FortiOS - New Features Guide

Version 6.2.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

March 28, 2019
FortiOS 6.2.0 New Features Guide
01-620-538749-20190328

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-03-28	Initial release of FortiOS 6.2.0.

Expanding Fabric Family

This section lists the new features added to FortiOS for the expanding fabric family.

Telemetry Integration - New FTNT Products

With this version, you can add other Fortinet products to the Security Fabric. The following products are supported:

- FortiMail
- FortiWeb
- FortiADC
- FortiDDOS
- FortiWLC

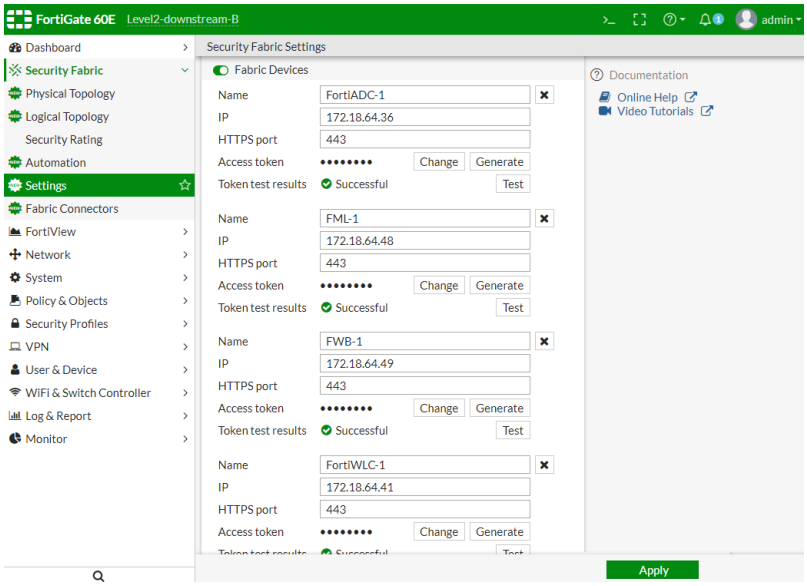
In FortiGate, you can show device details and widgets in the following pages:

- Security Fabric Settings
- Security Fabric Physical Topology
- Security Fabric Logical Topology
- Dashboard widgets

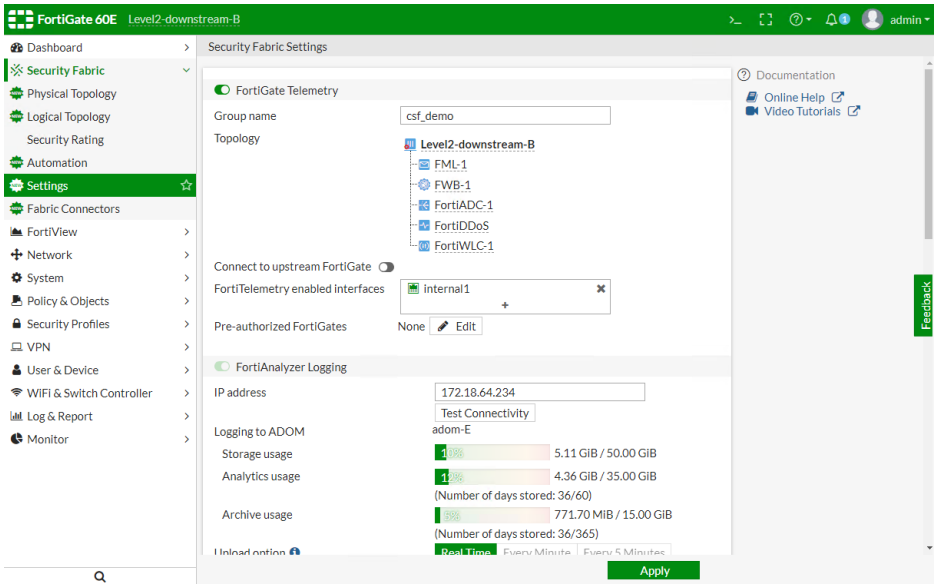
Sample configuration

To configure Security Fabric devices in the GUI:

1. In *Security Fabric* > *Settings*, configure *Fabric Devices* so that they appear in the *Topology* field.



2. In the *FortiGate Telemetry* section, the *Topology* field shows the devices.



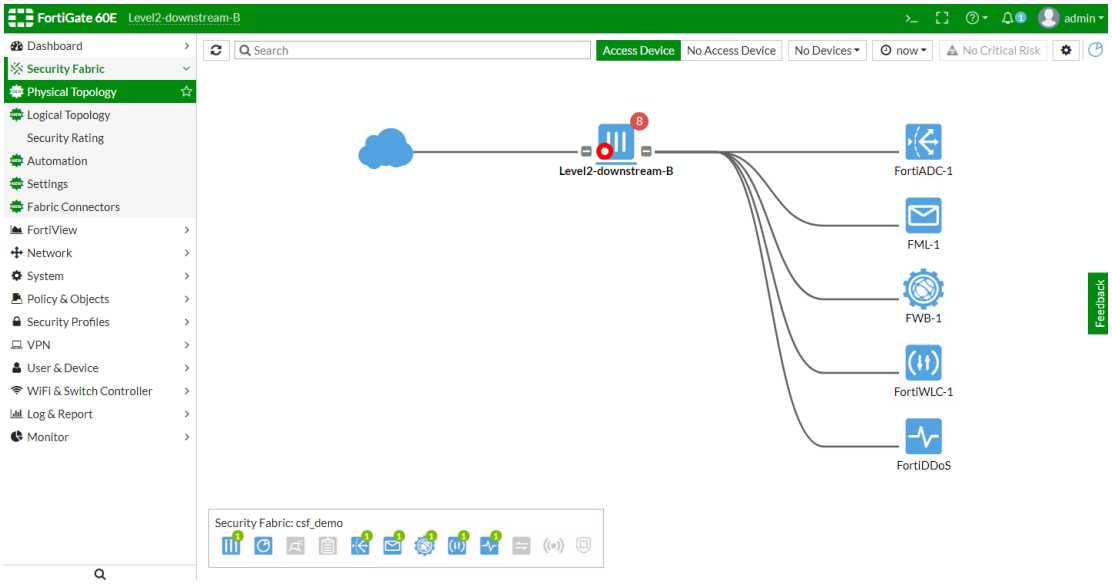
To configure Security Fabric devices in the CLI:

```
config system csf
...
    config fabric-device
        edit "FortiADC-1"
            set device-ip 172.18.64.36
            set access-token xxxxxx
        next
```

```
        edit "FML-1"
            set device-ip 172.18.64.48
            set access-token xxxxxx
        next
        edit "FWB-1"
            set device-ip 172.18.64.49
            set access-token xxxxxx
        next
    end
end
```

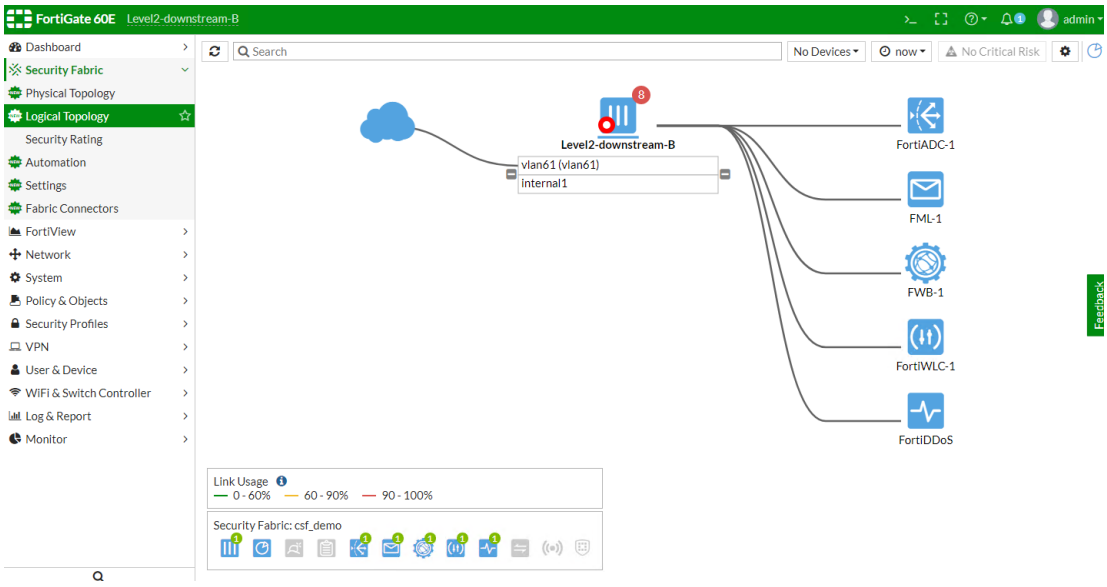
To configure the Security Fabric Physical Topology in the GUI:

1. Go to *Security Fabric* > *Physical Topology* to configure the physical topology.



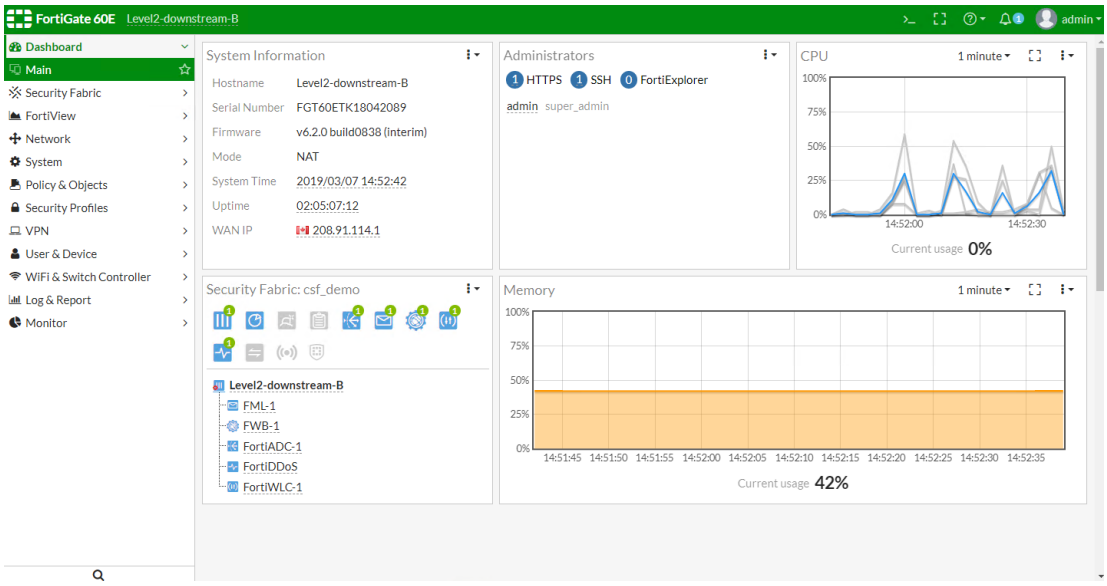
To configure the Security Fabric Logical Topology in the GUI:

1. Go to *Security Fabric* > *Logical Topology* to configure the logical topology.



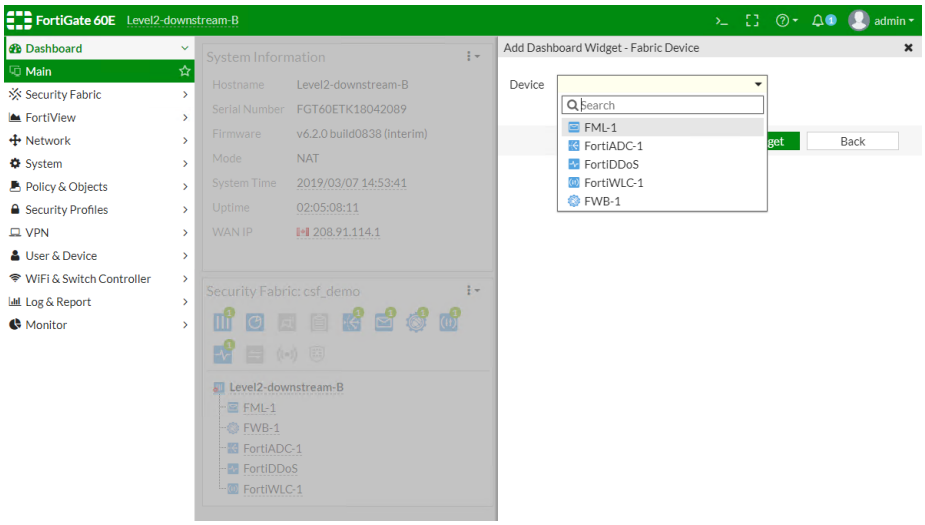
To view Security Fabric devices in the Dashboard:

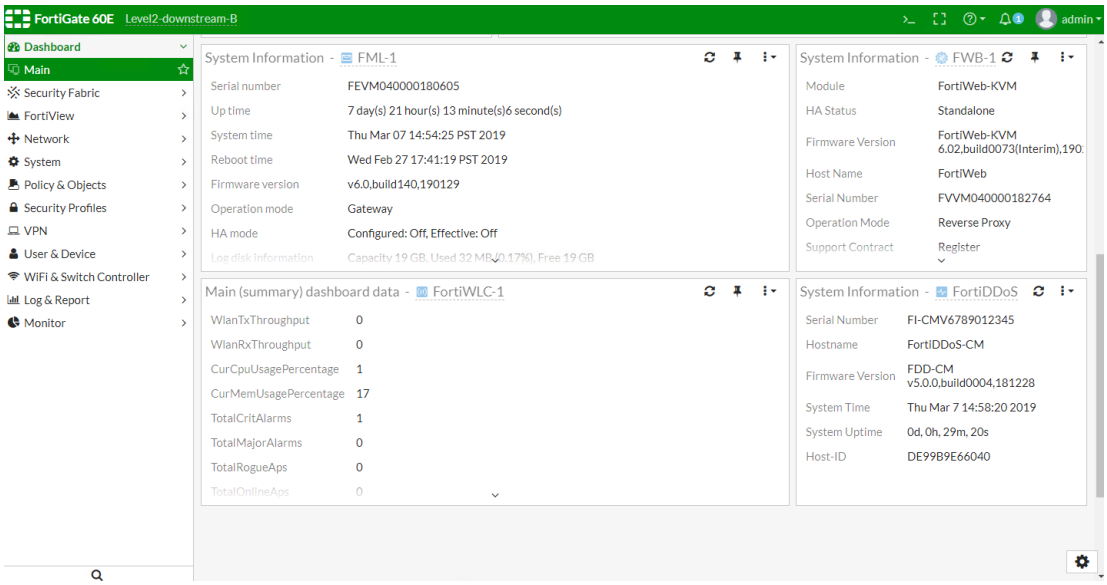
1. Go to *Dashboard* > *Main*. The Security Fabric widget includes the Security Fabric devices.



To add Security Fabric devices in the Dashboard:

1. When you add a widget, you can add Security Fabric devices.

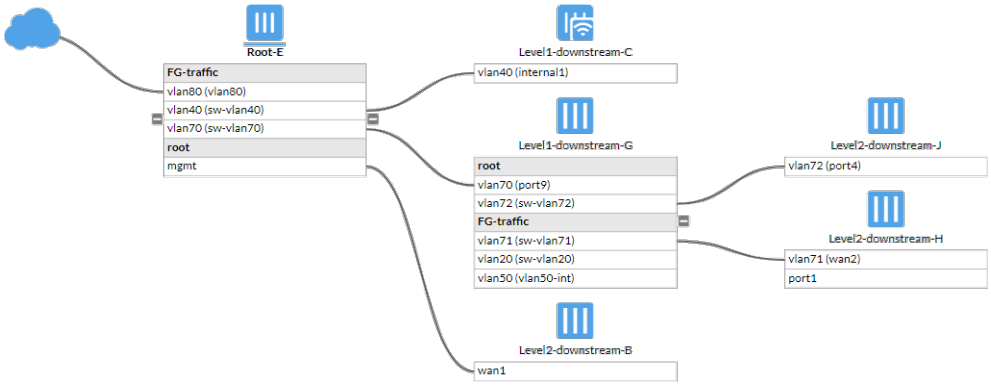




Split-Task VDOM Support

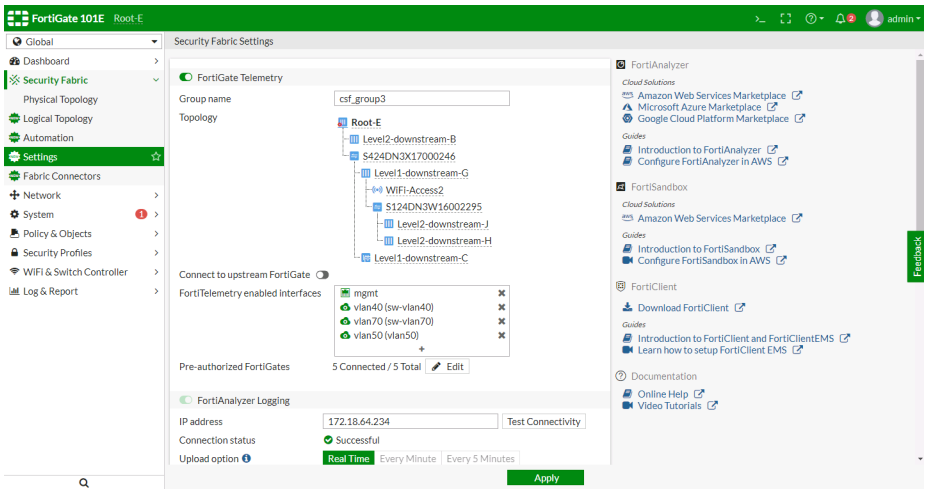
This feature adds support for Security Fabric in split-task VDOM mode.

Security Fabric topology



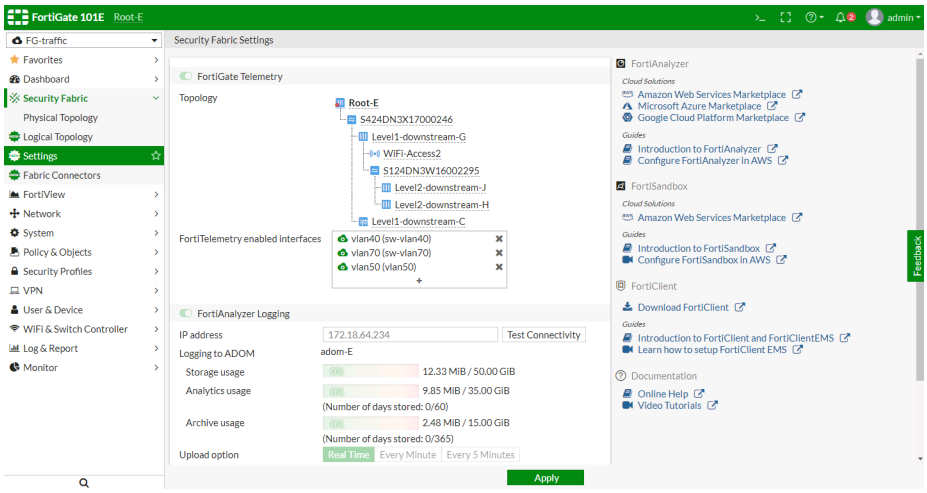
Security Fabric setting

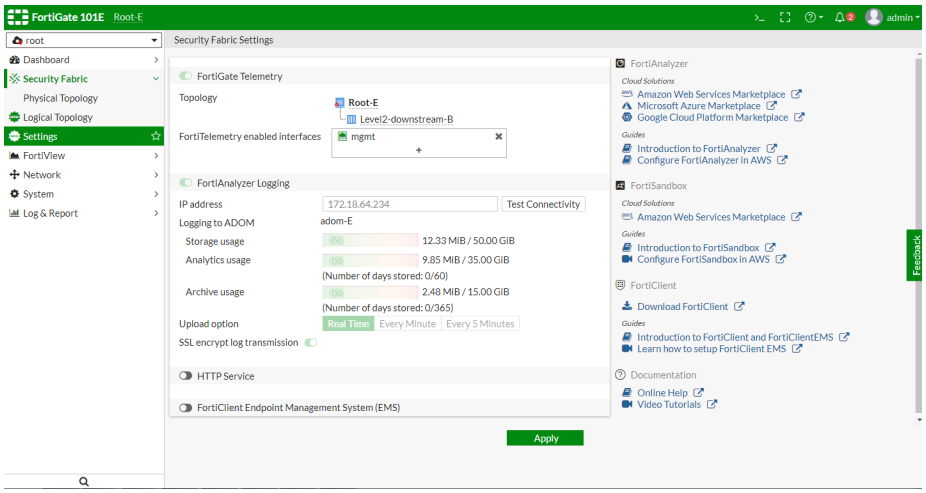
FortiGate Telemetry can now be enabled in split-task VDOM mode. FortiGate telemetry settings are available on the *Security Fabric* > *Settings* page.



Telemetry settings are shown in both global and VDOM contexts, but in VDOM contexts only the *Topology* and *FortiTelemetry enabled interfaces* fields are shown.

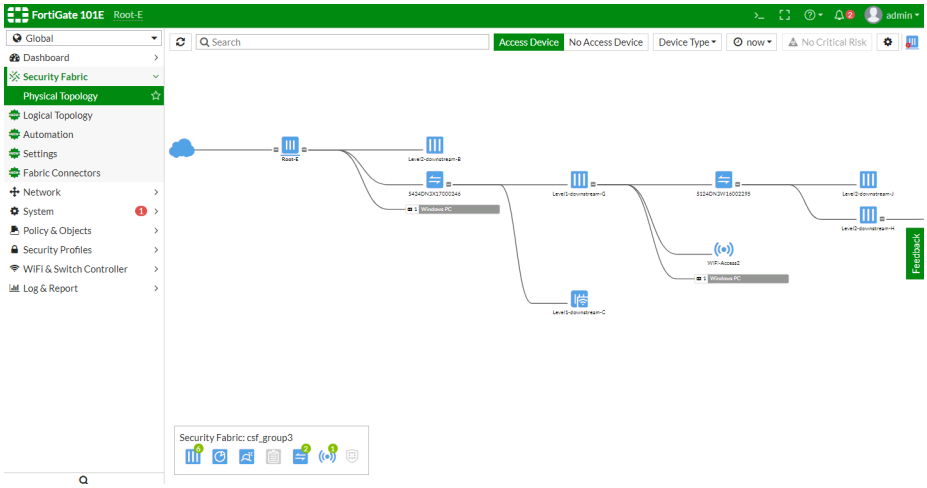
If the upstream FortiGate has split-task VDOM mode enabled, it can allow downstream FortiGates to join the Security Fabric in the *root* and *FG-traffic* VDOMs. If the downstream FortiGate has split-task VDOM mode enabled, it can only connect to the upstream FortiGate via the downstream FortiGate interface in the *root* VDOM.



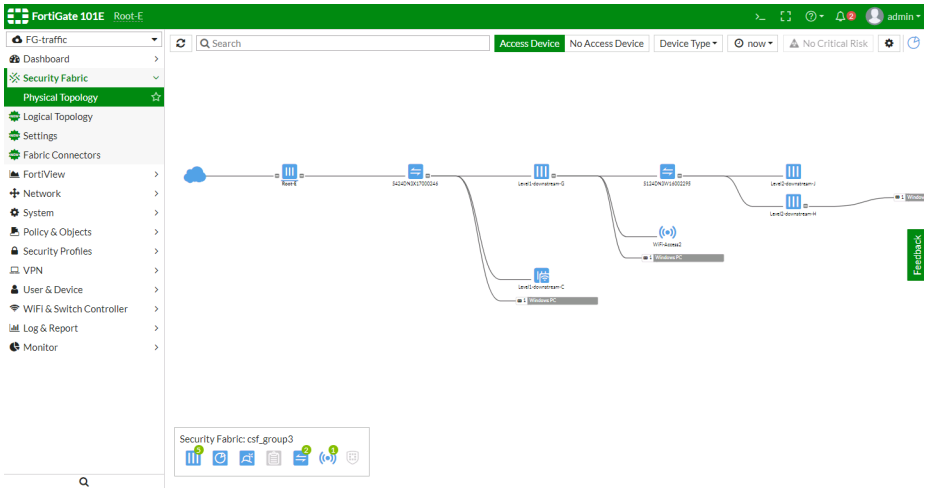


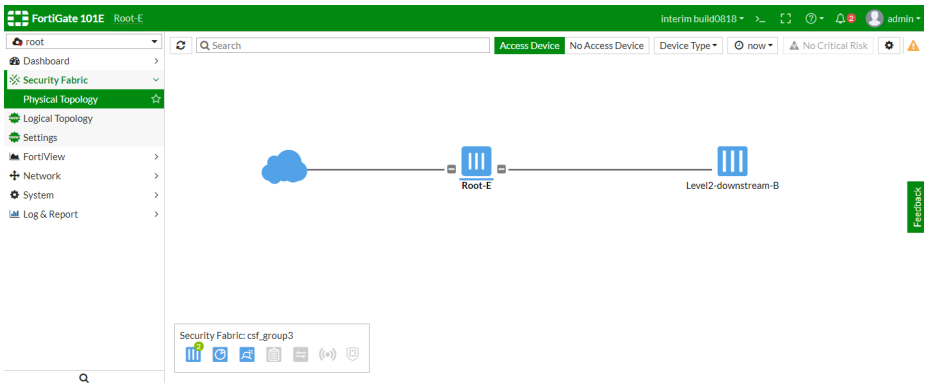
Physical topology

The global Physical Topology page shows the root FortiGate and all downstream FortiGates that are in the same Security Fabric.



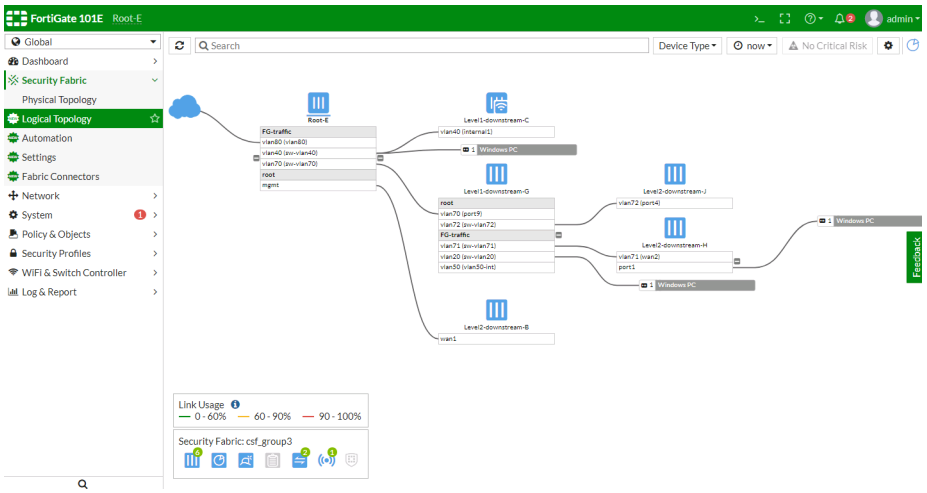
The *root* or *FG-traffic* VDOMs' Physical Topology page shows the root FortiGate and only the downstream FortiGates that connect to the current VDOM on the root FortiGate.



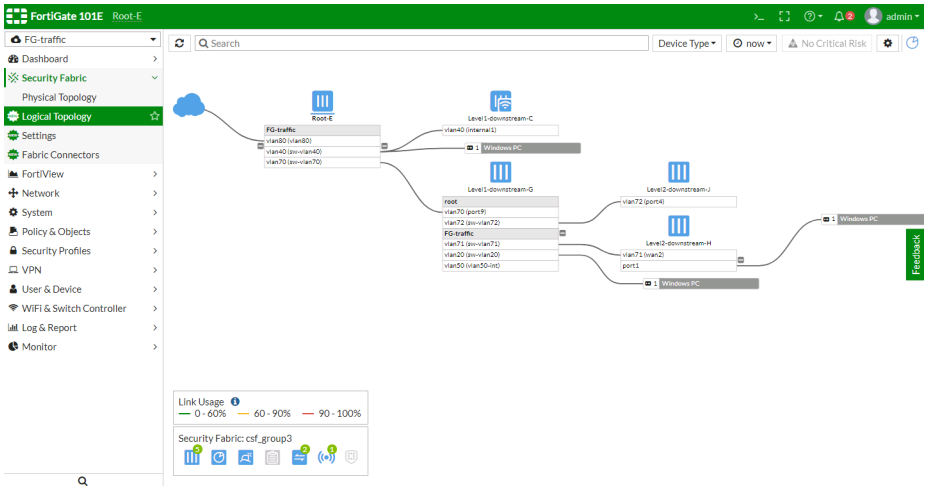


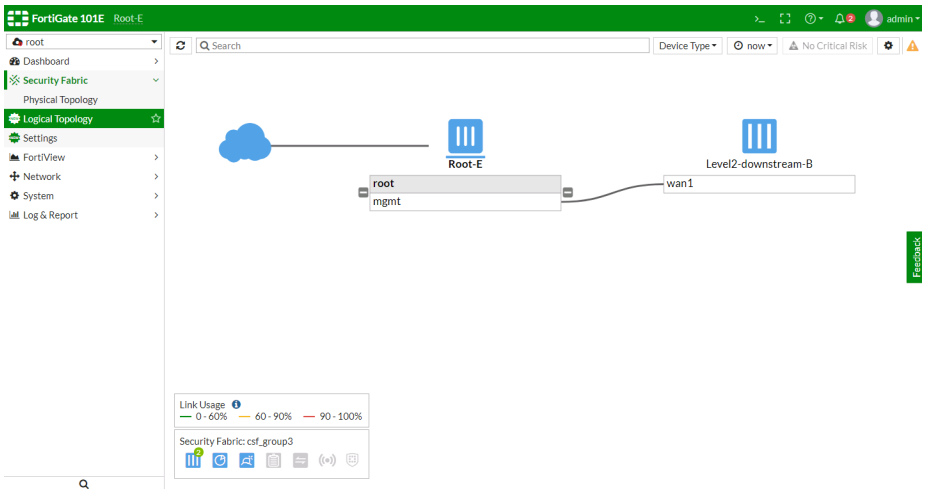
Logical topology

FortiGate interfaces are grouped by VDOMs. The global Logical Topology page shows the root FortiGate and all downstream FortiGates that are in the same Security Fabric, including interfaces' connection information.



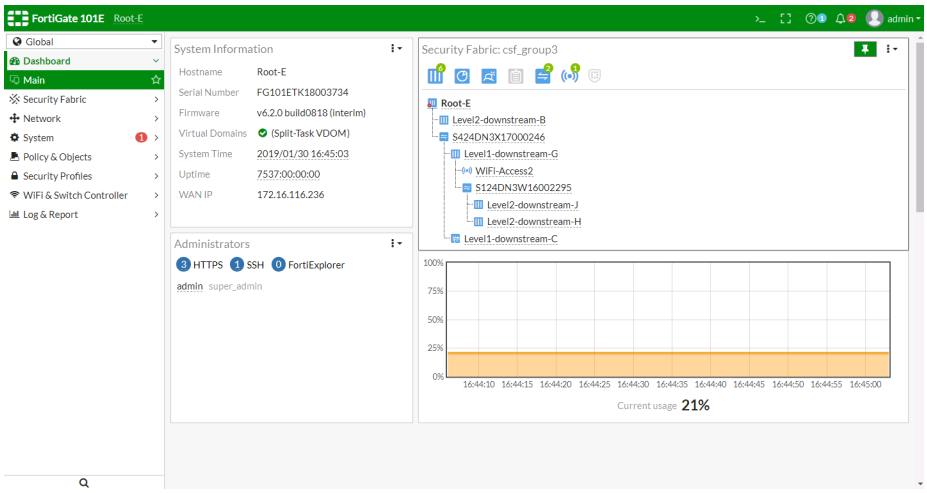
The *root* or *FG-traffic* VDOMs' Logical Topology page shows the root FortiGate and only the downstream FortiGates that connect to the current VDOM on the root FortiGate, including interfaces' connection information.



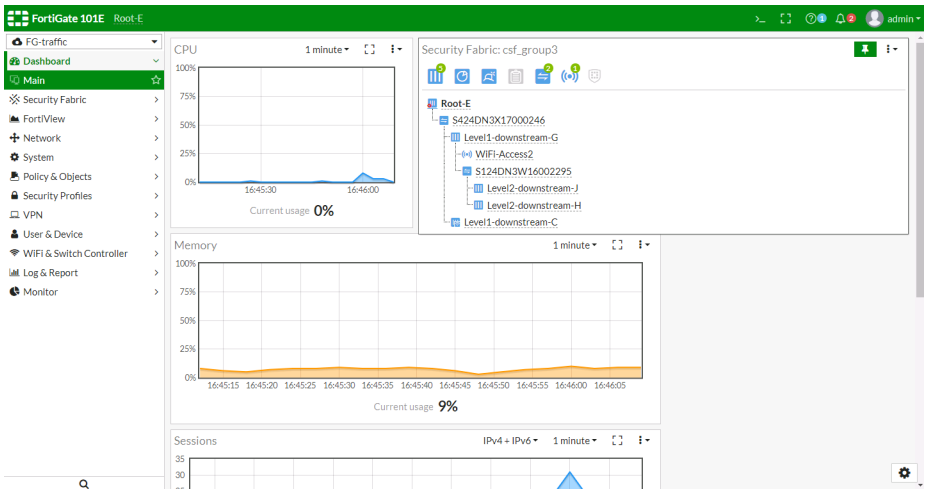


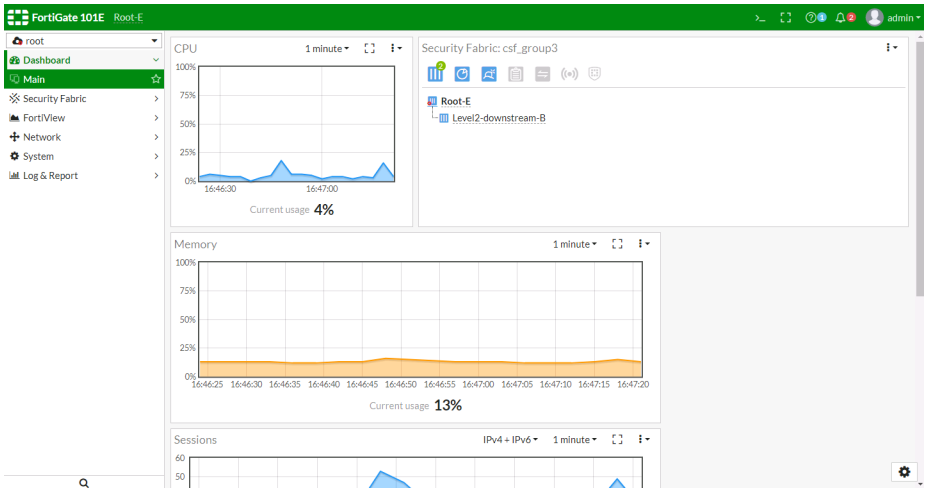
Dashboard Security Fabric widget

The global Dashboard page shows the root FortiGate and all downstream FortiGates in the Security Fabric widget.



The *root* or *FG-traffic* VDOMs' Dashboard page shows the root FortiGate and only the downstream FortiGates that connect to the current VDOM on the root FortiGate in the Security Fabric widget.





Fabric Member Synchronization

This section lists new fabric member synchronization features added to FortiOS for the expanding fabric family.

Simplify FortiAnalyzer Pairing

This version simplifies the pairing of FortiAnalyzer and FortiGate by using certificate verification to allow the FortiGate admin to preauthorize access.

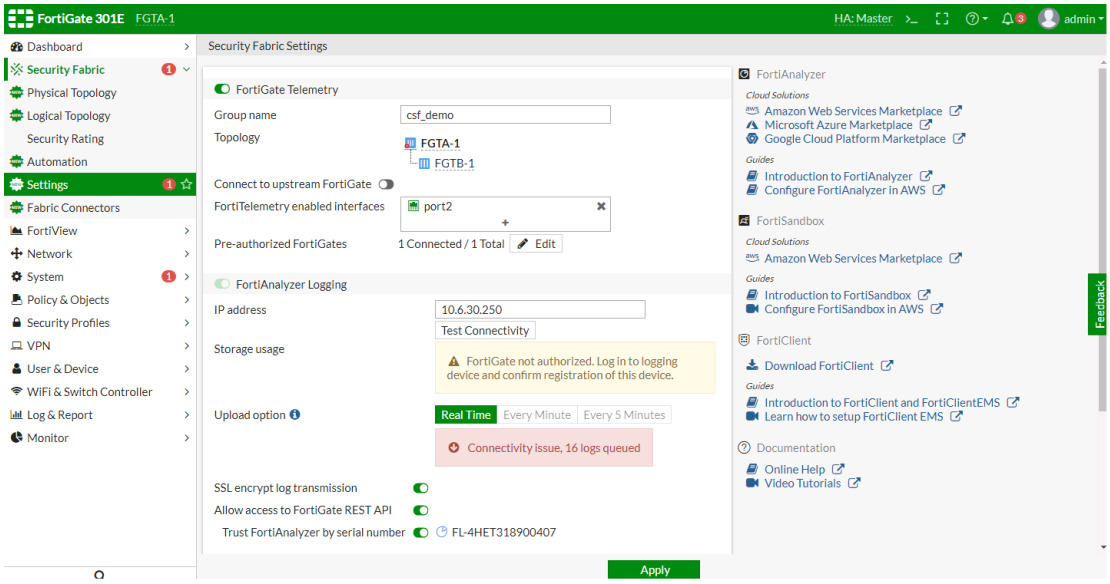
When configuring FortiAnalyzer in the root FortiGate, FortiGate has an option to allow FortiAnalyzer to access the FortiGate REST API. FortiGate verifies the FortiAnalyzer by retrieving the FortiAnalyzer serial number and checking it against the FortiAnalyzer certificate. After verification, the FortiAnalyzer serial number is stored in the FortiGate configuration.

Then on the FortiAnalyzer side, the admin authorizes FortiGates in the same Security Fabric. After authorization, the FortiGates can form a Security Fabric in the FortiAnalyzer side without entering the admin credentials of the root FortiGate.

Sample configuration

To configure FortiAnalyzer in the root FortiGate GUI:

1. Go to *Security Fabric* > *Settings*.
2. Enable *FortiGate Telemetry* and configure settings.



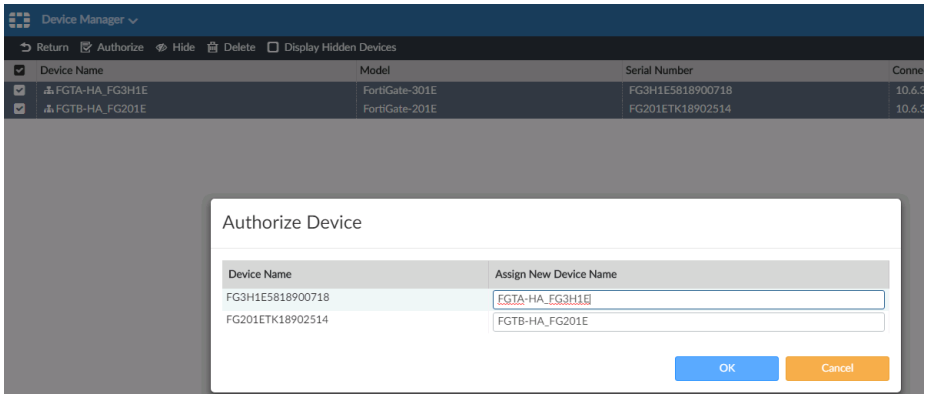
To configure FortiAnalyzer in the root FortiGate CLI:

```
config log fortianalyzer setting
    set status enable
```

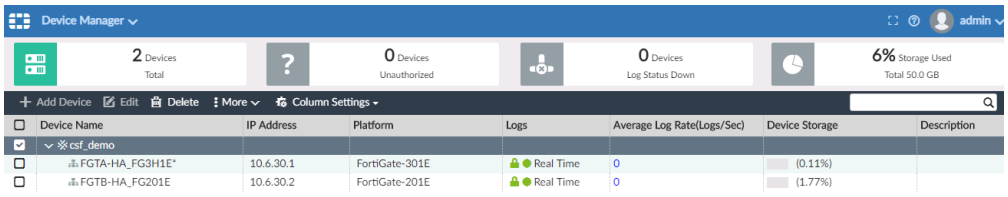
```
    set server "10.6.30.250"
    set certificate-verification enable
    set serial "FL-4HET318900407"
    set access-config enable
    set upload-option realtime
    set reliable enable
end
```

To authorize FortiGates in the same Security Fabric using the FortiAnalyzer GUI:

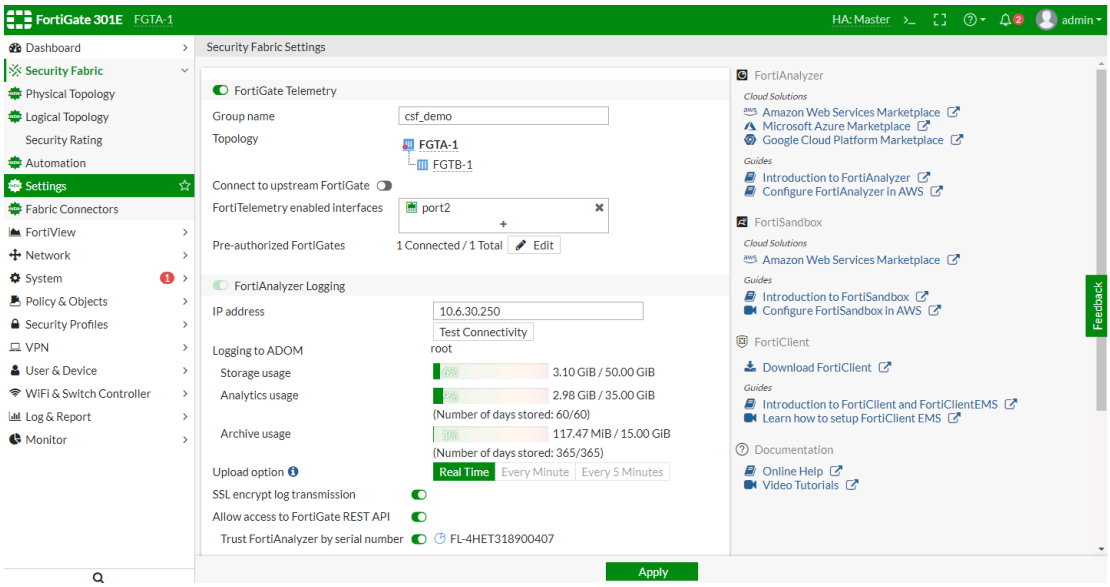
1. In FortiAnalyzer, go to *Device Manager* and select the FortiGates to be authorized.



2. After a moment, the FortiGates can form a Security Fabric in the FortiAnalyzer without entering the admin credentials of the root FortiGate.



3. Go to the FortiGate to see the FortiAnalyzer logging information.

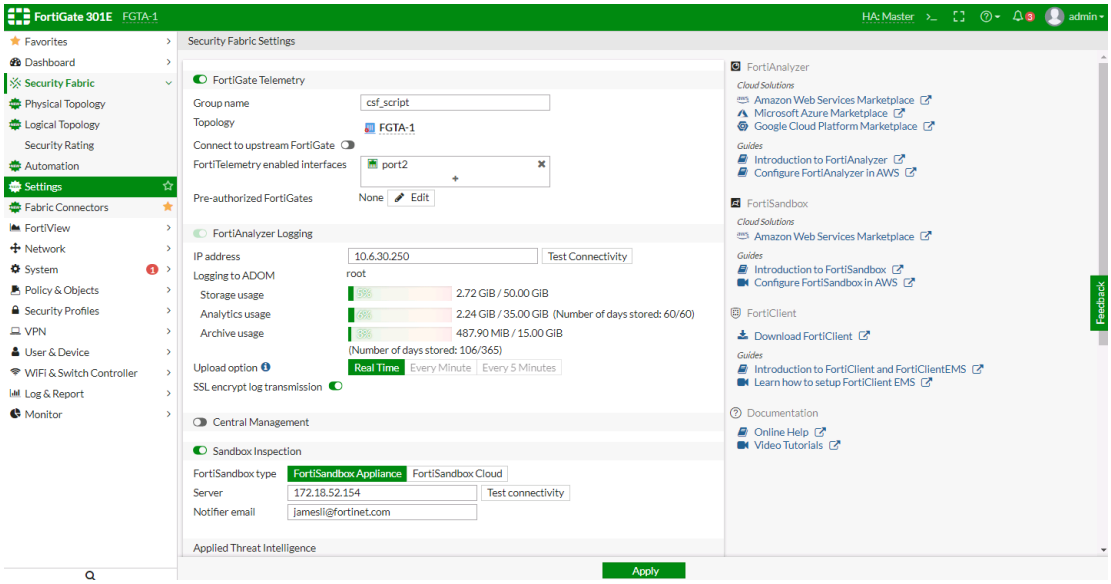


FortiSandbox

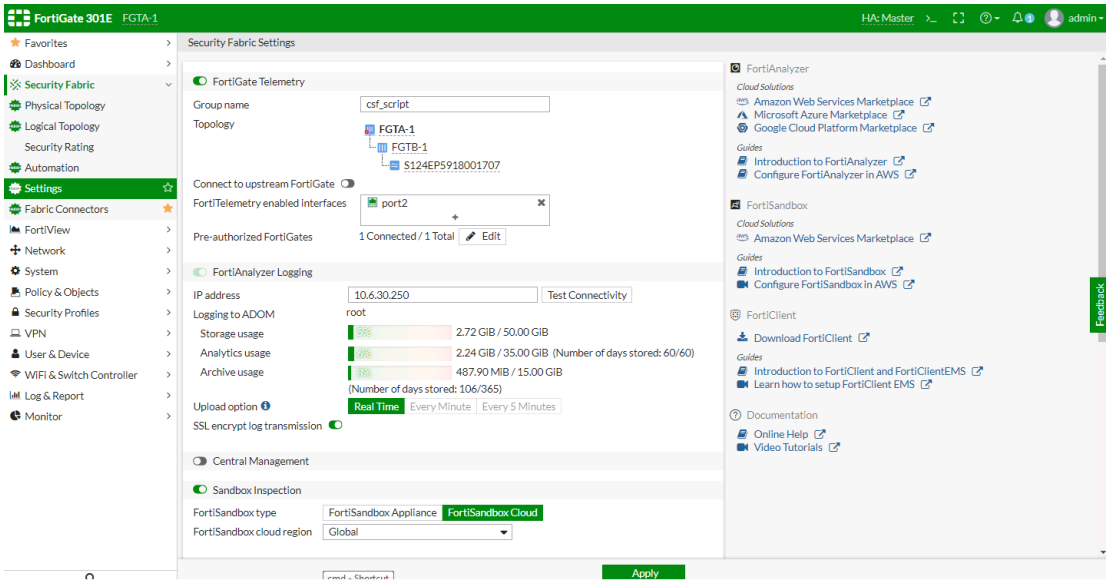
FortiSandbox connection information is defined on the Security Fabric Settings page, and is now synchronized between all fabric members.

