interface.

267.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

268.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

268.3 Parameters

268.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

268.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
  - name: Configure Mobile tunnels, an implementation of Network Mobility (NEMO)
    ↪ extensions for Mobile IPv4 RFC5177.
    fortios_system_mobile_tunnel:
      vdom: "{{ vdom }}"
      state: "present"
      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"
```

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:

268.7 Status

- This module is not guaranteed to have a backwards compatible interface.

268.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

269.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

269.3 Parameters

269.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

(continues on next page)

(continued from previous page)

```
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"
traffic_check: "enable"
username1: "<your_own_value>"
username2: "<your_own_value>"
username3: "<your_own_value>"
wireless_port: "48"
```

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:

269.7 Status

- This module is not guaranteed to have a backwards compatible interface.

269.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

270.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

270.3 Parameters

270.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

270.7 Status

- This module is not guaranteed to have a backwards compatible interface.

270.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

271.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

271.3 Parameters

271.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

271.7 Status

- This module is not guaranteed to have a backwards compatible interface.

271.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

272.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

272.3 Parameters

272.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

272.7 Status

- This module is not guaranteed to have a backwards compatible interface.

272.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

273.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

273.3 Parameters

273.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

273.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure system NTP information.
  fortios_system_ntp:
    vdom: "{{ vdom }}"
    system_ntp:
      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"
```

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:

273.7 Status

- This module is not guaranteed to have a backwards compatible interface.

273.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

274.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

274.3 Parameters

274.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

274.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Configure object tagging.
  fortios_system_object_tagging:
    vdom: "{{ vdom }}"
    state: "present"
    system_object_tagging:
      address: "disable"
      category: "<your_own_value>"
      color: "5"
      device: "disable"
      interface: "disable"
      multiple: "enable"
      tags:
      -
        name: "default_name_10"
```

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:

274.7 Status

- This module is not guaranteed to have a backwards compatible interface.

274.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

275.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

275.3 Parameters

275.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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.
    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"
```

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:

275.7 Status

- This module is not guaranteed to have a backwards compatible interface.

275.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

276.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

276.3 Parameters

276.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      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"
```

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:

276.7 Status

- This module is not guaranteed to have a backwards compatible interface.

276.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

277.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

277.3 Parameters

277.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_physical_switch:
      age_enable: "enable"
      age_val: "4"
      name: "default_name_5"
      port:
        -
          name: "default_name_7"
          speed: "auto"
          status: "up"
```

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:

277.7 Status

- This module is not guaranteed to have a backwards compatible interface.

277.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

278.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

278.3 Parameters

278.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_pppoe_interface:
      ac_name: "<your_own_value>"
      auth_type: "auto"
      device: "<your_own_value> (source system.interface.name)"
      dial_on_demand: "enable"
      disc_retry_timeout: "7"
      idle_timeout: "8"
      ipunnumbered: "<your_own_value>"
      ipv6: "enable"
      lcp_echo_interval: "11"
      lcp_max_echo_fails: "12"
      name: "default_name_13"
      padt_retry_timeout: "14"
      password: "<your_own_value>"
      pppoe_unnumbered_negotiate: "enable"
      service_name: "<your_own_value>"
      username: "<your_own_value>"
```

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:

278.7 Status

- This module is not guaranteed to have a backwards compatible interface.

278.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

279.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

279.3 Parameters

279.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

279.7 Status

- This module is not guaranteed to have a backwards compatible interface.

279.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

280.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

280.3 Parameters

280.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_proxy_arp:
      end_ip: "<your_own_value>"
      id: "4"
      interface: "<your_own_value> (source system.interface.name)"
      ip: "<your_own_value>"
```

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:

280.7 Status

- This module is not guaranteed to have a backwards compatible interface.

280.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

281.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

281.3 Parameters

281.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_replacemsg_admin:
      buffer: "<your_own_value>"
      format: "none"
      header: "none"
      msg_type: "<your_own_value>"
```

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:

281.7 Status

- This module is not guaranteed to have a backwards compatible interface.

281.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

282.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

282.3 Parameters

282.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

282.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Replacement messages.
  fortios_system_replacemsg_alertmail:
    vdom: "{{ vdom }}"
    state: "present"
    system_replacemsg_alertmail:
      buffer: "<your_own_value>"
      format: "none"
      header: "none"
      msg_type: "<your_own_value>"
```

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:

282.7 Status

- This module is not guaranteed to have a backwards compatible interface.

282.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

283.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

283.3 Parameters

283.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_replacemsg_auth:
      buffer: "<your_own_value>"
      format: "none"
      header: "none"
      msg_type: "<your_own_value>"
```

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:

283.7 Status

- This module is not guaranteed to have a backwards compatible interface.

283.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

284.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

284.3 Parameters

284.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        system_replacemsg_device_detection_portal:
          buffer: "<your_own_value>"
          format: "none"
          header: "none"
          msg_type: "<your_own_value>"
```

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:

284.7 Status

- This module is not guaranteed to have a backwards compatible interface.

284.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

285.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

285.3 Parameters

285.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        system_replacemsg_ec:
          buffer: "<your_own_value>"
          format: "none"
          header: "none"
          msg_type: "<your_own_value>"
```

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:

285.7 Status

- This module is not guaranteed to have a backwards compatible interface.

285.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

286.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

286.3 Parameters

286.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        system_replacemsg_fortiguard_wf:
          buffer: "<your_own_value>"
          format: "none"
          header: "none"
          msg_type: "<your_own_value>"
```

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:

286.7 Status

- This module is not guaranteed to have a backwards compatible interface.

286.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

287.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

287.3 Parameters

287.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

287.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Replacement messages.
      fortios_system_replacemsg_ftp:
        vdom: "{{ vdom }}"
        state: "present"
        system_replacemsg_ftp:
          buffer: "<your_own_value>"
          format: "none"
          header: "none"
          msg_type: "<your_own_value>"
```

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:

287.7 Status

- This module is not guaranteed to have a backwards compatible interface.

287.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

288.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

288.3 Parameters

288.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_replacemsg_group:
      admin:
        -
          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:
        -
```

(continues on next page)

(continued from previous page)

```

    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:
-
    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>"

```

(continues on next page)

(continued from previous page)

```
    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>"
```

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:

288.7 Status

- This module is not guaranteed to have a backwards compatible interface.