To configure a FortiSandbox appliance or FortiSandbox Cloud through the root FortiGate:

1. Navigate to *Security Fabric* > *Settings*.
2. Sandbox inspection displays as enabled and shows FortiSandbox settings for the *FortiSandbox Appliance* or *FortiSandbox Cloud*.
   - FortiSandbox Appliance:

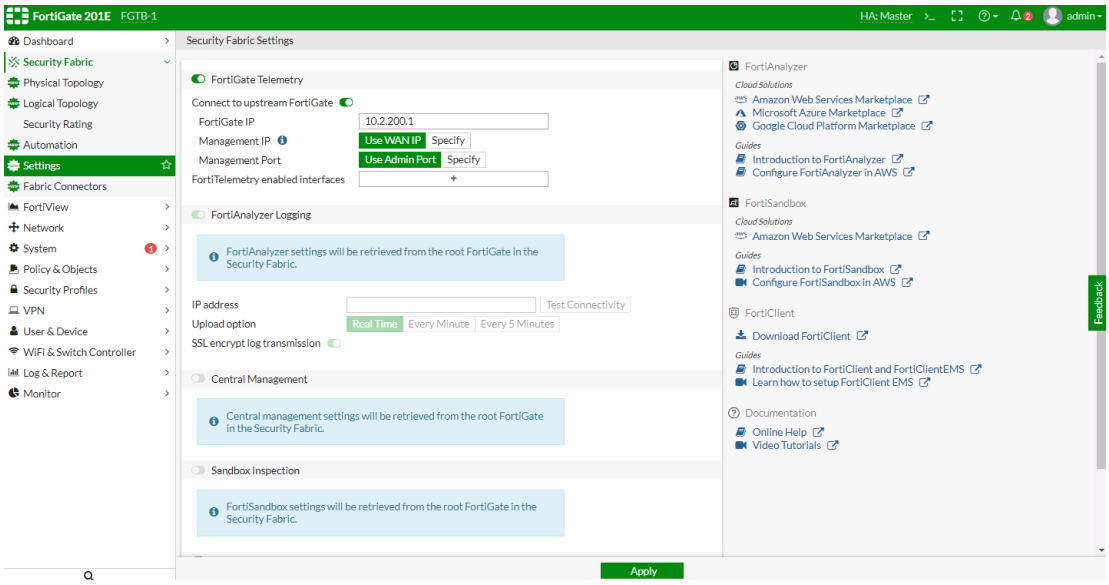


   - FortiSandbox Cloud:

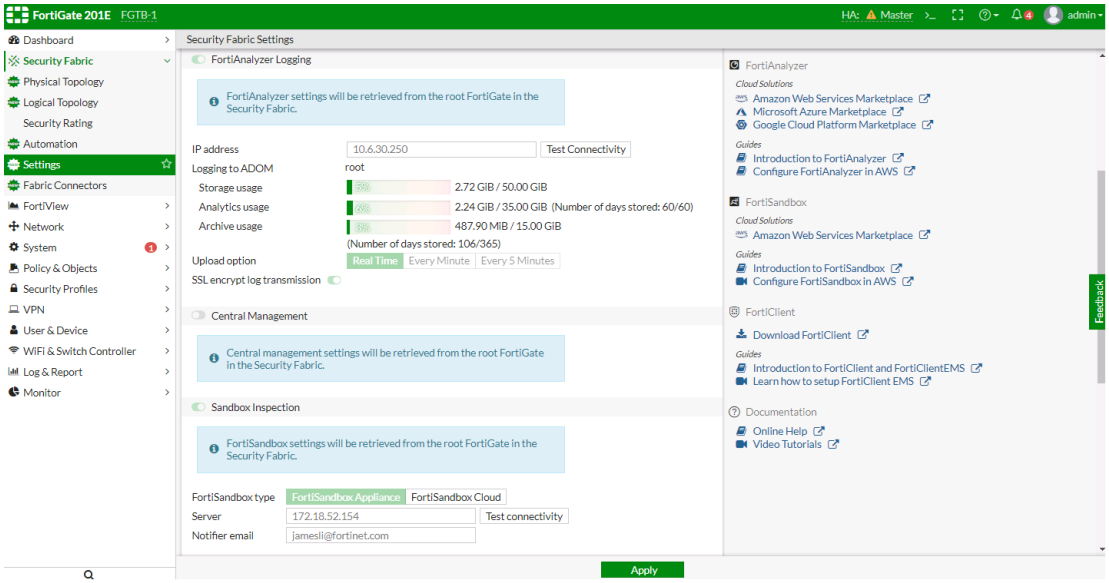


To view FortiSandbox settings from a downstream FortiGate:

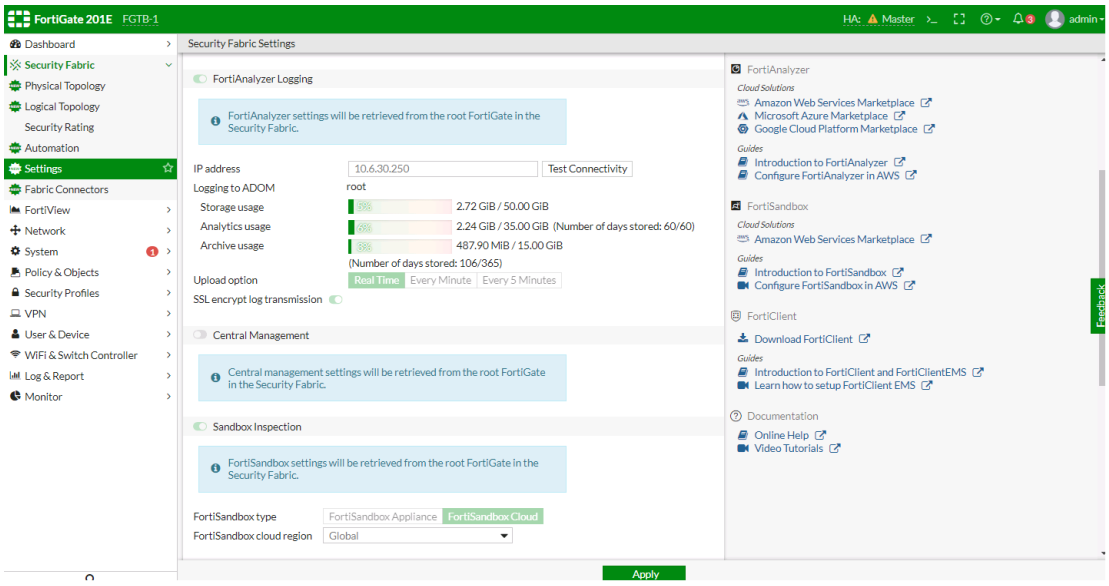
1. Navigate to *Security Fabric* > *Settings*.
2. FortiSandbox settings cannot be accessed when configuring a downstream FortiGate to join the Security Fabric.



3. Once the downstream FortiGate successfully joins the Security Fabric, FortiSandbox settings are synced from the root FortiGate and cannot be changed from the downstream FortiGate.
   - FortiSandbox Appliance:



- FortiSandbox Cloud:

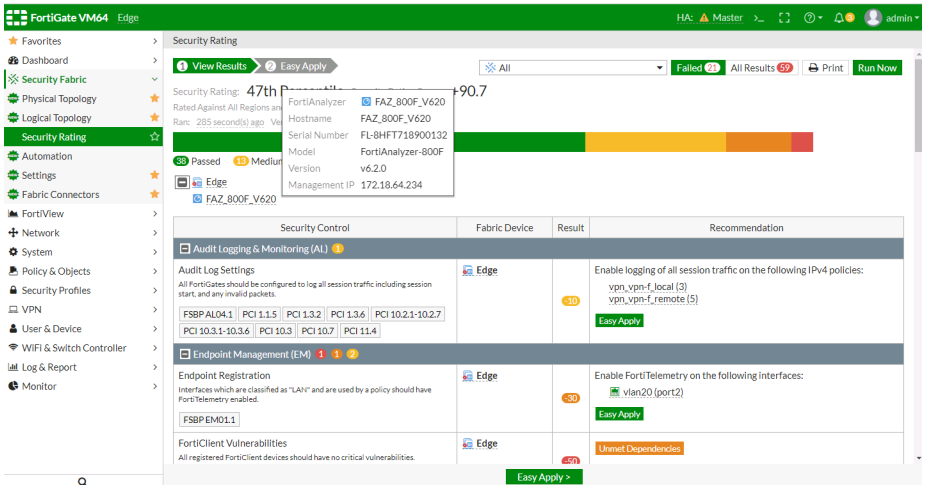


Security Rating – Extend Checks to FortiAnalyzer

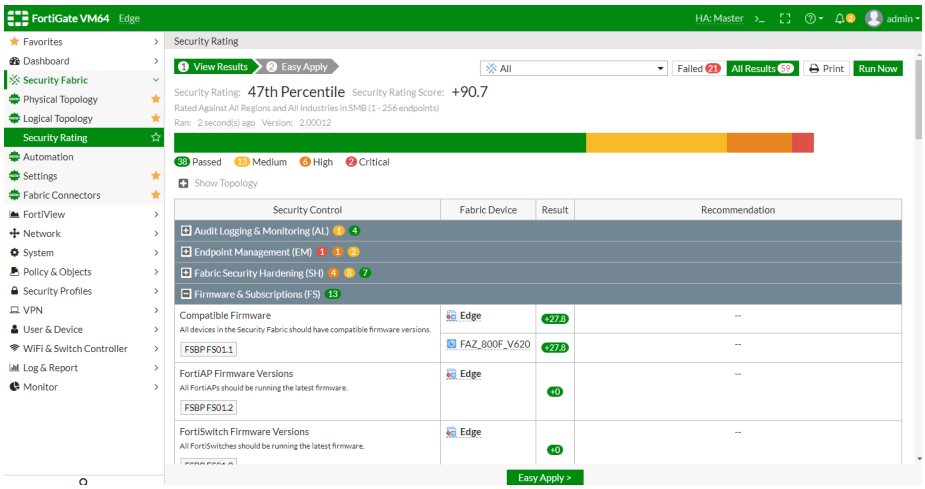
In 6.2, the Security Rating feature can verify FortiAnalyzer configurations and report the results for *Compatible Firmware* and *Admin Idle Timeout*.

To view FortiAnalyzer information and tests in Security Rating:

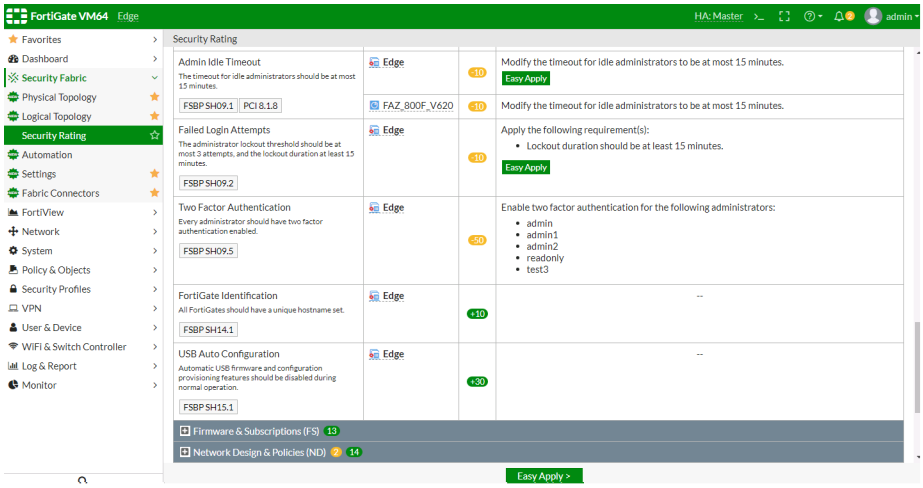
1. Navigate to *Security Fabric* > *Security Rating*.
2. The Security Rating results page displays the FortiAnalyzer icon in the topology field, and FortiAnalyzer information is available through the tooltip.



3. The *Compatible Firmware* and *Admin Idle Timeout* tests for FortiAnalyzer are now available:
   - Compatible Firmware:



   - Admin Idle Timeout:



Security Rating – Historical Rating Dashboard Widget

A new System Dashboard widget is added in FortiGate which retrieves and displays the historical security rating trends for the Security Fabric.

This version adds a historical security rating score chart to the existing Security Rating Dashboard widget that shows the security rating results over time.

The Security Rating Dashboard widget has two new views:

- A view to show the historical security rating scores over time, along with the industry average for comparison.
- A view to show historical security rating scores percentile over time.

The following are available in both views:

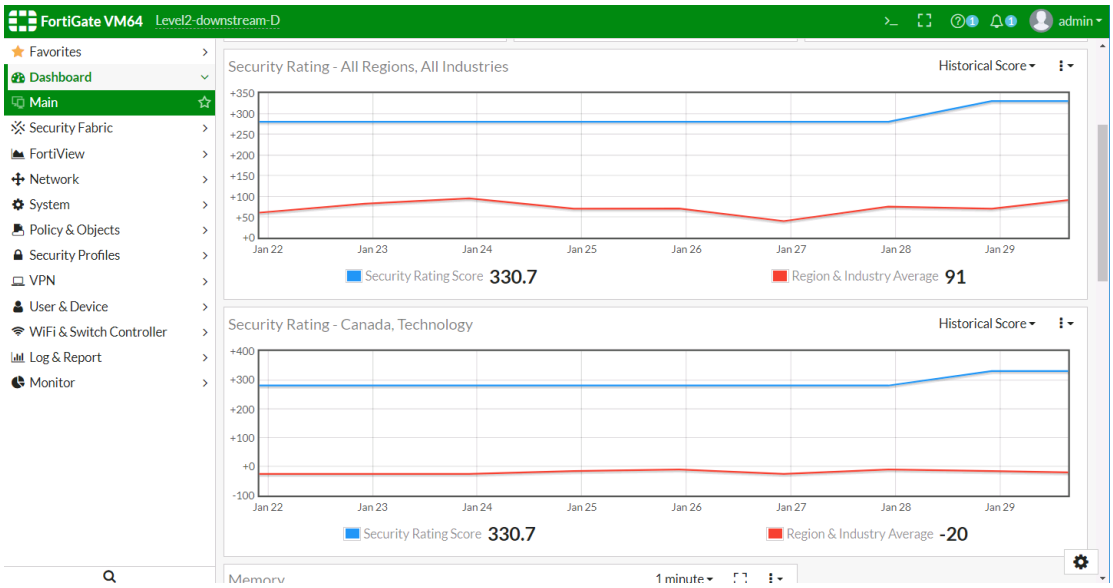
- You can select *All Industries* or *My Industry*.
- You can select *All Regions* or *My Region*.

- You can select *Account Registered Region and Industry*.
- The widget displays only one result per day from FortiAnalyzer.

Sample Security Rating widget showing historical score

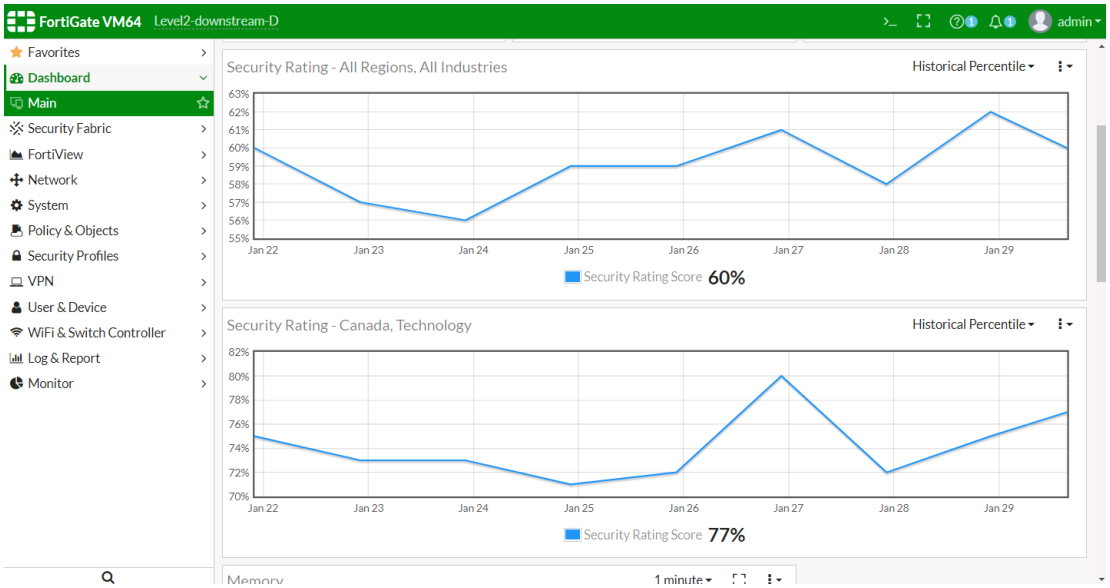
The blue line represents the FortiGate Security Rating score.

The red line represents the Region & Industry Average score.



Sample Security Rating widget showing historical percentile

The blue line represents the FortiGate Security Rating percentile against the selected Region and Industry.



Dynamic Policy – FortiClient EMS (Connector)

FortiOS 6.2.0 introduces a dynamic policy connector for FortiClient EMS. This allows objects to be defined on the FortiGate which map to tags/groups on EMS. EMS dynamically updates these endpoint groups when host compliance or other events happen. This causes FortiOS to dynamically adjust the security policy based on those group definitions.

EMS can define compliance verification rules based on criteria such as certificates, the logged in domain, files present, OS versions, running processes, and registry keys. When a FortiClient endpoint registers to EMS, EMS dynamically groups the endpoint based on the compliance verification rules. FortiOS can receive the dynamic endpoint groups from EMS via the FSSO protocol, using the new "fortiems" FSSO agent type which supports SSL and imports trusted certificates.

After FortiOS pulls the tags from EMS via the FSSO protocol, you can create user groups based on the tags, then apply dynamic firewall policies to the user groups. When host compliance or other events happen, EMS sends updates to FortiOS to update the dynamic policies.

The following instructions assume that EMS is installed, configured, and has endpoints connected. For information on configuring EMS, see the *FortiClient EMS Administration Guide*.

This feature is only available when using FortiOS with EMS 6.2.0 Beta 1 or a later version.

To add a compliance verification rule in EMS:

This example creates a compliance verification rule that applies to endpoints that have Windows 10 installed.

1. In EMS, go to *Compliance Verification* > *Compliance Verification Rules*, and click *Add*.
2. In the *Name* field, enter the desired rule name. Note that EMS uses the tag name to dynamically group endpoints, not the rule name configured in this field.
3. Toggle *Status* on or off to enable or disable the rule.
4. For *Type*, select *Windows*, *Mac*, or *Linux*. This affects what rule types are available. In this example, *Windows* is selected.
5. From the *Rule* dropdown list, select the rule type and configure the related options. Ensure you click the + button after entering each criterion.

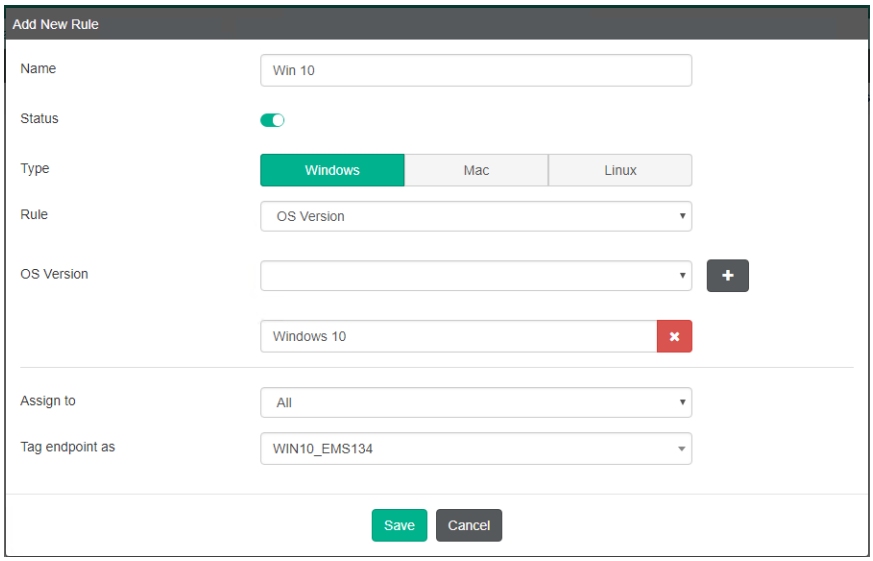
Rule type	Description
Certificate	In the *Subject* and *Issuer* fields, enter the certificate subject and issuer. You can enter multiple certificates using the + button. You can also use the NOT option to indicate that the rule requires that a certain certificate is not present for the endpoint. The endpoint must satisfy all conditions to satisfy this rule. For example, if the rule is configured to require certificate A, certificate B, and NOT certificate C, then the endpoint must have both certificates A and B and not certificate C.
Logged in Domain	In the *Domain* field, enter the domain name. You can enter multiple domain names using the + button. If the rule is configured for multiple domains, the endpoint is considered as satisfying the rule if it belongs to one of the configured domains. This option is not available for Linux endpoints.

Rule type	Description
File	In the *File* field, enter the file path. You can enter multiple files using the + button. You can also use the NOT option to indicate that the rule requires that a certain file is not present on the endpoint. The endpoint must satisfy all conditions to satisfy this rule. For example, if the rule is configured to require file A, file B, and NOT file C, then the endpoint must have both files A and B and not file C.
OS Version	From the *OS Version* field, select the OS version. You can enter multiple OS versions using the + button. If the rule is configured for multiple OS versions, the endpoint is considered as satisfying the rule if it has one of the configured OS versions installed.
Running Process	In the *Running Process* field, enter the process name. You can enter multiple processes using the + button. You can also use the NOT option to indicate that the rule requires that a certain process is not running on the endpoint. The endpoint must satisfy all conditions to satisfy this rule. For example, if the rule is configured to require process A, process B, and NOT process C, then the endpoint must have both processes A and B running and process C not running.
Registry Key	In the *Registry Key* field, enter the registry key value. You can enter values using the + button. You can also use the NOT option to indicate that the rule requires that a certain registry key is not present on the endpoint. The endpoint must satisfy all conditions to satisfy this rule. For example, if the rule is configured to require registry key A, registry key B, and NOT registry key C, then the endpoint must have both registry keys A and B and not registry key C. This option is only available for Windows endpoints.

In this example, *OS Version* is selected from the *Rule* dropdown list, and *Windows 10* is then selected from the *OS Version* dropdown list.

6. Under *Assign to*, select *All*.
7. In the *Tag endpoint as* dropdown list, select an existing tag or enter a new tag. In this example, a new tag, WIN10_EMS134, is created. EMS uses this tag to dynamically group together endpoints that satisfy the rule, as well as any other rules that are configured to use this tag.

8. Click *Save*.



9. Go to *Compliance Verification* > *Host Tag Monitor*. All endpoints that have Windows 10 installed are shown grouped by the WIN10_EMS134 tag.

To configure the fortiems FSSO agent:

In the FortiOS CLI, run the following commands. In this example, the FSSO agent name is ems_02, and the EMS server is located at 172.16.200.134.

```
config user fsso
   edit "ems_02"
      set server "172.16.200.134"
      set password 123456
      set type fortiems
      set ssl enable
      set ssl-trusted-cert "Fortinet_CA"
   next
end
```

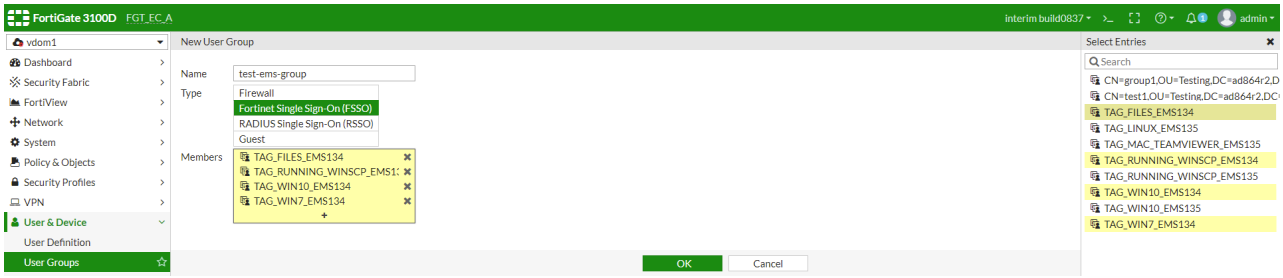
To configure EMS FSSO groups:

In the FortiOS CLI, run the following commands. In this example, the FSSO groups for two FSSO agents, ems_02 and ems_03, are being configured. The WIN10_EMS134 dynamic endpoint group is added to the ems_02 FSSO group, and the MAC_TEAMVIEWER_EMS135 dynamic endpoint group is added to the ems_03 FSSO group.

```
config user adgrp
   edit "TAG_WIN10_EMS134"
      set server-name "ems_02"
   next
   edit "TAG_MAC_TEAMVIEWER_EMS135"
      set server-name "ems_03"
   next
end
```

To configure a user group based on EMS tags:

1. In FortiOS, go to *User & Device* > *User Groups*. Click Create *New*.
2. In the *Name* field, enter the desired name.
3. For *Type*, select *Fortinet Single Sign-On (FSSO)*.
4. In the *Members* field, click +. The *Select Entries* pane appears. You can identify the dynamic endpoint groups pulled from EMS because the names begin with TAG_, followed by the tag name from EMS.

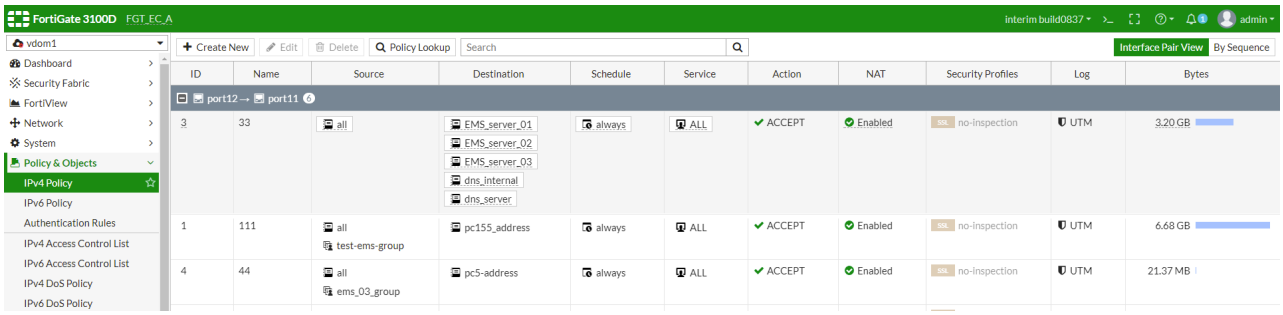


5. Select the desired dynamic endpoint groups. Endpoints that currently belong to this dynamic endpoint group in EMS will be members of this FortiOS user group.
6. Click *OK*.

To create a dynamic firewall policy for the user group:

You can now create a dynamic firewall policy for the user group. In this example, an IPv4 policy is created for the user group.

1. In FortiOS, go to *Policy & Objects* > *IPv4 Policy*. Click *Create New*.
2. In the *Source* field, click +. The *Select Entries* pane appears. On the *User* tab, select the user group configured above.
3. Configure other options as desired. Click *OK*.
4. Go to *Policy & Objects* > *IPv4 Policy* to ensure the policy was created and applied to the desired user group. FortiOS will update this policy when it receives updates from EMS.



Dynamic Policy - Fabric Devices

A new dynamic address group is added in 6.2, which represents the configured IP addresses of all Fortinet devices connected to the Security Fabric. In this first phase, it includes FortiManager, FortiAnalyzer, FortiClient EMS, FortiMail, FortiAP(s), and FortiSwitch(es). Like other dynamic address groups for fabric connectors, this can be used in IPv4 policies and objects.

Firewall address now includes a new default address object called FABRIC_DEVICE, and you can apply the address object to the following types of policies:

- IPv4 firewall policy (including virtual wire pairs)
- IPv4 shaping policy
- IPv4 ACL policy
- Policy64 and Policy46 (IPv4 only)
- Consolidated policy (IPv4 only)

You cannot apply the FABRIC_DEVICE object to the following types of policies:

- All IPv6 policies
- IPv4 explicit proxy policy

You also cannot use the FABRIC_DEVICE object with the following settings:

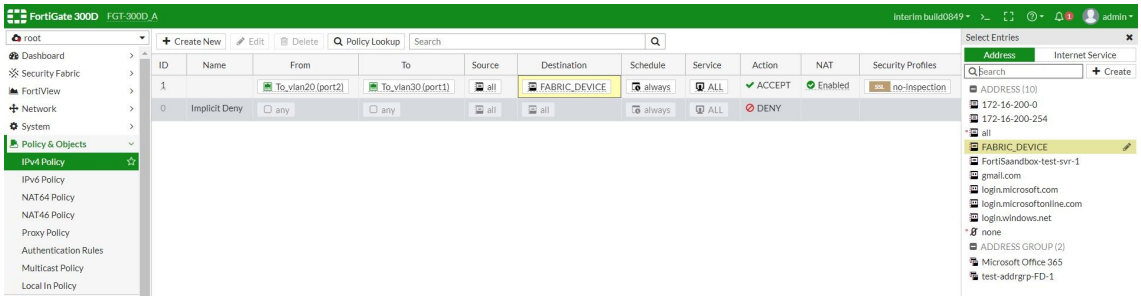
- Custom/extension internet-service
- Exclusion of addrgrp

Initially the FABRIC_DEVICE object, does not have an address value. The address value is populated dynamically as things change. As a result, you cannot edit the FABRIC_DEVICE object, add any addresses to the object, or remove any addresses from the object.

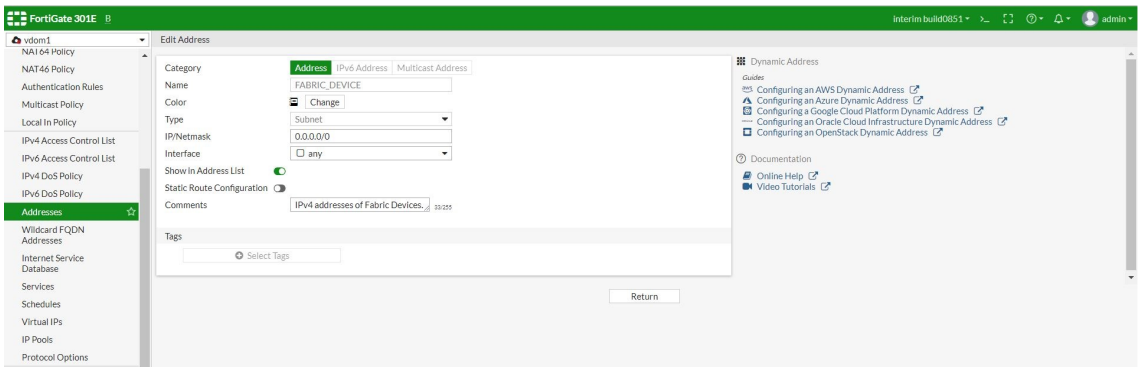
The address values of the FABRIC_DEVICE object are populated based on:

- FortiAnalyzer IP (from the *Fabric Settings* pane)
- FortiManager IP (from the *Fabric Settings* pane)
- FortiMail IP (from the *Fabric Settings* pane)
- FortiClient EMS IP (from the *Fabric Settings* pane)
- FortiAP IPs (from the *FortiAP Setup* pane or DHCP)
- FortiSwitch IPs (from the *FortiSwitch Setup* page or DHCP)

Example of the FABRIC_DEVICE object applied in an IPv4 policy:



Example of the FABRIC_DEVICE object in the *Edit Address* pane. The pane includes only a *Return* button because the object is read-only:



Example of the FABRIC_DEVICE object applied in an IPv4 policy:

```
FGT-300D_A (root) # show fu firewall address FABRIC_DEVICE
config firewall address
   edit "FABRIC_DEVICE"
      set type ipmask
      set comment "IPv4 addresses of Fabric Devices."
      set visibility enable
      set associated-interface ''
      set color 0
      set allow-routing disable
      set subnet 0.0.0.0 0.0.0.0
   next
end
FGT-300D_A (root) #
FGT-300D_A (root) # show firewall policy
config firewall policy
   edit 1
      set uuid cbe9e74c-37c6-51e9-9cf1-9510b503f2bf
      set srcintf "port2"
      set dstintf "port1"
      set srcaddr "all"
      set dstaddr "FABRIC_DEVICE"
      set action accept
      set schedule "always"
      set service "ALL"
      set utm-status enable
      set fsso disable
      set nat enable
   next
end
FGT-300D_A (root) #
```

Example of the diagnose command, which is used to list what IP addresses are included in FABRIC_DEVICE. For now, this is only method to list content in the FABRIC_DEVICE object:

```
FGT-300D_A (root) # diagnose firewall iprope list 100004
policy index=1 uuid_idx=25 action=accept
flag (8050108): redir nat master use_src pol_stats
flag2 (4000): resolve_sso
flag3 (20):
schedule(always)
cos_fwd=255  cos_rev=255
group=00100004 av=00004e20 au=00000000 split=00000000
host=0 chk_client_info=0x0 app_list=0 ips_view=0
```

```
misc=0 dd_type=0 dd_mode=0
zone(1): 10 -> zone(1): 9
source(1): 0.0.0.0-255.255.255.255, uuid_idx=3,
dest(5): 172.18.64.48-172.18.64.48, uuid_idx=1, 172.18.60.25-172.18.60.25, uuid_idx=1,
     172.18.52.154-172.18.52.154, uuid_idx=1, 172.18.28.31-172.18.28.31, uuid_idx=1,
     172.18.62.6-172.18.62.6, uuid_idx=1,
service(1):
   [0:0x0:0/(0,65535)->(0,65535)] helper:auto
FGT-300D_A (root) #
```

Wireless

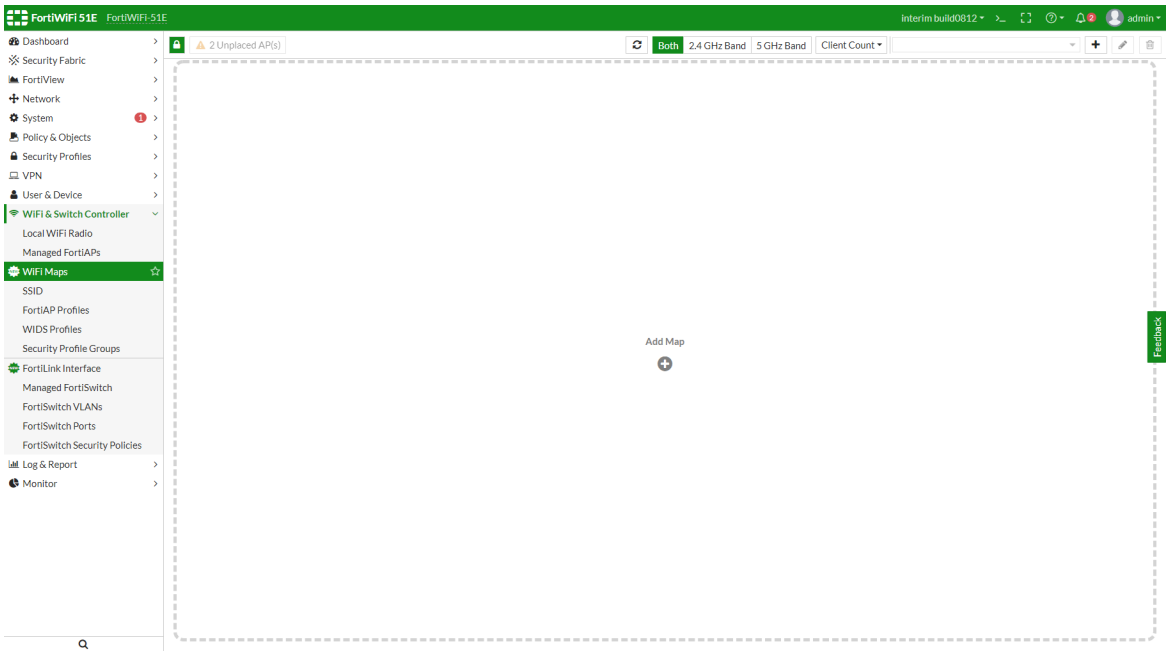
This section lists new wireless features added to FortiOS for the expanding fabric family.

WiFi Location Map

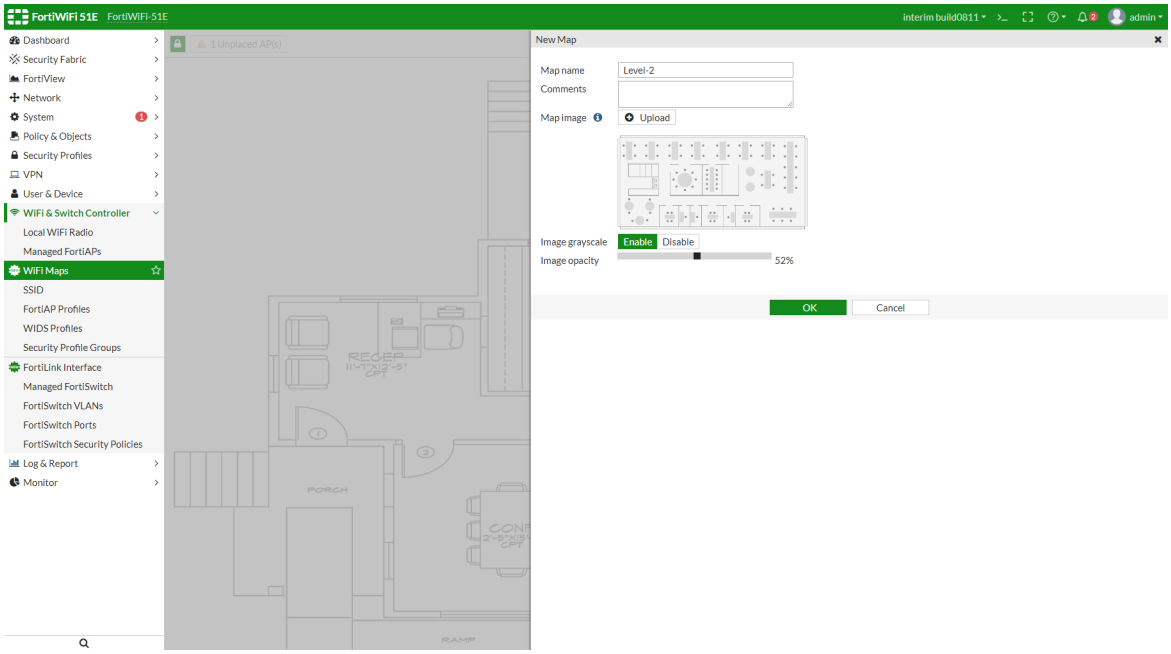
This feature allows you to upload custom maps or floor plans and then place FortiAP units on the map. *Wifi Maps* show real-time status and alerts for the FortiAP units on the map. This features gives you an intuitive view of the location and status of each FortiAP unit on the map.

To set up WiFi Maps:

1. Obtain a floor plan or map of where FortiAP units are located.
2. Go to *WiFi & Switch Controller* > *WiFi Maps* and click *Add Map*.

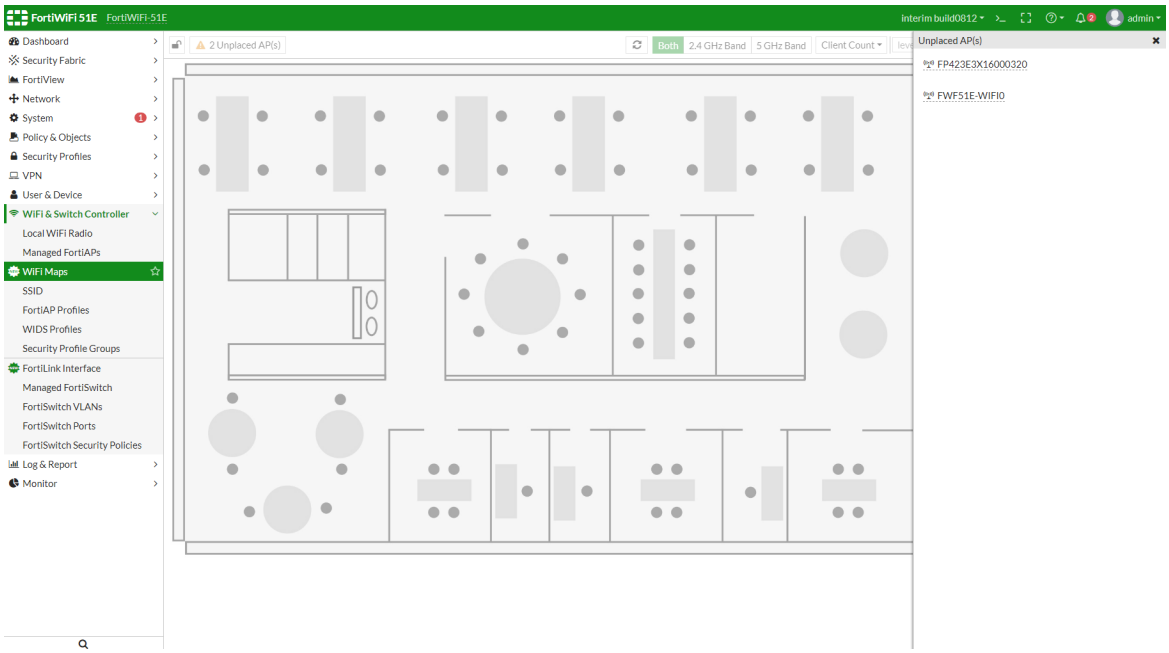


3. Click *Upload* and specify a map in PNG, JPEG, or GIF format to be uploaded.
   a. Enter the *Map name*, for example, *Level-2*.
   b. If you want, enable *Image grayscale* to change a color map to grayscale.
   c. Set *Image opacity* to specify map transparency.

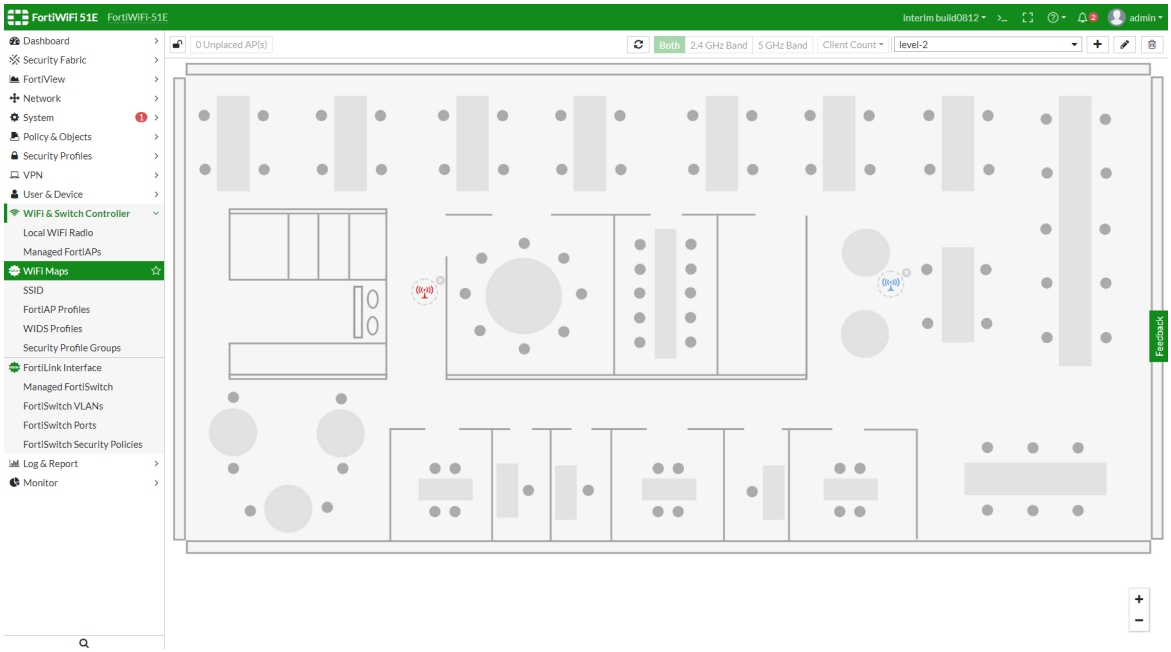


4. Click *OK*.
   After setting up a WiFi map, you can place FortiAP units on the map.

5. At the top left, click the lock icon to modify the map; and then click the *Unplaced AP(s)* icon to display the list of unplaced APs.