288.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

289.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

289.3 Parameters

289.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        system_replacemsg_http:
          buffer: "<your_own_value>"
          format: "none"
          header: "none"
          msg_type: "<your_own_value>"
```

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:

289.7 Status

- This module is not guaranteed to have a backwards compatible interface.

289.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

290.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

290.3 Parameters

290.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_replacemsg_icap:
      buffer: "<your_own_value>"
      format: "none"
      header: "none"
      msg_type: "<your_own_value>"
```

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:

290.7 Status

- This module is not guaranteed to have a backwards compatible interface.

290.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

291.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

291.3 Parameters

291.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

291.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Configure replacement message images.
      fortios_system_replacemsg_image:
        vdom: "{{ vdom }}"
        state: "present"
        system_replacemsg_image:
          image_base64: "<your_own_value>"
          image_type: "gif"
          name: "default_name_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:

291.7 Status

- This module is not guaranteed to have a backwards compatible interface.

291.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

292.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

292.3 Parameters

292.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_replacemsg_mail:
      buffer: "<your_own_value>"
      format: "none"
      header: "none"
      msg_type: "<your_own_value>"
```

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:

292.7 Status

- This module is not guaranteed to have a backwards compatible interface.

292.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

293.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

293.3 Parameters

293.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        system_replacemsg_nac_quar:
          buffer: "<your_own_value>"
          format: "none"
          header: "none"
          msg_type: "<your_own_value>"
```

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:

293.7 Status

- This module is not guaranteed to have a backwards compatible interface.

293.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

294.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

294.3 Parameters

294.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        system_replacemsg_nntp:
          buffer: "<your_own_value>"
          format: "none"
          header: "none"
          msg_type: "<your_own_value>"
```

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:

294.7 Status

- This module is not guaranteed to have a backwards compatible interface.

294.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

295.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

295.3 Parameters

295.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_replacemsg_spam:
      buffer: "<your_own_value>"
      format: "none"
      header: "none"
      msg_type: "<your_own_value>"
```

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:

295.7 Status

- This module is not guaranteed to have a backwards compatible interface.

295.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

296.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

296.3 Parameters

296.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

296.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Replacement messages.
  fortios_system_replacemsg_sslvpn:
    vdom: "{{ vdom }}"
    state: "present"
    system_replacemsg_sslvpn:
      buffer: "<your_own_value>"
      format: "none"
      header: "none"
      msg_type: "<your_own_value>"
```

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:

296.7 Status

- This module is not guaranteed to have a backwards compatible interface.

296.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

297.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

297.3 Parameters

297.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        system_replacemsg_traffic_quota:
          buffer: "<your_own_value>"
          format: "none"
          header: "none"
          msg_type: "<your_own_value>"
```

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:

297.7 Status

- This module is not guaranteed to have a backwards compatible interface.

297.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

298.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

298.3 Parameters

298.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        system_replacemsg_utm:
          buffer: "<your_own_value>"
          format: "none"
          header: "none"
          msg_type: "<your_own_value>"
```

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:

298.7 Status

- This module is not guaranteed to have a backwards compatible interface.

298.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

299.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

299.3 Parameters

299.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_replacemsg_webproxy:
      buffer: "<your_own_value>"
      format: "none"
      header: "none"
      msg_type: "<your_own_value>"
```

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:

299.7 Status

- This module is not guaranteed to have a backwards compatible interface.

299.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

300.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

300.3 Parameters

300.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

300.7 Status

- This module is not guaranteed to have a backwards compatible interface.

300.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

301.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

301.3 Parameters

301.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

(continues on next page)

(continued from previous page)

```
    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>"
```

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:

301.7 Status

- This module is not guaranteed to have a backwards compatible interface.

301.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

302.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

302.3 Parameters

302.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        system_session_helper:
          id: "3"
          name: "default_name_4"
          port: "5"
          protocol: "6"
```

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:

302.7 Status

- This module is not guaranteed to have a backwards compatible interface.

302.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

303.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

303.3 Parameters

303.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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>"
```

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:

303.7 Status

- This module is not guaranteed to have a backwards compatible interface.

303.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

304.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

304.3 Parameters

304.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

304.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure VDOM settings.
  fortios_system_settings:
    vdom: "{{ vdom }}"
    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"
```

(continues on next page)

(continued from previous page)

```

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_fortixtender_controller: "enable"
gui_icap: "enable"
gui_implicit_policy: "enable"
gui_ips: "enable"
gui_load_balance: "enable"
gui_local_in_policy: "enable"
gui_local_reports: "enable"
gui_multicast_policy: "enable"
gui_multiple_interface_policy: "enable"
gui_multiple_utm_profiles: "enable"
gui_nat46_64: "enable"
gui_object_colors: "enable"
gui_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>"

```

(continues on next page)

(continued from previous page)

```
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"
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"
```

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:

304.7 Status

- This module is not guaranteed to have a backwards compatible interface.

304.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

305.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

305.3 Parameters

305.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

305.7 Status

- This module is not guaranteed to have a backwards compatible interface.

305.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

306.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

306.3 Parameters

306.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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>"
```

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:

306.7 Status

- This module is not guaranteed to have a backwards compatible interface.

306.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

307.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

307.3 Parameters

307.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      system_sms_server:
        mail_server: "<your_own_value>"
        name: "default_name_4"
```

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:

307.7 Status

- This module is not guaranteed to have a backwards compatible interface.

307.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

308.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

308.3 Parameters

308.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

(continues on next page)

(continued from previous page)

```
trap_v2c_rport: "27"  
trap_v2c_status: "enable"
```

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:

308.7 Status

- This module is not guaranteed to have a backwards compatible interface.

308.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

309.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

309.3 Parameters

309.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

309.7 Status

- This module is not guaranteed to have a backwards compatible interface.

309.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

310.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

310.3 Parameters

310.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

310.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: SNMP user configuration.
  fortios_system_snmp_user:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

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:

310.7 Status

- This module is not guaranteed to have a backwards compatible interface.

310.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

311.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

311.3 Parameters

311.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

311.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Configure logical storage.
  fortios_system_storage:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

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:

311.7 Status

- This module is not guaranteed to have a backwards compatible interface.

311.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

312.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

312.3 Parameters

312.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
    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"
```

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:

312.7 Status

- This module is not guaranteed to have a backwards compatible interface.

312.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

313.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

313.3 Parameters

313.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      system_switch_interface:
        intra_switch_policy: "implicit"
        member:
          -
            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)"
```

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:

313.7 Status

- This module is not guaranteed to have a backwards compatible interface.

313.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

314.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

314.3 Parameters

314.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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
    fortios_system_tos_based_priority:
      vdom: "{{ vdom }}"
      state: "present"
      system_tos_based_priority:
        id: "3"
        priority: "low"
        tos: "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:

314.7 Status

- This module is not guaranteed to have a backwards compatible interface.

314.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

315.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

315.3 Parameters

315.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    system_vdom:
      name: "default_name_3"
      short_name: "<your_own_value>"
      temporary: "5"
      vcluster_id: "6"
```

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:

315.7 Status

- This module is not guaranteed to have a backwards compatible interface.