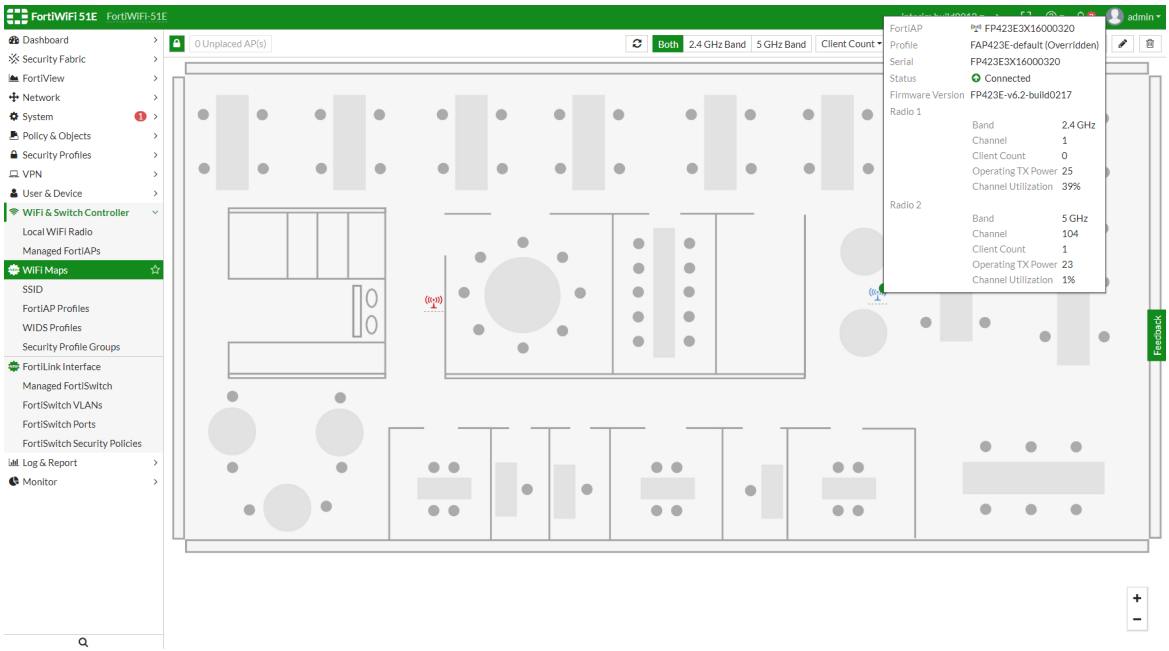
6. Drag and drop each FortiAP unit onto its location on the map.



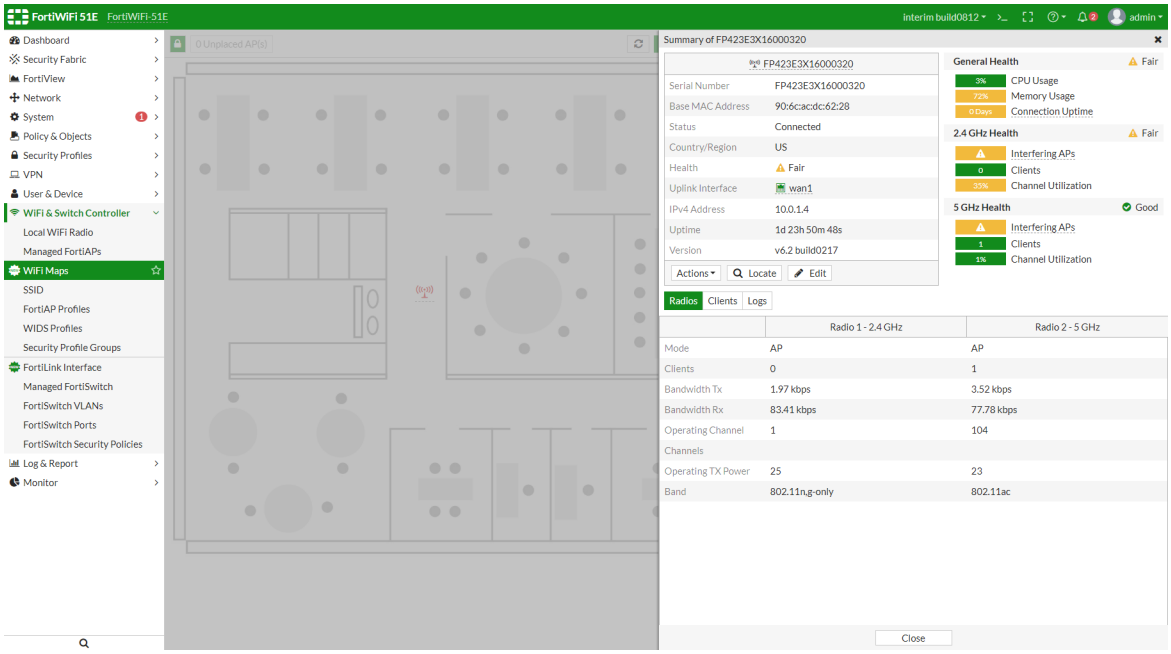
7. When all FortiAP units have been placed on the map, click the lock icon.

The WiFi map shows where each FortiAP unit is located.

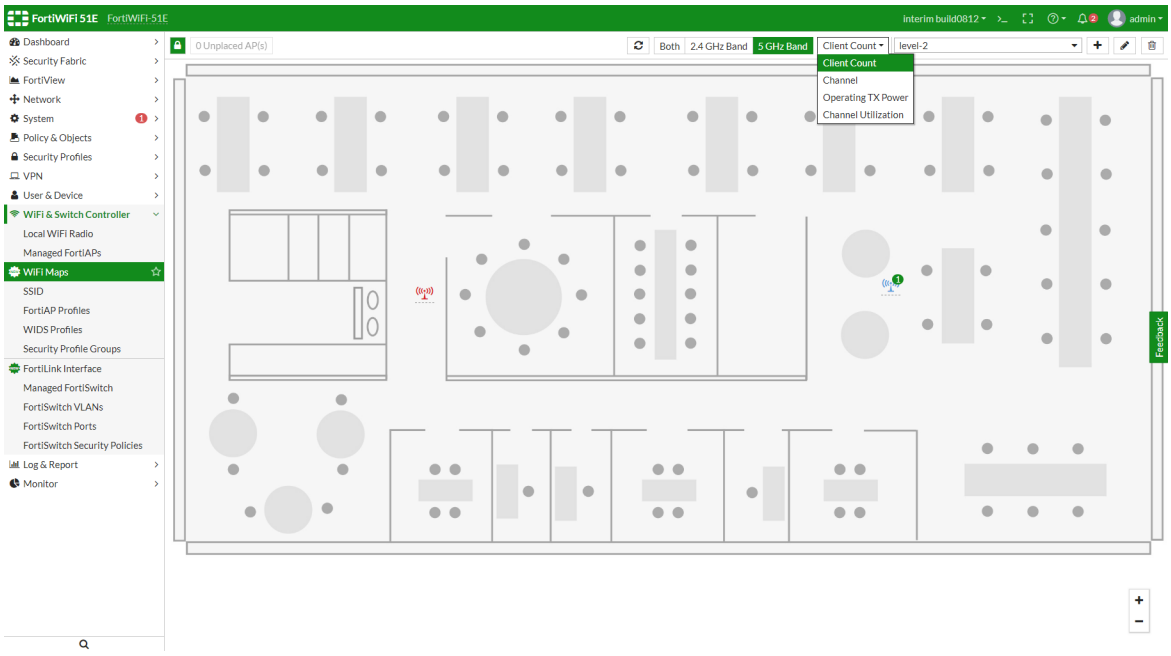
To view a FortiAP unit's operating data, hover over that FortiAP icon.



To view a FortiAP unit's detailed operating data, click that FortiAP icon.



In *Wifi Maps*, you can select to show the 2.4 GHz or 5 GHz band or both. You can also show numerical operating information such as client count, channel, radio TX power, and channel utilization.



You must use the GUI to upload WiFi maps.

To configure WiFi map settings using CLI commands, see the following examples:

```
config wireless-controller region
   edit "Level-2"
      set grayscale enable
      set opacity 40
   next
end


config wireless-controller wtp
   edit "FP423E3X16000320"
      set region "Level-2"
      set region-x "0.660498"
      set region-y "0.442825"
   next
end
```

Monitor and Suppress Phishing SSID

In addition to rogue AP detection, wireless administrators should also be concerned about phishing SSIDs, which are defined as either:

- An SSID defined on FortiGate that is broadcast from an uncontrolled AP
- A pre-defined pattern for an offending SSID pattern
  For example, you could define any SSID that contains your company name to be a phishing SSID.

This new feature enables FortiAP to monitor and report these SSIDs in logs and to optionally suppress them.

You can only configure this feature by using the CLI:

```
config wireless-controller setting
     set phishing-ssid-detect enable|disable
     set fake-ssid-action log|suppress
     config offending-ssid
        edit 1
           set ssid-pattern "OFFENDING*"
           set action log|suppress
        next
     end
end
```

The `set phishing-ssid-detect enable|disable` option enables or disables the phishing SSID detection feature. The default setting is `enable`.

The `set fake-ssid-action log|suppress` option defines what action FortiGate takes after detecting a fake SSID. The default setting is `log`, and can be set to either one or both.

The `set ssid-pattern OFFENDING*` option defines what criteria which will be used to match an offending SSID. In this case, it means all SSID names with leading string `OFFENDING`, which is not case-sensitive.

The `set action log|suppress` defines what action FortiGate takes after detecting the corresponding offending SSID pattern entry. The default setting is `log` and can be set to either one or both.

Log examples

WiFi event log sample for fake SSID detection

Following is a sample of the log that is generated when a fake SSID is first detected:

```
1: date=2019-03-01 time=14:53:23 logid="0104043567" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551480803 logdesc="Fake AP detected" ssid="CORP_
     WIFI_ACCESS" bssid="08:5b:0e:18:1b:d0" aptype=0 rate=130 radioband="802.11n-5G"
     channel=149 action="fake-ap-detected" manuf="Fortinet, Inc." security="WPA2 Personal"
     encryption="AES" signal=-41 noise=-95 live=173397 age=0 onwire="no"
     detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="FP321C3X15001615"
     radioiddetected=1 stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0
     msg="Detected Fake AP CORP_WIFI_ACCESS 08:5b:0e:18:1b:d0 chan 149 live 173397 age 0"
```

Following is a sample of the log that is periodically generated when a fake SSID is continuously detected:

```
1: date=2019-03-01 time=14:58:53 logid="0104043568" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551481133 logdesc="Fake AP on air" ssid="CORP_
     WIFI_ACCESS" bssid="08:5b:0e:18:1b:d0" aptype=0 rate=130 radioband="802.11n-5G"
     channel=149 action="fake-ap-on-air" manuf="Fortinet, Inc." security="WPA2 Personal"
     encryption="AES" signal=-41 noise=-95 live=173728 age=330 onwire="no"
     detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="N/A" radioiddetected=0
     stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0 msg="Fake AP On-
     air CORP_WIFI_ACCESS 08:5b:0e:18:1b:d0 chan 149 live 173728 age 330"
```

WiFi event log sample for fake SSID suppression

Following is a sample of the log that is generated when a fake SSID is suppressed:

```
1: date=2019-03-01 time=14:53:23 logid="0104043569" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551480803 logdesc="Rogue AP suppressed"
     ssid="CORP_WIFI_ACCESS" bssid="08:5b:0e:18:1b:d0" aptype=0 rate=130
     radioband="802.11n-5G" channel=149 action="rogue-ap-suppressed" manuf="Fortinet, Inc."
     security="WPA2 Personal" encryption="AES" signal=-41 noise=-95 live=173397 age=0
```

```
onwire="no" detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="N/A"
radioiddetected=0 stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0
msg="AP CORP_WIFI_ACCESS 08:5b:0e:18:1b:d0 chan 149 live 173397 age 0"
```

WiFi event log sample for offending SSID detection

Following a sample of the log that is generated when an offending SSID is first detected:

```
1: date=2019-03-01 time=14:53:33 logid="0104043619" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551480811 logdesc="Offending AP detected"
     ssid="OFFENDING_SSID" bssid="1a:5b:0e:b5:f3:bf" aptype=0 rate=130 radioband="802.11n-
     5G" channel=153 action="offending-ap-detected" manuf="Fortinet, Inc." security="WPA2
     Personal" encryption="AES" signal=-41 noise=-95 live=173406 age=8 onwire="no"
     detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="FP321C3X15001615"
     radioiddetected=1 stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0
     msg="Detected Offending AP OFFENDING_SSID 1a:5b:0e:b5:f3:bf chan 153 live 173406 age
     8"
```

Following is a sample of a log that is periodically generated when an offending SSID is continuously detected:

```
1: date=2019-03-01 time=14:55:54 logid="0104043620" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551480952 logdesc="Offending AP on air"
     ssid="OFFENDING_SSID_TEST" bssid="9a:5b:0e:18:1b:d0" aptype=0 rate=130
     radioband="802.11n-5G" channel=149 action="offending-ap-on-air" manuf="N/A"
     security="WPA2 Personal" encryption="AES" signal=-41 noise=-95 live=173548 age=150
     onwire="no" detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="N/A"
     radioiddetected=0 stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0
     msg="Offending AP On-air OFFENDING_SSID_TEST 9a:5b:0e:18:1b:d0 chan 149 live 173548
     age 150"
```

WiFi event log sample for offending SSID suppression

Following is a sample of the log that is generated when an offending SSID is suppressed:

```
1: date=2019-03-01 time=14:53:33 logid="0104043569" type="event" subtype="wireless"
     level="warning" vd="root" eventtime=1551480811 logdesc="Rogue AP suppressed"
     ssid="OFFENDING_SSID" bssid="1a:5b:0e:b5:f3:bf" aptype=0 rate=130 radioband="802.11n-
     5G" channel=153 action="rogue-ap-suppressed" manuf="Fortinet, Inc." security="WPA2
     Personal" encryption="AES" signal=-41 noise=-95 live=173406 age=8 onwire="no"
     detectionmethod="N/A" stamac="N/A" apscan="N/A" sndetected="N/A" radioiddetected=0
     stacount=0 snclosest="FP321C3X15001615" radioidclosest=1 apstatus=0 msg="AP OFFENDING_
     SSID 1a:5b:0e:b5:f3:bf chan 153 live 173406 age 8"
```

WiFi QoS Enhancement

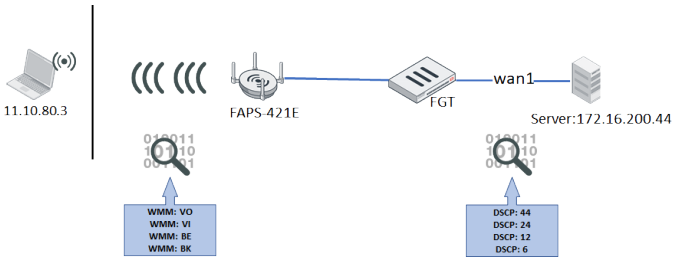
This features enables FortiGate to preserve the WiFi Multi-Media (WMM) QoS marking of packets by translating them to Differentiated Services Code Point (DSCP) values when forwarding upstream.

The following QoS profile commands are added to the CLI:

`wmm-dscp-marking`	Enable/disable WMM Differentiated Services Code Point (DSCP) marking (default = disable).
`wmm-vo-dscp`	DSCP marking for voice access (default = 48).
`wmm-vi-dscp`	DSCP marking for video access (default = 32).

wmm-be-dscp	DSCP marking for best effort access (default = 0).
wmm-bk-dscp	DSCP marking for background access (default = 8).

This feature requires a FortiAP-S or FortiAP-W2 device.



To configure WMM QoS marking of packets:

1. Create a QoS profile with wmm-dscp-marking enabled, and modify the wmm-dscp settings:

```
config wireless-controller qos-profile
    edit qos-wifi
        set wmm-dscp-marking enable
        set wmm-vo-dscp 44
        set wmm-vi-dscp 24
        set wmm-be-dscp 12
        set wmm-bk-dscp 6
end
```

2. Select the QoS profile on a VAP interface:

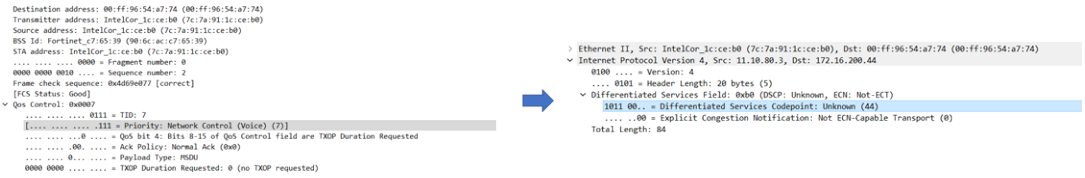
```
config wireless-controller vap
    edit "stability3"
        set qos-profile "qos-wifi"
    next
end
```

3. Verify that the wmm-dscp-marking values are pushed on FortiAP:

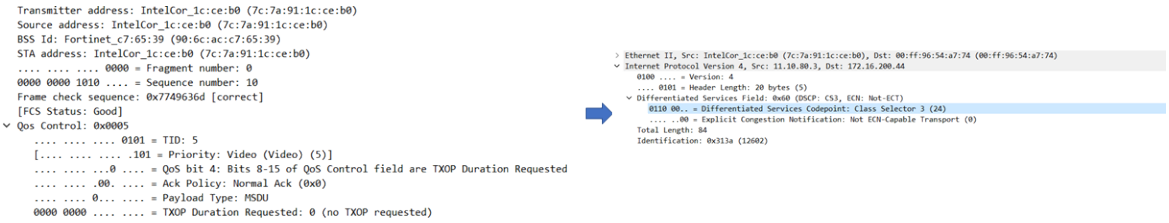
```
cw_diag -c k-qos wlan00
WLAN Kernel QoS Settings
..
....
WLAN wlan00 :
    wmm                          : 1
    wmm uapsd                    : 1
    call admission control       : 0
    call capacity                : 0
    bandwidth admission control  : 0
    bandwidth capacity           : 0
    dscp mapping                 : 0
    dscp marking                 : 1
         vo dscp                 : 44
         vi dscp                 : 24
```

```
be dscp                 : 12
bk dscp                 : 6
```

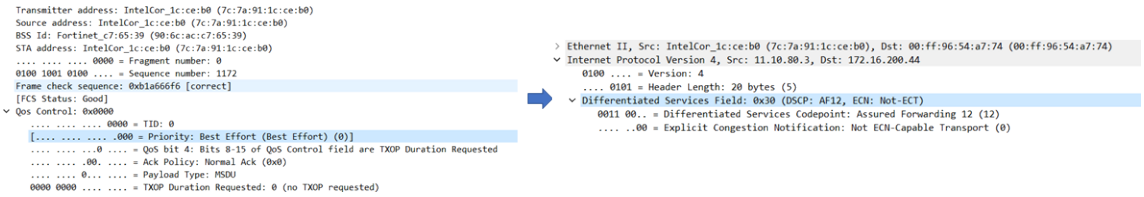
4. Verify that, when sending traffic from a client with a WMM setting of VO, the FortiGate receives the packets with a DSCP TID value or 44:



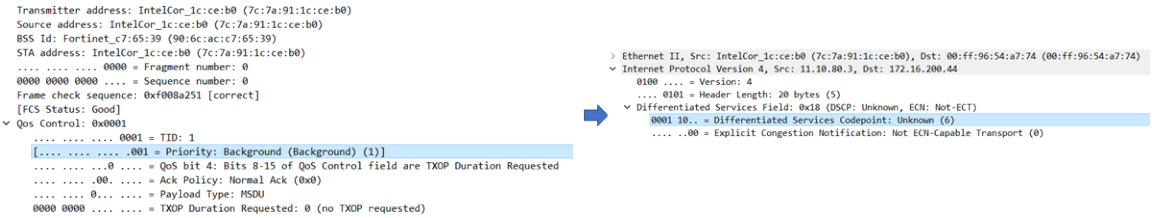
5. Verify that, when sending traffic from a client with a WMM setting of VI, the FortiGate receives the packets with a DSCP TID value or 24:



6. Verify that, when sending traffic from a client with a WMM setting of BE, the FortiGate receives the packets with a DSCP TID value or 12:



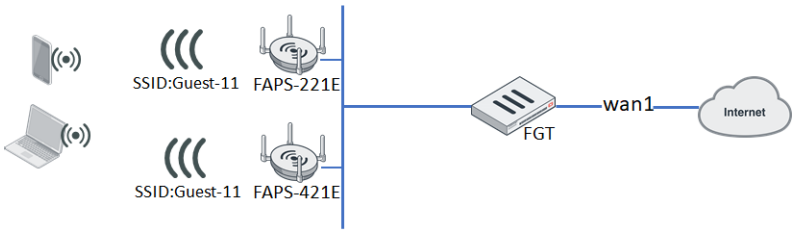
7. Verify that, when sending traffic from a client with a WMM setting of BK, the FortiGate receives the packets with a DSCP TID value or 6:



Troubleshooting – Extended Logging

This version adds new logging information in four key areas to aid in wireless troubleshooting: Association, Authentication, DHCP, and DNS.

In previous versions, there were not enough detailed wireless event logs to show client connection procession, and IT administrators sometimes had difficulty troubleshooting wireless connection problems by checking logs. In this version, the FortiAP can send more detailed events of client connections (such as probe, associate, authentication, 4-way handshake, DHCP), and FortiGate can create associated logs of these event.



New probe, authentication, and associate logs when wireless clients try to connect a broadcasted SSID with any security-mode

Probe request and response logs

Action	Description	Message	Detail
probe-req	Probe request from wireless station	AP received probe request frame from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:52 logid="0104043681" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886190 logdesc="Probe request from wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="probe-req" reason="Reserved 0" msg="AP received probe request frame from client f0:98:9d:76:64:c4" remotewtptime="49.326391"
probe-resp	Probe response to wireless station	AP sent probe response frame to client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:52 logid="0104043682" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886190 logdesc="Probe response to wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="probe-resp" reason="Reserved 0" msg="AP sent probe response frame to client f0:98:9d:76:64:c4" remotewtptime="49.326459"

Authentication request and response logs

Action	Description	Message	Detail
auth-req	Authentication request from wireless station	AP received authentication request frame from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043675" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Authentication request from wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="auth-req" reason="Reserved 0" msg="AP received authentication request frame from client f0:98:9d:76:64:c4" remotewtptime="44.902962"
auth-	Authentication	AP sent	date=2019-01-30 time=14:09:48 logid="0104043676" type="event"

Action	Description	Message	Detail
resp	response to wireless station	authentication response frame to client f0:98:9d:76:64:c4	subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Authentication response to wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="auth-resp" reason="Reserved 0" msg="AP sent authentication response frame to client f0:98:9d:76:64:c4" remotewtptime="44.903038"

Associate request and response logs

Action	Description	Message	Detail
assoc-req	Association request from wireless station	AP received association request frame from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043677" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Association request from wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="assoc-req" reason="Reserved 0" msg="AP received association request frame from client f0:98:9d:76:64:c4" remotewtptime="44.915155"
assoc-resp	Association response to wireless station	AP sent association response frame to client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043679" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Association response to wireless station" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="assoc-resp" reason="Reserved 0" msg="AP sent association response frame to client f0:98:9d:76:64:c4" remotewtptime="44.916829"

New WPA 4-Way handshake logs when wireless clients try to connect WPA2-Personal/WPA2-Enterprise SSID

Complete WPA 4-Way handshake logs

Action	Description	Message	Detail
WPA-1/4-key-msg	AP sent 1/4 message of 4 way handshake to wireless client	AP sent 1/4 message of 4-way handshake to client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043650" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="AP sent 1/4 message of 4 way handshake to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="WPA-1/4-key-msg"

Action	Description	Message	Detail
			reason="Reserved 0" msg="AP sent 1/4 message of 4-way handshake to client f0:98:9d:76:64:c4" remotewtptime="44.920791"
WPA-2/4-key-msg	Wireless client sent 2/4 message of 4 way handshake	AP received 2/4 message of 4-way handshake from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043651" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Wireless client sent 2/4 message of 4 way handshake" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="WPA-2/4-key-msg" reason="Reserved 0" msg="AP received 2/4 message of 4-way handshake from client f0:98:9d:76:64:c4" remotewtptime="44.926647"
WPA-3/4-key-msg	AP sent 3/4 message of 4 way handshake to wireless client	AP sent 3/4 message of 4-way handshake to client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043652" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="AP sent 3/4 message of 4 way handshake to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="WPA-3/4-key-msg" reason="Reserved 0" msg="AP sent 3/4 message of 4-way handshake to client f0:98:9d:76:64:c4" remotewtptime="44.928406"
WPA-4/4-key-msg	Wireless client sent 4/4 message of 4 way handshake	AP received 4/4 message of 4-way handshake from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043653" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Wireless client sent 4/4 message of 4 way handshake" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Personal" encryption="AES" action="WPA-4/4-key-msg" reason="Reserved 0" msg="AP received 4/4 message of 4-way handshake from client f0:98:9d:76:64:c4" remotewtptime="44.933383"

Invalid 2/4 handshake logs with wrong PSK input

Action	Description	Message	Detail
WPA-invalid-2/4-key-msg	Wireless client 4 way handshake failed with invalid 2/4	Probably wrong password entered, invalid MIC in 2/4 message of 4-	date=2019-01-31 time=16:41:02 logid="0104043648" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548981661 logdesc="Wireless client 4 way handshake failed with invalid 2/4 message" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11"

Action	Description	Message	Detail
	message	way handshake from client f0:98:9d:76:64:c4	radioid=1 stamac="f0:98:9d:76:64:c4" channel=11 security="WPA2 Personal" encryption="AES" action="WPA-invalid-2/4-key-msg" reason="Reserved 0" msg="Probably wrong password entered, invalid MIC in 2/4 message of 4-way handshake from client f0:98:9d:76:64:c4" remotewtptime="0.0"

New RADIUS authentication logs when clients connect WPA2-Enterprise with User-group or Radius-auth SSID

RADIUS authenticate success log when client pass authentication

Action	Description	Message	Detail
RADIUS-auth-success	Wireless client RADIUS authentication success	Wireless client RADIUS authentication success	date=2019-01-30 time=14:36:09 logid="0104043630" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548887768 logdesc="Wireless client RADIUS authentication success" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability4" ssid="Guest-21" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Enterprise" encryption="AES" action="RADIUS-auth-success" reason="Reserved 0" msg="Client f0:98:9d:76:64:c4 RADIUS authentication success" remotewtptime="0.0"

RADIUS authenticate failure log when client fails to pass authentication

Action	Description	Message	Detail
RADIUS-auth-failure	Wireless client RADIUS authentication failure	Client f0:98:9d:76:64:c4 RADIUS authentication failure	date=2019-01-30 time=14:35:51 logid="0104043629" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548887750 logdesc="Wireless client RADIUS authentication failure" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability4" ssid="Guest-21" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Enterprise" encryption="AES" action="RADIUS-auth-failure" reason="Reserved 0" msg="Client f0:98:9d:76:64:c4 RADIUS authentication failure" remotewtptime="0.0"

New RADIUS MAC authentication logs when clients try to connect a SSID with radius-mac-auth enabled

RADIUS MAC authenticate success log when client passes RADIUS MAC authentication

Action	Description	Message	Detail
RADIUS-MAC-auth-	Wireless client RADIUS MAC authentication	Client b4:ae:2b:cb:d1:72 RADIUS MAC	date=2019-01-30 time=15:54:40 logid="0104043633" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548892477 logdesc="Wireless client RADIUS MAC

Action	Description	Message	Detail
success	success	authentication success	authentication success" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="b4:ae:2b:cb:d1:72" channel=6 security="WPA2 Personal" encryption="AES" action="RADIUS-MAC-auth-success" reason="Reserved 0" msg="Client b4:ae:2b:cb:d1:72 RADIUS MAC authentication success" remotewtptime="0.0"

RADIUS MAC authenticate failure log when client fails to pass RADIUS MAC authentication

Action	Description	Message	Detail
RADIUS-MAC-auth-success	Wireless client RADIUS MAC authentication success	Client 1c:87:2c:b6:a8:49 RADIUS MAC authentication failure	date=2019-01-30 time=15:47:42 logid="0104043632" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548892061 logdesc="Wireless client RADIUS MAC authentication failure" sn="FP320C3X17001909" ap="320C-TEST" vap="stability3" ssid="Guest-11" radioid=2 stamac="1c:87:2c:b6:a8:49" channel=40 security="WPA2 Personal" encryption="AES" action="RADIUS-MAC-auth-failure" reason="Reserved 0" msg="Client 1c:87:2c:b6:a8:49 RADIUS MAC authentication failure" remotewtptime="0.0"

New DHCP logs when clients try to acquire IP after connected

Complete DHCP Discover/Offer/Request/ACK logs

Action	Description	Message	Detail
DHCP-DISCOVER	Wireless station sent DHCP DISCOVER	DHCP DISCOVER from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:48 logid="0104043663" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886188 logdesc="Wireless station sent DHCP DISCOVER" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="f0:98:9d:76:64:c4" security="WPA2 Personal" encryption="AES" action="DHCP-DISCOVER" reason="N/A" msg="DHCP DISCOVER from client f0:98:9d:76:64:c4" remotewtptime="45.123652"
DHCP-OFFER	DHCP server sent DHCP OFFER	DHCP OFFER of IP 11.10.80.2 from server 11.10.80.1 for client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:49 logid="0104043664" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886189 logdesc="DHCP server sent DHCP OFFER" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="f0:98:9d:76:64:c4" security="WPA2 Personal" encryption="AES" action="DHCP-OFFER" reason="N/A" msg="DHCP OFFER of IP 11.10.80.2 from server 11.10.80.1 for client f0:98:9d:76:64:c4" remotewtptime="46.156969"

Action	Description	Message	Detail
DHCP-REQUEST	Wireless station sent DHCP REQUEST	DHCP REQUEST for IP 11.10.80.2 offered by server 11.10.80.1 from client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:50 logid="0104043666" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886190 logdesc="Wireless station sent DHCP REQUEST" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="f0:98:9d:76:64:c4" security="WPA2 Personal" encryption="AES" action="DHCP-REQUEST" reason="N/A" msg="DHCP REQUEST for IP 11.10.80.2 offered by server 11.10.80.1 from client f0:98:9d:76:64:c4" remotewtptime="47.243792"
DHCP-ACK	DHCP server sent DHCP ACK	DHCP ACK for IP 11.10.80.2 from server 11.10.80.1 for client f0:98:9d:76:64:c4	date=2019-01-30 time=14:09:50 logid="0104043667" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548886190 logdesc="DHCP server sent DHCP ACK" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="f0:98:9d:76:64:c4" security="WPA2 Personal" encryption="AES" action="DHCP-ACK" reason="N/A" msg="DHCP ACK for IP 11.10.80.2 from server 11.10.80.1 for client f0:98:9d:76:64:c4" remotewtptime="47.246381"

Error logs when DHCP failure happens

Action	Description	Message	Detail
DHCP-NAK	DHCP server sent DHCP NAK	IP address not assigned, DHCP NAK from server 11.10.80.1 for client b4:ae:2b:cb:d1:72	date=2019-01-30 time=15:22:08 logid="0104043661" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548890528 logdesc="DHCP server sent DHCP NAK" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" stamac="b4:ae:2b:cb:d1:72" security="WPA2 Personal" encryption="AES" action="DHCP-NAK" reason="requested address not available" msg="IP address not assigned, DHCP NAK from server 11.10.80.1 for client b4:ae:2b:cb:d1:72" remotewtptime="289.83561"
DHCP-no-response	Wireless station DHCP process failed with no server response	DHCP server not responding for client b4:ae:2b:cb:d1:72	date=2019-02-01 time=10:39:07 logid="0104043658" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1549046347 logdesc="Wireless station DHCP process failed with no server response" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" stamac="b4:ae:2b:cb:d1:72" security="WPA2 Personal" encryption="AES" action="DHCP-no-response" reason="N/A" msg="DHCP server not responding for client b4:ae:2b:cb:d1:72" remotewtptime="457.629929"
DHCP-no-ACK	No DHCP ACK from server	No DHCP ACK for IP 11.10.80.3 requested by client b4:ae:2b:cb:d1:72	date=2019-02-01 time=10:38:56 logid="0104043660" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1549046336 logdesc="No DHCP ACK from server" sn="PS421E3X15000017" ap="PS421E3X15000017"

Action	Description	Message	Detail
			vap="stability3" ssid="Guest-11" stamac="b4:ae:2b:cb:d1:72" security="WPA2 Personal" encryption="AES" action="DHCP-no-ACK" reason="N/A" msg="No DHCP ACK for IP 11.10.80.3 requested by client b4:ae:2b:cb:d1:72" remotewtptime="448.236740"
DHCP-self-assigned-IP	Wireless station is using self-assigned IP	Detected self assigned IP 169.254.210.208 of client b4:ae:2b:cb:d1:72	date=2019-02-01 time=10:38:51 logid="0104043670" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1549046330 logdesc="Wireless station is using self-assigned IP" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" stamac="b4:ae:2b:cb:d1:72" security="WPA2 Personal" encryption="AES" action="DHCP-self-assigned-IP" reason="N/A" msg="Detected self assigned IP 169.254.210.208 of client b4:ae:2b:cb:d1:72" remotewtptime="441.742363"

New GTK-Rekey logs when clients perform gtk-rekey

Action	Description	Message	Detail
WPA-group-1/2-key-msg	AP sent 1/2 message of group key handshake to wireless client	AP sent 1/2 message of group key handshake to client f0:98:9d:76:64:c4	date=2019-01-30 time=15:12:01 logid="0104043654" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548889920 logdesc="AP sent 1/2 message of group key handshake to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability4" ssid="Guest-21" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Enterprise" encryption="AES" action="WPA-group-1/2-key-msg" reason="Reserved 0" msg="AP sent 1/2 message of group key handshake to client f0:98:9d:76:64:c4" remotewtptime="3778.128070"
WPA-group-2/2-key-msg	Wireless client sent 2/2 message of group key handshake	AP received 2/2 message of group key handshake from client f0:98:9d:76:64:c4	date=2019-01-30 time=15:12:01 logid="0104043655" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548889920 logdesc="Wireless client sent 2/2 message of group key handshake" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability4" ssid="Guest-21" radioid=1 stamac="f0:98:9d:76:64:c4" channel=6 security="WPA2 Enterprise" encryption="AES" action="WPA-group-2/2-key-msg" reason="Reserved 0" msg="AP received 2/2 message of group key handshake from client f0:98:9d:76:64:c4" remotewtptime="3778.228253"

New Fast-BSS-Transition (FT) logs when 802.11r clients roam between 2 FAPs

FT logs when clients succeed to roaming

Action	Description	Message	Detail
FT-action-req	Wireless client sent FT action reqeust	AP received FT action request frame from client f0:98:9d:76:64:c4	date=2019-01-31 time=15:13:23 logid="0104043642" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548976403 logdesc="Wireless client sent FT action reqeust" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=1 security="WPA2 Personal" encryption="AES" action="FT-action-req" reason="Reserved 0" msg="AP received FT action request frame from client f0:98:9d:76:64:c4" remotewtptime="146.847041"
FT-action-resp	FT action response was sent to wireless client	AP sent FT action response frame to client f0:98:9d:76:64:c4	date=2019-01-31 time=15:13:23 logid="0104043643" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548976403 logdesc="FT action response was sent to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=1 stamac="f0:98:9d:76:64:c4" channel=1 security="WPA2 Personal" encryption="AES" action="FT-action-resp" reason="Reserved 0" msg="AP sent FT action response frame to client f0:98:9d:76:64:c4" remotewtptime="146.849137"
FT-reassoc-req	Wireless client sent FT reassociation request	AP received FT reassociation request frame from client f0:98:9d:76:64:c4	date=2019-01-31 time=15:13:23 logid="0104043646" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548976403 logdesc="Wireless client sent FT reassociation request" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=40 security="WPA2 Personal" encryption="AES" action="FT-reassoc-req" reason="Reserved 0" msg="AP received FT reassociation request frame from client f0:98:9d:76:64:c4" remotewtptime="146.899110"
FT-reassoc-resp	FT reassociation response was sent to wireless client	AP sent FT reassociation response frame to client f0:98:9d:76:64:c4	date=2019-01-31 time=15:13:23 logid="0104043647" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548976403 logdesc="FT reassociation response was sent to wireless client" sn="PS221E3X16000022" ap="PS221E3X16000022" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=40 security="WPA2 Personal" encryption="AES" action="FT-reassoc-resp" reason="Reserved 0" msg="AP sent FT reassociation response frame to client f0:98:9d:76:64:c4" remotewtptime="146.904372"
FT-auth-req	Wireless client sent FT auth request	AP received FT authentication request frame from client	date=2019-01-31 time=16:49:18 logid="0104043644" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548982158 logdesc="Wireless client sent FT auth request" sn="PS421E3X15000017" ap="PS421E3X15000017"

Action	Description	Message	Detail
		f0:98:9d:76:64:c4	vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=100 security="WPA2 Personal" encryption="AES" action="FT-auth-req" reason="Reserved 0" msg="AP received FT authentication request frame from client f0:98:9d:76:64:c4" remotewtptime="1805.311496"
FT-auth-resp	FT auth response was sent to wireless client	AP sent FT authentication response frame to client f0:98:9d:76:64:c4	date=2019-01-31 time=16:49:18 logid="0104043645" type="event" subtype="wireless" level="notice" vd="vdom1" eventtime=1548982158 logdesc="FT auth response was sent to wireless client" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=100 security="WPA2 Personal" encryption="AES" action="FT-auth-resp" reason="Reserved 0" msg="AP sent FT authentication response frame to client f0:98:9d:76:64:c4" remotewtptime="1805.312777"

Error logs when FT failure

Action	Description	Message	Detail
FT-invalid-action-req	Wireless client sent invalid FT action request	Receive invalid FT request action frame from client f0:98:9d:76:64:c4	date=2019-01-31 time=16:49:17 logid="0104043639" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548982157 logdesc="Wireless client sent invalid FT action request" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=100 security="WPA2 Personal" encryption="AES" action="FT-invalid-action-req" reason="Reserved 0" msg="Receive invalid FT request action frame from client f0:98:9d:76:64:c4" remotewtptime="0.0"
FT-invalid-auth-req	Wireless client sent invalid FT auth request	Receive invalid FT authentication request frame from client f0:98:9d:76:64:c4	date=2019-01-31 time=16:49:18 logid="0104043640" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1548982157 logdesc="Wireless client sent invalid FT auth request" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" radioid=2 stamac="f0:98:9d:76:64:c4" channel=100 security="WPA2 Personal" encryption="AES" action="FT-invalid-auth-req" reason="Reserved 0" msg="Receive invalid FT authentication request frame from client f0:98:9d:76:64:c4" remotewtptime="0.0"

New DNS error logs in DNS service failure

Action	Description	Message	Detail
DNS-no-domain	Wireless station DNS process failed	DNS lookup of uop.umeng.com from client	date=2019-02-01 time=09:42:03 logid="0104043673" type="event" subtype="wireless" level="warning" vd="vdom1" eventtime=1549042922 logdesc="Wireless station DNS process

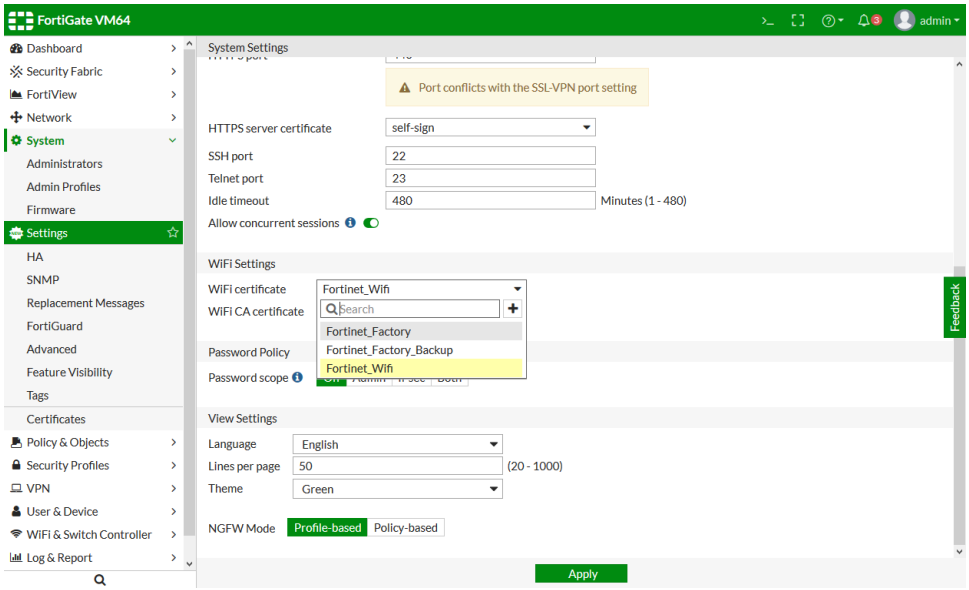
Action	Description	Message	Detail
	due to non-existing domain	3c:2e:ff:83:91:33 failed with \"non-existing domain\"	failed due to non-existing domain" sn="PS421E3X15000017" ap="PS421E3X15000017" vap="stability3" ssid="Guest-11" stamac="3c:2e:ff:83:91:33" security="WPA2 Personal" encryption="AES" action="DNS-no-domain" reason="Server 100.100.16.172 replied \"non-existing domain\"" msg="DNS lookup of uop.umeng.com from client 3c:2e:ff:83:91:33 failed with \"non-existing domain\"" remotewtptime="1130.445518"

Override WiFi Certificates (from GUI)

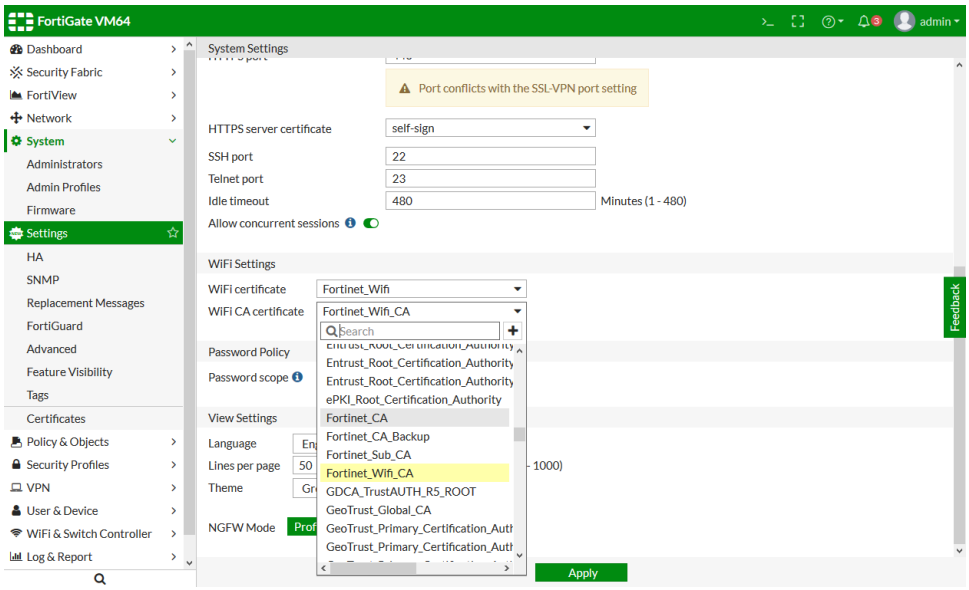
This feature enables selecting an uploaded WiFi certificate and WiFi CA certificate in the GUI, and not just the CLI.

To select a WiFi and WiFi CA certificate:

1. Go to *System* > *Settings*.
2. Select the WiFi certificate from the *WiFi certificate* dropdown menu.



3. Select the WiFi CA certificate from the WiFi CA certificate dropdown menu.

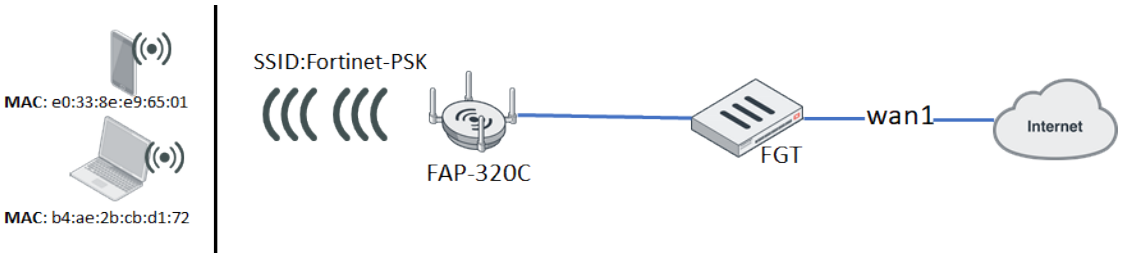


Wireless MAC Filter Updates

This feature changes the MAC filter function on SSIDs so that it is only based on the MAC address of clients. Previously, the MAC filter worked with device-detection and clients could be filtered by MAC address or device type.

The filter configuration in the CLI is moved from `user device` and `user device-access-list` to `wireless-controller address` and `wireless-controller addrgrp` respectively.

The new MAC filter function is independent from the security mode of the SSID. To enable it on an SSID, the wireless controller address and address group must be configured.



To block a specific client from connecting to an SSID using a MAC filter:

1. Create a wireless controller address with the client's MAC address, and set the policy to deny:

```
config wireless-controller address
    edit "client_1"
        set mac b4:ae:2b:cb:d1:72
        set policy deny
    next
end
```

2. Create a wireless controller address group using the above address and setting the default policy to allow:

```
config wireless-controller addrgrp
   edit mac_grp
       set addresses "client_1"
       set default-policy allow
   next
end
```

3. On the VAP, select the above address group:

```
config wireless-controller vap
    edit wifi-vap
        set ssid "Fortinet-psk"
        set security wpa2-only-personal
        set passphrase fortinet
        set address-group "mac_grp"
    next
end
```

The client's MAC address (*b4:ae:2b:cb:d1:72* in this example) will be denied a connection to the SSID (*Fortinet-psk*), but other clients (such as *e0:33:8e:e9:65:01*) will be allowed to connect.

To allow a specific client to connect to an SSID using a MAC filter:

1. Create a wireless controller address with the client's MAC address, and set the policy to allow:

```
config wireless-controller address
    edit "client_1"
        set mac b4:ae:2b:cb:d1:72
        set policy allow
    next
end
```

2. Create a wireless controller address group using the above address and setting the default policy to deny:

```
config wireless-controller addrgrp
   edit mac_grp
       set addresses "client_1"
       set default-policy deny
   next
end
```

3. On the VAP, select the above address group:

```
config wireless-controller vap
    edit wifi-vap
        set ssid "Fortinet-psk"
        set security wpa2-only-personal
        set passphrase fortinet
        set address-group "mac_grp"
    next
end
```

The client's MAC address (*b4:ae:2b:cb:d1:73* in this example) will be allowed to connect to the SSID (*Fortinet-psk*), but other clients (such as *e0:33:8e:e9:65:01*) will be denied a connection.

Change SSID to VDOM Object

This feature changes the wireless-controller VAP (for SSID configuration) from a global object to a VDOM object, simplifying tracking the object reference count. It also removes the `vdom` setting from VAP configuration. When multi-vdom is enabled on a FortiGate, the wireless-controller VAP can be added, edited, or deleted only inside of a VDOM.

To create a VAP entry:

1. When `vdom-mode` is `no-vdom`:

```
# config wireless-controller vap
(vap) # edit new
new entry 'new' added
(new) # set ssid new
(new) # set passphrase 12345678
(new) # set vdom
   command parse error before 'vdom'
(new) # end
# show wireless-controller vap new
   config wireless-controller vap
      edit "new"
         set ssid "new"
         set passphrase ENC
               qmVlo9Zn3C4aVZMIw9LrHhXX+wDNn2BMT9hP3vmZGQFZZz+gQ6Lb1jS9UkAkbQabWkGq8uDZDf
               qwtWV8lZdMDOFyDC0Kgh/yCuCkM5xM1bm9gvnGC9+84VY2mvkV4pUeiugJ/8o1m++buXmP9CdU
               mLz7eY/VZwYlKnSyFvk7DphbfZJapCOXtgN2zseNoITPQUTKLA==
      next
   end
```

2. When `vdom-mode` is `multi-vdom`:
   - A VAP cannot be created in global:

```
# config global
(global) # config wireless-controller vap
   command parse error before 'vap'
   Command fail. Return code 1
(global) #
```

   - A VAP can only be created in a VDOM:

```
# config vdom
(vdom) # edit vdom2
   current vf=vdom2:1
(vdom2) # config wireless-controller vap
(vap) # edit new
   new entry 'new' added
(new) # set ssid new
(new) # set passphrase 12345678
(new) # set vdom
   command parse error before 'vdom'
(new) # end
(vdom2) # sh wireless-controller vap new
   config wireless-controller vap
      edit "new"
         set ssid "new"
         set passphrase ENC
               IidSvoD1C6feNonhsYfUTnOtO89UE/S/wWmOxRHLCud+eR0LD8xuYzWzsRg9/c299Vd2UA
               809NSUfyRBRD/pFFd/QS6ArQPs4sLVtPiftE63uI53d9azeQv6e5tkQjg4Z7Ztlv2hE47n
               KkdVXeWZE3mpfRhSxvDUKVzwpR1b8pdwbzDGFlPs+JcoNso6ZeRCuMg54g==
```

```
        next
    end
(vdom2) #
```

3. When `vdom-mode` is `multi-vdom`, references to user-group and radius can be checked correctly when they are used by a VAP interface:
   - A VAP interface with security-mode set to WPA2-Enterprise and RADIUS authentication:

```
(vdom2) # show wireless-controller vap new
   config wireless-controller vap
      edit "new"
         set ssid "new"
         set security wpa2-only-enterprise
         set auth radius
         set radius-server "peap"
      next
   end
   (vdom2) # diagnose sys cmdb refcnt show user.radius.name peap
   entry used by table wireless-controller.vap:name 'new'
```

   - A VAP interface with security-mode set to WPA2-Enterprise and User-group authentication:

```
(vdom2) # show wireless-controller vap new
   config wireless-controller vap
      edit "new"
         set ssid "new"
         set security wpa2-only-enterprise
         set auth usergroup
         set usergroup "group-radius"
      next
   end
   (vdom2) # diagnose sys cmdb refcnt show user.group.name group-radius
   entry used by child table usergroup:name 'group-radius' of table wireless-
        controller.vap:name 'new'
```

Switching

This section lists new switching features added to FortiOS for the expanding fabric family.

FortiLink Setup

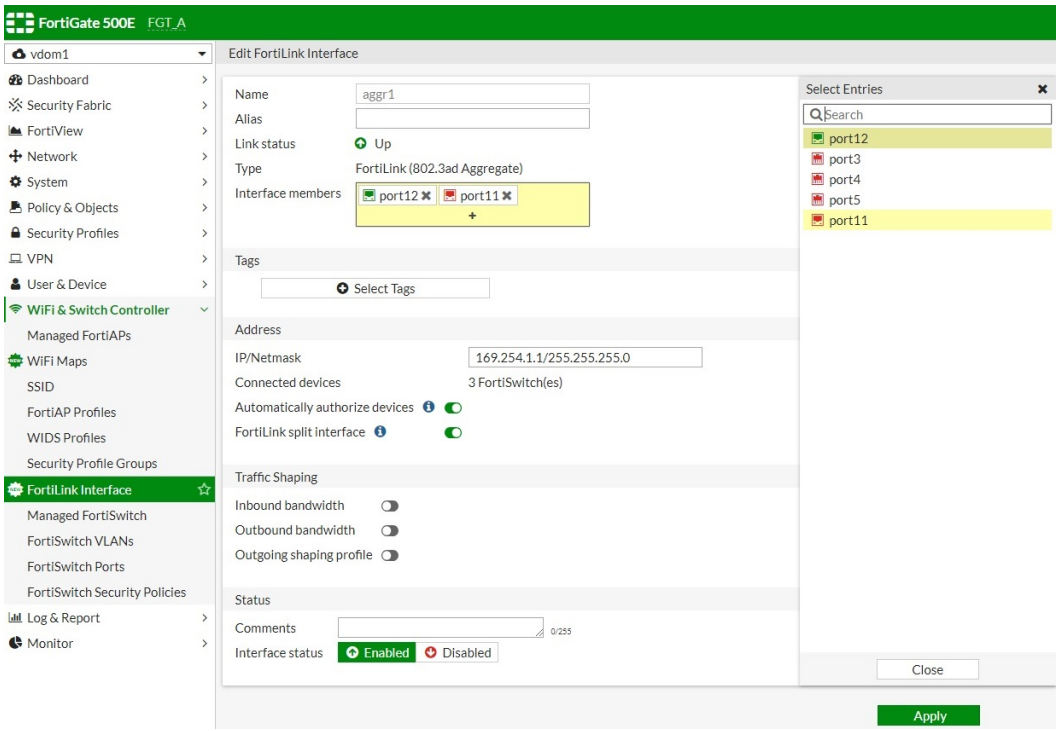
Starting in 6.2, you can configure FortiLink interfaces by using a dedicated pane under the *WiFI & Switch Controller* > *FortiLink Interface* menu. In previous versions, you set up a general address interface under the *System* > *Interfaces* menu.

You can create and edit FortiLink interfaces on the *FortiLink Interface* pane. The options available on the pane will be based on the capability of the FortiGate model.

By automatically creating FortiLink interfaces as a logical aggregate or hard/soft switch, it becomes a simple process to modify the interface(s) being used by FortiLink. Policies created no longer need to be migrated if the physical port in use changes.

To configure FortiLink interfaces:

1. Go to *WiFi & Switch Controller* > *FortiLink Interface*.



Voice VLAN Auto-Assignment

You can leverage LLDP-MED to assign voice traffic to the desired voice VLAN. After detection and setup, the IP phone on the network is segmented to its own VLAN for policy, prioritization, and reporting. The LLDP reception capabilities in FortiOS have been extended to support LLDP-MED assignment for voice, voice signaling, guest, guest voice signaling, softphone, video conferencing, streaming video, and video signaling.

You can configure this feature using the FortiOS CLI. Configuration consists of the following steps:

1. Setting up the VLAN for the voice device
2. Setting up the DHCP server for the voice VLAN
3. Setting up the LLDP network policy

4. Enabling LLDP on the physical interface that the VLAN belongs to
5. Applying the LLDP network policy on the physical interface
6. Confirming that the VLAN was assigned

To set up the VLAN for the voice device:

```
config system interface
   edit "vlan_100"
      set vdom "root"
      set ip 192.168.1.99 255.255.255.0
      set alias "voice_vlan"
      set device-identification enable
      set role lan
      set snmp-index 25
      set interface "port10"
      set vlanid 100
   next
end
```

To set up the DHCP server for the voice VLAN:

```
config system dhcp server
   edit 1
      set dns-service default
      set default-gateway 192.168.1.99
      set netmask 255.255.255.0
      set interface "vlan_100"
      config ip-range
         edit 1
            set start-ip 192.168.1.110
            set end-ip 192.168.1.210
         next
      end
   next
end
```

To set up the LLDP network policy:

```
config system lldp network-policy
   edit "1"
      config voice
         set status enable
         set tag dot1q
         set vlan 100
      end
   next
end
```

To enable LLDP on the physical interface that the VLAN belongs to:

```
config system interface
   edit "port10"
      set vdom "root"
      set type physical
      set lldp-reception enable
```

```
      set lldp-transmission enable
      set snmp-index 14
   next
end
```

To apply the LLDP network policy on the physical interface:

```
config system interface
   edit "port10"
      set lldp-network-policy "1"
   next
end
```

To confirm that the VLAN was assigned:

To confirm that the VLAN was assigned as expected, connect an IP phone to the network. Check the IP address on the phone. The IP address should belong to the voice VLAN.

You can also sniff on the FortiGate incoming interface to see if traffic from the IP phone has the desired VLAN tag.

In the example commands above, the voice VLAN was configured as VLAN 100. Therefore, voice traffic from the IP phone should be in VLAN 100.

Dynamic VLAN 'Name' Assignment from Radius Attribute

Starting in 6.2, when FortiSwitch receives a VLAN assignment from Radius, it determines if the data is an integer or string representation. If the representation is an integer, FortiSwitch assigns the VLAN. If the representation is a string, the 802.1x agent will search each VLAN's description field for all VLANs (names defined by FortiOS VLAN description). If found, the 802.1x agent will make the assignment.

Example

On the FortiGate, all VLANs are specified as a system interface. Each system interface has a well-defined and unique name. When running FortiLink, the switch has no knowledge of the name association. The switch communicates directly with the Radius server and needs to know the mapping to make the proper selection.

As a result, this information must be provided to the switch. In order to make the feature generic and applicable to the switch in standalone mode as well, the system interface description field is leveraged. The switch-controller synchronizes this field to the switch for information purposes, and the description-to-description synchronization has been removed. All descriptions on the FortiGate remain on the FortiGate. The switch-controller synchronizes the FortiGate system interface name to the switch VLAN description.

When FortiSwitch receives a VLAN assignment from Radius, it determines if the data is an integer or string representation. If the representation is an integer, FortiSwitch assigns the VLAN. If the representation is a string, the 802.1x agent will search each VLAN's description field for all VLANs (names defined by FortiOS VLAN description). If found, the 802.1x agent will make the assignment.

To configure dynamic VLAN name assignment:

1. Configure a Radius server:
   - Set Tunnel-Type to "VLAN".
   - Set Tunnel-Medium-Type to "IEEE-802".

- Set Tunnel-Private-Group-Id to "my.vlan.10". In this option, you designate the VLAN name instead of VLAN ID.

2. Configure FortiGate:

```
edit "my.vlan.10"
   set vdom "root"
   set ip 1.1.1.254 255.255.255.0
   set allowaccess ping
   set interface "my.fortlink"
   set vlanid 10
next
end
```

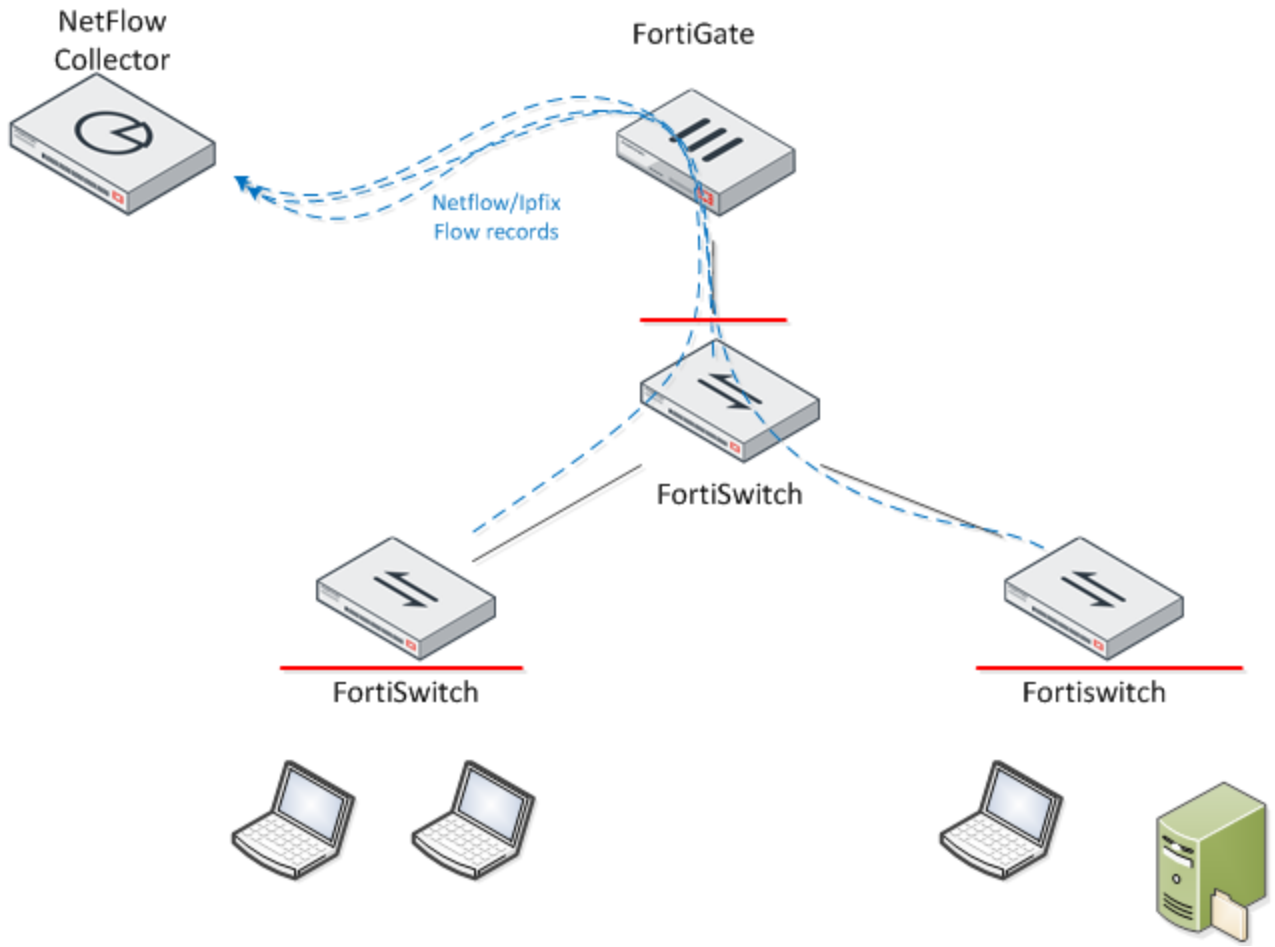
3. Configure FortiSwitch:

```
# show switch vlan
config switch vlan
   edit 10
   set description "my.vlan.10"   --------> VLAN name will be stored into the
        "description", which is not new CLI but just new API mapping to be implemented in
        backend.
next
```

Netflow / IPFIX Support

Support for Netflow (v1, v5, v9) and IPFIX (IP Flow Information Export) is added to FortiSwitch 6.2, and the resulting data will be available to FortiAnalyzer (and FortiView) for new traffic statistics and topology views. Traffic sampling data can be used to show which users or devices behind switches are generating the highest traffic in those networks.

You can now configure Netflow/IPFIX on managed FortiSwitch units on switch controller.



You can configure flow-tracking related parameters by using the default values:

```
# conf switch-controller  flow-tracking
(flow-tracking) # get
sample-mode  : perimeter
sample-rate  : 512
format  : netflow9
collector-ip  : 0.0.0.0   ------> all-zero IP address implies disabled
collector-port  : 0
transport  : udp
level  : ip
filter  :   -------> complies with tcpdump/wireshark filter syntax
max-export-pkt-size : 512
timeout-general  : 3600
timeout-icmp  : 300
timeout-max  : 604800
timeout-tcp  : 3600
timeout-tcp-fin  : 300
timeout-tcp-rst  : 120
timeout-udp  : 300 aggregates:
```

Following are the sampling mode options:

- Perimeter sampling: RX sampling enabled on all non-fabric FortiSwitch ports, including access port and FortiLink port, but not the FortiLink ISL port.

- Device-Ingress sampling: RX sampling enabled on all FortiSwitch ports.
- Local sampling: Sampling must be enabled on specific FortiSwitch ports by using `config switch-controller managed-switch` and `config ports`.

QoS Assignment and Rate Limiting for Quarantined VLANs

When devices are quarantined, they are isolated from the rest of the network. However, they can still impact the network if not controlled beyond isolation. A quarantined host, which offers heavy traffic, could congest the network and create a DOS-style reduction in service to authorized hosts.

Within the quarantined VLAN, two restrictions are available within the network:

- Traffic policing (also known as rate limiting)
- QoS (Quality of Service) assignment (also known as priority assignment)

Each quarantined host's traffic can be subject to rate limiting and priority adjustment. This reduces the impact that any quarantined host can have on authorized traffic on the network.

You can only configure this feature by using the CLI.

```
config switch-controller traffic-policy
(traffic-policy) # get
== [ quarantine ]   ---> Newly added pre-defined traffic-policy for quarantine. It can also be
     applied to other switch VLAN interfaces based on configuration.
name: quarantine
== [ sniffer ] name: sniffer
(traffic-policy) # edit quarantine
   (quarantine) # show
        config switch-controller traffic-policy
           edit "quarantine"
                   set description "Rate control for quarantined traffic"
                   set guaranteed-bandwidth 163840
                   set guaranteed-burst 8192
                   set maximum-burst 163840
                   set cos-queue 0
                next
              end
config system interface
edit "qtn.aggr1"
   set vdom "root"
   set ip 10.254.254.254 255.255.255.0
   set description "Quarantine VLAN"
   set security-mode captive-portal
   set replacemsg-override-group "auth-intf-qtn.aggr1"
   set device-identification enable
   set snmp-index 30
   set switch-controller-access-vlan enable
   set switch-controller-traffic-policy "quarantine" ---> By default, switch-controller-
        traffic-policy is empty. Users need to apply the necessary traffic-policy, not only
        limited to "quarantine".
   set color 6
   set interface "aggr1"
   set vlanid 4093
next
```

Persistent MAC Learning (Sticky MAC)

Persistent MAC learning or sticky MAC is a port security feature where dynamically learned MAC addresses are retained when a switch or interface comes back online. The benefits of this feature include:

- Prevent traffic loss from trusted workstations and servers since there is no need to relearn MAC address after a restart.
- Protect the switch and the whole network when combined with MAC-learning-limit against security attacks such as Layer 2 DoS and overflow attacks.

Persistent MAC learning is configured in FortiGate and implemented in FortiSwitch.

This feature is disabled by default. You can use persistent MAC learning together with MAC limiting to restrict the number of persistent MAC addresses.

This feature is hardware and CPU intensive and can take several minutes depending on the number of entries.

You can only use CLI to configure this feature.

This feature is supported on all FortiSwitch models in FSW 6.0.

This feature is supported on models in FSW 3.6 higher than the 124D series.

To enable sticky MAC on FortiGate:

```
config switch-controller managed-switch
   edit <switch-serial-number>
      conf ports
         edit <port-number>
            set sticky-mac enable
         next
      end
   next
end
```

Before saving sticky Mac entries into CMDB, you might want to delete the unsaved sticky MAC items so that only the items you want are saved.

Saving sticky MAC items copies the sticky MAC items from memory to CMDB on FortiSwitches and FortiGates.

To delete unsaved sticky MAC items:

```
execute switch-controller switch-action sticky-mac delete-unsaved <all | interface><switch-
     serial-number>
```

To save sticky MAC items into CMDB:

```
execute switch-controller switch-action sticky-mac save <all | interface><switch-serial-
     number>
```

Split Port Mode (for QSFP /QSFP28)

The quad, small, form-factor pluggable plus (QSFP/QSPF28) is a transceiver module that offers high-density 40/100 Gigabit Ethernet connectivity options for data center and high-performance computing networks. The QSFP transceiver module is a hot-swappable, parallel fiber-optic/copper module with four independent optical transmit and receive channels. These channels can terminate in another Ethernet QSFP transceiver, or the channels can be broken out to four separate physical ports.

Configuration of which FortiSwitch ports are split is controlled directly on the FortiSwitch. An administrator needs to manually log into the FortiSwitch and set the desired split port configuration. After a split port configuration change is made on the FortiSwitch, it will automatically reboot. If the FortiSwitch was previously discovered or authorized, it should be deleted to allow the switch to be newly discovery again.

This feature requires a FortiSwitch model with SFP+ 40G ports, and FortiSwitch must be in Fortlink mode when changing the split configuration.

To use FortiSwitch with split ports with the switch controller (previously discovered):

1. On FortiSwitch, change the split mode:
   This change requires a reboot.
   ```
   config switch phy-mode
      set port29-phy-mode 4x10G
      set port30-phy-mode 4x10G
   end
   ```
2. Delete the FortiSwitch from `managed-switch` stanza.
3. Discover and authorize.

To use FortiSwitch with split ports with the switch controller (out of the box with factory defaults):

1. Discover and Authorize.
   This change requires a reboot.
2. On FortiSwitch, change split mode.
   This change requires a reboot.
3. Delete switch from `managed-switch` stanza.
4. Discover and authorize.

No CLI changes; however, FortiGate introduces a new FortiSwitch port index:

```
# conf switch-controller  managed-switch
(managed-switch) # edi S524DN4K15000008
# conf ports
edit "port29.1"
   set speed 10000
   set vlan "vsw.port11"
   set allowed-vlans "qtn.port11"
   set untagged-vlans "qtn.port11"
   set export-to "root"
next
......
edit "port29.4"
   set speed 10000
```

```
    set vlan "vsw.port11"
    set allowed-vlans "qtn.port11"
    set untagged-vlans "qtn.port11"
    set export-to "root"
next
edit "port30.1"
    set speed 10000
    set vlan "vsw.port11"
    set allowed-vlans "qtn.port11"
    set untagged-vlans "qtn.port11"
    set export-to "root"
next
......
edit "port30.4"
    set speed 10000
    set vlan "vsw.port11"
    set allowed-vlans "qtn.port11"
    set untagged-vlans "qtn.port11"
    set export-to "root"
next
```

Virtual Switch Extensions

The Virtual Switch concept was introduced in previous releases. It provides a container for physical ports to be loaned out to other VDOMs, which allows local management of the resource. In the original feature, only a minimum of switch capability was introduced, such as VLAN, `allowed-vlan`, status, speed, `poe-status`, and `poe-reset`.

This extends some of the port capabilities including:

- poe-pre-standard-detection
- learning-limit
- qos-policy
- port-security-policy
- trunk ports (with some limitations)

Example

The following example shows how to export managed FortiSwitch ports to multi-tenant VDOMs. Some of the capabilities are available in previous releases of FortiOS, and the 6.2.0 release expands the functionality.

To export managed FortiSwitch ports to multi-tenant VDOMs:

1. Configure switch VLAN interfaces, and assign them to the tenant VDOM:
   In this example, the owner VDOM is root, and the tenant VDOM is vdom2.

```
(root) #  config system interface
   edit "tenant-vlan1"
      set vdom "vdom2"
      set device-identification enable
      set fortiheart beat enable
      set role lan
      set snmp-index 34
      set interface "aggr1"
```

```
      set vlanid 101
   next
end
```

2. In the tenant VDOM, designate `default-virtual-switch-vlan`, which is used to set the native VLAN of ports leased from the owner VDOM:

```
(vdom2) # config switch-controller
   global set default-virtual-switch-vlan "tenant-vlan1"
end
```

3. Owner vdom admin can export managed fsw ports to tenant vdom, as below

```
  (root) # conf switch-controller  managed-switch
(managed-switch) # edit S248EPTF1800XXXX
(S248EPTF1800XXXX) # conf ports
   (ports) # edit port1
   (port1) # set export-to ?
   <string>  string  please input string value
   root  vdom
   vdom1  vdom
   vdom2  vdom
   vdom3  vdom
   (port1) # set export-to vdom2
(port1) # end
```

   Alternatively, the admin of the owner VDOM can export managed FortiSwitch ports to shared virtual-switch pools for the tenant VDOM to pick, for example:

```
 (root) # config switch-controller virtual-port-pool
   edit "pool1"
   next
end
(root) # conf switch-controller  managed-switch
(managed-switch) # edit S248EPTF18001384
(S248EPTF18001384) # conf ports
   (ports) # edit port8
   (port8) # set export-to-pool pool1
   (port8) # next
   (ports) # edit port9
   (port9) # set export-to-pool pool1
   (port9) # end
```

4. The admin of the tenant VDOM logs in, and configures the ports of the leased managed FortiSwitch, or the admin continues to lease/release ports from virtual switch pool.

   Then in each tenant VDOM, the tenant admin can configure and leverage the FortiSwitch ports locally with limited range of operations based on the available CLI operations:

```
login: vdom2
Password: *****
Welcome !
$ show switch-controller  managed-switch
   config switch-controller managed-switch
      edit "S248EPTF1800XXXX"
         set type virtual
         set owner-vdom "root"
            config ports
               edit "port1"
                  set poe-capable 1
                  set vlan "tenant-vlan1"
               next
               edit "port6"
                  set poe-capable 1
```

```
                set vlan "tenant-vlan1"
              next
$ conf switch-controller managed-switch
   (managed-switch) $ edit S248EPTF1800XXXX
      (S248EPTF1800XXXX) $ config ports
              (ports) $ edit port1
              (port1) $ set
              port-owner Switch port name.
              speed Switch port speed; default and available settings depend on hardware.
              status Switch port admin status: up or down.
              poe-status Enable/disable PoE status.
              poe-pre-standard-detection Enable/disable PoE pre-standard detection. --> expanded to tenant VDOM in FortiOS 6.2
              poe-capable PoE capable.
              vlan Assign switch ports to a VLAN.
              allowed-vlans Configure switch port tagged vlans
              untagged-vlans Configure switch port untagged vlans
              type Interface type: physical or trunk port.
              qos-policy Switch controller QoS policy from available options. --> expanded to tenant VDOM in FortiOS 6.2
              storm-control-policy  Switch controller storm control policy from available options.
              port-security-policy  Switch controller authentication policy to apply to this managed switch from available options.--> expanded to tenant VDOM in FortiOS 6.2
              learning-limit Limit the number of dynamic MAC addresses on this Port (1 - 128, 0 = no limit, default).--> expanded to tenant VDOM in FortiOS 6.2
              (ports) # edit trunk1
              (trunk) # set type trunk --> expanded to tenant VDOM in FortiOS 6.2
              $ exe switch-controller virtual-port-pool request S248EPTF1800XXXX port8
              $ exe switch-controller virtual-port-pool show
```

MSTI Support

In 6.0, the switch controller maps all user VLANs into the MSTI-CST (common spanning tree) instance 0. While reserving MSTI-0 (CST) and MSTI-15 for FortiLink management VLAN=4094. In 6.2, the administrator can control MSTI 1-14.

Each instance is a full and complete spanning tree. Any user VLAN may be mapped to any instance, allowing the spanning trees to have different topologies for each MSTI. Each instance allows the setting of various parameters such as cost and priority.

You must configure this feature by using the CLI.

To configure MSTI support:

1. Create or modify `stp-instance` between 1 to 14:

```
                                    root) # conf switch-controller  stp-instance
                                    (stp-instance) # edit 15
                                    please enter a value of 1 to 14.
                                    (stp-instance) # edit 1                  ----------------> crea
be applied to all managed fsws
                                    new entry '1' added
                                    (1) # set vlan-range
```

```
                                    *vlan-name    VLAN name.
                                    cam.aggr1       interface
                                    snf.aggr1       interface
                                    tenant-vlan3    interface
                                    tenant-vlan4    interface
                                    voi.aggr1       interface
                                    vsw.aggr1       interface
                                    (1) # set vlan-range tenant-vlan3 vsw.aggr1
                                    (1) # end
```

2. Configure specific stp priority on different managed FortiSwitch units:

```
(root) # conf switch-controller  managed-switch
                                    (managed-switch) # edit S248EPTF1800XXXX

                                    (S248EPTF1800XXXX) # conf stp-instance

                                    (stp-instance) # edit 1

                                    # get
                                    id                  : 1
                                    priority            : 32768     ------> Default priority
                                    (1) # set priority  8192

                                (1) # end
```

FortiLink Auto Network Configuration Policy

In 6.0, FortiLink supports automatic network detection and configuration. As links can automatically appear and disappear, this presents challenges when customization is desired. Currently administrators can only select the default QoS policy, which is applied to all FortiSwitch units in the network. In some cases, this is enough, but more flexibility is warranted for larger and more complex topologies.

In 6.2, the Switch Controller introduces a network `auto-config` option, which contains configurable defaults, policy customization, and an individual interface override. This will allow the administrator simple yet flexible control.

Following is a description of the new options:

- `auto-config default`: Provides the default actions for the first hop (fgt-policy) and lower-tier devices (isl-policy).
- `auto-config policy`: A database which contains policies that can be applied as a system-wide default or to a specific interface.
- `auto-config custom`: Allows for the override of the `auto-config default` on a specific interface. This information is retained and is reapplied if a interface leaves and then is rediscovered.

To configure automatic network detection:

1. Create or modify an auto-config policy:

```
(root) # config switch-controller  auto-config  policy
   (policy) # edit test123
   (test123) # get
   name  : test123
   qos-policy  : default   ---> leverage the default qos-policy
```

```
storm-control-policy: auto-config   ---> leverage auto-config storm-control-policy by
     default
poe-status  : enable   ---> If target of auto-config is poe port, keep poe-status
     enabled by default
```

2. Designate an auto-config policy to FortiLink, ISL, or ICL on Managed FortiSwitches.

```
(root) # config switch-controller  auto-config
  default  (default) # get
     fgt-policy  : test123
     isl-policy  : test123
     icl-policy  : test123
  (default) # set  ?
  fgt-policy  Default FortiLink auto-config policy.
  isl-policy  Default ISL auto-config policy.
  icl-policy  Default ICL auto-config policy.
```

3. Customize an auto-config policy for a specific FGT, ICL, or ISL interface.

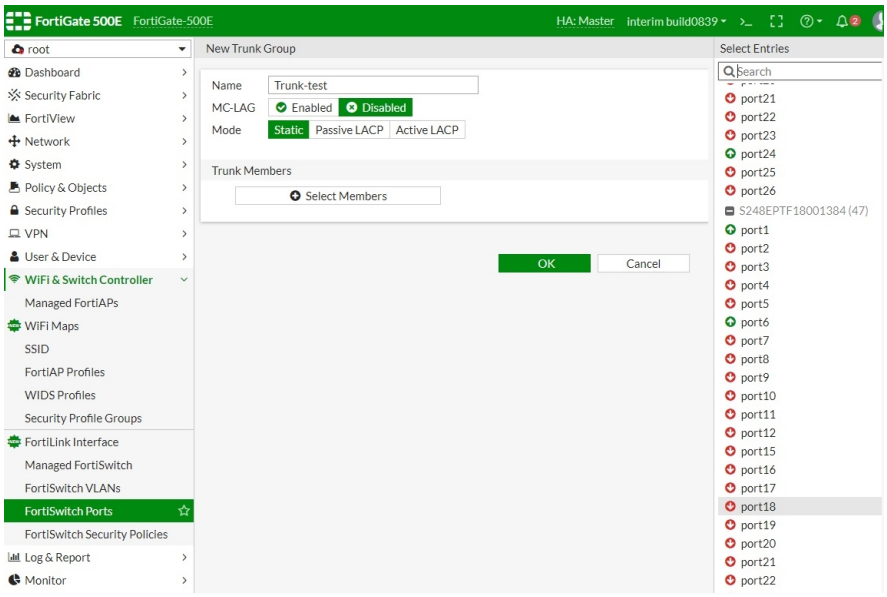
```
 (root) # config switch-controller  auto-config custom
  (custom) # edit
  *name  Auto-Config FortiLink or ISL/ICL interface name.
  (custom) # edit G5H0E391790XXXX
     new entry 'G5H0E391790XXXX' added
     (G5H0E391790XXXX) # conf switch-binding
        (switch-binding) # edit
           *switch-id  Switch name.
        (switch-binding) # edit S524DN4K1500XXXX
           new entry 'S524DN4K1500XXXX' added
              (S524DN4K1500XXXX) # get
                 switch-id  : S524DN4K1500XXXX
                 policy  : default
```

FortiLink MLAG Configuration in GUI

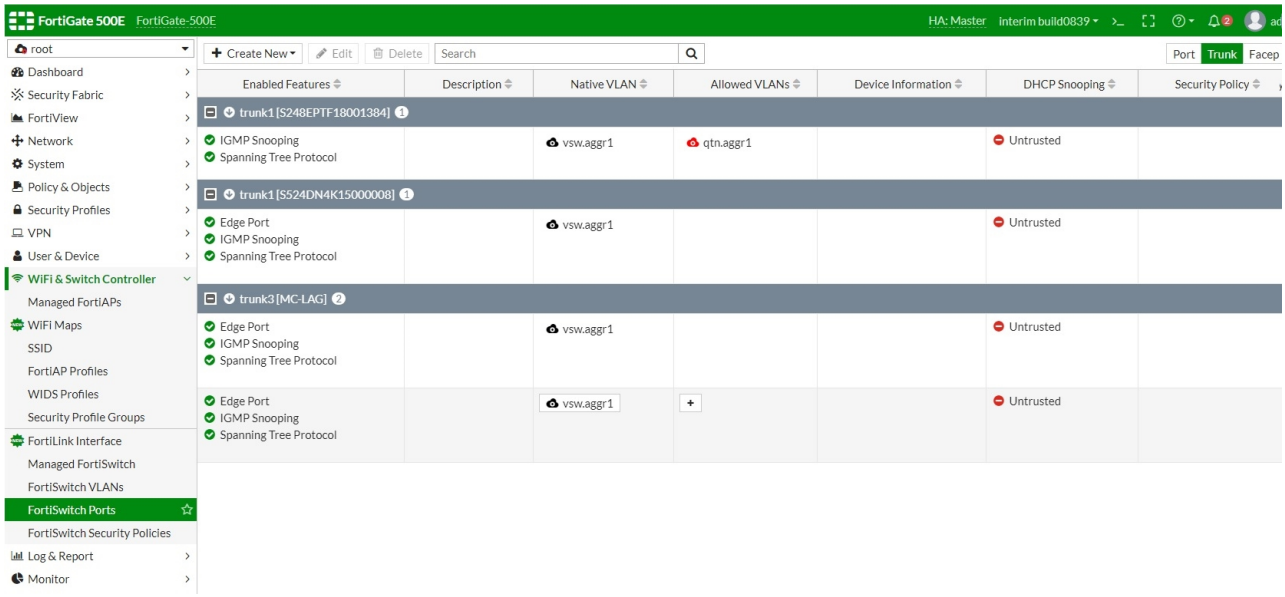
In this version, you can enable MLAG in the GUI and view ports grouped by trunks. You need to configure ports from two switches, i.e., two MLAG peer switches, to be included in one MLAG.

Sample configuration

In *WiFi & Switch Controller* > *FortiSwitch Ports*, there is a new *MC-LAG* option.



In *WiFi & Switch Controller* > *FortiSwitch Ports*, there is a separated Trunk view.



FortiLink Network Sniffer Extension

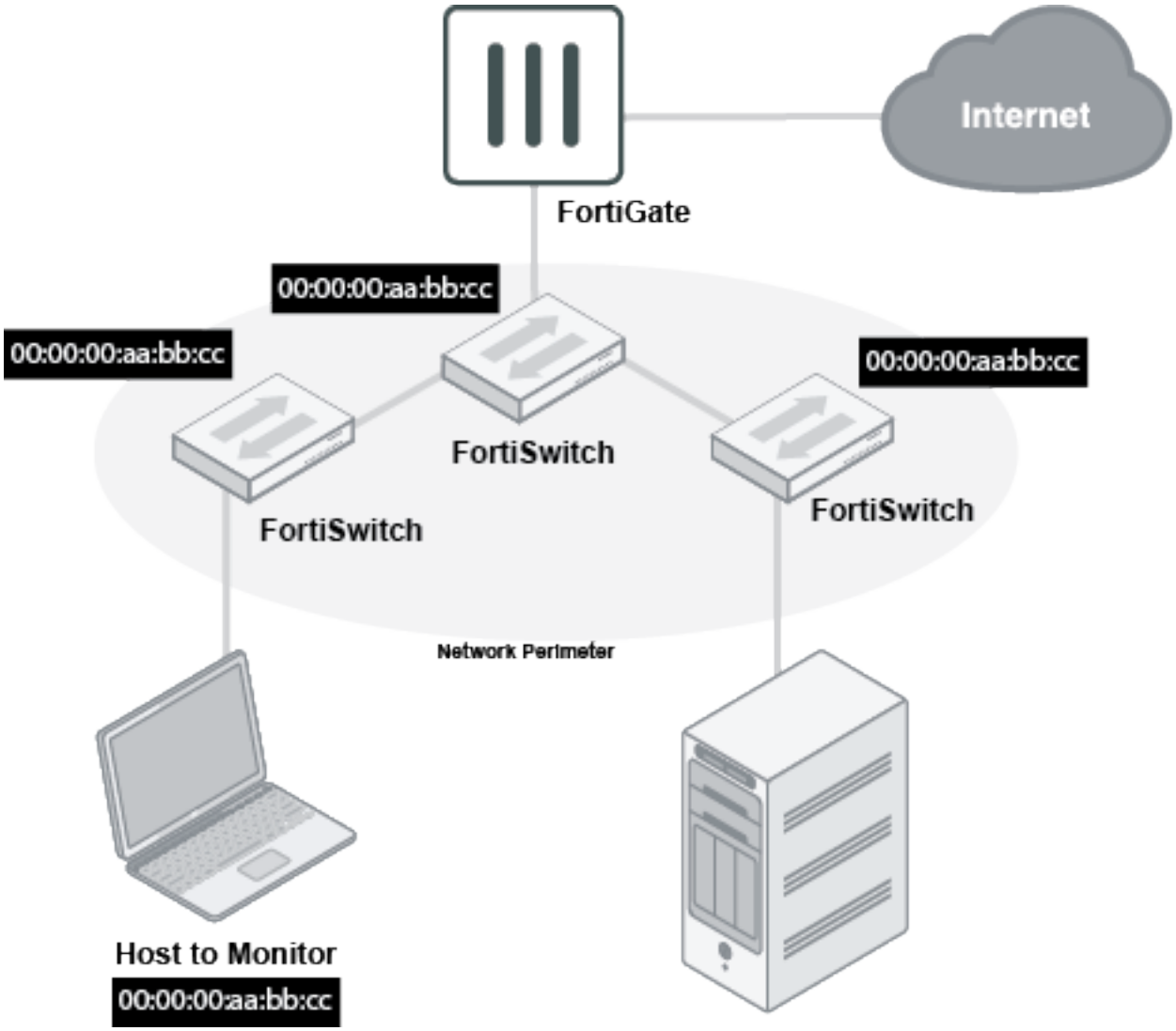
In 6.0, the switch controller introduced traffic mirroring with a single switch. This provides a general capability, but can result in large volumes of traffic being mirrored. In 6.2, the new switch controller option of `traffic-sniffer` provides a targeted approach: mirrored traffic is always directed towards the FortiGate on a dedicated VLAN. This allows for easy sniffing by using the CLI or GUI. Additionally, the traffic can also be routed through the FortiGate using Encapsulated Remote Switched Port Analyzer (ERSPAN) for external analysis and storage.

With the new option, you can define targeted sniffers by IP or MAC address. Traffic matching is replicated to the FortiGate, which is helpful when you know what device you are looking for, but you don't know where it is located.

FortiLink networks can have multiple switches, and traffic typically traverses several switches. If each switch mirrors any match, the sniffer would see multiple copies of traffic. To reduce this, the targets are applied at the perimeter of the FortiSwitch network. Traffic entering by a user port or traffic from FortiGate is considered eligible for mirroring.

You can also enable traditional port-based sniffers in the ingress or egress directions.

All sniffer traffic arrives at the FortiGate using ERSPAN, an the traffic is encapsulated in generic routing encapsulation (GRE).



You can only configuring this feature by using the CLI:

- Use pre-defined sniffer-used switch vlan interface:

```
config system interface
   edit "snf.aggr1" ---> Newly added pre-defined switch vlan interface. Created
        automatically after the first FortiSwitch is discovered and authorized.
      set vdom "root"
      set ip 10.254.253.254 255.255.254.0
      set allowaccess ping
      set description "Sniffer VLAN"
      set snmp-index 33
      set switch-controller-traffic-policy "sniffer"
```

```
      set color 6
      set interface "aggr1"
      set vlanid 4092
   next
end
```

- Enable traffic sniffer based on target IP or MAC addresses on target ports of managed FortiSwitch units:

```
config switch-controller traffic-sniffer ---> newly added>
   set erspan-ip 2.2.2.2 ---> Designated ERSPAN collector
   config target-mac
      edit 11:11:11:11:11:11
      next
   end
   config target-ip
      edit 4.4.4.4
      next
   end
   config target-port
      edit "S524DN4K1500XXXX"
         set in-ports "port2" "port4" "port6"
         set out-ports "port3" "port5" "port7"
      next
   end
end
```

- Use troubleshooting tools:

```
FortiGate-500E (root) # diag switch-controller  switch-info mirror status S524DN4K1500XXXX

Managed Switch : S524DN4K1500XXXX
flink.sniffer
      Mode  : ERSPAN-auto
      Status  : Active
      Source-Ports:
            Ingress: port2, port4, port6
            Egress : port3, port5, port7
         Used-by-ACLs  : True
         Auto-config-state  : Resolved/Running
            Last-update  : 1464 seconds ago
            Issues  : None
            Collector-IP : 2.2.2.2
            Source-IP  : 10.254.252.208
            Source-MAC  : 08:5b:0e:ff:40:27
            Next-Hop  :
               IP  : 10.254.253.254
               MAC  : 00:09:0f:09:00:0c
               Via-System-Interface : sniffer
               VLAN  : 4092(tagged)
               Via-Switch-Interface : G5H0E391790XXXX
```

Fabric Connectors

This section lists the new features added to FortiOS for Security Fabric connectors.

Multiple Concurrent SDN/Cloud Connectors

This feature introduces support for multiple connectors of all SDN connector types to be defined. Previously, only a single connector could be configured for most types, and the SDN connector had to be specified when creating a dynamic firewall address. Now, multiple instances can be configured for every SDN connector, and the specific connector instance must be specified when creating a dynamic firewall address.

This example shows two Microsoft Azure SDN connectors being created, and then being used in new dynamic firewall addresses.

To create and use two new SDN connectors with the CLI:

1. Create two new SDN connectors:

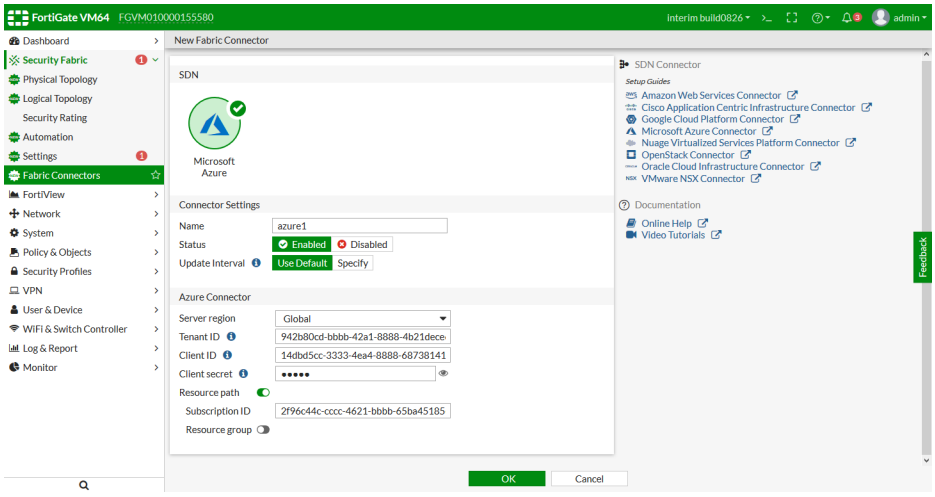
```
config system sdn-connector
    edit "azure1"
        set type azure
        set tenant-id "942b80cd-bbbb-42a1-8888-4b21dece61ba"
        set subscription-id "2f96c44c-cccc-4621-bbbb-65ba45185e0c"
        set client-id "14dbd5cc-3333-4ea4-8888-68738141feb1"
        set client-secret xxxxx
        set update-interval 30
    next
    edit "azure2"
        set type azure
        set tenant-id "942b80cd-bbbb-42a1-8888-4b21dece61ba"
        set client-id "3baa0acc-ffff-4444-b292-0777a2c36be6"
        set client-secret xxxxx
        set update-interval 30
    next
end
```

2. Create new dynamic firewall addresses that use the new connectors:

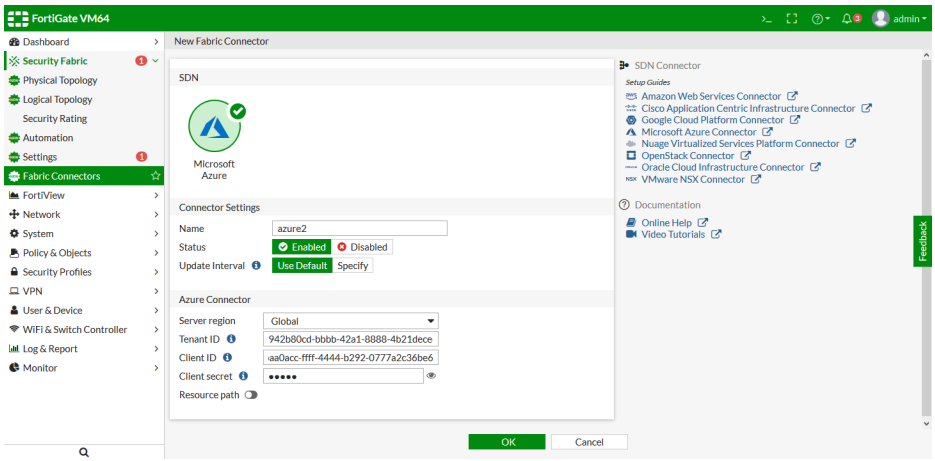
```
config firewall address
    edit "azure-address-location1"
        set type dynamic
        set color 2
        set sdn azure1
        set filter "location=WestUs"
    next
    edit "azure-address-location2"
        set type dynamic
        set color 2
        set sdn azure2
        set filter "location=NorthEurope"
    next
end
```

To create and use two new SDN connectors with the GUI:

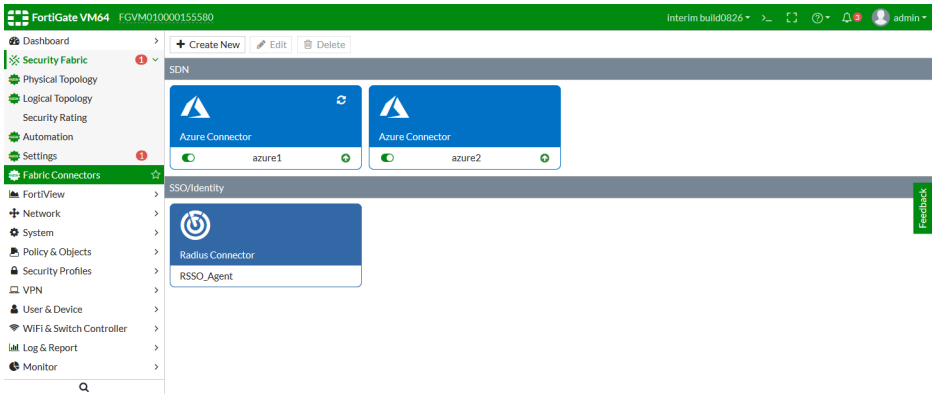
1. Create two new SDN connectors:
   a. Go to *Security Fabric* > *Fabric Connectors*, and click *Create New* in the toolbar.
   b. Click on *Microsoft Azure*.
   c. Fill in the required information, then click *OK*.



d. Repeat the above steps for the second connector.