315.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

316.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

316.3 Parameters

316.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

316.7 Status

- This module is not guaranteed to have a backwards compatible interface.

316.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

317.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

317.3 Parameters

317.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      system_vdom_exception:
        id: "3"
        object: "log.fortianalyzer.setting"
        oid: "5"
        scope: "all"
        vdom:
          -
            name: "default_name_8 (source system.vdom.name) "
```

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:

317.7 Status

- This module is not guaranteed to have a backwards compatible interface.

317.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

318.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

318.3 Parameters

318.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

318.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure VDOM links.
  fortios_system_vdom_link:
    vdom: "{{ vdom }}"
    state: "present"
    system_vdom_link:
      name: "default_name_3"
      type: "ppp"
      vcluster: "vcluster1"
```

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:

318.7 Status

- This module is not guaranteed to have a backwards compatible interface.

318.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

319.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

319.3 Parameters

319.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

319.7 Status

- This module is not guaranteed to have a backwards compatible interface.

319.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

320.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

320.3 Parameters

320.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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>"
```

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:

320.7 Status

- This module is not guaranteed to have a backwards compatible interface.

320.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

321.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

321.3 Parameters

321.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      system_vdom_radius_server:
        name: "default_name_3 (source system.vdom.name)"
        radius_server_vdom: "<your_own_value> (source system.vdom.name)"
        status: "enable"
```

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:

321.7 Status

- This module is not guaranteed to have a backwards compatible interface.

321.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

322.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

322.3 Parameters

322.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

322.7 Status

- This module is not guaranteed to have a backwards compatible interface.

322.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

323.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

323.3 Parameters

323.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

323.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Configure virtual hardware switch interfaces.
  fortios_system_virtual_switch:
    vdom: "{{ vdom }}"
    state: "present"
    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>"
```

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:

323.7 Status

- This module is not guaranteed to have a backwards compatible interface.

323.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

324.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

324.3 Parameters

324.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

324.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
  - name: Configure redundant internet connections using SD-WAN (formerly virtual WAN
    ↪link).
    fortios_system_virtual_wan_link:
      vdom: "{{ vdom }}"
      system_virtual_wan_link:
        fail_alert_interfaces:
          -
            name: "default_name_4 (source system.interface.name)"
        fail_detect: "enable"
        health_check:
          -
            addr_mode: "ipv4"
            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:
              -
```

(continues on next page)

(continued from previous page)

```

        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>"
        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:

```

(continues on next page)

(continued from previous page)

```

-
  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"
  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"

```


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:

324.7 Status

- This module is not guaranteed to have a backwards compatible interface.

324.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

325.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

325.3 Parameters

325.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

325.7 Status

- This module is not guaranteed to have a backwards compatible interface.

325.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

326.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

326.3 Parameters

326.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

326.5 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
  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 }}"
```

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:

326.7 Status

- This module is not guaranteed to have a backwards compatible interface.

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.

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*

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

327.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

327.3 Parameters

327.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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:
        -
          ip: "<your_own_value>"
        remote_ip6:
          -
            ip6: "<your_own_value>"
      vni: "12"
```

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:

327.7 Status

- This module is not guaranteed to have a backwards compatible interface.

327.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

328.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

328.3 Parameters

328.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
      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"
```


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:

328.7 Status

- This module is not guaranteed to have a backwards compatible interface.

328.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

329.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

329.3 Parameters

329.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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.
    fortios_system_zone:
      vdom: "{{ vdom }}"
      state: "present"
      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)"
```

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:

329.7 Status

- This module is not guaranteed to have a backwards compatible interface.

329.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

330.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

330.3 Parameters

330.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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 }}"
    state: "present"
    user_adgrp:
      name: "default_name_3"
      server_name: "<your_own_value> (source user.fssso.name) "
```

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:

330.7 Status

- This module is not guaranteed to have a backwards compatible interface.

330.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

331.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

331.3 Parameters

331.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    user_device:
      alias: "<your_own_value>"
      avatar: "<your_own_value>"
      category: "none"
      comment: "Comment."
      mac: "<your_own_value>"
      master_device: "<your_own_value> (source user.device.alias)"
      tagging:
        -
          category: "<your_own_value> (source system.object-tagging.category)"
          name: "default_name_11"
          tags:
            -
              name: "default_name_13 (source system.object-tagging.tags.name)"
      type: "unknown"
      user: "<your_own_value>"
```

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:

331.7 Status

- This module is not guaranteed to have a backwards compatible interface.

331.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

332.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

332.3 Parameters

332.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

332.7 Status

- This module is not guaranteed to have a backwards compatible interface.

332.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

333.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

333.3 Parameters

333.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    user_device_category:
      comment: "Comment."
      desc: "<your_own_value>"
      name: "default_name_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:

333.7 Status

- This module is not guaranteed to have a backwards compatible interface.

333.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

334.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

334.3 Parameters

334.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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)"
```

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:

334.7 Status

- This module is not guaranteed to have a backwards compatible interface.

334.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

335.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

335.3 Parameters

335.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

335.7 Status

- This module is not guaranteed to have a backwards compatible interface.

335.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

336.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

336.3 Parameters

336.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

336.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure FortiToken.
  fortios_user_fortitoken:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

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:

336.7 Status

- This module is not guaranteed to have a backwards compatible interface.

336.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

337.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

337.3 Parameters

337.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
    vdom: "{{ vdom }}"
    state: "present"
    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>"
```

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:

337.7 Status

- This module is not guaranteed to have a backwards compatible interface.

337.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

338.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

338.3 Parameters

338.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

338.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Configure FSSO active directory servers for polling mode.
      fortios_user_fsso_polling:
        vdom: "{{ vdom }}"
        state: "present"
        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>"
```

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:

338.7 Status

- This module is not guaranteed to have a backwards compatible interface.

338.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

339.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

339.3 Parameters

339.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

339.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Configure user groups.
  fortios_user_group:
    vdom: "{{ vdom }}"
    state: "present"
    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) "
```

(continues on next page)

(continued from previous page)

```

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"

```

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:

339.7 Status

- This module is not guaranteed to have a backwards compatible interface.