Two Microsoft Azure connectors will now be created.

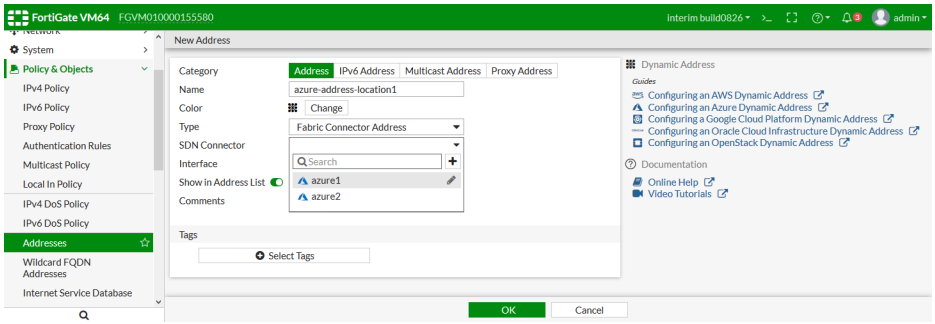


2. Create new dynamic firewall addresses that use the new connectors:

a. Go to *Policy and Objects* > *Addresses* and click *Create New* > *Address* in the toolbar.

b. Enter a name for the address, and select *Fabric Connector Address* for the *Type*.

c. Select one of the previously created SDN connectors from the *SDN Connector* drop down list.



d. Configure the rest of the required information, then click *OK* to create the address.

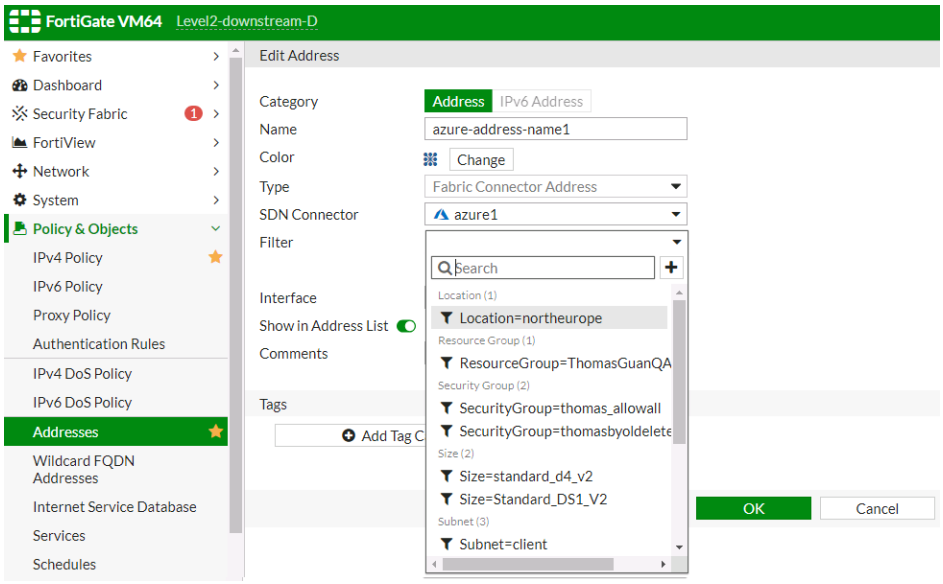
e. Repeat the above steps to create the second address, selecting the other Microsoft Azure SDN connector.

Filter Lookup Improvement for SDN Connectors

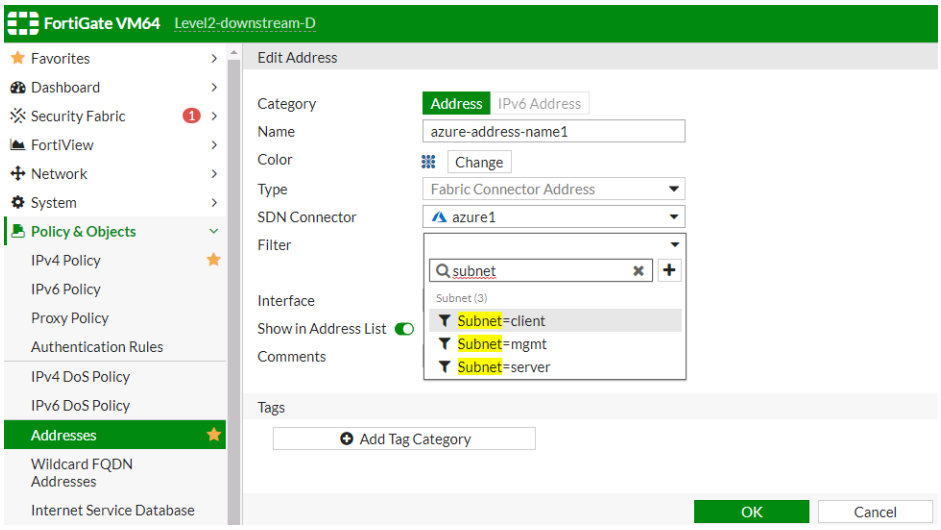
In 6.0, when configuring dynamic address mappings for filters in AWS, FortiGate can query the filters automatically, while for other clouds the configuration is a manual process. In 6.2, the same capability is expanded to SDN connectors for Azure, GCP, OpenStack, Kubernetes, and AliCloud.

To use the improved filter lookup:

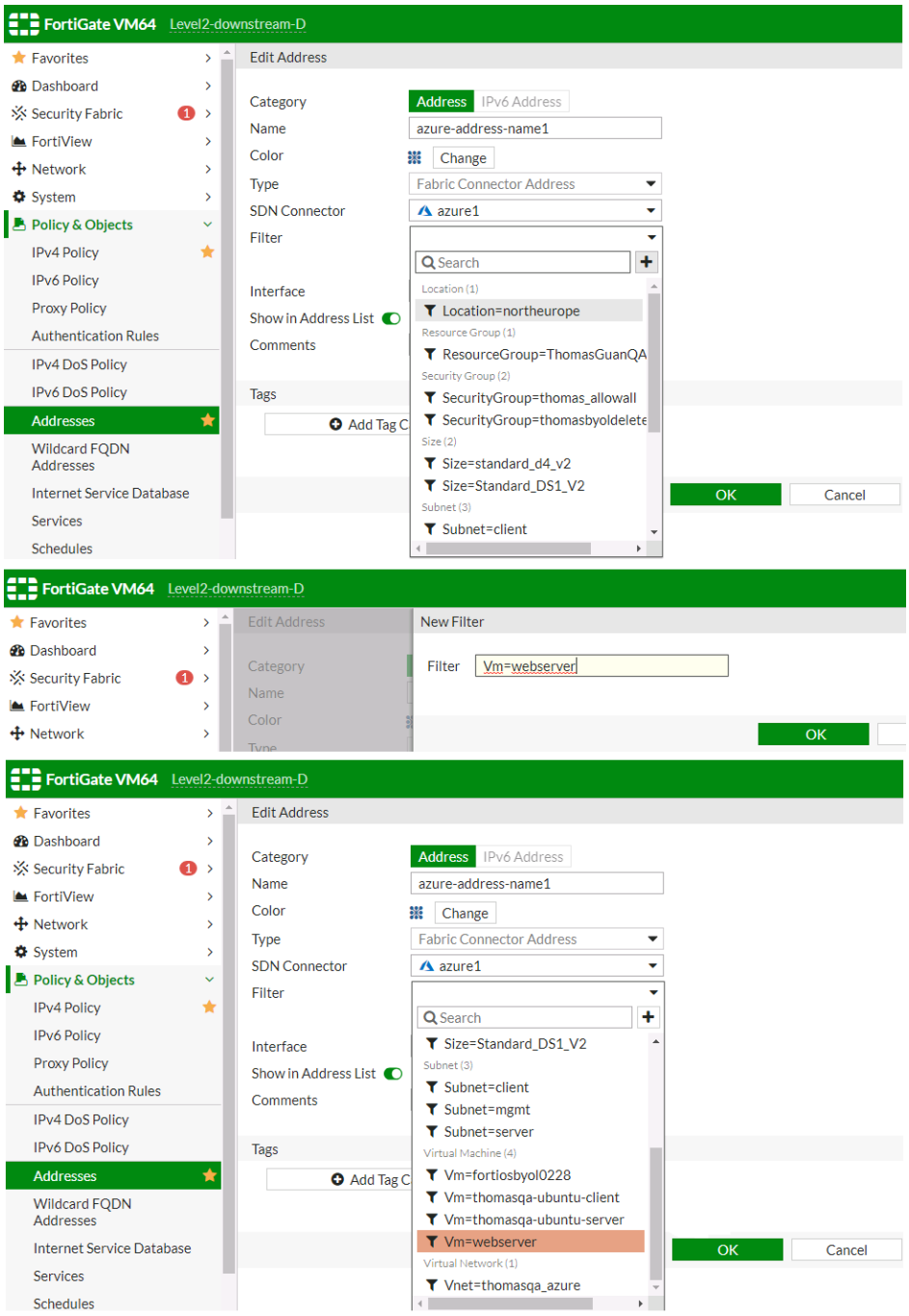
1. Navigate to *Policy & Objects* > *Addresses*.
2. Create or edit an SDN connector type dynamic IP address.
   Supported SDN connector types include: AWS, Azure, GCP, OpenStack, Kubernetes, and AliCloud. The example below is for an Azure SDN connector.
3. In the address *Filter* field, users can:
   - List all available filters in Omniselect.



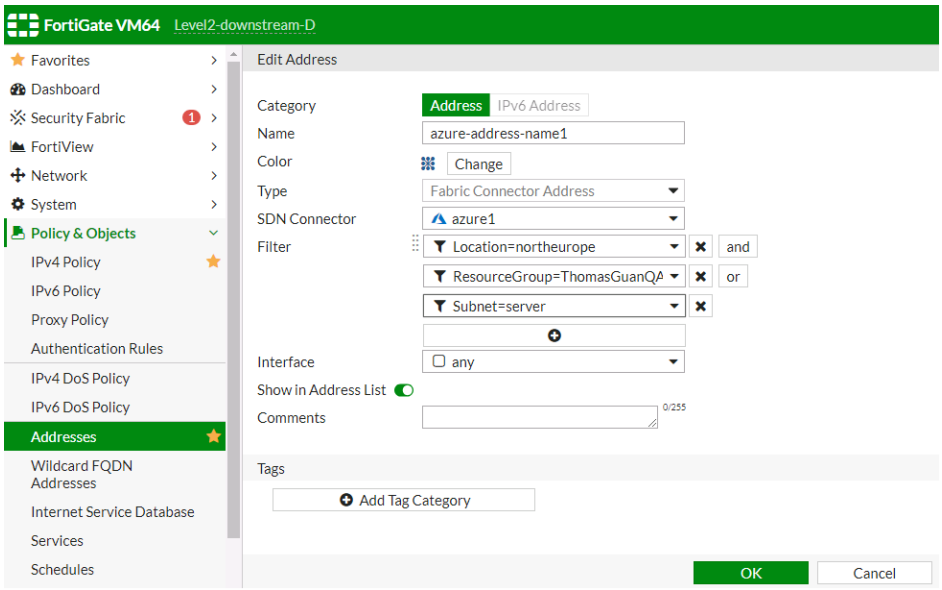
   - Search the available filters in Omniselect.



- Create custom filters in Omniselect.



- Set filter logic [and|or] in multiple Omniselects.



Cloud Connector - AliCloud

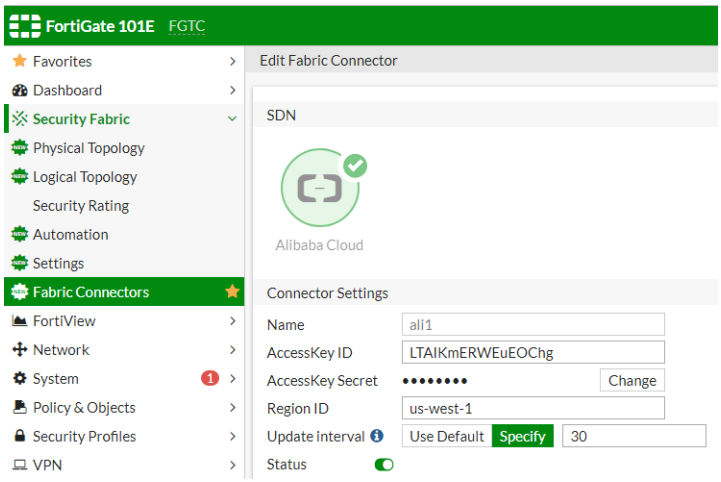
FortiOS now supports automatically updating dynamic addresses for AliCloud using an AliCloud SDN connector, including mapping the following attributes from AliCloud instances to dynamic address groups in FortiOS:

- ImageId
- InstanceId
- SecurityGroupId
- VpcId
- VSwitchId
- TagKey
- TagValue

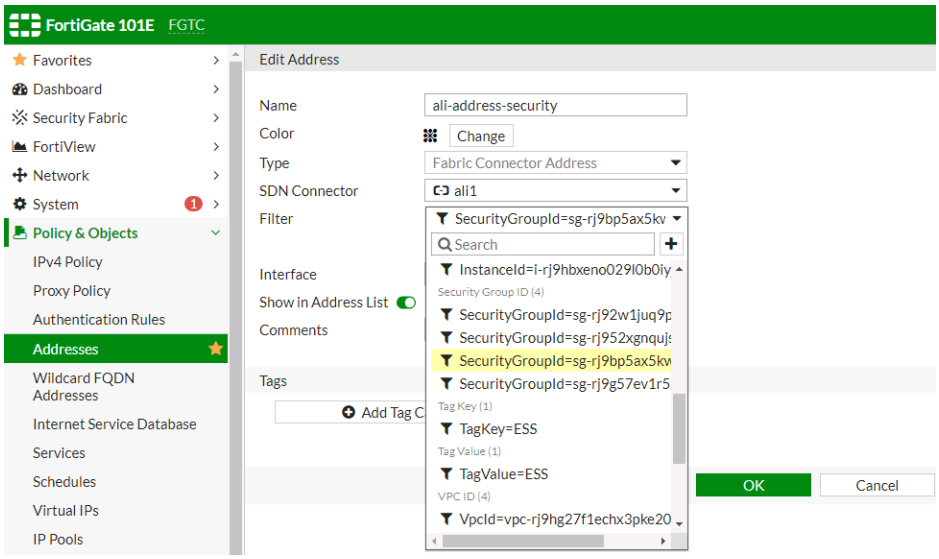
To configure AliCloud SDN connector using the GUI:

1. Configure the AliCloud SDN connector:
   a. Go to *Security Fabric* > *Fabric Connectors*.
   b. Click *Create New*, and select *Alibaba Cloud*.
   c. Configure as shown, substituting the access key, secret, and region ID for your deployment. The update

interval is in seconds.

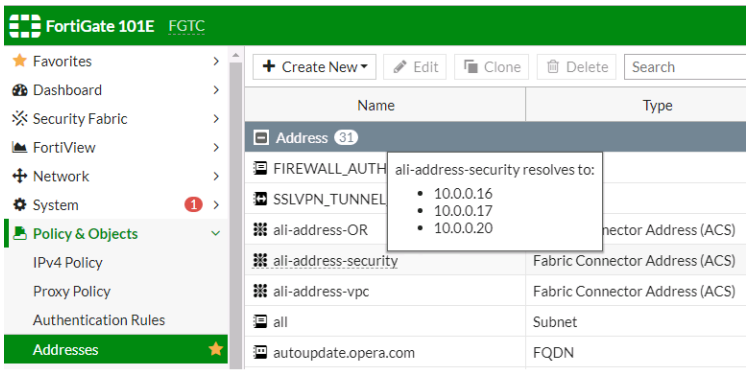


2. Create a dynamic firewall address for the configured AliCloud SDN connector:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Click *Create New*, then select *Address*.
   c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list. In this example, the AliCloud SDN Connector will automatically populate and update IP addresses only for instances that belong to the specified security group:



3. Ensure that the AliCloud SDN connector resolves dynamic firewall IP addresses:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Hover over the address created in step 2 to see a list of IP addresses for instances that belong to the security

group configured in step 2:



To configure AliCloud SDN connector using CLI commands:

1. Configure the AliCloud SDN connector:

```
config system sdn-connector
   edit "ali1"
      set type acs
      set access-key "LTAIKmERWEuEOChg"
      set secret-key xxxxx
      set region "us-west-1"
      set update-interval 30
   next
end
```

2. Create a dynamic firewall address for the configured AliCloud SDN connector with the supported AliCloud filter. In this example, the AliCloud SDN Connector will automatically populate and update IP addresses only for instances that belong to the specified security group:

```
config firewall address
   edit "ali-address-security"
      set type dynamic
      set sdn "ali1"
      set filter "SecurityGroupId=sg-rj9bp5ax5kwy3gqdizqb"
   next
end
```

3. Confirm that the AliCloud SDN connector resolves dynamic firewall IP addresses using the configured filter:

```
config firewall address
   edit "ali-address-security"
      set uuid 62a76df2-18f6-51e9-b555-360b18359ebe
      set type dynamic
      set sdn "ali1"
      set filter "SecurityGroupId=sg-rj9bp5ax5kwy3gqdizqb"
      config list
         edit "10.0.0.16"
         next
         edit "10.0.0.17"
         next
         edit "10.0.0.20"
         next
      end
   next
end
```

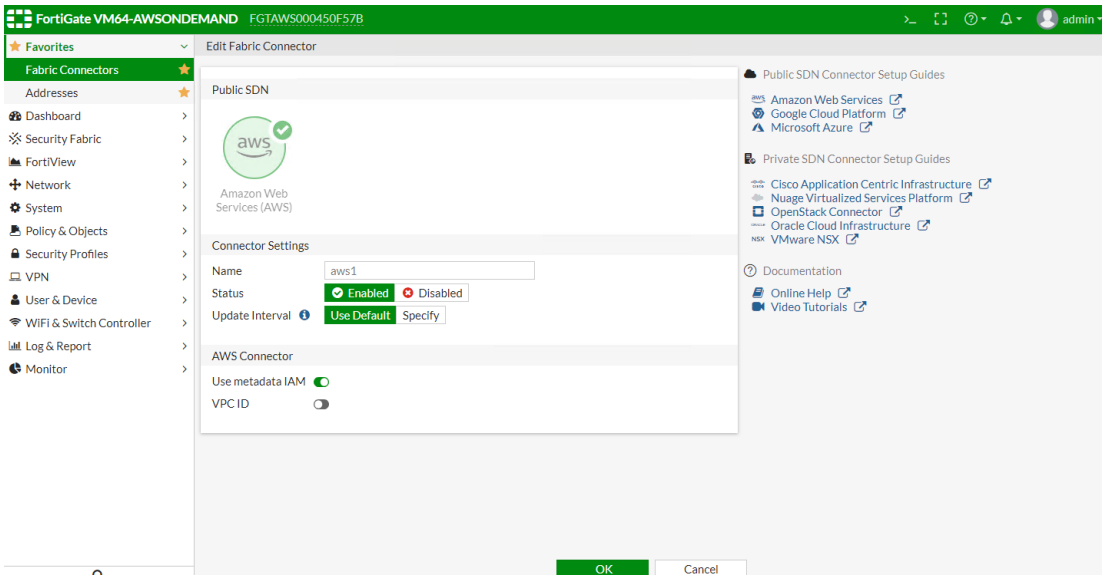
Cloud Connector - AWS - IAM Support

For instances running in AWS (on demand or BYOL), you can now set up the AWS connector by using AWS Identify and Access Management (IAM) credentials.

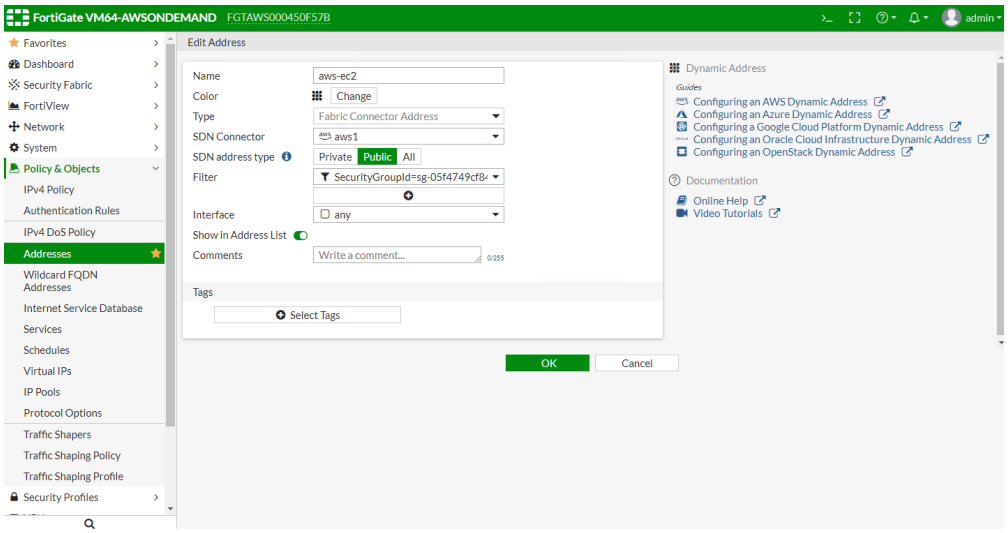
IAM authentication is available only for FGT-AWS and FGT-AWSONDEMAND platforms.

To configure AWS SDN connector using the GUI:

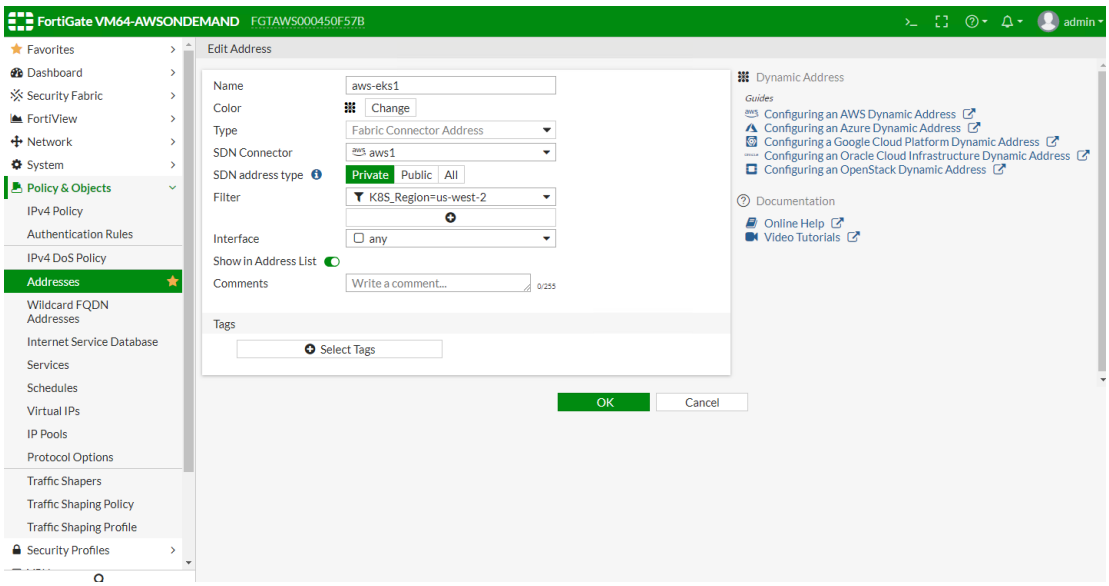
1. Configure the AWS SDN connector:
   a. Go to *Security Fabric* > *Fabric Connectors*.
   b. Click *Create New*, and select *Amazon Web Services (AWS)*.
   c. Configure as shown:



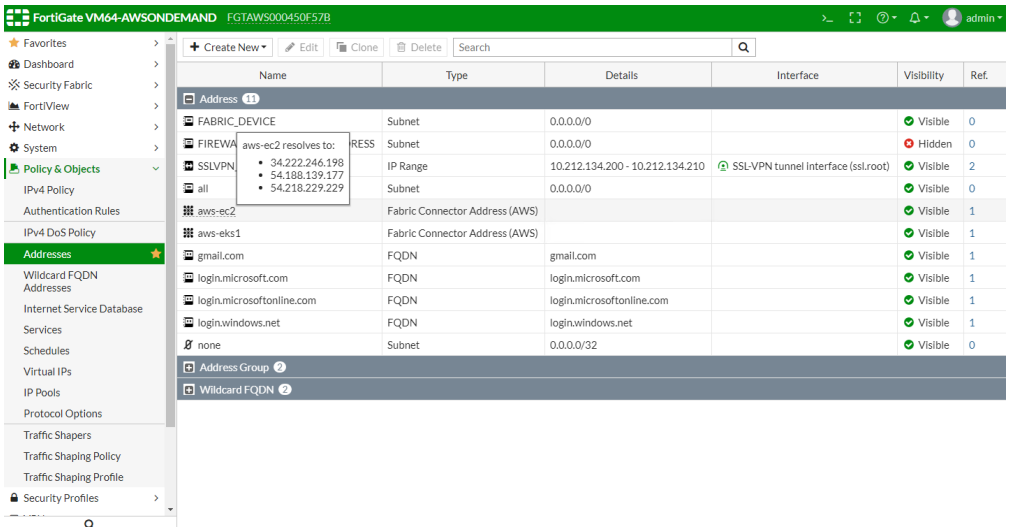
2. Create a dynamic firewall address for the configured AWS SDN connector:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Click *Create New*, then select *Address*.
   c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list. Following is an example for a public SDN address type:



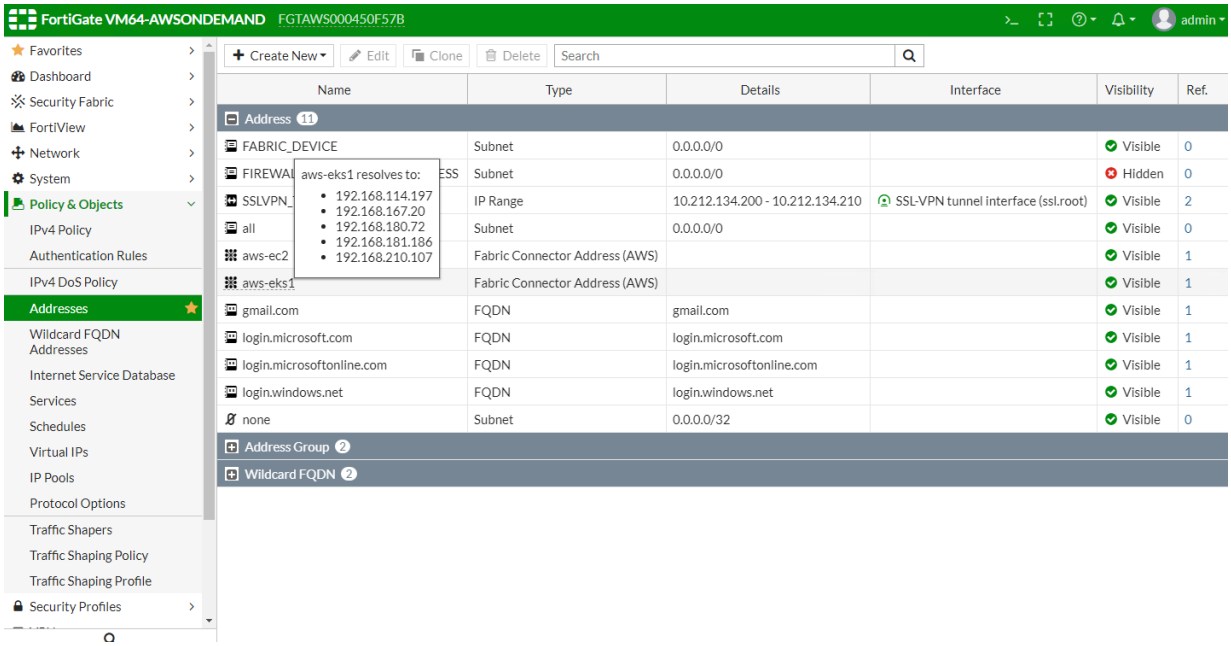
Following is an example for a private SDN address type:



3. Ensure that the AWS SDN connector resolves dynamic firewall IP addresses:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Hover over the address created in step 2 to see a list of IP addresses for instances that belong to the security group configured in step 2.
   Following is an example for a public SDN address type:



Following is an example for a private SDN address type:



To configure AWS SDN connector using CLI commands:

1. Configure the AWS connector:

```
config system sdn-connector
   edit "aws1"
      set status enable
      set type aws
      set use-metadata-iam enable
      set update-interval 60
   next
end
```

2. Create a dynamic firewall address for the configured AWS SDN connector with the supported filter: Dynamic firewall address IPs are resolved by the SDN connector.

```
config firewall address
```

```
    edit "aws-ec2"
       set type dynamic
       set sdn "aws1"
       set filter "SecurityGroupId=sg-05f4749cf84267548"
       set sdn-addr-type public
    next
    edit "aws-eks1"
       set type dynamic
       set sdn "aws1"
       set filter "K8S_Region=us-west-2"
    next
end
```

3. Confirm that the AWS SDN connector resolves dynamic firewall IP addresses using the configured filter:

```
config firewall address
    edit "aws-ec2"
       set uuid e756e786-3a2e-51e9-9d40-9492098de42d
       set type dynamic
       set sdn "aws1"
       set filter "SecurityGroupId=sg-05f4749cf84267548"
       set sdn-addr-type public
       config list
          edit "34.222.246.198"
          next
          edit "54.188.139.177"
          next
          edit "54.218.229.229"
          next
       end
    next
    edit "aws-eks1"
       set uuid d84589aa-3a10-51e9-b1ac-08145abce4d6
       set type dynamic
       set sdn "aws1"
       set filter "K8S_Region=us-west-2"
       config list
          edit "192.168.114.197"
          next
          edit "192.168.167.20"
          next
          edit "192.168.180.72"
          next
          edit "192.168.181.186"
          next
          edit "192.168.210.107"
          next
       end
    next
end
```

SDN Connector - VMware ESXi

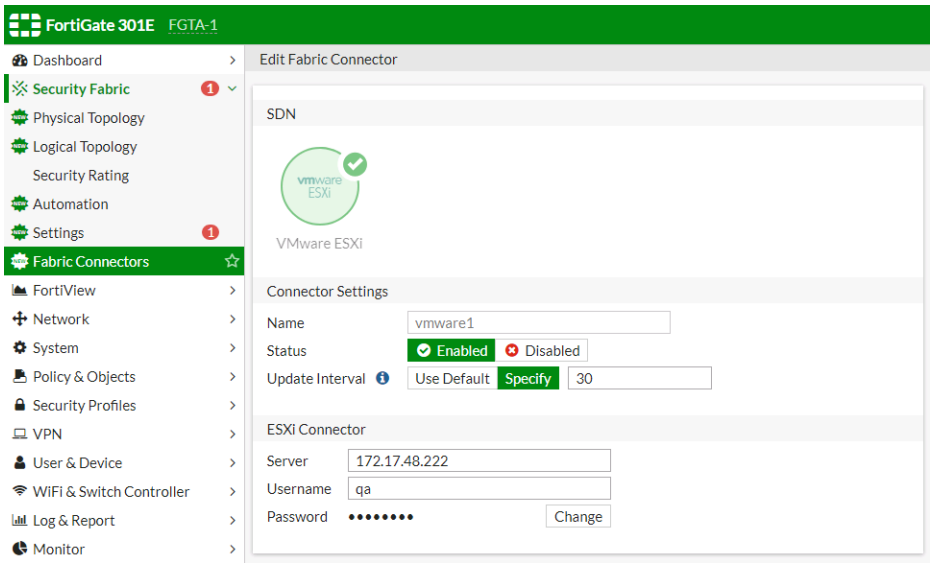
FortiOS now supports automatically updating dynamic addresses for VMware ESXi and vCenter servers using a VMware ESXi SDN connector, including mapping the following attributes from VMware ESXi and vCenter objects to dynamic

address groups in FortiOS:

- vmid
- host
- name
- uuid
- vmuuid
- vmnetwork
- guestid
- guestname
- annotation

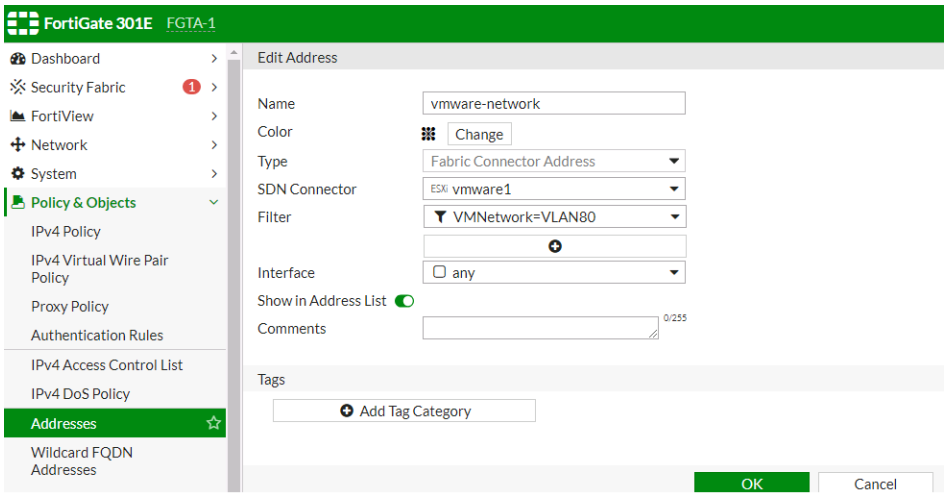
To configure VMware ESXi SDN connector using the GUI:

1. Configure the VMware ESXi SDN connector:
   a. Go to *Security Fabric* > *Fabric Connectors*.
   b. Click *Create New*, and select *VMware ESXi*.
   c. Configure as shown, substituting the server IP address, username, and password for your deployment. The update interval is in seconds.

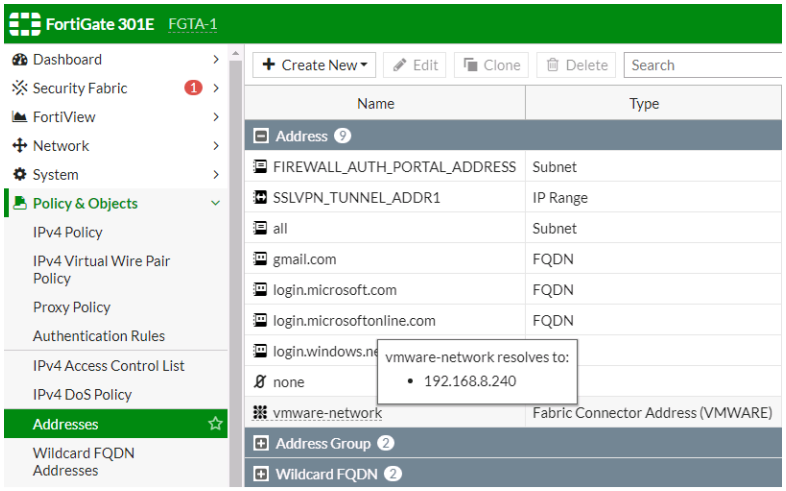


2. Create a dynamic firewall address for the configured VMware ESXi SDN connector:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Click *Create New*, then select *Address*.
   c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list. In this example, the VMware ESXi SDN Connector will automatically populate and update IP addresses only for instances that

belong to VLAN80:



3. Ensure that the VMware ESXi SDN connector resolves dynamic firewall IP addresses:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Hover over the address created in step 2 to see a list of IP addresses for instances that belong to VLAN80 as configured in step 2:



To configure VMware ESXi SDN connector using CLI commands:

1. Configure the VMware ESXi SDN connector:

```
config system sdn-connector
   edit "vmware1"
      set type vmware
      set server "172.17.48.222"
      set username "example_username"
      set password xxxxx
      set update-interval 30
   next
end
```

2. Create a dynamic firewall address for the configured VMware ESXi SDN connector with the supported VMware ESXi filter. In this example, the VMware ESXi SDN Connector will automatically populate and update IP addresses only for instances that belong to the specified VLAN:

```
config firewall address
```

```
    edit "vmware-network"
       set type dynamic
       set sdn "vmware1"
       set filter "vmnetwork=VLAN80"
    next
end
```

3. Confirm that the VMware ESXi SDN connector resolves dynamic firewall IP addresses using the configured filter:

```
config firewall address
    edit "vmware-network"
       set uuid abfa1748-1b80-51e9-d0fd-ea322b3bba2d
       set type dynamic
       set sdn "vmware1"
       set filter "vmnetwork=VLAN80"
       config list
          edit "192.168.8.240"
          next
       end
    next
end
```

Kubernetes (K8s)

This section lists the new features added to FortiOS for Kubernetes.

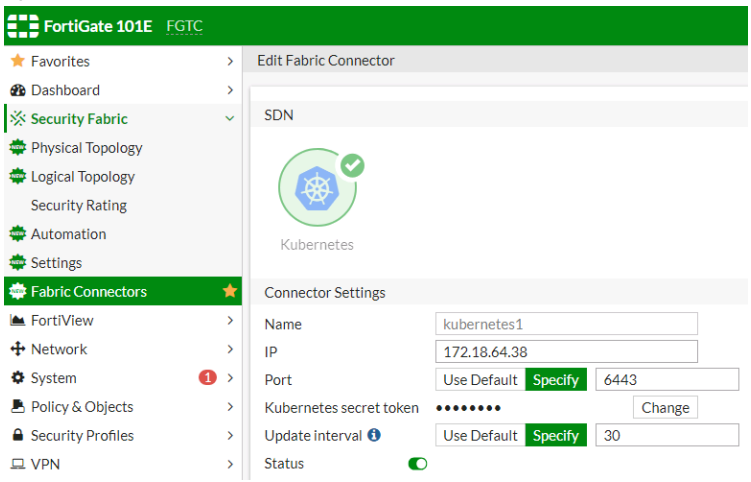
Private Cloud K8s Connector

FortiOS now supports automatically updating dynamic addresses for Kubernetes (K8S) using a K8S SDN connector, enabling FortiOS to manage K8S pods as global address objects, as with other connectors. This includes mapping the following attributes from K8S instances to dynamic address groups in FortiOS:

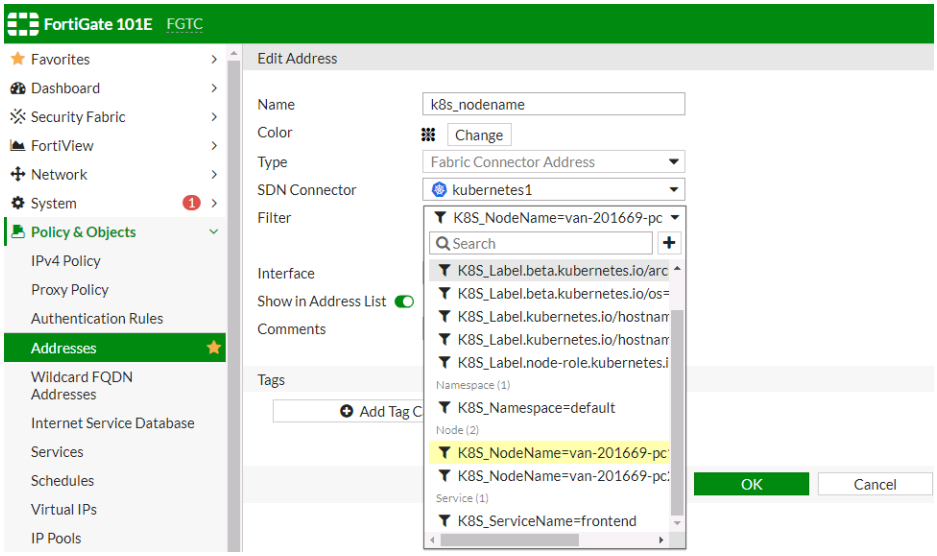
Filter	Description
Namespace	Filter service IP addresses in a given namespace.
ServiceName	Filter service IP addresses by the given service name.
NodeName	Filter node IP addresses by the given node name.
Label.XXX	Filter service or node IP addresses with the given label XXX.

To configure K8S SDN connector using the GUI:

1. Configure the K8S SDN connector:
   a. Go to *Security Fabric* > *Fabric Connectors*.
   b. Click *Create New*, and select *Kubernetes*.
   c. Configure as shown substituting the IP address, port number, and secret token for your deployment. The update interval is in seconds.

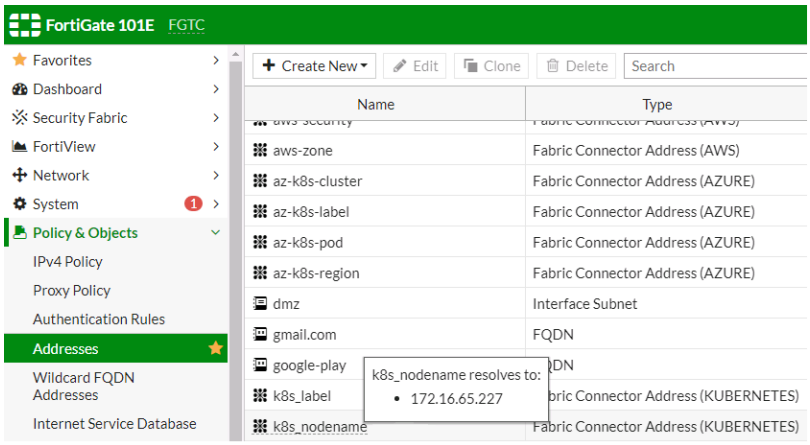


2. Create a dynamic firewall address for the configured K8S SDN connector:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Click *Create New*, then select *Address*.
   c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list. In this example, the K8S SDN connector will automatically populate and update IP addresses only for node instances that match the specified node name:



3. Ensure that the K8S SDN connector resolves dynamic firewall IP addresses:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Hover over the address created in step 2 to see a list of IP addresses for node instances that match the node

name configured in step 2:



To configure K8S SDN connector using CLI commands:

1. Configure the K8S SDN connector:

```
config system sdn-connector
   edit "kubernetes1"
      set type kubernetes
      set server "172.18.64.38"
      set server-port 6443
      set secret-token xxxxx
      set update-interval 30
   next
end
```

2. Create a dynamic firewall address for the configured K8S SDN connector with the supported K8S filter. In this example, the K8S SDN connector will automatically populate and update IP addresses only for node instances that match the specified node name:

```
config firewall address
   edit "k8s_nodename"
      set type dynamic
      set sdn "kubernetes1"
      set filter "K8S_NodeName=van-201669-pc1"
   next
end
```

3. Confirm that the K8S SDN connector resolves dynamic firewall IP addresses using the configured filter:

```
config firewall address
   edit "k8s_nodename"
      set uuid 462112a2-1ab1-51e9-799c-652621ba8c0c
      set type dynamic
      set sdn "kubernetes1"
      set filter "K8S_NodeName=van-201669-pc1"
      config list
         edit "172.16.65.227"
         next
      end
   next
end
```

AWS Kubernetes (EKS) Connector

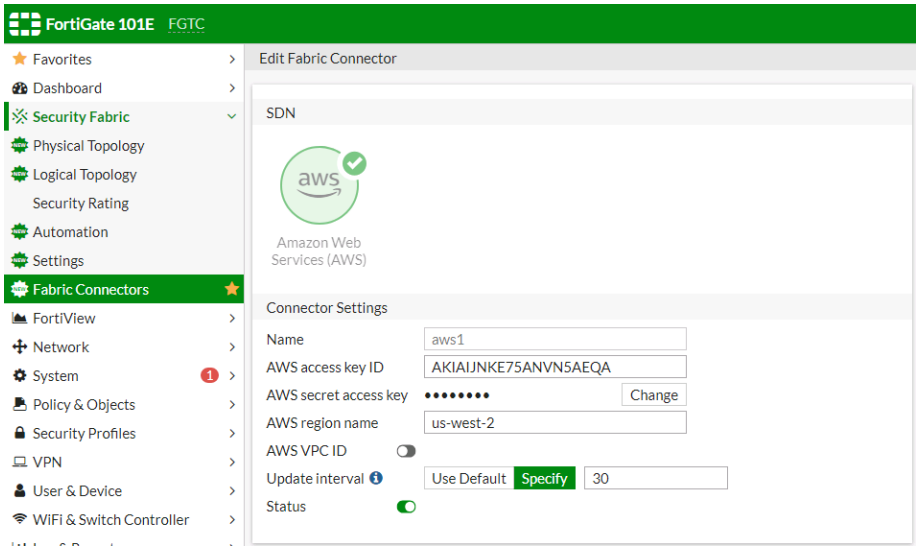
This feature extends the existing AWS SDN connector to support dynamic address groups based on AWS Kubernetes (EKS) filters.