339.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

340.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

340.3 Parameters

340.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    user_krb_keytab:
      keytab: "<your_own_value>"
      ldap_server: "<your_own_value> (source user.ldap.name)"
      name: "default_name_5"
      principal: "<your_own_value>"
```

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:

340.7 Status

- This module is not guaranteed to have a backwards compatible interface.

340.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

341.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

341.3 Parameters

341.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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>"
```

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:

341.7 Status

- This module is not guaranteed to have a backwards compatible interface.

341.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

342.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

342.3 Parameters

342.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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>"
```


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:

342.7 Status

- This module is not guaranteed to have a backwards compatible interface.

342.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

343.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

343.3 Parameters

343.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    user_password_policy:
      expire_days: "3"
      name: "default_name_4"
      warn_days: "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:

343.7 Status

- This module is not guaranteed to have a backwards compatible interface.

343.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

344.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

344.3 Parameters

344.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

344.7 Status

- This module is not guaranteed to have a backwards compatible interface.

344.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

345.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

345.3 Parameters

345.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    user_peergrp:
      member:
        -
          name: "default_name_4 (source user.peer.name)"
          name: "default_name_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:

345.7 Status

- This module is not guaranteed to have a backwards compatible interface.

345.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

346.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

346.3 Parameters

346.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

346.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    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"
    user_pop3:
      name: "default_name_3"
      port: "4"
      secure: "none"
      server: "192.168.100.40"
```

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:

346.7 Status

- This module is not guaranteed to have a backwards compatible interface.

346.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

347.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

347.3 Parameters

347.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
        -
          description: "<your_own_value>"
          entry_id: "6"
          mac: "<your_own_value>"
          tag:
            -
              tags: "<your_own_value>"
```

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:

347.7 Status

- This module is not guaranteed to have a backwards compatible interface.

347.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

348.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

348.3 Parameters

348.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
      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"
      rsoo: "enable"
      rsoo_context_timeout: "24"
      rsoo_endpoint_attribute: "User-Name"
      rsoo_endpoint_block_attribute: "User-Name"
      rsoo_ep_one_ip_only: "enable"
```

(continues on next page)

(continued from previous page)

```
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"
```

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:

348.7 Status

- This module is not guaranteed to have a backwards compatible interface.

348.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

349.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

349.3 Parameters

349.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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) "
```

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:

349.7 Status

- This module is not guaranteed to have a backwards compatible interface.

349.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

350.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

350.3 Parameters

350.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

350.7 Status

- This module is not guaranteed to have a backwards compatible interface.

350.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

351.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

351.3 Parameters

351.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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>"
```

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:

351.7 Status

- This module is not guaranteed to have a backwards compatible interface.

351.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

352.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

352.3 Parameters

352.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

352.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure VoIP profiles.
  fortios_voip_profile:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

(continues on next page)

(continued from previous page)

```

block_update: "disable"
bye_rate: "31"
call_keeplive: "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"
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"

```

(continues on next page)

(continued from previous page)

```

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) "
status: "disable"
strict_register: "disable"
subscribe_rate: "106"
unknown_header: "discard"
update_rate: "108"

```

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:

352.7 Status

- This module is not guaranteed to have a backwards compatible interface.

352.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

353.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

353.3 Parameters

353.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

353.7 Status

- This module is not guaranteed to have a backwards compatible interface.

353.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

354.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

354.3 Parameters

354.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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) "
```

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:

354.7 Status

- This module is not guaranteed to have a backwards compatible interface.

354.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

355.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

355.3 Parameters

355.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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>"
```

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:

355.7 Status

- This module is not guaranteed to have a backwards compatible interface.

355.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

356.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

356.3 Parameters

356.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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: OSCP server configuration.
  fortios_vpn_certificate_ocsp_server:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

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:

356.7 Status

- This module is not guaranteed to have a backwards compatible interface.

356.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

357.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

357.3 Parameters

357.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    vpn_certificate_remote:
      name: "default_name_3"
      range: "global"
      remote: "<your_own_value>"
      source: "factory"
```

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:

357.7 Status

- This module is not guaranteed to have a backwards compatible interface.

357.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

358.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

358.3 Parameters

358.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

358.7 Status

- This module is not guaranteed to have a backwards compatible interface.

358.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

359.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

359.3 Parameters

359.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    vpn_ipsec_concentrator:
      member:
        -
          name: "default_name_4 (source vpn.ipsec.manualkey.name vpn.ipsec.phase1.
↪name) "
          name: "default_name_5"
          src_check: "disable"
```

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:

359.7 Status

- This module is not guaranteed to have a backwards compatible interface.

359.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

360.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

360.3 Parameters

360.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

360.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Configure FortiClient policy realm.
  fortios_vpn_ipsec_forticlient:
    vdom: "{{ vdom }}"
    state: "present"
    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) "
```

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:

360.7 Status

- This module is not guaranteed to have a backwards compatible interface.

360.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

361.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

361.3 Parameters

361.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    vpn_ipsec_manualkey:
      authentication: "null"
      authkey: "<your_own_value>"
      enckey: "<your_own_value>"
      encryption: "null"
      interface: "<your_own_value> (source system.interface.name)"
      local_gw: "<your_own_value>"
      localspi: "<your_own_value>"
      name: "default_name_10"
      npu_offload: "enable"
      remote_gw: "<your_own_value>"
      remotespi: "<your_own_value>"
```

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:

361.7 Status

- This module is not guaranteed to have a backwards compatible interface.

361.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

362.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

362.3 Parameters

362.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        vpn_ipsec_manualkey_interface:
          addr_type: "4"
          auth_alg: "null"
          auth_key: "<your_own_value>"
          enc_alg: "null"
          enc_key: "<your_own_value>"
          interface: "<your_own_value> (source system.interface.name)"
          ip_version: "4"
          local_gw: "<your_own_value>"
          local_gw6: "<your_own_value>"
          local_spi: "<your_own_value>"
          name: "default_name_13"
          npu_offload: "enable"
          remote_gw: "<your_own_value>"
          remote_gw6: "<your_own_value>"
          remote_spi: "<your_own_value>"
```

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:

362.7 Status

- This module is not guaranteed to have a backwards compatible interface.

362.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

363.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

363.3 Parameters

363.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    vpn_ipsec_phase1:
      acct_verify: "enable"
      add_gw_route: "enable"
      add_route: "disable"
      assign_ip: "disable"
      assign_ip_from: "range"
      authmethod: "psk"
      authmethod_remote: "psk"
      authpasswd: "<your_own_value>"
      authusr: "<your_own_value>"
      authusrggrp: "<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"
```

(continues on next page)

(continued from previous page)

```

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) "
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>"

```

(continues on next page)

(continued from previous page)

```

    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)"
    wizard_type: "custom"
    xauthtype: "disable"

```

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:

363.7 Status

- This module is not guaranteed to have a backwards compatible interface.