To filter out the Kubernetes IP addresses, the following address filters have been introduced:

k8s_cluster	Name of Kubernetes cluster.
k8s_namespace	Namespace of a Kubernetes service or pod.
k8s_svcname	Name of a Kubernetes service.
k8s_nodename	Name of a Kubernetes node.
k8s_zone	Zone of a Kubernetes node.
k8s_region	Region of a Kubernetes node.
k8s_podname	Name of a Kubernetes pod.
k8s_label.xxx	Name of label of a Kubernetes resource (cluster/service/node/Pod).

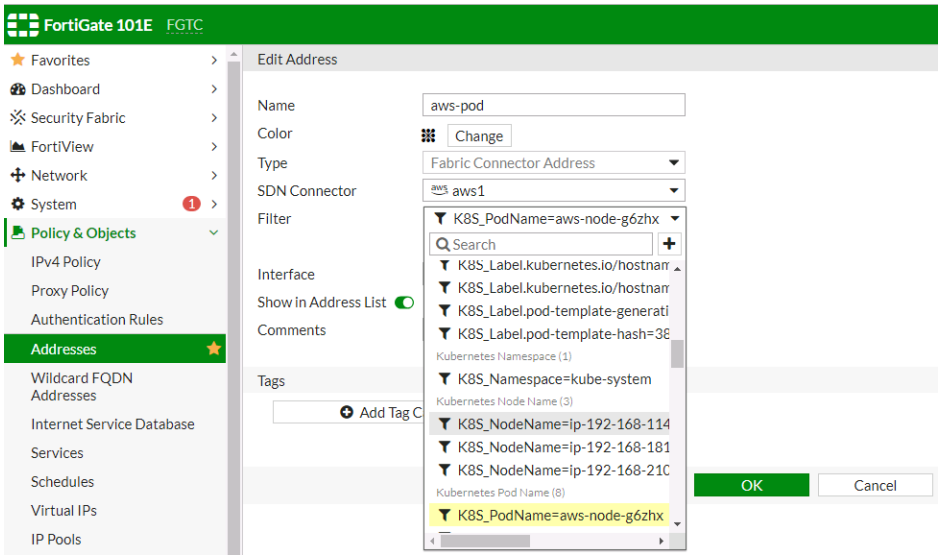
To enable an AWS SDN connector to fetch IP addresses from AWS Kubernetes:

1. In *Fabric Connectors*, configure an SDN connector for AWS Kubernetes.

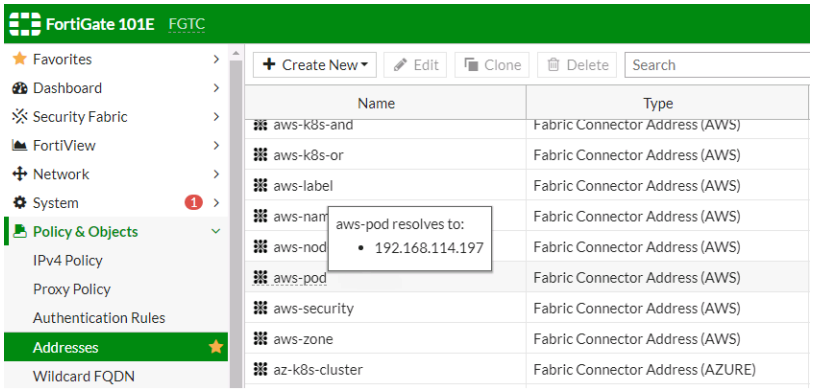


2. Go to *Policies & Objects* > *Addresses* and create a dynamic firewall address for the configured SDN connector using the supported Kubernetes filter.

3. To filter out the Kubernetes IP addresses, select the address filter or filters.



4. Configure the rest of the settings, then click *OK*.
The dynamic firewall address IP is resolved by the SDN connector.



To configure an AWS Kubernetes connector through the CLI:

1. Configure an SDN connector for Kubernetes:

```
config system sdn-connector
   edit "aws1"
      set type aws
      set access-key "AKIAIJNKE75ANVN5AEQA"
      set secret-key xxxxx
      set region "us-west-2"
      set update-interval 30
   next
end
```

2. Create a dynamic firewall address for the SDN connector with a supported Kubernetes filter:

```
config firewall address
   edit "aws-pod"
      set type dynamic
      set sdn "aws1"
      set filter "K8S_PodName=aws-node-g6zhx"
   next
```

```
    end
```

The dynamic firewall address IP is resolved by the SDN connector:

```
config firewall address
   edit "aws-pod"
      set uuid a7a37298-19e6-51e9-851a-2c551ffc174d
      set type dynamic
      set sdn "aws1"
      set filter "K8S_PodName=aws-node-g6zhx"
      config list
         edit "192.168.114.197"
         next
      end
   next
end
```

Azure Kubernetes (AKS) Connector

This feature extends the existing Azure SDN connector to support dynamic address groups based on Azure Kubernetes (AKS) filters.

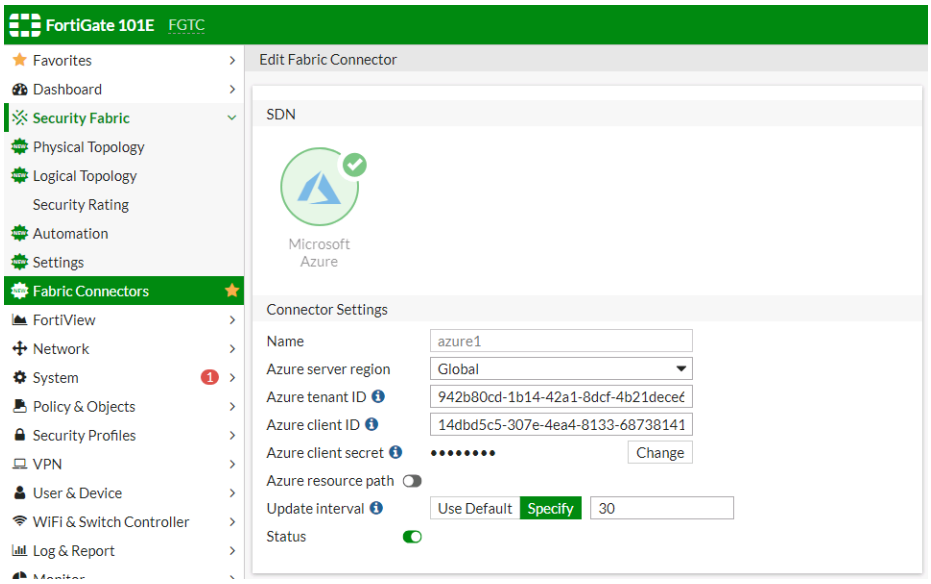
To filter out the Kubernetes IP addresses, the following address filters have been introduced:

k8s_cluster	Kubernetes cluster name.
k8s_namespace	Namespace of a Kubernetes service or pod.
k8s_svcname	Kubernetes service name.
k8s_nodename	Kubernetes node name.
k8s_region	Kubernetes node region.
k8s_podname	Kubernetes pod name.
k8s_label.xxx	Name of label of a Kubernetes resource (cluster/service/node/Pod).

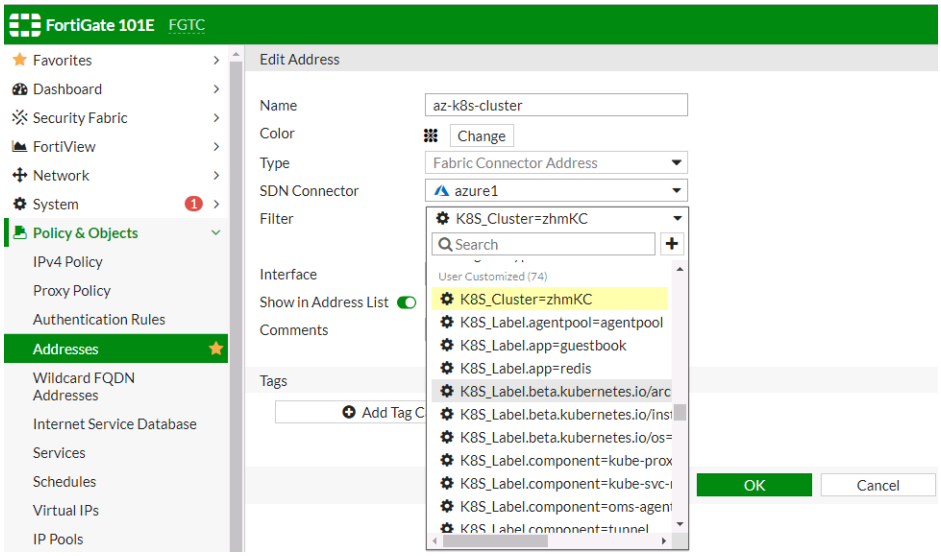
To enable an Azure SDN connector to fetch IP addresses from Azure Kubernetes:

1. Configure the Azure SDN connector:
   a. Go to *Security Fabric* > *Fabric Connectors*.
   b. Click *Create New*, and select *Azure*.
   c. Configure as shown substituting the region, tenant and client IDs, and client secret for your deployment. The

update interval is in seconds.

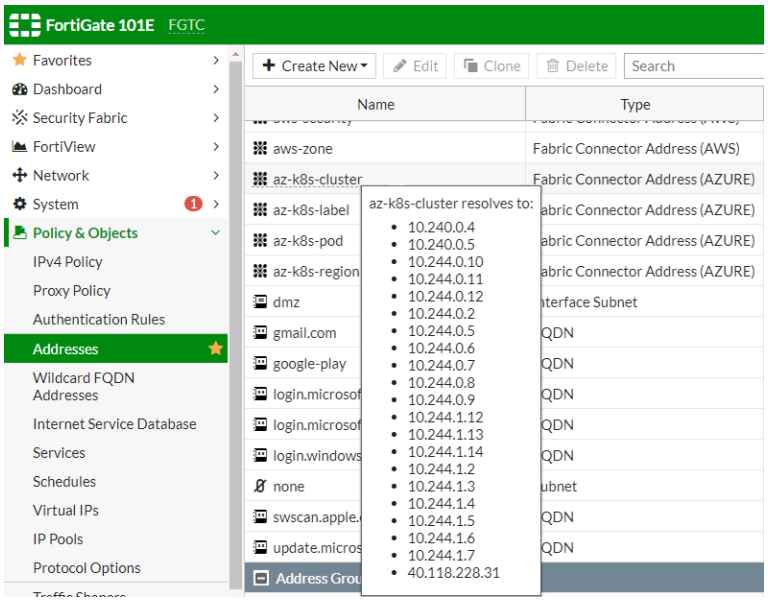


2. Create a dynamic firewall address for the configured K8S SDN connector:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Click *Create New*, then select *Address*.
   c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list. In this example, the Azure SDN connector will automatically populate and update IP addresses only for instances that belong to the zhmKC cluster:



3. Ensure that the K8S SDN connector resolves dynamic firewall IP addresses:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Hover over the address created in step 2 to see a list of IP addresses for instances that belong to the

zhmKC cluster as configured in step 2:



To configure an Azure Kubernetes connector through the CLI:

1. Configure an SDN connector for Kubernetes:

```
config system sdn-connector
   edit "azure1"
      set type azure
      set tenant-id "942b80cd-1b14-42a1-8dcf-4b21dece61ba"
      set client-id "14dbd5c5-307e-4ea4-8133-68738141feb1"
      set client-secret xxxxx
      set update-interval 30
   next
end
```

2. Create a dynamic firewall address for the SDN connector with a supported Kubernetes filter. In this example, the Azure SDN connector will automatically populate and update IP addresses only for instances that belong to the zhmKC cluster:

```
config firewall address
   edit "az-k8s-cluster"
      set type dynamic
      set sdn "azure1"
      set filter "K8S_Cluster=zhmKC"
   next
end
```

3. Confirm that the Azure SDN connector resolves dynamic firewall IP addresses using the configured filter: :

```
config firewall address
   edit "az-k8s-cluster"
      set uuid c3859270-1919-51e9-4a99-47d8caf97a01
      set type dynamic
      set sdn "azure1"
      set filter "K8S_Cluster=zhmKC"
      config list
         edit "10.240.0.4"
         next
         edit "10.240.0.5"
```

```
            next
            edit "10.244.0.10"
            next
        end
    next
end
```

GCP Kubernetes (GKE) Connector

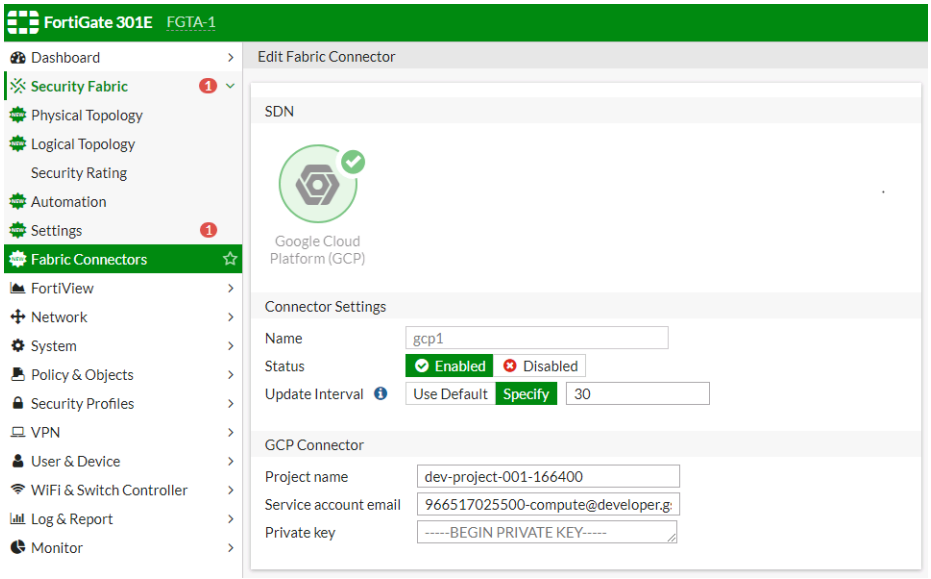
This feature extends the existing Google Cloud Platform (GCP) SDN connector to support dynamic address groups based on GCP Kubernetes Engine (GKE) filters.

To filter out the Kubernetes IP addresses, the following address filters have been introduced:

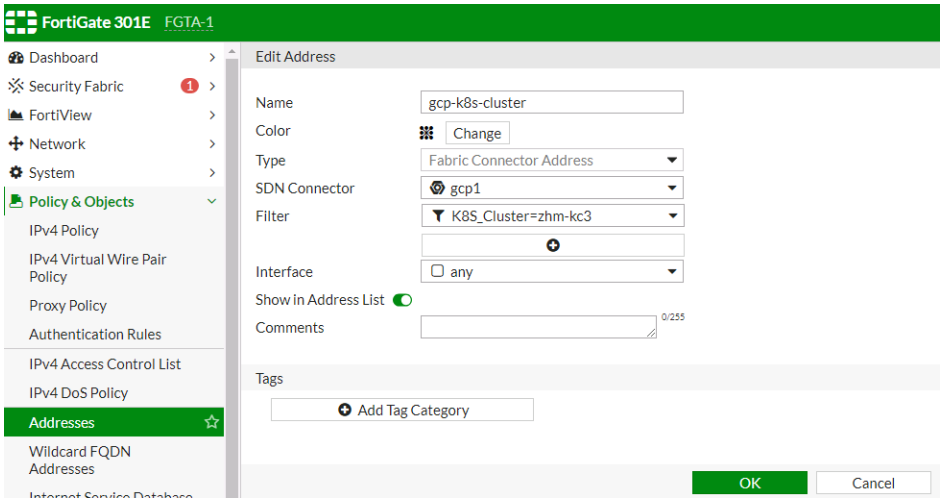
k8s_cluster	Name of Kubernetes cluster.
k8s_nodepool	Name of node pool for a Kubernetes cluster.
k8s_namespace	Namespace of a Kubernetes service or pod.
k8s_servicename	Name of a Kubernetes service.
k8s_nodename	Name of a Kubernetes node.
k8s_zone	Zone of a Kubernetes node.
k8s_region	Region of a Kubernetes node.
k8s_podname	Name of a Kubernetes pod.
k8s_label.xxx	Name of label of a Kubernetes resource (cluster/service/node/Pod).

To enable a GCP SDN connector to fetch IP addresses from GKE:

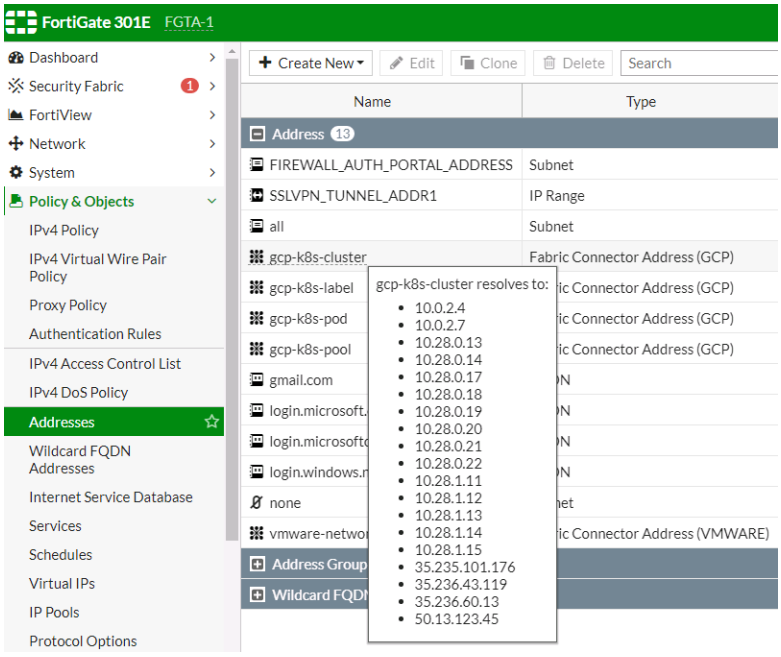
1. In *Fabric Connectors*, configure an SDN connector for GCP.



2. Go to *Policies & Objects* > *Addresses* and create a dynamic firewall address for the configured SDN connector using the supported Kubernetes filter.
3. To filter out the Kubernetes IP addresses, select the address filter or filters. In this example, the GCP SDN connector will automatically populate and update IP addresses only for instances that belong to the zhm-kc3 cluster:



4. Configure the rest of the settings, then click *OK*.
   The dynamic firewall address IP is resolved by the SDN connector.



To configure a GCP Kubernetes connector through the CLI:

1. Configure an SDN connector for Kubernetes:

```
config system sdn-connector
   edit "gcp1"
      set type gcp
      set gcp-project "dev-project-001-166400"
      set service-account "966517025500-compute@developer.gserviceaccount.com"
```

```
        set update-interval 30
    next
end
```

2. Create a dynamic firewall address for the SDN connector with a supported Kubernetes filter:

```
config firewall address
    edit "gcp-k8s-cluster"
        set type dynamic
        set sdn "gcp1"
        set filter "K8S_Cluster=zhm-kc3"
    next
end
```

The dynamic firewall address IP is resolved by the SDN connector:

```
config firewall address
    edit "gcp-k8s-cluster"
        set uuid e4a1aa3c-25be-51e9-e9af-78ab2eebe6ee
        set type dynamic
        set sdn "gcp1"
        set filter "K8S_Cluster=zhm-kc3"
        config list
            edit "10.0.2.4"
            next
            edit "10.0.2.7"
            next
            edit "10.28.0.13"
            next
        end
    next
end
```

Oracle Kubernetes (OKE) Connector

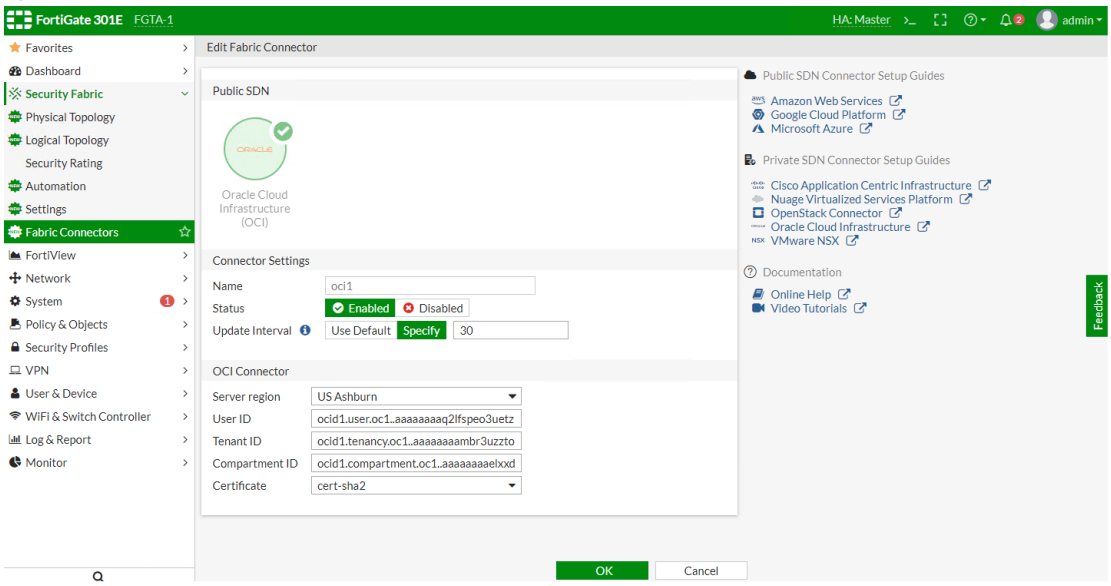
This project extends the existing SDN connector for OCI to support dynamic address groups based on Oracle Kubernetes (OKE) filters.

To filter out the Kubernetes IP addresses, the following address filters have been introduced:

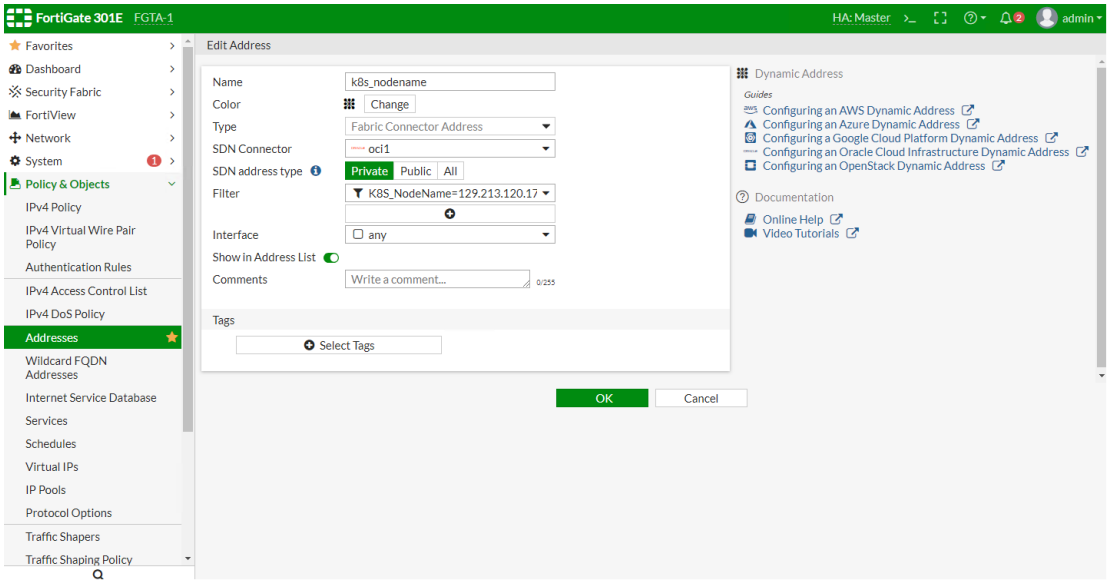
k8s_compartment	Name of compartment that the Kubernetes cluster created in.
k8s_cluster	Name of Kubernetes cluster.
k8s_namespace	Namespace of a Kubernetes service or pod.
k8s_servicename	Name of a Kubernetes service.
k8s_nodename	Name of a Kubernetes node.
k8s_region	Region of a Kubernetes node.
k8s_zone	Zone of a Kubernetes node.
k8s_podname	name of a Kubernetes pod.
k8s_label.xxx	Name of label of a Kubernetes resource (cluster/service/node/Pod)

To enable an OCI SDN connector to fetch IP addresses from Oracle Kubernetes:

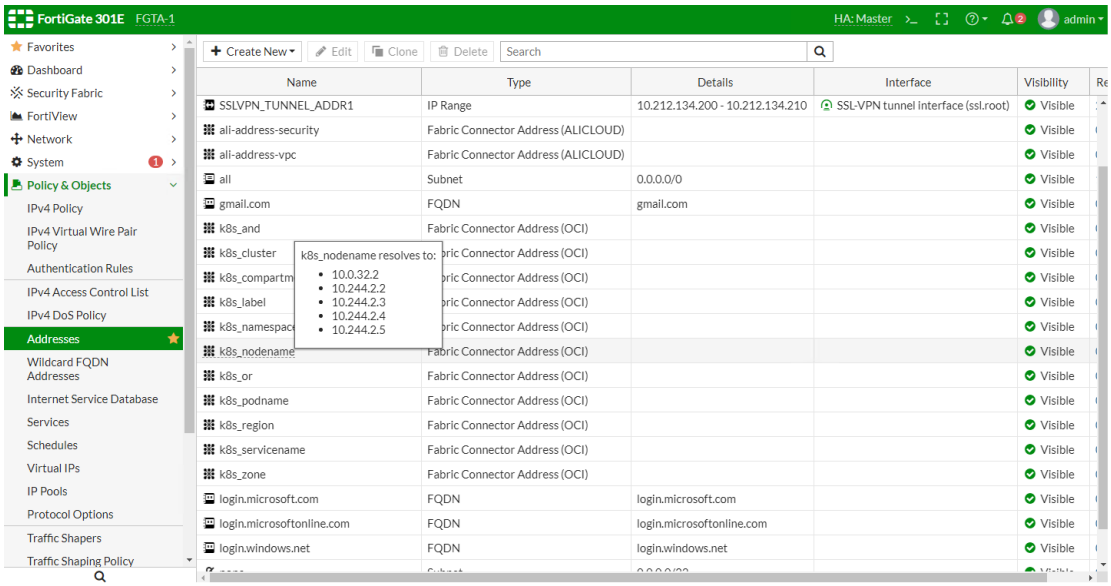
1. Configure the OCI SDN connector:
   a. Go to *Security Fabric* > *Fabric Connectors*.
   b. Click *Create New*, and select *Oracle Cloud Infrastructure (OCI)*.
   c. Configure as shown substituting the region, tenant and client IDs, and client secret for your deployment. The update interval is in seconds.



2. Create dynamic firewall addresses for the configured SDN connector with supported Kubernetes filter:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Click *Create New*, then select *Address*.
   c. Configure the addresses.



3. Confirm that the SDN connector resolves dynamic firewall IP addresses:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Hover over the address created in step 2 to see a list of IP addresses for instances:



To configure an SDN connector through the CLI:

1. Configure the OCI SDN connector:

```
config system sdn-connector
   edit "oci1"
      set type oci
      set tenant-id
           "ocid1.tenancy.oc1..aaaaaaaambr3uzztoyhweohbzqqdo775h7d3t54zpmzkp4b2cf35vs55c
           xxx"
      set user-id
           "ocid1.user.oc1..aaaaaaaaq2lfspeo3uetzbzpiv2pqvzzevozccnys347stwssvizqlatfxx
           x"
      set compartment-id
           "ocid1.compartment.oc1..aaaaaaaaelxxdjazqo7nzczpgypyiqcgkmytjry6nfq5345vw7eav
           pwnmxxx"
      set oci-region ashburn
      set oci-cert "cert-sha2"
      set update-interval 30
   next
end
```

2. Create dynamic firewall addresses for the configured SDN connector with supported Kubernetes filter:

```
config firewall address
   edit "k8s_nodename"
      set type dynamic
      set sdn "oci1"
      set filter "K8S_NodeName=129.213.120.172"
   next
end
```

3. Confirm that the SDN connector resolves dynamic firewall IP addresses:

```
config firewall address
   edit "k8s_nodename"
      set uuid 052f1420-3ab8-51e9-0cf8-6db6bc3395c0
```

```
        set type dynamic
        set sdn "oci1"
        set filter "K8S_NodeName=129.213.120.172"
        config list
           edit "10.0.32.2"
           next
           edit "10.244.2.2"
           next
           edit "10.244.2.3"
           next
           edit "10.244.2.4"
           next
           edit "10.244.2.5"
           next
        end
     next
  end
```

SDN Connector - Azure Stack

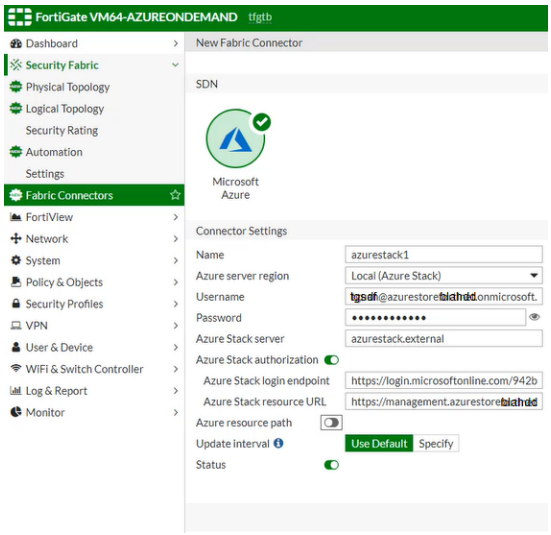
FortiOS now supports automatically updating dynamic addresses for Azure Stack on-premises environments using an Azure Stack SDN connector, including mapping the following attributes from Azure Stack instances to dynamic address groups in FortiOS:

- vm
- tag
- size
- securitygroup
- vnet
- subnet
- resourcegroup
- vmss

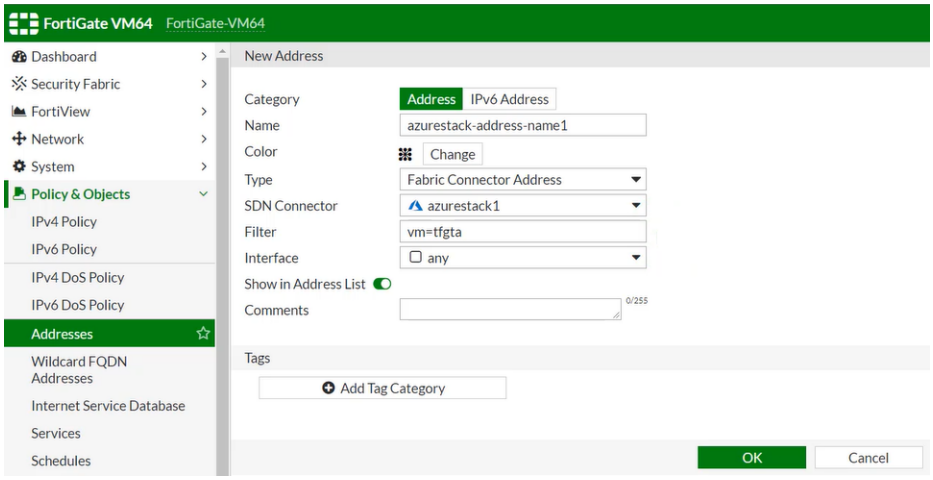
To configure Azure Stack SDN connector using the GUI:

1. Configure the Azure Stack SDN connector:
   a. Go to *Security Fabric* > *Fabric Connectors*.
   b. Click *Create New*, and select *Microsoft Azure*.
   c. Configure as shown, substituting the Azure Stack settings for your deployment. The update interval is in

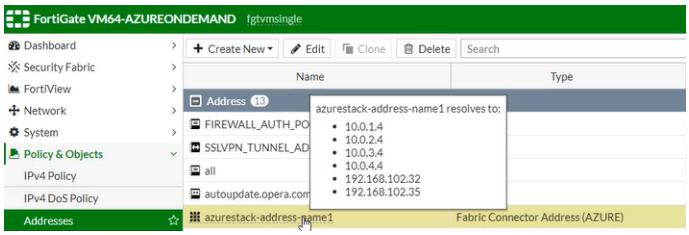
seconds.



2. Create a dynamic firewall address for the configured Azure Stack SDN connector:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Click *Create New*, then select *Address*.
   c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list. In this example, the Azure Stack SDN Connector will automatically populate and update IP addresses only for instances that are named tfgta:



3. Ensure that the Azure Stack SDN connector resolves dynamic firewall IP addresses:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Hover over the address created in step 2 to see a list of IP addresses for instances that are named tftgta as configured in step 2:



To configure Azure Stack SDN connector using CLI commands:

1. Configure the Azure Stack SDN connector:

```
config system sdn-connector
   edit "azurestack1"
      set type azure
      set azure-region local
      set server "azurestack.external"
      set username "username@azurestoreexamplecompany.onmicrosoft.com"
      set password xxxxx
      set log-in endpoint "https://login.microsoftonline.com/942b80cd-1b14-42a1-8dcf-
           4b21dece61ba"
      set resource-url
           "https://management.azurestoreexamplecompany.onmicrosoft.com/12b6fedd-9364-4cf0-
           822b-080d70298323"
      set update-interval 30
   next
end
```

2. Create a dynamic firewall address for the configured Azure Stack SDN connector with the supported Azure Stack filter. In this example, the Azure Stack SDN Connector will automatically populate and update IP addresses only for instances that are named tfgta:

```
config firewall address
   edit "azurestack-address-name1"
      set type dynamic
      set sdn "azurestack1"
      set filter "vm=tfgta"
   next
end
```

3. Confirm that the Azure Stack SDN connector resolves dynamic firewall IP addresses using the configured filter:

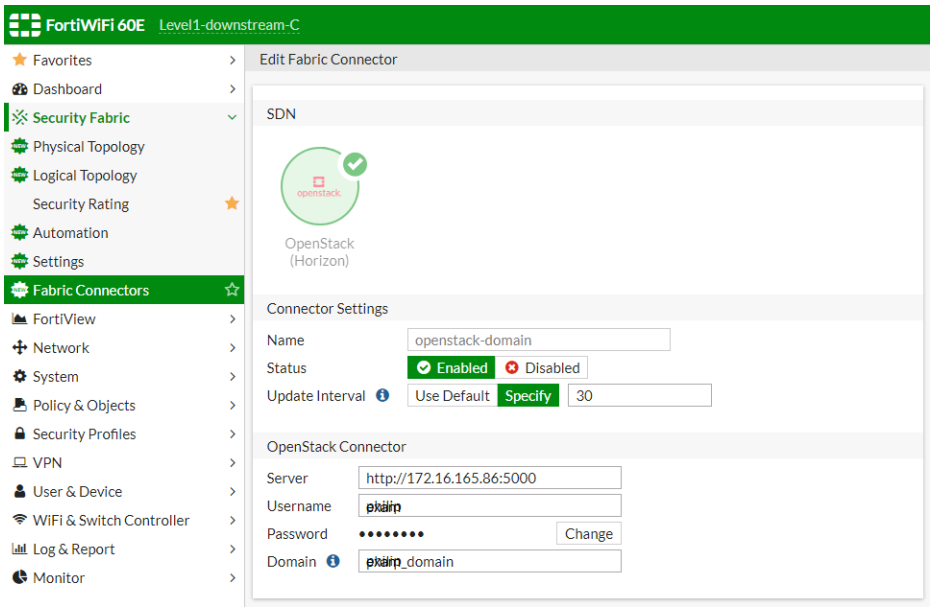
```
config firewall address
   edit "azurestack-address-name1"
      set type dynamic
      set sdn "azurestack1"
      set filter "vm=tfgta"
      config list
         edit "10.0.1.4"
         next
         edit "10.0.2.4"
         next
         edit "10.0.3.4"
         next
         edit "10.0.4.4"
         next
         edit "192.168.102.32"
         next
         edit "192.168.102.35"
         next
      end
   next
end
```

SDN Connector - OpenStack Domain Filter

A domain attribute is now available for selection when configuring an OpenStack SDN Connector in FortiOS. When a domain is configured for the OpenStack SDN Connector, FortiOS resolves OpenStack SDN dynamic firewall addresses from the specified OpenStack domain. If a domain is not specified, FortiOS resolves the dynamic firewall addresses using the default OpenStack domain.

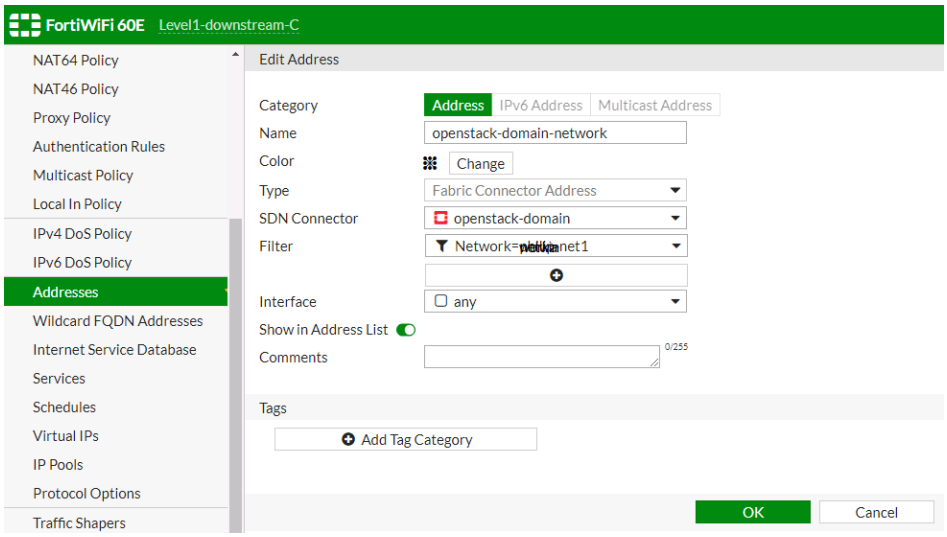
To configure OpenStack SDN connector with a domain using the GUI:

1. Configure the OpenStack SDN connector:
   a. Go to *Security Fabric* > *Fabric Connectors*.
   b. Click *Create New*, and select *Openstack (Horizon)*.
   c. In the *Domain* field, enter the desired domain name from OpenStack. The SDN Connector will only resolve IP addresses for instances that belong to the specified domain.
   d. Configure as shown, substituting the server IP address, username, and password for your deployment. The update interval is in seconds.

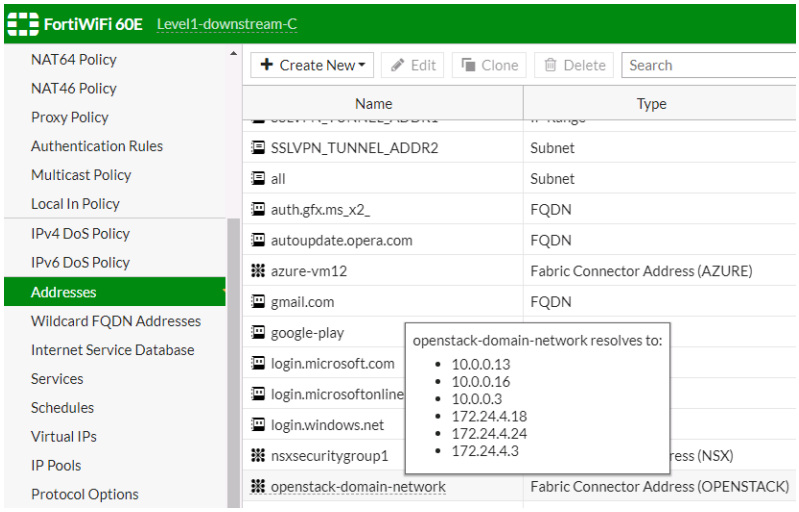


2. Create a dynamic firewall address for the configured OpenStack SDN connector:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Click *Create New*, then select *Address*.
   c. Configure the address as shown, selecting the desired filter in the *Filter* dropdown list. The OpenStack SDN Connector will automatically populate and update IP addresses only for instances that belong to the

specified domain and network:



3. Ensure that the OpenStack SDN connector resolves dynamic firewall IP addresses:
   a. Go to *Policy & Objects* > *Addresses*.
   b. Hover over the address created in step 2 to see a list of IP addresses for instances that belong to the specified domain and specified network as configured in steps 1 and 2:



To configure OpenStack SDN connector with a domain using CLI commands:

1. Configure the OpenStack SDN connector. The SDN Connector will only resolve IP addresses for instances that belong to the specified domain:

```
config system sdn-connector
   edit "openstack-domain"
      set type openstack
      set server "http://172.16.165.86:5000"
      set username "example_username"
      set password xxxxx
      set domain "example_domain"
      set update-interval 30
   next
end
```

2. Create a dynamic firewall address for the configured OpenStack SDN connector with the supported OpenStack filter. The OpenStack SDN Connector will automatically populate and update IP addresses only for instances that belong to the specified domain and the specified network:

```
config firewall address
   edit "openstack-domain-network"
      set type dynamic
      set sdn "openstack-domain"
      set filter "Network=example-net1"
   next
end
```

3. Confirm that the OpenStack SDN connector resolves dynamic firewall IP addresses using the configured domain and filter:

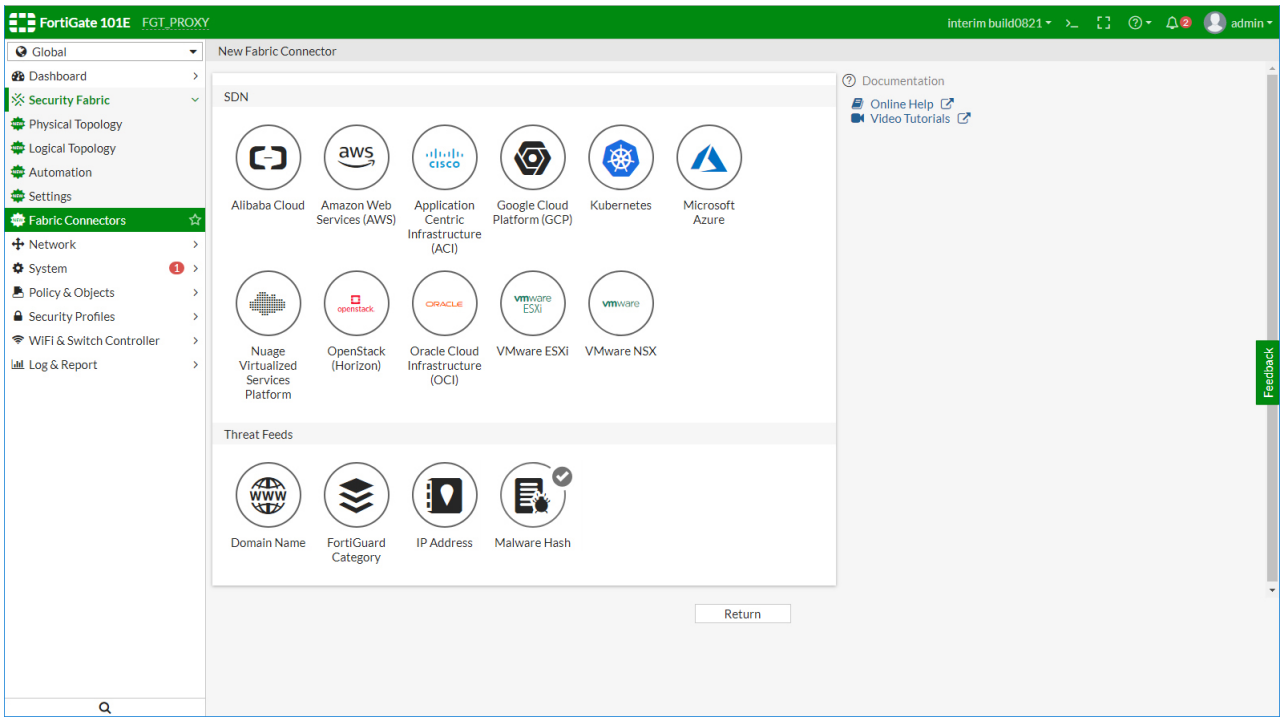
```
config firewall address
   edit "openstack-domain-network"
      set uuid 02837298-234d-51e9-efda-559c6001438a
      set type dynamic
      set sdn "openstack-domain"
      set filter "Network=example-net1"
      config list
         edit "10.0.0.13"
         next
         edit "10.0.0.16"
         next
         edit "10.0.0.3"
         next
         edit "172.24.4.18"
         next
         edit "172.24.4.24"
         next
         edit "172.24.4.3"
         next
      end
   next
end
```

External Block List (Threat Feed) - File Hashes

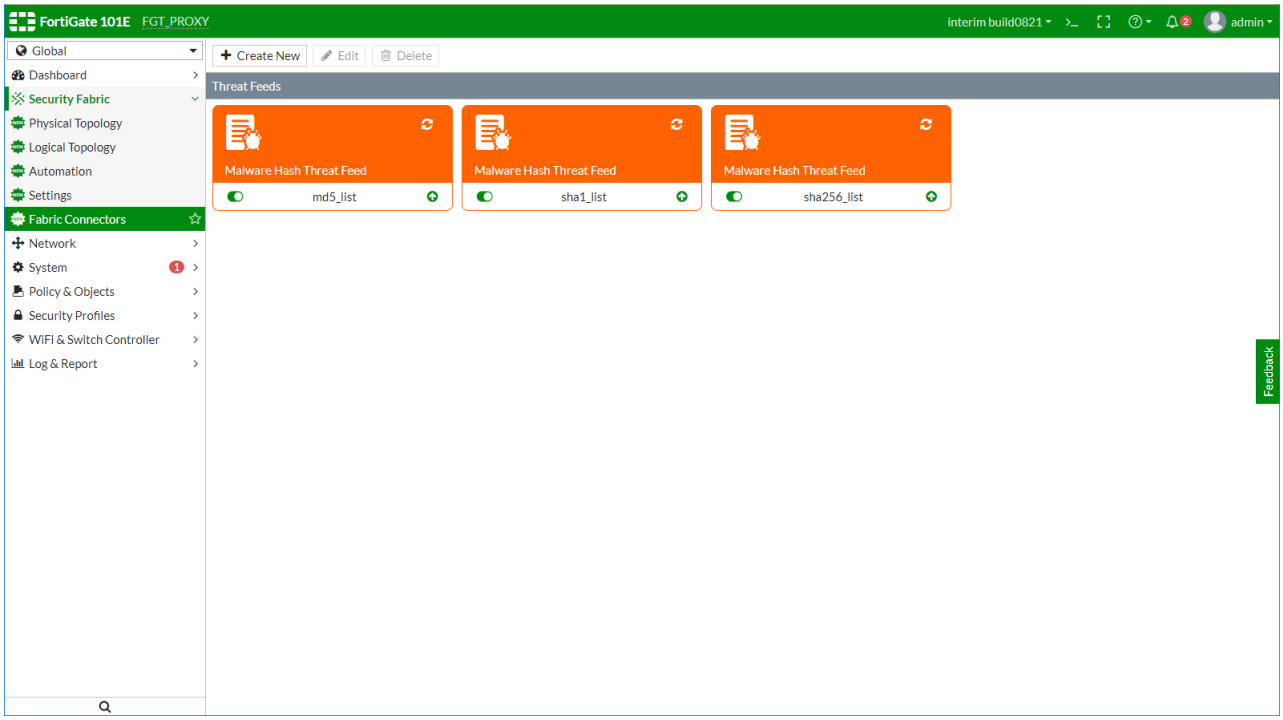
This version adds a new type of *Threat Feed* connector that supports a list of file hashes which can be used as part of Virus Outbreak Prevention.