363.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

364.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

364.3 Parameters

364.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        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>"
          authusrggrp: "<your_own_value> (source user.group.name)"
          auto_discovery_forwarder: "enable"
          auto_discovery_psk: "enable"
          auto_discovery_receiver: "enable"
          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>"
```

(continues on next page)

(continued from previous page)

```

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>"
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>"

```

(continues on next page)

(continued from previous page)

```

        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"
        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) "

```

(continues on next page)

(continued from previous page)

```
vni: "133"  
wizard_type: "custom"  
xauthtype: "disable"
```

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:

364.7 Status

- This module is not guaranteed to have a backwards compatible interface.

364.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

365.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

365.3 Parameters

365.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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 }}"
        state: "present"
        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"
```

(continues on next page)

(continued from previous page)

```

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"

```

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:

365.7 Status

- This module is not guaranteed to have a backwards compatible interface.

365.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

366.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

366.3 Parameters

366.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

(continues on next page)

(continued from previous page)

```

    phasename: "<your_own_value> (source vpn.ipsec.phasel-interface.name) "
    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>"

```

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:

366.7 Status

- This module is not guaranteed to have a backwards compatible interface.

366.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

367.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

367.3 Parameters

367.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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 }}"
      vpn_l2tp:
        eip: "<your_own_value>"
        enforce_ipsec: "enable"
        sip: "<your_own_value>"
        status: "enable"
        usrgrp: "<your_own_value> (source user.group.name)"
```

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:

367.7 Status

- This module is not guaranteed to have a backwards compatible interface.

367.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

368.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

368.3 Parameters

368.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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>"
```

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:

368.7 Status

- This module is not guaranteed to have a backwards compatible interface.

368.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

369.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

369.3 Parameters

369.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
          usrggrp: "<your_own_value> (source user.group.name) "
```

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:

369.7 Status

- This module is not guaranteed to have a backwards compatible interface.

369.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

370.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

370.3 Parameters

370.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
```

(continues on next page)

(continued from previous page)

```

-
    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"
    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)"

```

(continues on next page)

(continued from previous page)

```
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"
```

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:

370.7 Status

- This module is not guaranteed to have a backwards compatible interface.

370.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

371.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

371.3 Parameters

371.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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>"
```

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:

371.7 Status

- This module is not guaranteed to have a backwards compatible interface.

371.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

372.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

372.3 Parameters

372.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

(continues on next page)

(continued from previous page)

```

        sso_password: "<your_own_value>"
        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"

```

(continues on next page)

(continued from previous page)

```

os_check_list:
-
    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>"

```

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:

372.7 Status

- This module is not guaranteed to have a backwards compatible interface.

372.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

373.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

373.3 Parameters

373.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      vpn_ssl_web_realm:
        login_page: "<your_own_value>"
        max_concurrent_user: "4"
        url_path: "<your_own_value>"
        virtual_host: "<your_own_value>"
```

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:

373.7 Status

- This module is not guaranteed to have a backwards compatible interface.

373.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

374.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

374.3 Parameters

374.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

374.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure SSL VPN user bookmark.
  fortios_vpn_ssl_web_user_bookmark:
    vdom: "{{ vdom }}"
    state: "present"
    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"
```

(continues on next page)

(continued from previous page)

```
custom_lang: "<your_own_value> (source system.custom-language.name) "  
name: "default_name_28"
```

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:

374.7 Status

- This module is not guaranteed to have a backwards compatible interface.

374.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

375.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

375.3 Parameters

375.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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) "
```

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:

375.7 Status

- This module is not guaranteed to have a backwards compatible interface.

375.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

376.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

376.3 Parameters

376.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        waf_main_class:
          id: "3"
          name: "default_name_4"
```

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:

376.7 Status

- This module is not guaranteed to have a backwards compatible interface.

376.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

377.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

377.3 Parameters

377.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

(continues on next page)

(continued from previous page)

```
    id: "24"
    line_length: "enable"
    malformed: "enable"
    max_cookie: "enable"
    max_header_line: "enable"
    max_range_segment: "enable"
    max_url_param: "enable"
    method: "enable"
    param_length: "enable"
    pattern: "<your_own_value>"
    regex: "enable"
    url_param_length: "enable"
    version: "enable"
  header_length:
    action: "allow"
    length: "39"
    log: "enable"
    severity: "high"
    status: "enable"
  hostname:
    action: "allow"
    log: "enable"
    severity: "high"
    status: "enable"
  line_length:
    action: "allow"
    length: "50"
    log: "enable"
    severity: "high"
    status: "enable"
  malformed:
    action: "allow"
    log: "enable"
    severity: "high"
    status: "enable"
  max_cookie:
    action: "allow"
    log: "enable"
    max_cookie: "62"
    severity: "high"
    status: "enable"
  max_header_line:
    action: "allow"
    log: "enable"
    max_header_line: "68"
    severity: "high"
    status: "enable"
  max_range_segment:
    action: "allow"
    log: "enable"
    max_range_segment: "74"
    severity: "high"
    status: "enable"
  max_url_param:
    action: "allow"
    log: "enable"
    max_url_param: "80"
```

(continues on next page)

(continued from previous page)

```

        severity: "high"
        status: "enable"
    method:
        action: "allow"
        log: "enable"
        severity: "high"
        status: "enable"
    param_length:
        action: "allow"
        length: "90"
        log: "enable"
        severity: "high"
        status: "enable"
    url_param_length:
        action: "allow"
        length: "96"
        log: "enable"
        severity: "high"
        status: "enable"
    version:
        action: "allow"
        log: "enable"
        severity: "high"
        status: "enable"
    extended_log: "enable"
    external: "disable"
    method:
        default_allowed_methods: "get"
        log: "enable"
        method_policy:
            -
                address: "<your_own_value> (source firewall.address.name firewall.
↪addrgrp.name)"
                allowed_methods: "get"
                id: "113"
                pattern: "<your_own_value>"
                regex: "enable"
                severity: "high"
                status: "enable"
    name: "default_name_118"
    signature:
        credit_card_detection_threshold: "120"
        custom_signature:
            -
                action: "allow"
                case_sensitivity: "disable"
                direction: "request"
                log: "enable"
                name: "default_name_126"
                pattern: "<your_own_value>"
                severity: "high"
                status: "enable"
                target: "arg"
        disabled_signature:
            -
                id: "132 (source waf.signature.id)"
    disabled_sub_class:

```

(continues on next page)

(continued from previous page)