To configure Malware Hash:

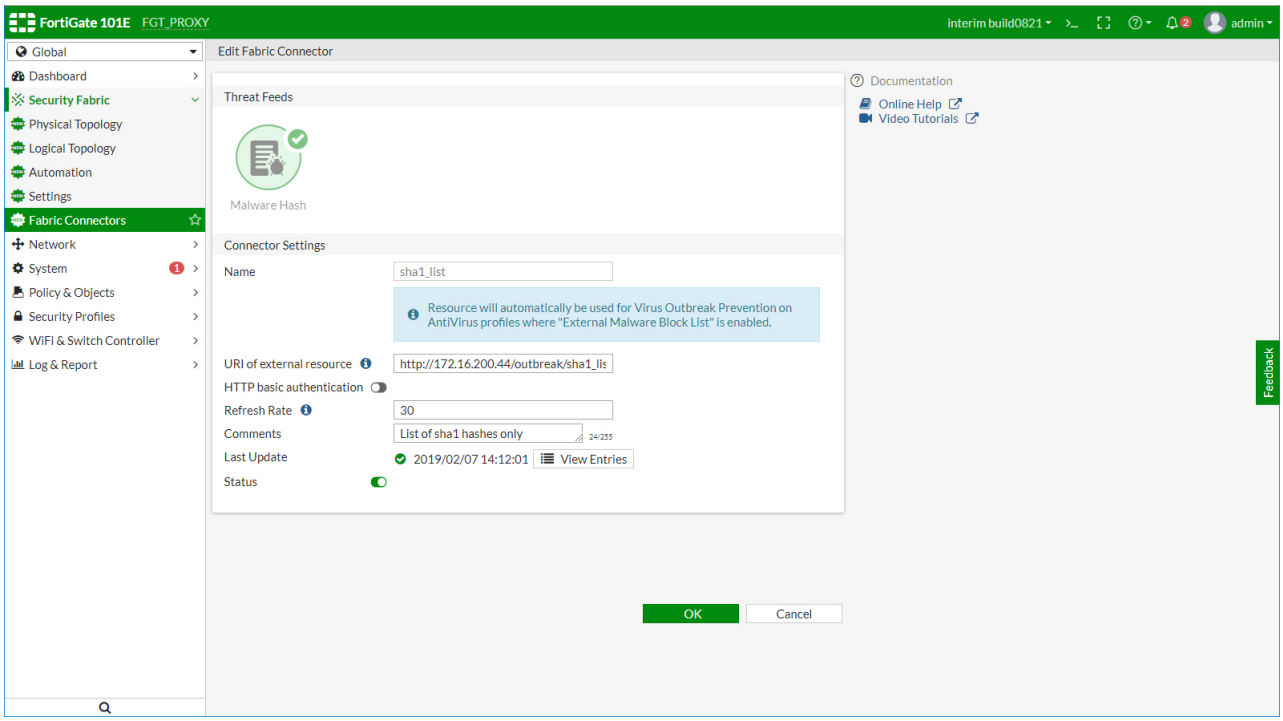
1. Navigate to *Security Fabric* > *Fabric Connectors* and click *Create New*.
2. In the *Threat Feeds* section, click *Malware Hash*.



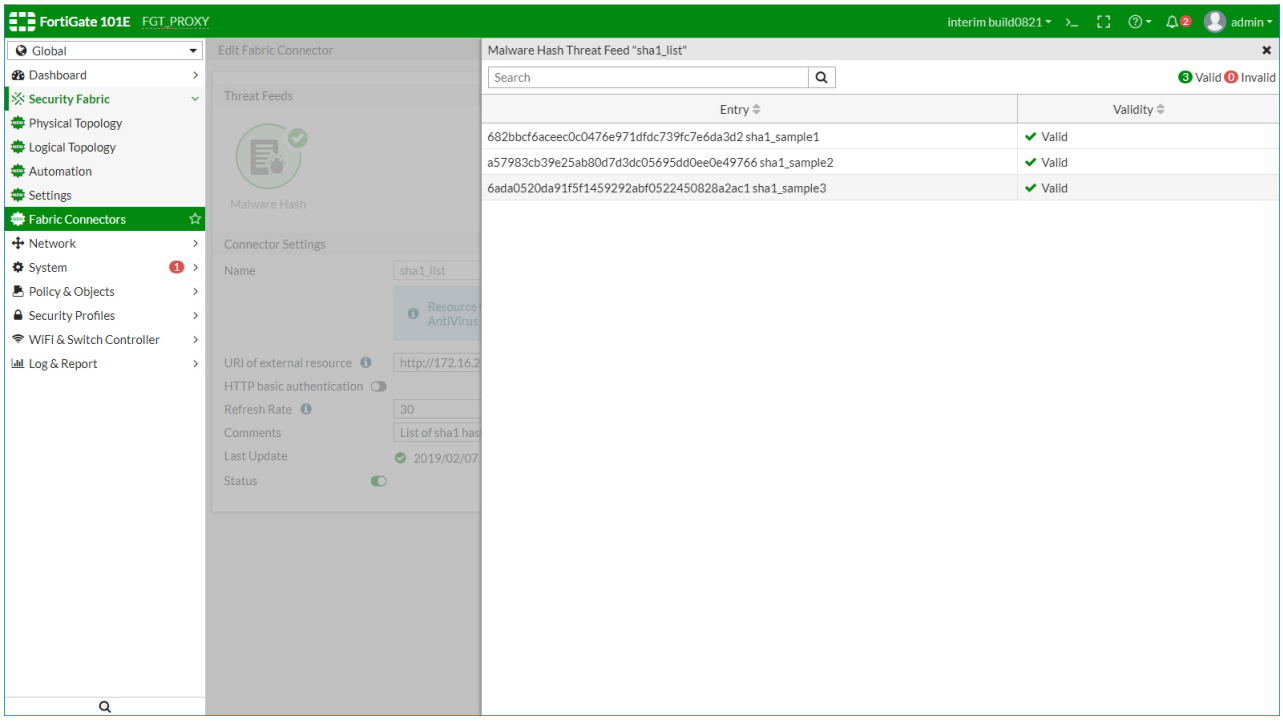
The *Malware Hash* source objects are displayed.



3. To configure *Malware Hash*, fill in the *Connector Settings* section.



4. Beside the *Last Update* field, click *View Entries* to display the external Malware Hash list contents.



New Malware value for external-resource parameter in CLI

```
FGT_PROXY (external-resource) # edit sha1_list
new entry 'sha1_list' added
```

```
FGT_PROXY (sha1_list) # set type ?
category    FortiGuard category.
address     Firewall IP address.
domain      Domain Name.
malware     Malware hash.
```

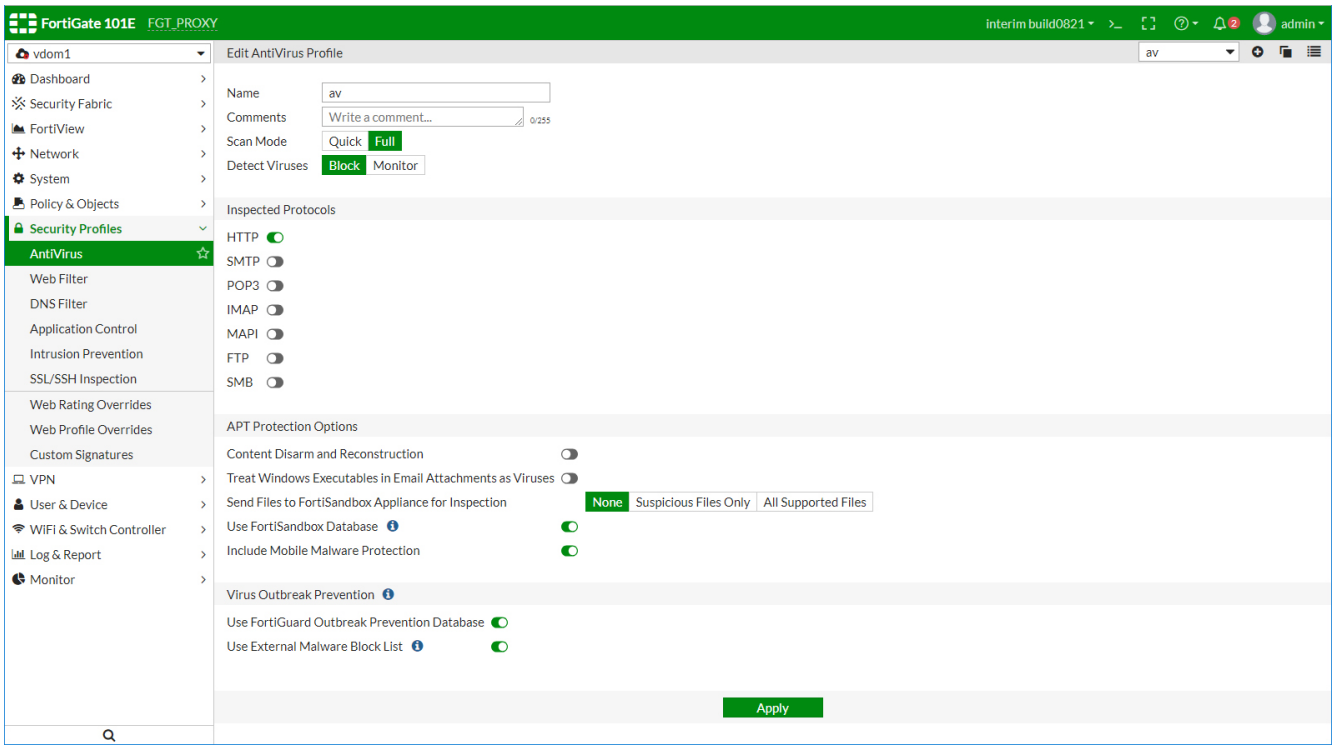
To configure external Malware Hash list sources in CLI:

```
config global

    config system external-resource
        edit "md5_list"
            set type malware
            set comments "List of md5 hashes only"
            set resource "http://172.16.200.44/outbreak/md5_list"
            set refresh-rate 30
        next
        edit "sha1_list"
            set type malware
            set comments "List of sha1 hashes only"
            set resource "http://172.16.200.44/outbreak/sha1_list"
            set refresh-rate 30
        next
        edit "sha256_list"
            set type malware
            set comments "List of sha256 hashes only"
            set resource "http://172.16.200.44/outbreak/sha256_list"
            set refresh-rate 30
        next
    end

end
```

Update to AntiVirus Profile

In *Security Profiles* > *AntiVirus*, the Virus Outbreak Prevention section allows you to enable the following options:

- Use Fortinet outbreak Prevention Database.
- Use External Malware Block List.



To view Virus Outbreak Prevention options in CLI:

```
FGT_PROXY (vdom1) # config antivirus profile
FGT_PROXY (profile) # edit av
FGT_PROXY (av) # config outbreak-prevention
FGT_PROXY (outbreak-prevention) # set
ftgd-service          Enable/disable FortiGuard Virus outbreak prevention service.
external-blocklist    Enable/disable external malware blocklist.

FGT_PROXY (outbreak-prevention) # set
```

To configure Virus Outbreak Prevention options in CLI:

You must first enable `outbreak-prevention` in the protocol and then enable `external-blocklist` under `outbreak-prevention`.

```
config antivirus profile
    edit "av"
        set analytics-db enable
        config http
            set options scan
            set outbreak-prevention full-archive
        end
        config ftp
            set options scan
            set outbreak-prevention files
        end
        config imap
            set options scan
            set outbreak-prevention full-archive
```

```
        end
        config pop3
            set options scan
            set outbreak-prevention full-archive
        end
        config smtp
            set options scan
            set outbreak-prevention files
        end
        config mapi
            set options scan
            set outbreak-prevention full-archive
        end
        config nntp
            set options scan
            set outbreak-prevention full-archive
        end
        config smb
            set options scan
            set outbreak-prevention full-archive
        end
        config outbreak-prevention
            set ftgd-service enable
            set external-blocklist enable
        end
    next
end
```

Update to utm-virus category logs

This feature adds the fields `filehash` and `filehashsrc` to outbreak prevention detection events.

Example of the utm-virus log generated when a file is detected by FortiGuard queried outbreak prevention:

```
2: date=2018-07-30 time=13:57:59 logid="0204008202" type="utm" subtype="virus" event-
type="outbreak-prevention" level="warning" vd="root" evnttime=1532984279 msg="Blocked by Virus
Outbreak Prevention service." action="blocked" service="HTTP" sessionid=174777 srcip-
p=192.168.101.20 dstip=172.16.67.148 srcport=37044 dstport=80 srcintf="lan" srcintfrole="lan"
dstintf="wan1" dstintfrole="wan" policyid=1 proto=6 direction="incoming" filename="zhvo_test.-
com" checksum="583369a5" quarskip="No-skip" virus="503e99fe40ee120c45bc9a30835e7256fff3e46a"
dtype="File Hash" filehash="503e99fe40ee120c45bc9a30835e7256fff3e46a"    file-
hashsrc="fortiguard" url="http://172.16.67.148/zhvo_test.com" profile="mhash_test" agent-
t="Firefox/43.0" analyticssubmit="false" crscore=30 crlevel="high&#8220;
```

Example of the utm-virus log generated when a file is detected by External Malware Hash List outbreak prevention:

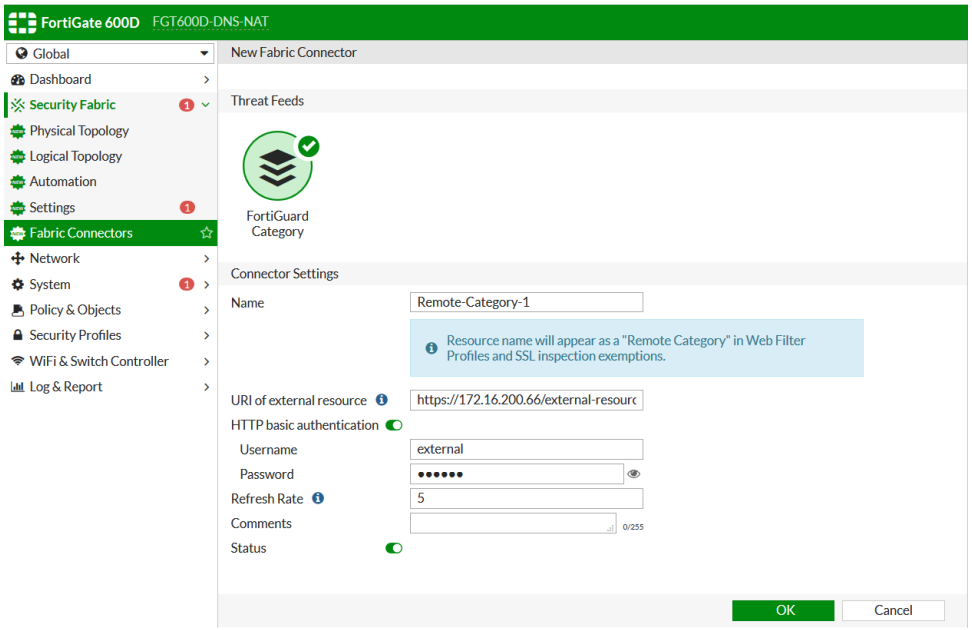
```
1: date=2018-07-30 time=13:59:41 logid="0207008212" type="utm" subtype="virus" event-
type="malware-list" level="warning" vd="root" eventtime=1532984381 msg="Blocked by local mal-
ware list." action="blocked" service="HTTP" sessionid=174963 srcip=192.168.101.20
dstip=172.16.67.148 srcport=37045 dstport=80 srcintf="lan" srcintfrole="lan" dstintf="wan1"
dstintfrole="wan" policyid=1 proto=6 direction="incoming" filename="mhash_block.com" check-
sum="90f0cb57" quarskip="No-skip" virus="mhash_block.com" dtype="File Hash" file-
hash="93bdd30bd381b018b9d1b89e8e6d8753"    filehashsrc="test_list"
url="http://172.16.67.148/mhash_block.com" profile="mhash_test" agent="Firefox/43.0" ana-
lyticssubmit="false"
```

External Block List (Threat Feed) - Authentication

In FortiOS 6.2, the external *Threat Feed* connector (block list retrieved by HTTPS) now supports username and password authentication.

To enable username and password authentication:

1. Navigate to *Security Fabric* > *Fabric Connectors*.
2. Edit an existing *Threat Feed* or create a new one by selecting *Create New*.
3. In *Connector Settings*, select the *HTTP basic authentication* toggle to enable the feature.
4. Enter a username and password.



5. Select *OK* to save your changes.

SD-WAN

This section lists the new features added to FortiOS for SD-WAN.

Overlay Controller VPN (OCVPN)

This section lists the new features added to FortiOS for OCVPN.

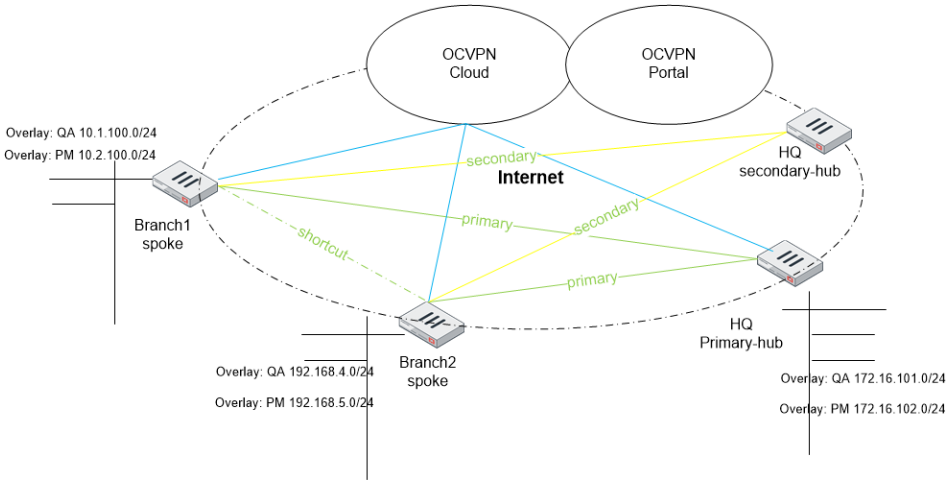
Hub-and-Spoke Support

This version extends OCVPN to support hub-and-spoke topology in addition to full mesh support.

This feature includes support for the following:

- OCVPN portal with FortiCare SSO.
- Enforce limits for OCVPN free service.
- Define multiple overlay network using OCVPN hub-and-spoke.
- ADVPN for hub-and-spoke. The ADVPN shortcut is enabled by default.

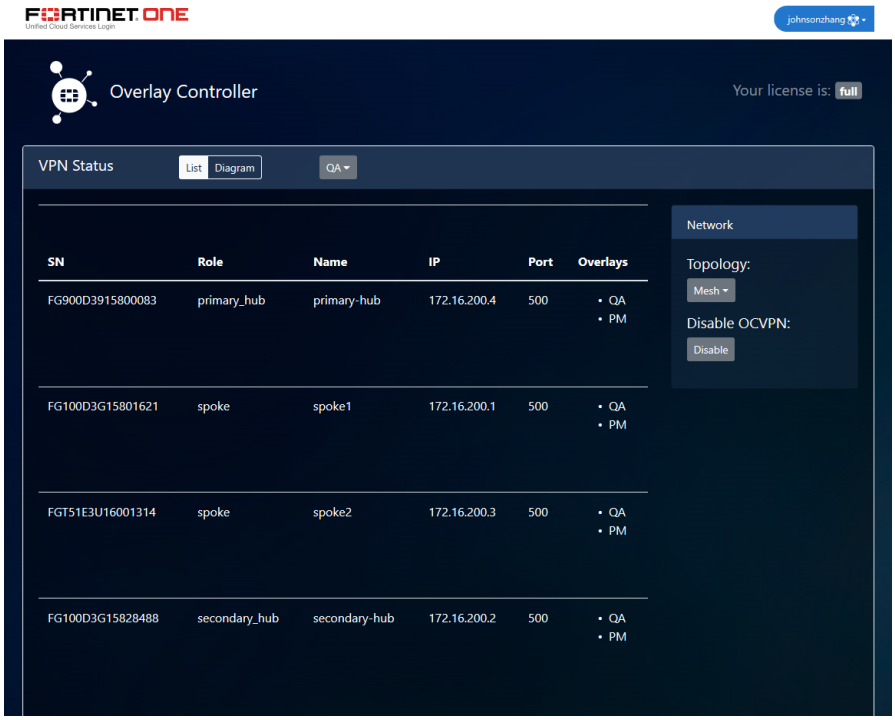
Sample topology



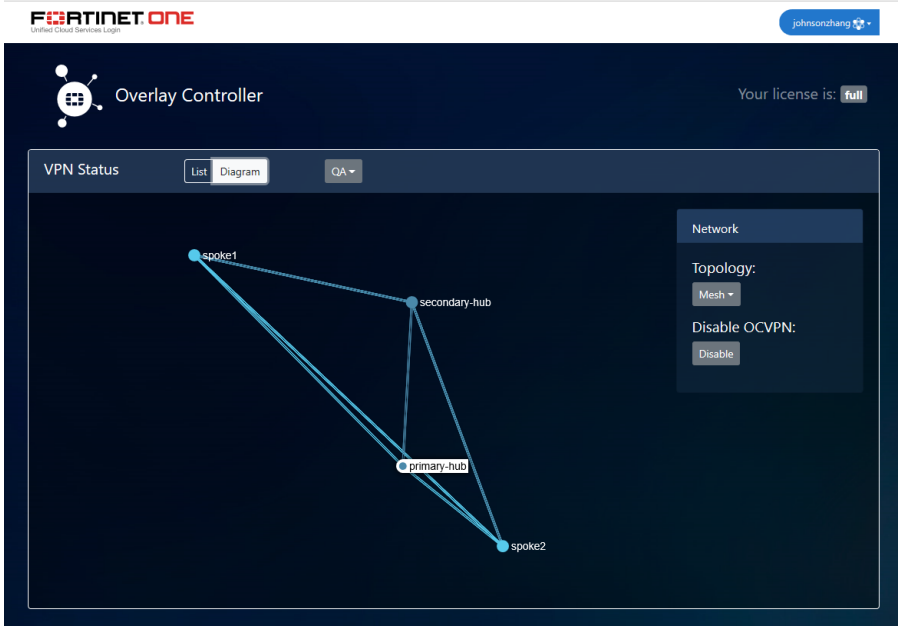
OCVPN portal with FortiCare SSO

The OCVPN portal can display customer and portal information including:

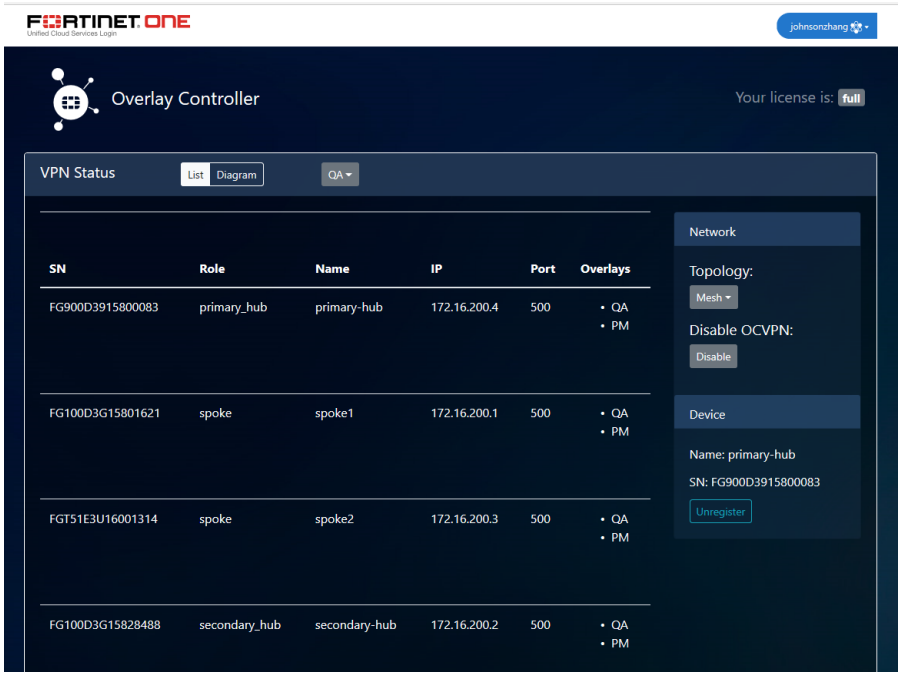
- The customer OCVPN license type: free or full.
- Registered device information including:
  - Device serial number.
  - OCVPN role.
  - Hostname.
  - WAN IP address.
  - Configured overlays.



You can display the OCVPN network topology in a diagram.



You can unregister OCVPN devices on the portal.



OCVPN free license limit

The current OCVPN free license limit is three devices and full mesh only.

There is currently no limit to the free licenses on the OCVPN cloud side.

Warning messages appear when the free license limit is reached. For example:

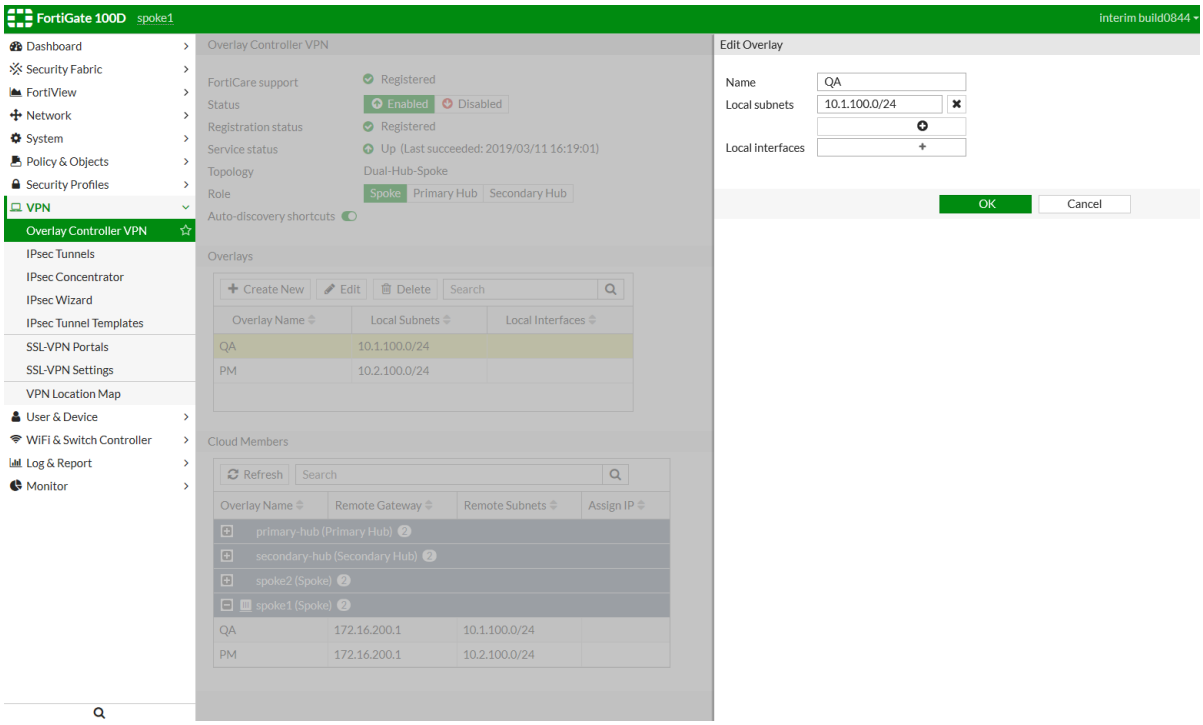
```
"Primary-Hub role is not supported with OCVPN free license.  Please upgrade to
full OCVPN license to use hub and spoke topology.
object check operator error, -9999, discard the setting
Command fail. Return code -9999"

"OCVPN free license limit (3) has been reached. Please upgrade to
full OCVPN license to register additional devices.
object check operator error, -9999, discard the setting
Command fail. Return code -9999"
```

To check the OCVPN license type, see Diagnostic commands on page 116.

OCVPN hub-and-spoke with multiple overlays with ADVPN shortcut

To configure the Spoke in the GUI:

1. Go to *VPN* > *Overlay Controller VPN* and create or edit an overlay.
2. For *Role*, select *Spoke*.



To configure Spoke1 OCVPN in the CLI:

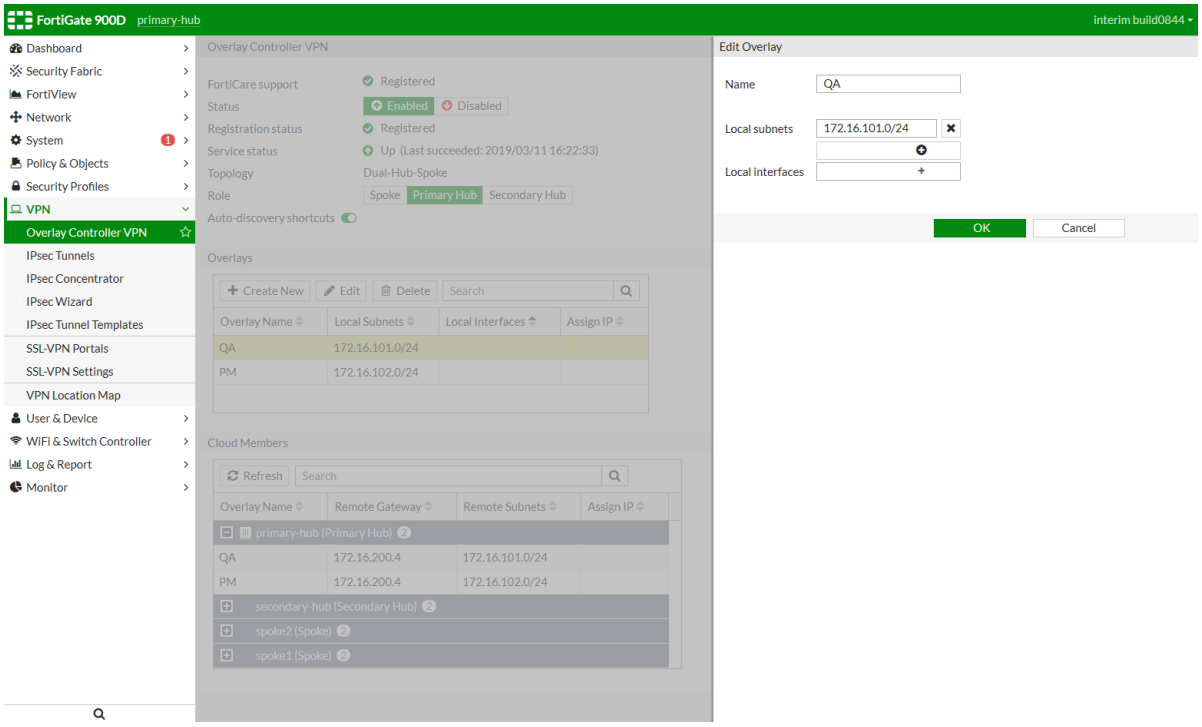
```
config vpn ocvpn
    set status enable
    config overlays
        edit 1
            set name "QA"
            config subnets
                edit 1
                    set subnet 10.1.100.0 255.255.255.0
                next
            end
        next
        edit 2
            set name "PM"
            config subnets
                edit 1
                    set subnet 10.2.100.0 255.255.255.0
                next
            end
        next
    end
end
```

To configure Spoke2 OCVPN in the CLI:

```
config vpn ocvpn
    set status enable
    config overlays
        edit 1
            set name "QA"
            config subnets
                edit 1
                    set subnet 192.168.4.0 255.255.255.0
                next
            end
        next
        edit 2
            set name "PM"
            config subnets
                edit 1
                    set subnet 192.168.5.0 255.255.255.0
                next
            end
        next
    end
end
```

To configure the Primary Hub in the GUI:

1. Go to *VPN* > *Overlay Controller VPN* and create or edit an overlay.
2. For *Role*, select *Primary Hub*.

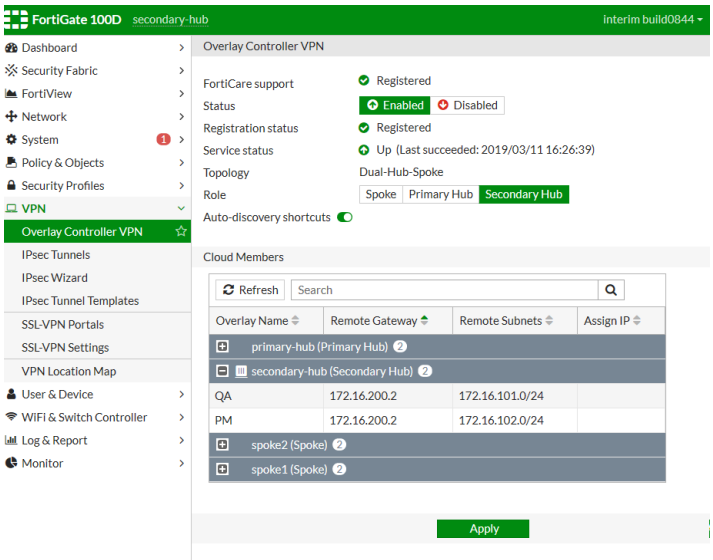


To configure the Primary Hub in the CLI:

```
config vpn ocvpn
    set status enable
    set role primary-hub
    config overlays
        edit 1
            set name "QA"
            config subnets
                edit 1
                    set subnet 172.16.101.0 255.255.255.0
                next
            end
        next
        edit 2
            set name "PM"
            config subnets
                edit 1
                    set subnet 172.16.102.0 255.255.255.0
                next
            end
        next
    end
end
```

To configure the Secondary Hub in the GUI:

1. Go to *VPN* > *Overlay Controller VPN* and create or edit an overlay.
2. For *Role*, select *Secondary Hub*.



To configure the Secondary Hub in the CLI:

```
config vpn ocvpn
    set status enable
    set role secondary-hub
end
```

Diagnostic commands

To check the OCVPN license type:

```
# diagnose vpn ocvpn show-meta
Topology :: auto
License  :: full
Members  :: 4
Max-free :: 3
```

To check the OCVPN status:

```
# diagnose vpn ocvpn status
Current State        : Registered
Topology             : Dual-Hub-Spoke
Role                 : Spoke
Server Status        : Up
Registration time    : Mon Mar 11 16:42:31 2019
Poll time            : Mon Mar 11 16:55:53 2019

# diagnose vpn ocvpn status
Current State        : Registered
Topology             : Dual-Hub-Spoke
Role                 : Primary-Hub
Server Status        : Up
Registration time    : Mon Mar 11 16:42:25 2019
Update time          : Mon Mar 11 15:10:28 2019
Poll time            : Mon Mar 11 16:55:35 2019
```

ADVPN Support

OCVPN hub-and-spoke includes support for ADVPN.

For information on hub-and-spoke support, see Hub-and-Spoke Support on page 109.

Multiple VPN Support

OCVPN hub-and-spoke includes support for multiple overlay VPNs..

For information on hub-and-spoke support, see Hub-and-Spoke Support on page 109.

SD-WAN Bandwidth Monitoring Service

This version adds a new bandwidth measuring tool to detect true upload and download speeds. The bandwidth tests can be run on demand or on schedule, and can be used with the SD-WAN SLA and rules to balance SD-WAN traffic.

This feature needs a license which is part of 360 Protection Bundle in 6.2, or you must have a SWNO license.

This speed test tool compatible with iperf3.6 with SSL support. This tool can send traffic to test uploading bandwidth to the FortiCloud speed test service. It can initiate the connection with the server and initiate downloading requests to the server.

This tool's daily running quota is limited to avoid abusing the usage for valid customers. The current daily quota is 10. FortiGate first downloads the speed test server list. The server list expires after 24 hours. Based on customer's input, it selects one of the servers to do the speed test. The speed test includes uploading speed test and downloading speed test. After the test is done, the results are printed on the terminal.

To download the speed test server list:

```
FortiGate-VM64-KVM # execute speed-test-server download
Download completed.
```

To check the speed test server list:

```
FG3H0E5818904285 (root) # execute speed-test-server list
AWS_West valid
        Host: 34.210.67.183 5204 fortinet
        Host: 34.210.67.183 5205 fortinet
        Host: 34.210.67.183 5206 fortinet
        Host: 34.210.67.183 5207 fortinet
Google_West valid
        Host: 35.197.55.210 5204 fortinet
        Host: 35.197.55.210 5205 fortinet
        Host: 35.197.55.210 5206 fortinet
        Host: 35.197.55.210 5207 fortinet
        Host: 35.230.2.124 5204 fortinet
        Host: 35.230.2.124 5205 fortinet
        Host: 35.230.2.124 5206 fortinet
        Host: 35.230.2.124 5207 fortinet
        Host: 35.197.18.234 5204 fortinet
        Host: 35.197.18.234 5205 fortinet
        Host: 35.197.18.234 5206 fortinet
        Host: 35.197.18.234 5207 fortinet
```

To run the speed test:

You can run the speed test without specifying a server. The system will automatically choose one server from the list and run the speed test.

```
FG3H0E5818904285 (root) # execute speed-test auto
The license is valid to run speed test.
Speed test quota for 2/1 is 9
current vdom=root
Run in uploading mode.
Connecting to host 35.230.2.124, port 5206
[ 16] local 172.16.78.185 port 2475 connected to 35.230.2.124 port 5206
[ ID] Interval Transfer Bitrate Retr Cwnd
[ 16] 0.00-1.01 sec 11.0 MBytes 91.4 Mbits/sec 0 486 KBytes
[ 16] 1.01-2.00 sec 11.6 MBytes 98.4 Mbits/sec 0 790 KBytes
[ 16] 2.00-3.01 sec 11.0 MBytes 91.6 Mbits/sec 15 543 KBytes
[ 16] 3.01-4.01 sec 11.2 MBytes 94.2 Mbits/sec 1 421 KBytes
[ 16] 4.01-5.01 sec 11.2 MBytes 93.5 Mbits/sec 0 461 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
```

```
[ ID] Interval Transfer Bitrate Retr
[ 16] 0.00-5.01 sec 56.1 MBytes 93.8 Mbits/sec 16 sender
[ 16] 0.00-5.06 sec 55.8 MBytes 92.6 Mbits/sec receiver

speed test Done.
Run in reverse downloading mode!
Connecting to host 35.230.2.124, port 5206
Reverse mode, remote host 35.230.2.124 is sending
[ 16] local 172.16.78.185 port 2477 connected to 35.230.2.124 port 5206
[ ID] Interval Transfer Bitrate
[ 16] 0.00-1.00 sec 10.9 MBytes 91.4 Mbits/sec
[ 16] 1.00-2.00 sec 11.2 MBytes 93.9 Mbits/sec
[ 16] 2.00-3.00 sec 11.2 MBytes 94.0 Mbits/sec
[ 16] 3.00-4.00 sec 11.2 MBytes 93.9 Mbits/sec
[ 16] 4.00-5.00 sec 10.9 MBytes 91.1 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval Transfer Bitrate Retr
[ 16] 0.00-5.03 sec 57.5 MBytes 95.9 Mbits/sec 40 sender
[ 16] 0.00-5.00 sec 55.4 MBytes 92.9 Mbits/sec receiver

speed test Done
```

To run the speed test on a server farm or data center:

```
FG3H0E5818904285 (root) # execute speed-test auto AWS_West
The license is valid to run speed test.
Speed test quota for 2/1 is 8
current vdom=root
Run in uploading mode.
Connecting to host 34.210.67.183, port 5205
```

To run the speed test on a local interface when there are multiple valid routes:

```
FG3H0E5818904285 (root) # execute speed-test port1 Google_West
The license is valid to run speed test.
Speed test quota for 2/1 is 6
bind to local ip 172.16.78.202
current vdom=root
Specified interface port1 does not comply with default outgoing interface port2 in routing
table!
Force to use the specified interface!
Run in uploading mode.
Connecting to host 35.197.18.234, port 5205
[ 11] local 172.16.78.202 port 20852 connected to 35.197.18.234 port 5205
[ ID] Interval Transfer Bitrate Retr Cwnd
[ 11] 0.00-1.01 sec 10.7 MBytes 89.0 Mbits/sec 0 392 KBytes
[ 11] 1.01-2.01 sec 10.5 MBytes 88.5 Mbits/sec 1 379 KBytes
[ 11] 2.01-3.01 sec 11.3 MBytes 94.5 Mbits/sec 0 437 KBytes
[ 11] 3.01-4.01 sec 11.2 MBytes 94.3 Mbits/sec 0 478 KBytes
[ 11] 4.01-5.00 sec 11.3 MBytes 95.2 Mbits/sec 0 503 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval Transfer Bitrate Retr
[ 11] 0.00-5.00 sec 55.1 MBytes 92.3 Mbits/sec 1 sender
[ 11] 0.00-5.04 sec 54.5 MBytes 90.7 Mbits/sec receiver

speed test Done.
```

```
Run in reverse downloading mode!
Connecting to host 35.197.18.234, port 5205
Reverse mode, remote host 35.197.18.234 is sending
[ 11] local 172.16.78.202 port 20853 connected to 35.197.18.234 port 5205
[ ID] Interval Transfer Bitrate
[ 11] 0.00-1.00 sec 10.9 MBytes 91.1 Mbits/sec
[ 11] 1.00-2.00 sec 11.2 MBytes 94.0 Mbits/sec
[ 11] 2.00-3.00 sec 11.2 MBytes 94.0 Mbits/sec
[ 11] 3.00-4.00 sec 11.2 MBytes 94.0 Mbits/sec
[ 11] 4.00-5.00 sec 11.2 MBytes 94.0 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval Transfer Bitrate Retr
[ 11] 0.00-5.03 sec 57.4 MBytes 95.8 Mbits/sec 33 sender
[ 11] 0.00-5.00 sec 55.7 MBytes 93.4 Mbits/sec receiver

speed test Done.
```

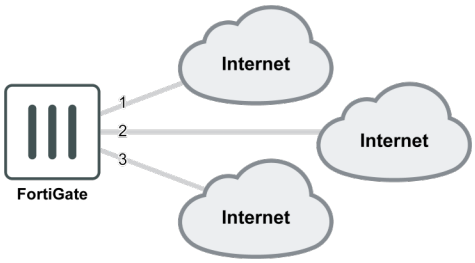
Rule Definition Improvements

This section lists rule definition improvements added to FortiOS for SD-WAN.

Load Balancing Per-Rule

This feature introduces SD-WAN load balancing for all implicit rules. When a rule is hit, traffic is hashed based on the defined load balancing algorithm among the selected SD-WAN members that satisfy the defined SLA.

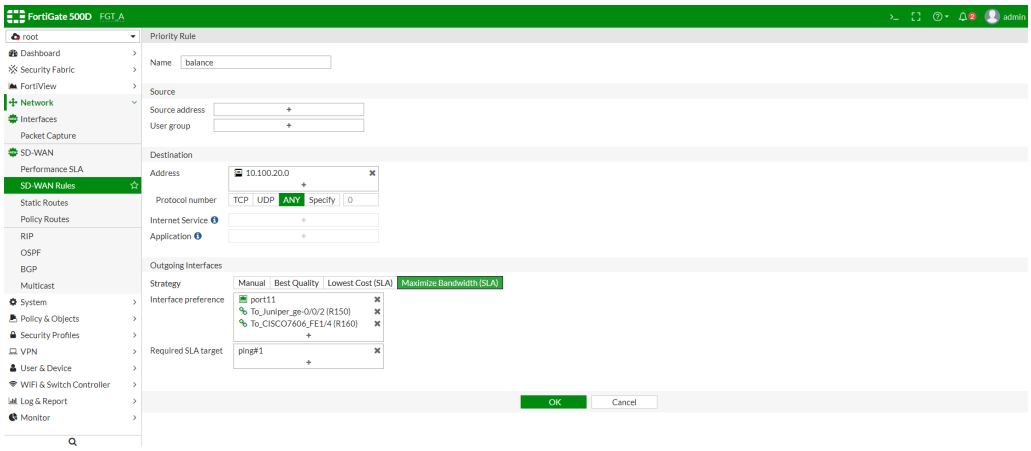
Previously, SD-WAN load balancing was only available on the last implicit rule. This covered all the SD-WAN interface members, but when an explicit SD-WAN rule was created, it prevented load balancing from occurring for that protocol, and traffic was only routed over a single interface.