```

-
  id: "134 (source waf.sub-class.id) "
  main_class:
  -
    action: "allow"
    id: "137 (source waf.main-class.id) "
    log: "enable"
    severity: "high"
    status: "enable"
  url_access:
  -
    access_pattern:
    -
      id: "143"
      negate: "enable"
      pattern: "<your_own_value>"
      regex: "enable"
      srcaddr: "<your_own_value> (source firewall.address.name firewall.
↪addrgrp.name) "
      action: "bypass"
      address: "<your_own_value> (source firewall.address.name firewall.addrgrp.
↪name) "
      id: "150"
      log: "enable"
      severity: "high"

```

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:

377.7 Status

- This module is not guaranteed to have a backwards compatible interface.

377.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

378.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

378.3 Parameters

378.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    waf_signature:
      desc: "<your_own_value>"
      id: "4"
```

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:

378.7 Status

- This module is not guaranteed to have a backwards compatible interface.

378.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

379.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

379.3 Parameters

379.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        waf_sub_class:
          id: "3"
          name: "default_name_4"
```

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:

379.7 Status

- This module is not guaranteed to have a backwards compatible interface.

379.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

380.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

380.3 Parameters

380.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        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>"
```

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:

380.7 Status

- This module is not guaranteed to have a backwards compatible interface.

380.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

381.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

381.3 Parameters

381.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

381.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Designate cache-service for wan-optimization and webcache.
  fortios_wanopt_cache_service:
    vdom: "{{ vdom }}"
    wanopt_cache_service:
      acceptable_connections: "any"
      collaboration: "enable"
      device_id: "<your_own_value>"
      dst_peer:
        -
          auth_type: "7"
          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"
```

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:

381.7 Status

- This module is not guaranteed to have a backwards compatible interface.

381.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

382.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

382.3 Parameters

382.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

382.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Configure WAN optimization content delivery network rules.
      fortios_wanopt_content_delivery_network_rule:
        vdom: "{{ vdom }}"
        state: "present"
        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:
```

(continues on next page)

(continued from previous page)

```

-
  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"

```

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:

382.7 Status

- This module is not guaranteed to have a backwards compatible interface.

382.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

383.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

383.3 Parameters

383.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    wanopt_peer:
      ip: "<your_own_value>"
      peer_host_id: "myhostname"
```

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:

383.7 Status

- This module is not guaranteed to have a backwards compatible interface.

383.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

384.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

384.3 Parameters

384.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

(continues on next page)

(continued from previous page)

```

    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:
    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"

```

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:

384.7 Status

- This module is not guaranteed to have a backwards compatible interface.

384.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

385.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

385.3 Parameters

385.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

385.7 Status

- This module is not guaranteed to have a backwards compatible interface.

385.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

386.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

386.3 Parameters

386.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

386.7 Status

- This module is not guaranteed to have a backwards compatible interface.

386.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

387.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

387.3 Parameters

387.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

387.7 Status

- This module is not guaranteed to have a backwards compatible interface.

387.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

388.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

388.3 Parameters

388.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    web_proxy_debug_url:
      exact: "enable"
      name: "default_name_4"
      status: "enable"
      url_pattern: "<your_own_value>"
```

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:

388.7 Status

- This module is not guaranteed to have a backwards compatible interface.

388.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

389.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

389.3 Parameters

389.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

389.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure explicit Web proxy settings.
  fortios_web_proxy_explicit:
    vdom: "{{ vdom }}"
    web_proxy_explicit:
      ftp_incoming_port: "<your_own_value>"
      ftp_over_http: "enable"
      http_incoming_port: "<your_own_value>"
      https_incoming_port: "<your_own_value>"
      https_replacement_message: "enable"
      incoming_ip: "<your_own_value>"
      incoming_ip6: "<your_own_value>"
      ipv6_status: "enable"
      message_upon_server_error: "enable"
      outgoing_ip: "<your_own_value>"
      outgoing_ip6: "<your_own_value>"
      pac_file_data: "<your_own_value>"
      pac_file_name: "<your_own_value>"
      pac_file_server_port: "<your_own_value>"
      pac_file_server_status: "enable"
      pac_file_url: "<your_own_value>"
      pac_policy:
        -
          comments: "<your_own_value>"
          dstaddr:
            -
              name: "default_name_22 (source firewall.address.name firewall.addrgrp.
↪name)"
          pac_file_data: "<your_own_value>"
          pac_file_name: "<your_own_value>"
          policyid: "25"
          srcaddr:
            -
```

(continues on next page)

(continued from previous page)

```

        name: "default_name_27 (source firewall.address.name firewall.addrgrp.
↪name firewall.proxy-address.name firewall.proxy-addrgrp.name) "
        srcaddr6:
        -
            name: "default_name_29 (source firewall.address6.name firewall.
↪addrgrp6.name) "
            status: "enable"
            pref_dns_result: "ipv4"
            realm: "<your_own_value>"
            sec_default_action: "accept"
            socks: "enable"
            socks_incoming_port: "<your_own_value>"
            ssl_algorithm: "high"
            status: "enable"
            strict_guest: "enable"
            trace_auth_no_rsp: "enable"
            unknown_http_version: "reject"

```

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:

389.7 Status

- This module is not guaranteed to have a backwards compatible interface.

389.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

390.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

390.3 Parameters

390.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

390.7 Status

- This module is not guaranteed to have a backwards compatible interface.

390.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`fortios_web_proxy_forward_server_group` – Configure a forward server group consisting of 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*

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

391.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

391.3 Parameters

391.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      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"
```

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:

391.7 Status

- This module is not guaranteed to have a backwards compatible interface.

391.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

392.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

392.3 Parameters

392.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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) "
```

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:

392.7 Status

- This module is not guaranteed to have a backwards compatible interface.

392.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

393.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

393.3 Parameters

393.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

393.7 Status

- This module is not guaranteed to have a backwards compatible interface.

393.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

394.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

394.3 Parameters

394.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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>"
```

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:

394.7 Status

- This module is not guaranteed to have a backwards compatible interface.

394.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

395.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

395.3 Parameters

395.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

395.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Configure Wireless Internet service provider (WISP) servers.
      fortios_web_proxy_wisp:
        vdom: "{{ vdom }}"
        state: "present"
        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"
```

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:

395.7 Status

- This module is not guaranteed to have a backwards compatible interface.

395.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

396.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

396.3 Parameters

396.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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 }}"
    state: "present"
    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"
```

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:

396.7 Status

- This module is not guaranteed to have a backwards compatible interface.

396.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

397.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

397.3 Parameters

397.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    webfilter_content_header:
      comment: "Optional comments."
      entries:
        -
          action: "block"
          category: "<your_own_value>"
          pattern: "<your_own_value>"
      id: "8"
      name: "default_name_9"
```

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:

397.7 Status

- This module is not guaranteed to have a backwards compatible interface.

397.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

398.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

398.3 Parameters

398.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      request_packet_size_limit: "12"
      warn_auth_https: "enable"
```

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:

398.7 Status

- This module is not guaranteed to have a backwards compatible interface.

398.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

399.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

399.3 Parameters

399.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        webfilter_ftgd_local_cat:
          desc: "<your_own_value>"
          id: "4"
          status: "enable"
```

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:

399.7 Status

- This module is not guaranteed to have a backwards compatible interface.

399.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

400.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

400.3 Parameters

400.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        webfilter_ftgd_local_rating:
          rating: "<your_own_value>"
          status: "enable"
          url: "myurl.com"
```

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:

400.7 Status

- This module is not guaranteed to have a backwards compatible interface.

400.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

401.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

401.3 Parameters

401.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

401.7 Status

- This module is not guaranteed to have a backwards compatible interface.

401.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

402.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

402.3 Parameters

402.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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 }}"
    webfilter_ips_urlfilter_setting:
      device: "<your_own_value> (source system.interface.name)"
      distance: "4"
      gateway: "<your_own_value>"
      geo_filter: "<your_own_value>"
```

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:

402.7 Status

- This module is not guaranteed to have a backwards compatible interface.

402.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

403.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

403.3 Parameters

403.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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>"
```

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:

403.7 Status

- This module is not guaranteed to have a backwards compatible interface.

403.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

404.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

404.3 Parameters

404.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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)"
```

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:

404.7 Status

- This module is not guaranteed to have a backwards compatible interface.

404.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

405.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

405.3 Parameters

405.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

(continues on next page)

(continued from previous page)

```

        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"
log_all_url: "enable"
name: "default_name_36"
options: "activexfilter"
override:
    ovr_dcookie: "allow"
    ovr_dur: "<your_own_value>"
    ovr_dur_mode: "constant"
    ovr_scope: "user"
    ovr_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"

```

(continues on next page)

(continued from previous page)

```
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."
  id: "87"
youtube_channel_status: "disable"
```

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:

405.7 Status

- This module is not guaranteed to have a backwards compatible interface.

405.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

406.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

406.3 Parameters

406.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

406.7 Status

- This module is not guaranteed to have a backwards compatible interface.

406.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

407.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

407.3 Parameters

407.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

407.7 Status

- This module is not guaranteed to have a backwards compatible interface.

407.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

408.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

408.3 Parameters

408.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        wireless_controller_ap_status:
          bssid: "<your_own_value>"
          id: "4"
          ssid: "<your_own_value>"
          status: "rogue"
```

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:

408.7 Status

- This module is not guaranteed to have a backwards compatible interface.

408.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)

- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

409.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

409.3 Parameters

409.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
  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"
```

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:

409.7 Status

- This module is not guaranteed to have a backwards compatible interface.

409.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 410

`fortios_wireless_controller_bonjour_profile` – Configure Bonjour profiles. Bonjour is Apple’s zero configuration networking protocol. Bonjour profiles allow APs and FortiAPs to connect to networks using Bonjour in Fortinet’s FortiOS and FortiGate.

New in version 2.9.

- *Synopsis*
- *Requirements*
- *Parameters*
- *Notes*
- *Examples*
- *Return Values*
- *Status*
- *Authors*

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

410.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

410.3 Parameters

410.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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 connect to
      networks using Bonjour.
    fortios_wireless_controller_bonjour_profile:
      vdom: "{{ vdom }}"
      state: "present"
      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>"
```

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:

410.7 Status

- This module is not guaranteed to have a backwards compatible interface.

410.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

411.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

411.3 Parameters

411.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

411.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Configure wireless controller 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"
```

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:

411.7 Status

- This module is not guaranteed to have a backwards compatible interface.

411.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

412.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

412.3 Parameters

412.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

412.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
- name: Configure 3GPP public land mobile network (PLMN).
  fortios_wireless_controller_hotspot20_anqp_3gpp_cellular:
    vdom: "{{ vdom }}"
    state: "present"
    wireless_controller_hotspot20_anqp_3gpp_cellular:
      mcc_mnc_list:
        -
          id: "4"
          mcc: "<your_own_value>"
          mnc: "<your_own_value>"
      name: "default_name_7"
```

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:

412.7 Status

- This module is not guaranteed to have a backwards compatible interface.

412.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

413.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

413.3 Parameters

413.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
    vdom: "{{ vdom }}"
    state: "present"
    wireless_controller_hotspot20_anqp_ip_address_type:
      ipv4_address_type: "not-available"
      ipv6_address_type: "not-available"
      name: "default_name_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:

413.7 Status

- This module is not guaranteed to have a backwards compatible interface.

413.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

414.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

414.3 Parameters

414.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        wireless_controller_hotspot20_anqp_nai_realm:
          nai_list:
            -
              eap_method:
                -
                  auth_param:
                    -
                      id: "6"
                      index: "7"
                      val: "eap-identity"
                    index: "9"
                    method: "eap-identity"
                  encoding: "disable"
                  nai_realm: "<your_own_value>"
                  name: "default_name_13"
              name: "default_name_14"
```

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:

414.7 Status

- This module is not guaranteed to have a backwards compatible interface.

414.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

415.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

415.3 Parameters

415.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        wireless_controller_hotspot20_anqp_network_auth_type:
          auth_type: "acceptance-of-terms"
          name: "default_name_4"
          url: "myurl.com"
```

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:

415.7 Status

- This module is not guaranteed to have a backwards compatible interface.

415.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

416.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

416.3 Parameters

416.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        wireless_controller_hotspot20_anqp_roaming_consortium:
          name: "default_name_3"
          oi_list:
            -
              comment: "Comment."
              index: "6"
              oi: "<your_own_value>"
```

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:

416.7 Status

- This module is not guaranteed to have a backwards compatible interface.

416.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

417.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

417.3 Parameters

417.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        wireless_controller_hotspot20_anqp_venue_name:
          name: "default_name_3"
          value_list:
            -
              index: "5"
              lang: "<your_own_value>"
              value: "<your_own_value>"
```

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:

417.7 Status

- This module is not guaranteed to have a backwards compatible interface.

417.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

418.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

418.3 Parameters

418.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        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"
```

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:

418.7 Status

- This module is not guaranteed to have a backwards compatible interface.

418.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

419.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

419.3 Parameters

419.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    wireless_controller_hotspot20_h2qp_operator_name:
      name: "default_name_3"
      value_list:
        -
          index: "5"
          lang: "<your_own_value>"
          value: "<your_own_value>"
```

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:

419.7 Status

- This module is not guaranteed to have a backwards compatible interface.

419.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

420.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

420.3 Parameters

420.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

420.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Configure online sign up (OSU) provider list.
      fortios_wireless_controller_hotspot20_h2qp_osu_provider:
        vdom: "{{ vdom }}"
        state: "present"
        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"
```

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:

420.7 Status

- This module is not guaranteed to have a backwards compatible interface.

420.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

421.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

421.3 Parameters

421.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

421.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
- name: Configure WAN metrics.
  fortios_wireless_controller_hotspot20_h2qp_wan_metric:
    vdom: "{{ vdom }}"
    state: "present"
  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"
```

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:

421.7 Status

- This module is not guaranteed to have a backwards compatible interface.

421.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

422.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

422.3 Parameters

422.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
        vdom: "{{ vdom }}"
        state: "present"
        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)"
```

(continues on next page)

(continued from previous page)

```

    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"

```

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:

422.7 Status

- This module is not guaranteed to have a backwards compatible interface.

422.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

423.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

423.3 Parameters

423.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

423.7 Status

- This module is not guaranteed to have a backwards compatible interface.

423.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

424.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

424.3 Parameters

424.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    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"
```

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:

424.7 Status

- This module is not guaranteed to have a backwards compatible interface.

424.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

425.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

425.3 Parameters

425.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

425.7 Status

- This module is not guaranteed to have a backwards compatible interface.

425.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

426.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

426.3 Parameters

426.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

426.5 Examples

```
- hosts: fortigates
  collections:
    - fortinet.fortios
  connection: httpapi
  vars:
    vdom: "root"
    ansible_httpapi_use_ssl: yes
    ansible_httpapi_validate_certs: no
    ansible_httpapi_port: 443
  tasks:
    - name: Configure WiFi quality of service (QoS) profiles.
      fortios_wireless_controller_qos_profile:
        vdom: "{{ vdom }}"
        state: "present"
        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"
```

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:

426.7 Status

- This module is not guaranteed to have a backwards compatible interface.

426.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

427.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

427.3 Parameters

427.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
```

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:

427.7 Status

- This module is not guaranteed to have a backwards compatible interface.

427.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)

- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

428.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

428.3 Parameters

428.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
    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"
```

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:

428.7 Status

- This module is not guaranteed to have a backwards compatible interface.

428.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

429.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

429.3 Parameters

429.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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:
    vdom: "{{ vdom }}"
    state: "present"
    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)"
```

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:

429.7 Status

- This module is not guaranteed to have a backwards compatible interface.

429.8 Authors

- Link Zheng (@chillancezen)

- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

430.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

430.3 Parameters

430.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    wireless_controller_vap:
      acct_interim_interval: "3"
      alias: "<your_own_value>"
      auth: "psk"
      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"
```

(continues on next page)

(continued from previous page)

```

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>"
        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>"

```

(continues on next page)

(continued from previous page)

```
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"
```

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:

430.7 Status

- This module is not guaranteed to have a backwards compatible interface.

430.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)

- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

431.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

431.3 Parameters

431.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
        wireless_controller_vap_group:
          comment: "Comment."
          name: "default_name_4"
          vaps:
            -
              name: "default_name_6 (source wireless-controller.vap.name)"
```

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:

431.7 Status

- This module is not guaranteed to have a backwards compatible interface.

431.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

432.2 Requirements

The below requirements are needed on the host that executes this module.

- `ansible>=2.9.0`

432.3 Parameters

432.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
  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"
```

(continues on next page)

(continued from previous page)

```
eapol_logoff_thresh: "30"
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"
```

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:

432.7 Status

- This module is not guaranteed to have a backwards compatible interface.

432.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

433.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

433.3 Parameters

433.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

433.5 Examples

```
- hosts: fortigates
collections:
  - fortinet.fortios
connection: httpapi
vars:
  vdom: "root"
  ansible_httpapi_use_ssl: yes
  ansible_httpapi_validate_certs: no
  ansible_httpapi_port: 443
tasks:
  - name: Configure Wireless Termination Points (WTPs), that is, FortiAPs or APs to
    be managed by FortiGate.
    fortios_wireless_controller_wtp:
      vdom: "{{ vdom }}"
      state: "present"
      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)"
```

(continues on next page)

(continued from previous page)

```

    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:
        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"

```

(continues on next page)

(continued from previous page)

```
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) "
```

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:

433.7 Status

- This module is not guaranteed to have a backwards compatible interface.

433.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

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*

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

434.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

434.3 Parameters

434.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
    wireless_controller_wtp_group:
      name: "default_name_3"
      platform_type: "AP-11N"
      wtps:
        -
          wtp_id: "<your_own_value> (source wireless-controller.wtp.wtp-id) "
```

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:

434.7 Status

- This module is not guaranteed to have a backwards compatible interface.

434.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)

- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel Angel Munoz (@mamunozgonzalez)
- Nicolas Thomas (@thomnico)

Hint: If you notice any issues in this documentation, you can create a pull request to improve it.

`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*

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

435.2 Requirements

The below requirements are needed on the host that executes this module.

- ansible>=2.9.0

435.3 Parameters

435.4 Notes

Note:

- Legacy fortiosapi has been deprecated, httpapi is the preferred way to run playbooks
-

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"
      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"
```

(continues on next page)

(continued from previous page)

```

    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) "
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"

```

(continues on next page)

(continued from previous page)

```

    ap_sniffer_mgmt_other: "enable"
    ap_sniffer_mgmt_probe: "enable"
    auto_power_high: "82"
    auto_power_level: "enable"
    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"

```

(continues on next page)

(continued from previous page)

```

call_admission_control: "enable"
call_capacity: "134"
channel:
  -
    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"

```

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:

435.7 Status

- This module is not guaranteed to have a backwards compatible interface.

435.8 Authors

- Link Zheng (@chillancezen)
- Hongbin Lu (@fgtdev-hblu)
- Frank Shen (@frankshen01)
- Jie Xue (@JieX19)
- Miguel 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 436

Indices and tables

- [genindex](#)
- [modindex](#)
- [search](#)