To add load balancing to a rule with the GUI:

1. Go to *Network* > *SD-WAN Rules*.
2. Edit a rule, or create a new one.

3. Under *Outgoing Interfaces*, select a *Strategy*, *Interface preference*, and *Required SLA target* or *Measured SLA*.



4. Click *OK* to apply your changes.

To add load balancing to a rule with the CLI:

```
config system virtual-wan-link
    config service
        edit 1
            set name "balance"
            set mode load-balance
            set dst "10.100.20.0"
            config sla
                edit "ping"
                    set id 2
                next
            end
            set priority-members 1 2 3
        next
    end
end
```

To diagnose the load balancing status:

```
FGT_A (root) # diagnose sys virtual-wan-link  health-check
Health Check(ping):
Seq(2): state(alive), packet-loss(40.000%) latency(0.049), jitter(0.017) sla_map=0x3
Seq(1): state(alive), packet-loss(0.000%) latency(0.020), jitter(0.005) sla_map=0x3

FGT_A (root) # diagnose sys virtual-wan-link  service

Service(22): Address Mode(IPV4) flags=0x0
  TOS(0x0/0x0), Protocol(0: 1->65535), Mode(load-balance)
  Members:
    1: Seq_num(1), alive, sla(0x1), num of pass(1), selected
    2: Seq_num(2), alive, sla(0x1), num of pass(1), selected
  Dst fqdn: gmail.com(119)
```

DSCP Matching (Shaping)

This feature has three parts:

- DSCP matching in firewall policies
- DSCP matching in firewall shaping policies
- DSCP marking in firewall shaping policies

DSCP matching in firewall policies

Traffic is allowed or blocked according to the DSCP values in the incoming packets.

The following CLI variables are added to the `config firewall policy` command:

`tos-mask <mask_value>`	Non-zero bit positions are used for comparison. Zero bit positions are ignored (default = 0x00). This variable replaces the `dscp-match` variable.
`tos <tos_value>`	Type of Service (ToC) value that is used for comparison (default = 0x00). This variable is only available when `tos-mask` is not zero. This variable replaces the `dscp-value` variable.
`tos-negate {enable | disable}`	Enable/disable negated ToS match (default = disable). This variable is only available when `tos-mask` is not zero. This variable replaces the `dscp-negate` variable.

DSCP matching in firewall shaping policies

Shaping is applied to the session or not according to the DSCP values in the incoming packets. The same logic and commands as in firewall policies are used.

DSCP marking in firewall shaping policies

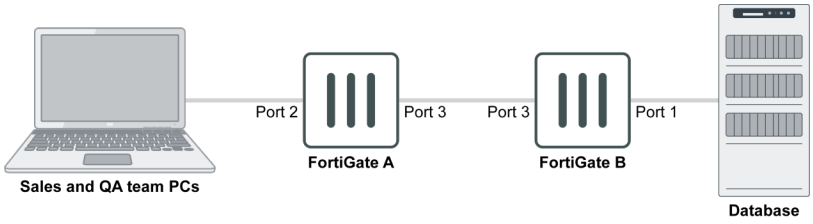
Traffic is allowed or blocked according to the DSCP values in the incoming packets. DSCP marking in firewall shaping policies uses the same logic and commands as in firewall policy and traffic-shaper.

When DSCP marking on `firewall shaper traffic-shaper`, `firewall shaping-policy`, and `firewall policy` all apply to the same session, `shaping-policy` overrides `policy`, and `shaper traffic-shaper` overrides both `shaping-policy` and `policy`.

The following CLI variables in `config firewall policy` are used to mark the packets:

`diffserv-forward {enable | disable}`	Enable/disable changing a packet's DiffServ values to the value specified in `diffservcode-forward` (default = disable).
`diffservcode-forward <dscp_value>`	The value that packet's DiffServ is set to (default = 000000). This variable is only available when `diffserv-forward` is enabled.
`diffserv-reverse {enable | disable}`	Enable/disable changing a packet's reverse (reply) DiffServ values to the value specified in `diffservcode-rev` (default = disable).
`diffservcode-rev <dscp_value>`	The value that packet's reverse (reply) DiffServ is set to (default = 000000). This variable is only available when `diffserv-rev` is enabled.

Examples



Example 1

FortiGate A marks traffic from the sales and QA teams with different DSCP values. FortiGate B does DSCP matching, allowing only the sales team to access the database.

1. Configure FortiGate A:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port3"
        set srcaddr "QA"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set diffserv-forward enable
        set diffservcode-forward 110000
        set nat enable
    next

    edit 5
        set srcintf "port2"
        set dstintf "port3"
        set srcaddr "Sales"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set diffserv-forward enable
        set diffservcode-forward 111011
        set nat enable
    next
end
```

2. Configure FortiGate B:

```
config firewall policy
    edit 2
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "Database"
        set action accept
        set schedule "always"
        set service "ALL"
```

```
        set tos-mask 0xf0
        set tos 0xe0
        set fsso disable
        set nat enable
    next
end
```

Example 2

FortiGate A marks traffic from the sales and QA teams with different DSCP values. FortiGate B uses a firewall shaping policy to do the DSCP matching, limiting the connection speed of the sales team to the database to 10MB/s.

1. Configure FortiGate A:

```
config firewall policy
    edit 1
        set srcintf "port2"
        set dstintf "port3"
        set srcaddr "QA"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set diffserv-forward enable
        set diffservcode-forward 110000
        set nat enable
    next

    edit 5
        set srcintf "port2"
        set dstintf "port3"
        set srcaddr "Sales"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set diffserv-forward enable
        set diffservcode-forward 111011
        set nat enable
    next
end
```

2. Configure FortiGate B:

```
config firewall policy
    edit 2
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

```
config firewall shaper traffic-shaper
    edit "10MB/s"
        set guaranteed-bandwidth 60000
        set maximum-bandwidth 80000
    next
end

config firewall shaping-policy
    edit 1
        set service "ALL"
        set dstintf "port1"
        set tos-mask 0xf0
        set tos 0xe0
        set traffic-shaper "10MB/s"
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

Example 3

FortiGate A has a traffic shaping policy to mark traffic from the QA team with a DSCP value of 100000, while reverse traffic is marked with 000011.

1. Configure FortiGate A:

```
config firewall shaping-policy
    edit 1
        set name "QA Team 50MB"
        set service "ALL"
        set dstintf "port3"
        set traffic-shaper "50MB/s"
        set traffic-shaper-reverse "50MB/s"
        set diffserv-forward enable
        set diffserv-reverse enable
        set srcaddr "QA"
        set dstaddr "all"
        set diffservcode-forward 100000
        set diffservcode-rev 000011
    next
end
```

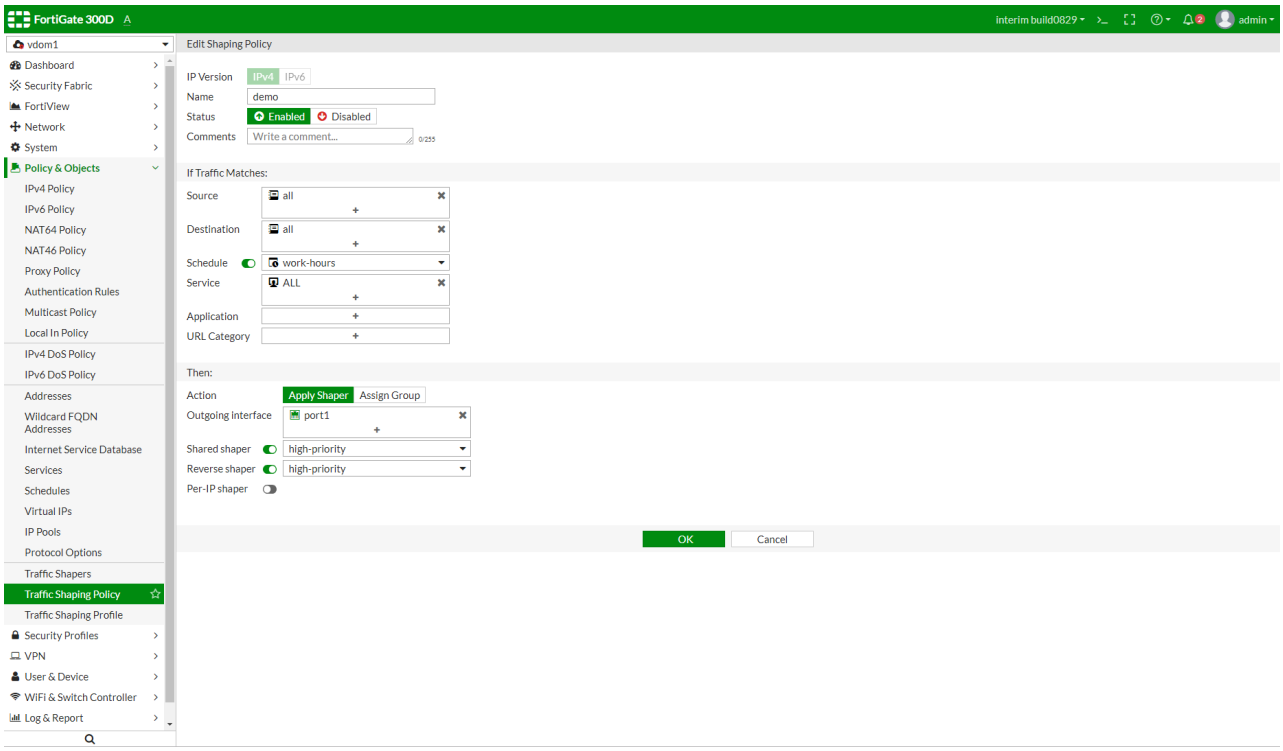
Traffic Shaping Schedules

In a shaping policy, there are many matching criteria available for administrators to match a specific traffic and apply a traffic shaper or shaping group to the traffic. This version adds a new matching criterion: *Schedule*. This feature gives shaping policy the ability to apply different shaping profiles at different times. Administrators can select a one-time schedule, recurring schedule, or schedule group.

Schedule is not a mandatory setting. If it is not set, then the current date and time are not used to match the traffic.

To configure Traffic Shaping Policy in GUI:

1. Navigate to *Policy & Objects* > *Traffic Shaping Policy*.
2. Create or edit a *Traffic Shaping Policy*.
3. Enable *Schedule* and select a schedule option.



4. Configure other options and click *OK*.

To configure Traffic Shaping Policy in CLI:

```
config firewall schedule recurring
    edit "work-hours"
        set start 07:00
        set end 20:00
        set day monday tuesday wednesday thursday friday
    next
end

config firewall shaping-policy
    edit 1
        set name "demo"
        set service "ALL"
        set schedule "work-hours"  <<< Can select schedule from one-time schedule, recurring
schedule or schedule group
        set dstintf "port1"
        set traffic-shaper "high-priority"
        set traffic-shaper-reverse "high-priority"
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

To troubleshoot Traffic Shaping Policy in CLI:

The selected schedule is listed in the `iprope`.

```
dia firewall iprope list 100015

policy index=1 uuid_idx=0 action=accept
flag (0):
schedule(work-hours)
shapers: orig=high-priority(2/0/134217728) reply=high-priority(2/0/134217728)
cos_fwd=0  cos_rev=0
group=00100015 av=00000000 au=00000000 split=00000000
host=1 chk_client_info=0x0 app_list=0 ips_view=0
misc=0 dd_type=0 dd_mode=0
zone(1): 0 -> zone(1): 9
source(1): 0.0.0.0-255.255.255.255, uuid_idx=28,
dest(1): 0.0.0.0-255.255.255.255, uuid_idx=28,
service(1):
    [0:0x0:0/(0,65535)->(0,65535)] helper:auto
```

Application Groups in Policies

This feature adds an application group command for firewall shaping policies.

The following CLI command is added:

```
config firewall shaping-policy
   edit 1
      set app-group <application group>...
      ......
   next
end
```

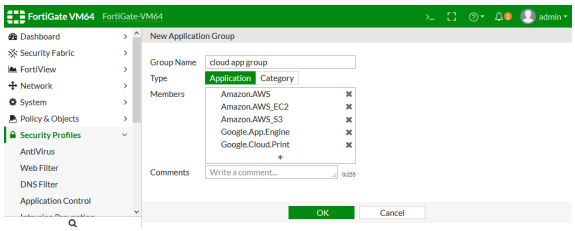
Example

In this example, there are two traffic shaping policies:

- Policy 1 is for traffic related to cloud applications that has high priority.
- Policy 2 is for other traffic and has low priority.

To create the shaping policies using the GUI:

1. Configure an application group for cloud applications:
   a. Go to *Security Profiles* > *Custom Signatures*.
   b. Click *Create New* > *Application Group*. The *New Application Group* page opens.



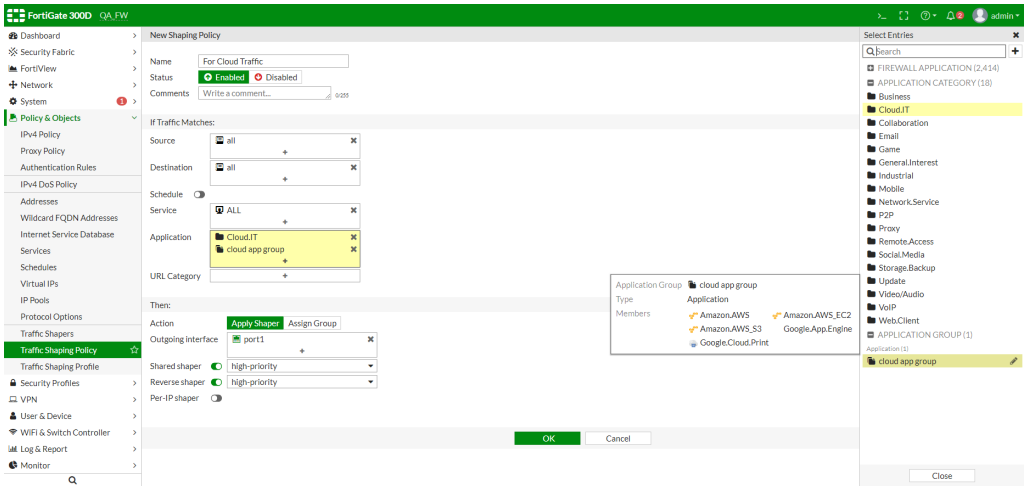
c. Enter a name for the group, select the type, and then add the group the members.

d. Click *OK*.

2. Create the shaping policy for the high priority cloud application traffic:

   a. Go to *Policy & Objects* > *Traffic Shaping Policy*.

   b. Click *Create New*. The *New Shaping Policy* page opens.

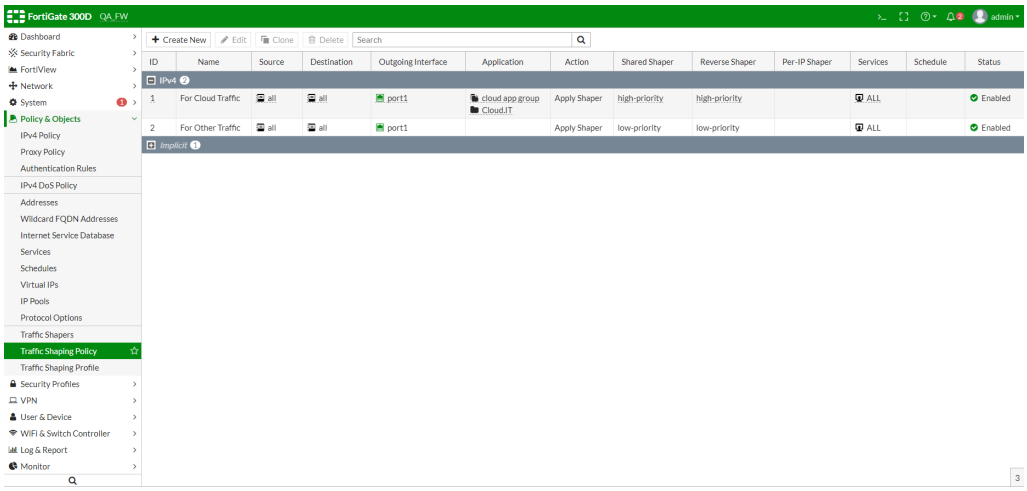


   c. Configure the shaping policy, selecting the previously created cloud application group, and setting both the *Shared shaper* and *Reverse shaper* to *high-priority*.

   d. Click *OK*.

At least one firewall policy must have application control enabled for the applications to match any policy traffic.

3. Create the shaping policy for all other traffic, setting both the *Shared shaper* and *Reverse shaper* to *low-priority*.



To create the shaping policies using the CLI:

1. Configure an application group for cloud applications:

```
config application group
    edit "cloud app group"
        set application 27210 36740 35944 24467 33048
    next
end
```

2. Create the shaping policies for the high priority cloud application traffic and the other, low priority traffic:

```
config firewall shaping-policy
    edit 1
        set name "For Cloud Traffic"
        set service "ALL"
        set app-category 30
        set app-group "cloud app group"
        set dstintf "port1"
        set traffic-shaper "high-priority"
        set traffic-shaper-reverse "high-priority"
        set srcaddr "all"
        set dstaddr "all"
    next
    edit 2
        set name "For Other Traffic"
        set service "ALL"
        set dstintf "port1"
        set traffic-shaper "low-priority"
        set traffic-shaper-reverse "low-priority"
        set srcaddr "all"
        set dstaddr "all"
    next
end
```

Internet Service Groups in Policies

This feature adds support for Internet Service Groups in traffic shaping and firewall policies. Service groups can be used as the source and destination of the policy. Internet Service Groups are used as criteria to match traffic; the shaper will be applied when the traffic matches.

To use a group as a destination, `internet-service` must be enabled. To use a group as a source, `internet-service-src` must be enabled.

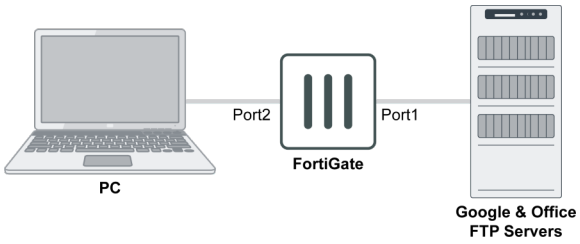
The following CLI variables are added to the `firewall policy` and `firewall shaping-policy` commands:

Variable	Description
internet-service-group <string>	Internet Service group name.
internet-service-custom-group <string>	Custom Internet Service group name.
internet-service-src-group <string>	Internet Service source group name.

Variable	Description
internet-service-src-custom-group <string>	Custom Internet Service source group name.

Examples

The following examples use the below topology.



Example 1

In this example, the PC is allowed to access Google, so all Google services are put into an Internet Service Group.

To configure access to Google services using an Internet Service Group using the CLI:

1. Create a Service Group:

```
config firewall internet-service-group
    edit "Google_Group"
        set direction destination
        set member 65537 65538 65539 65540 65542 65543 65544 65545 65550 65536 65646
    next
end
```

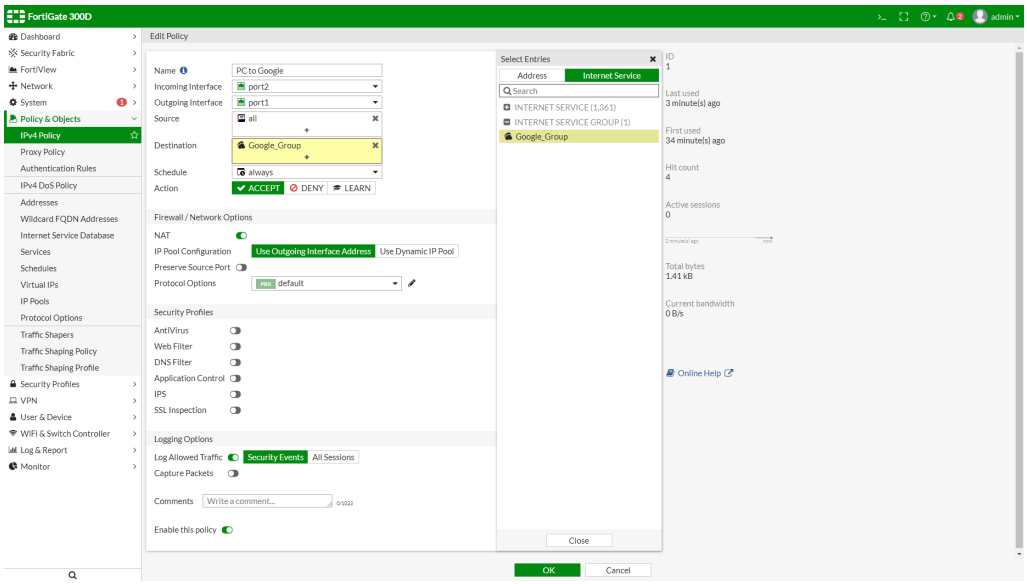
2. Create a firewall policy to allow access to all Google Services from the PC:

```
config firewall policy
    edit 1
        set name "PC to Google"
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "PC"
        set internet-service enable
        set internet-service-group "Google_Group"
        set action accept
        set schedule "always"
        set fsso disable
        set nat enable
    next
end
```

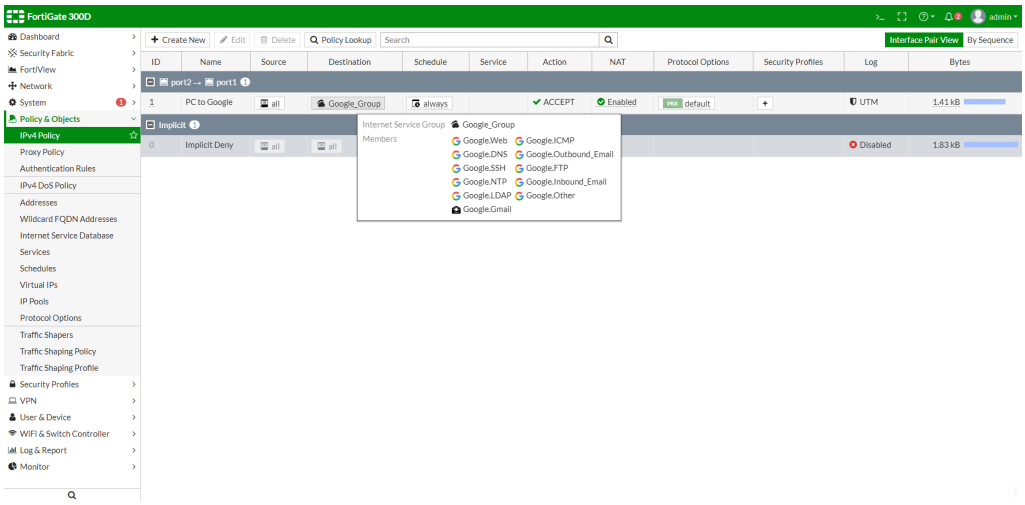
To configure access to Google services using an Internet Service Group in the GUI:

1. On the FortiGate, create a Service Group using the CLI.
2. Go to *Policy & Objects* > *IPv4 Policy*, and create a new policy.

3. Set the *Destination* as the just created Internet Service Group.



4. Configure the remaining options as shown, then click *OK*.
   On the policy page, hover over the group to view a list of its members.



Example 2

In this example, two office FTP servers are put into an Internet Custom Service Group, and the PC connection to the FTP servers is limited to 1Mbps.

To put two FTP servers into a custom service group and limit the PC connection speed to them using the CLI:

1. Create custom internet services for the internal FTP servers:

```
config firewall internet-service-custom
    edit "FTP_PM"
        config entry
            edit 1
```

```
                config port-range
                    edit 1
                        set start-port 21
                        set end-port 21
                    next
                end
                set dst "PM_Server"
            next
        end
    next
    edit "FTP_QA"
        config entry
            edit 1
                config port-range
                    edit 1
                        set start-port 21
                        set end-port 21
                    next
                end
                set dst "QA_Server"
            next
        end
    next
end
```

2. Create a custom internet server group and add the just created custom internet services to it:

```
config firewall internet-service-custom-group
    edit "Internal_FTP"
        set member "FTP_QA" "FTP_PM"
    next
end
```

3. Create a traffic shaper to limit the maximum bandwidth:

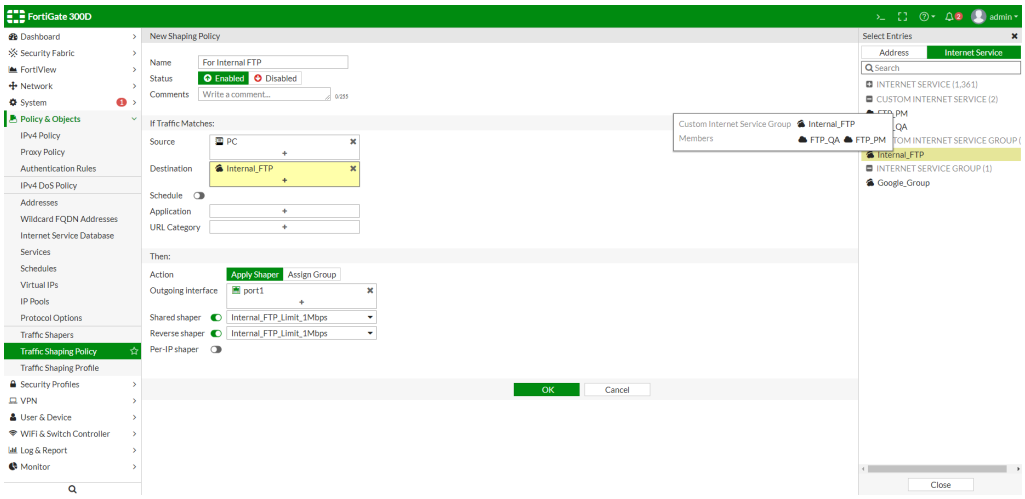
```
config firewall shaper traffic-shaper
    edit "Internal_FTP_Limit_1Mbps"
        set guaranteed-bandwidth 500
        set maximum-bandwidth 1000
        set priority medium
    next
end
```

4. Create a firewall shaping policy to limit the speed from the PC to the internal FTP servers:

```
config firewall shaping-policy
    edit 1
        set name "For Internal FTP"
        set internet-service enable
        set internet-service-custom-group "Internal_FTP"
        set dstintf "port1"
        set traffic-shaper "Internal_FTP_Limit_1Mbps"
        set traffic-shaper-reverse "Internal_FTP_Limit_1Mbps"
        set srcaddr "PC"
    next
end
```

To put two FTP servers into a custom service group and limit the PC connection speed to the using the GUI:

1. Create custom internet services for the internal FTP servers using the CLI.
2. Create a custom internet server group and add the just created custom internet services to it using the CLI.
3. Create a traffic shaper to limit the maximum bandwidth:
   a. Go to *Policy & Objects* > *Traffic Shapers*, and click *Create New*.
   b. Enter a *Name* for the shaper, such as *Internal_FTP_Limit_1Mbps*.
   c. Set the *Traffic Priority* to *Medium*.
   d. Enable *Max Bandwidth* and set it to *1000*.
   e. Enable *Guaranteed Bandwidth* and set it to *500*.
   f. Click *OK*.
4. Create a firewall shaping policy to limit the speed from the PC to the internal FTP servers:
   a. Go to *Policy & Objects* > *Traffic Shaping Policy*, and click *Create New*.
   b. Set the *Destination* as the just created Custom Internet Service Group, and apply the just create traffic shaper.



   c. Configure the remaining options as shown, then click *OK*.

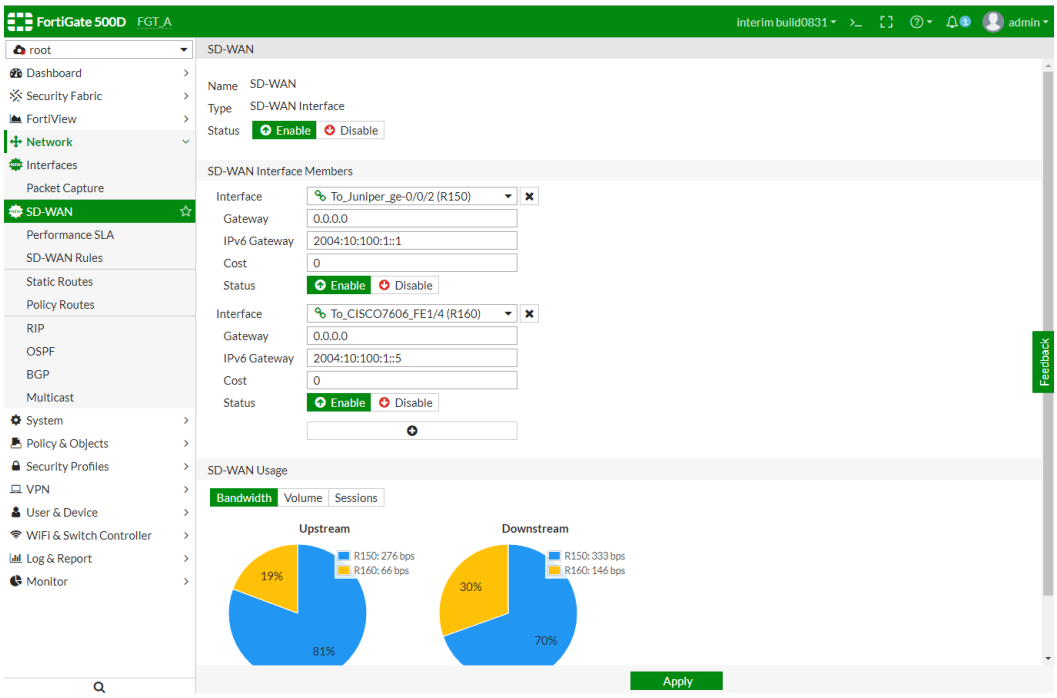
IPv6 Support (UI)

This version adds GUI support for SD-WAN setup, including:

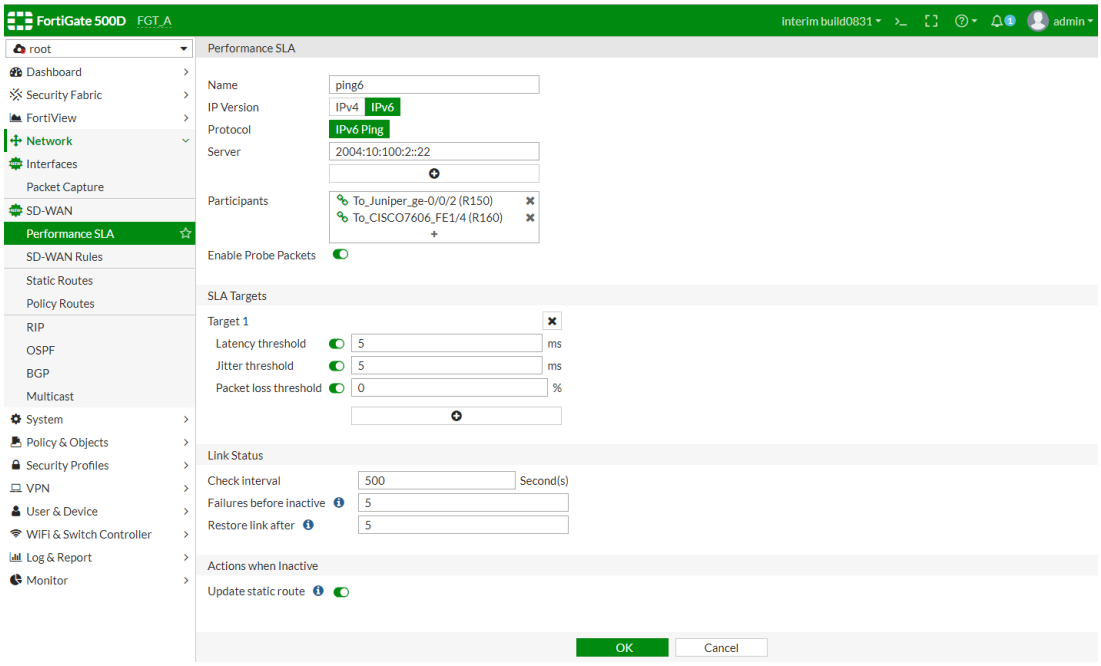
- SD-WAN Interfaces with IPv6 addressing (gateway).
- IPv6 Mode for Performance SLA.
- IPv6 SD-WAN Rules.

Sample configuration

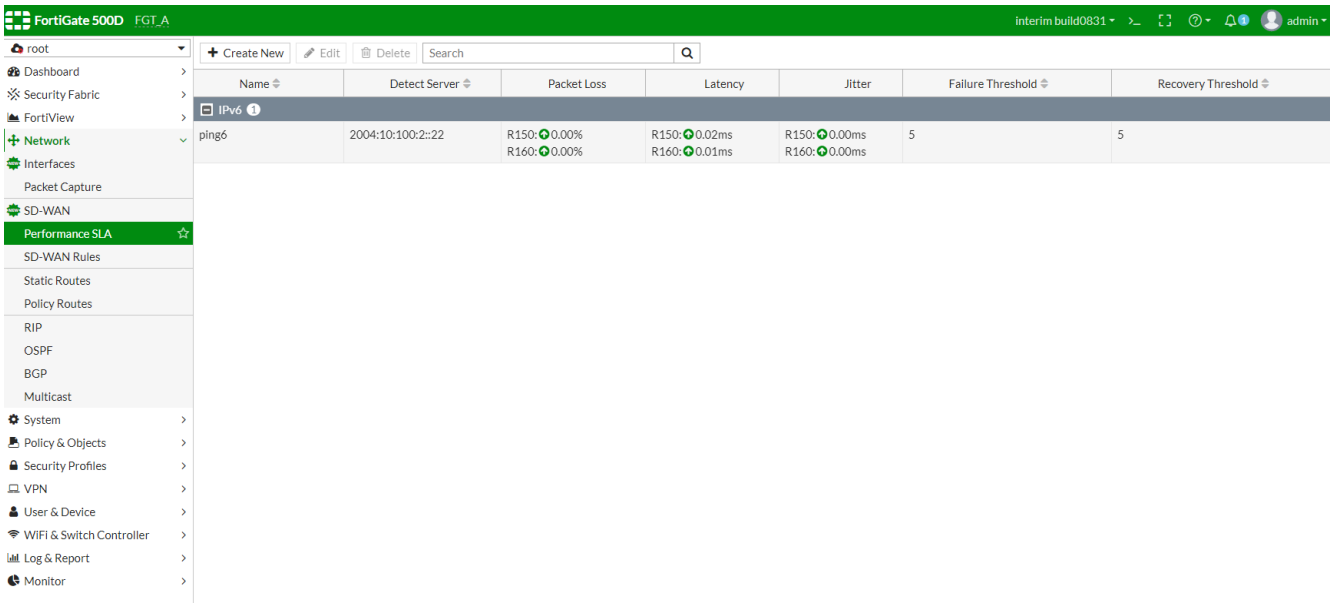
In *Network* > *SD-WAN*, set *Status* to *Enable* and configure *SD-WAN Interface Members* in the *IPv6 Gateway* field.



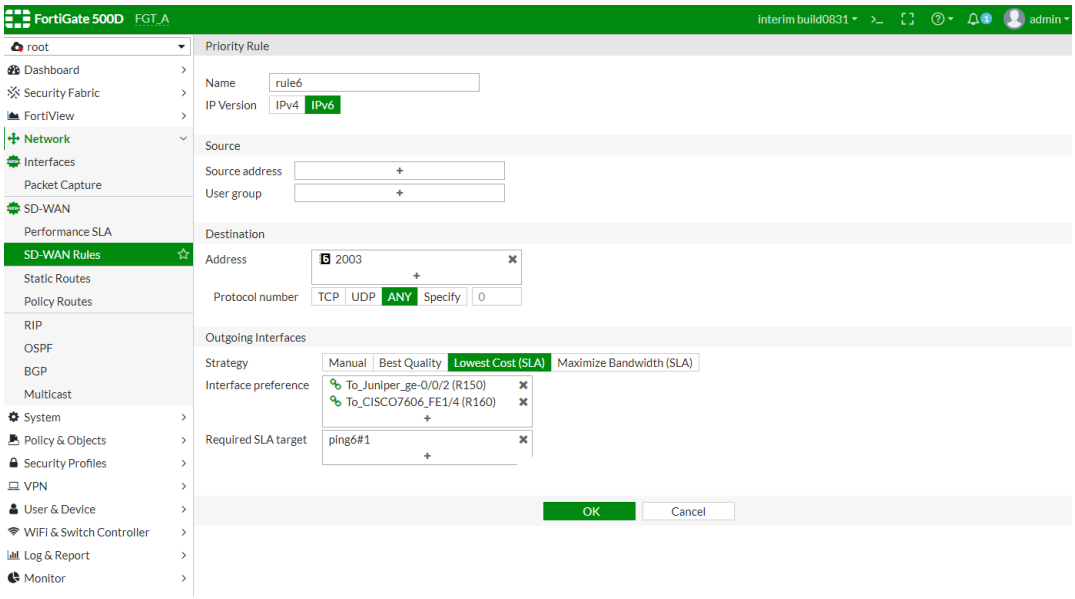
In *Network* > *Performance SLA*, set *IP Version* to *IPv6* and configure fields.



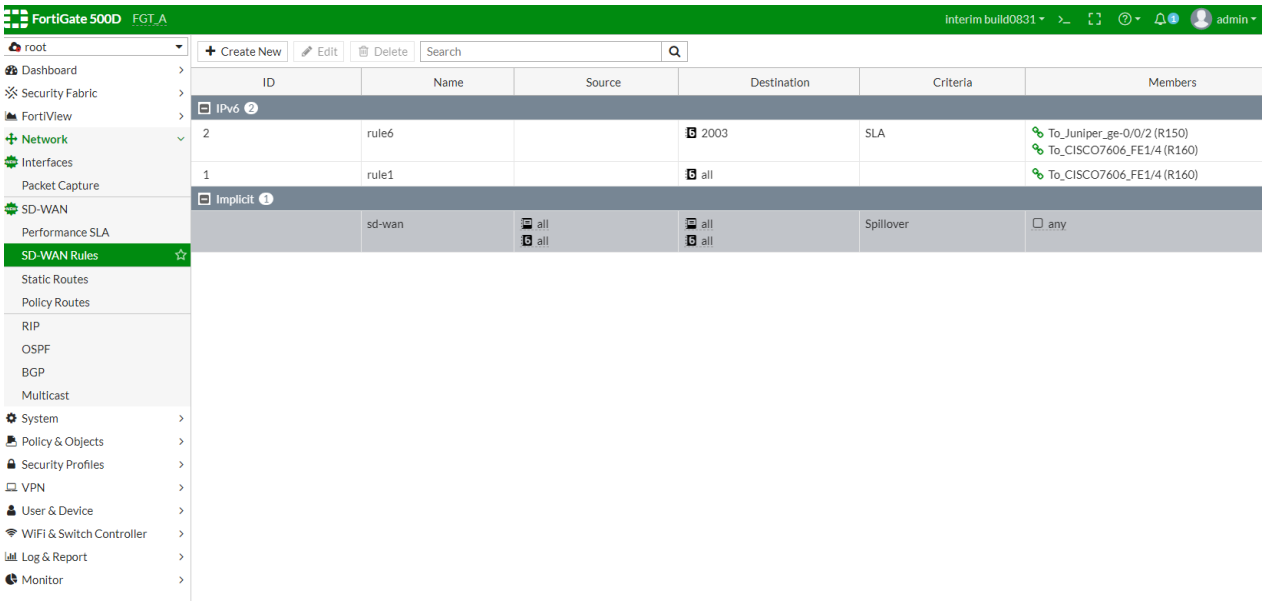
The *Performance SLA* page displays the entry you configured.



In *Network* > *SD-WAN Rules*, set *IP Version* to *IPv6* and configure SD-WAN IPv6 mode rules.



The *Network* > *SD-WAN Rules* page displays the rules you configured.



Forward Error Correction

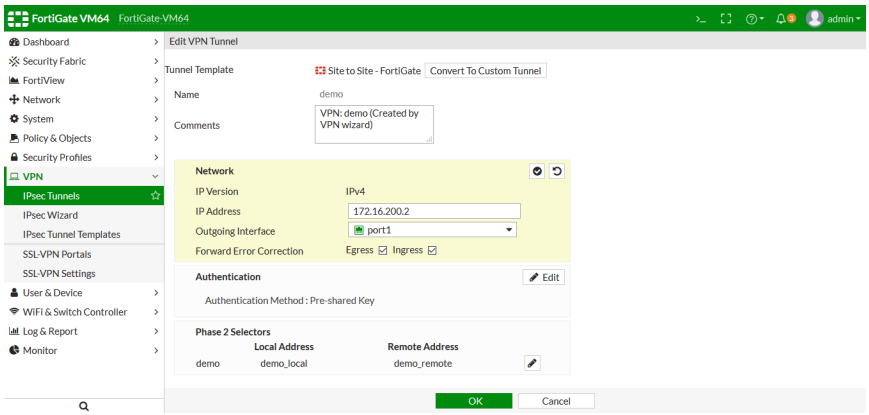
Forward Error Correction (FEC) is used to lower the packet loss ratio by consuming more bandwidth. This features adds Forward Error Correction (FEC) to IPsec VPN.

Six new parameters are added to the IPsec phase1-interface settings:

`fec-ingress`	Enable/disable Forward Error Correction for ingress IPsec traffic (default = disable).
`fec-egress`	Enable/disable Forward Error Correction for egress IPsec traffic (default = disable).
`fec-base`	The number of base Forward Error Correction packets (1 - 100, default = 20).
`fec-redundant`	The number of redundant Forward Error Correction packets (1 - 100, default = 10).
`fec-send-timeout`	The time before sending Forward Error Correction packets, in milliseconds (1 - 1000, default = 8).
`fec-receive-timeout`	The time before dropping Forward Error Correction packets, in milliseconds (1 - 1000, default = 5000).

FEC is disabled by default. FortiGate supports unidirectional and bidirectional FEC, and achieves the expected packet loss ration and latency by tuning the above parameters.

Two checkboxes are added to the IPsec phase1 settings in the GUI:



To configure FEC with the CLI:

```
config vpn ipsec phase1-interface
  edit "demo"
    ......................
    set fec-egress enable
    set fec-ingress enable
    set fec-base 20
    set fec-redundant 10
    set fec-send-timeout 8
    set fec-receive-timeout 5000
    ......................
  next
end
```

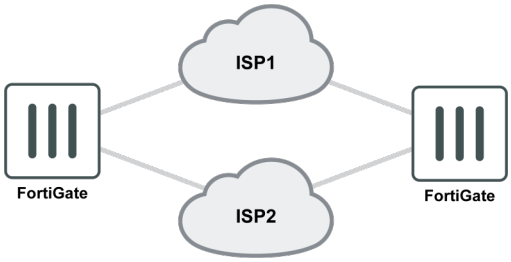
To debug the VPN tunnel:

```
FGT-A # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=demo ver=1 serial=1 172.16.200.1:0->172.16.200.2:0
bound_if=11 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/3600 options[0e10]=create_dev
frag-rfc fec-egress fec-ingress  accept_traffic=1

proxyid_num=1 child_num=0 refcnt=11 ilast=8 olast=8 ad=/0
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
fec-egress: base=20 redundant=10 remote_port=50000     <<<<<<<<<<<<<<<<<<<<<<<
fec-ingress: base=20 redundant=10                                <<<<<<<<<<<<<<<<<<<<<<<
proxyid=demo proto=0 sa=1 ref=2 serial=1
  src: 0:10.1.100.0/255.255.255.0:0
  dst: 0:173.1.1.0/255.255.255.0:0
  SA:  ref=3 options=10226 type=00 soft=0 mtu=1390 expire=42897/0B replaywin=2048
       seqno=1 esn=0 replaywin_lastseq=00000000 itn=0 qat=0
  life: type=01 bytes=0/0 timeout=42899/43200
  dec: spi=181f4f81 esp=aes key=16 6e8fedf2a77691ffdbf3270484cb2555
       ah=sha1 key=20 f92bcf841239d15d30b36b695f78eaef3fad05c4
  enc: spi=0ce10190 esp=aes key=16 2d684fb19cbae533249c8b5683937329
       ah=sha1 key=20 ba7333f89cd34cf75966bd9ffa72030115919213
  dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

Represent Multiple IPsec Tunnels as a Single Interface

With this feature, you can create a static aggregate interface using IPsec tunnels as members, with traffic load balanced between the members. An IP address can be assigned to the aggregate interface, dynamic routing can run on the interface, and the interface can be a member interface in SD-WAN.

The supported load balancing algorithms are: L3, L4, round-robin (default), and redundant.



1. Create a site to site VPN phase1 interface with net-device disabled:

```
config vpn ipsec phase1-interface
  edit tunnel1
    set interface port1
    set net-device disable
    set remote-ge 172.16.100.1
    set psksecret sample
  next
  edit tunnel2
    set interface port2
    set net-device disable
    set remote-ge 172.31.1.1
    set psksecret sample
  next
end
```

2. Configure IPsec aggregation:

```
config system ipsec-aggregate
  edit agg1
    set member tunnel1 tunnel2
  next
end
```

3. Configure a firewall policy:

```
config firewall policy
  edit 0
    set srcaddr all
    set srcintf port10
    set dstaddr all
    set dstintf agg1
    set schedule always
    set action accept
    set service ALL
  next
end
```

4. Configure a static route:

```
config router static
  edit 0
    set device agg1
  next
end
```

To debug the IPsec aggregation list:

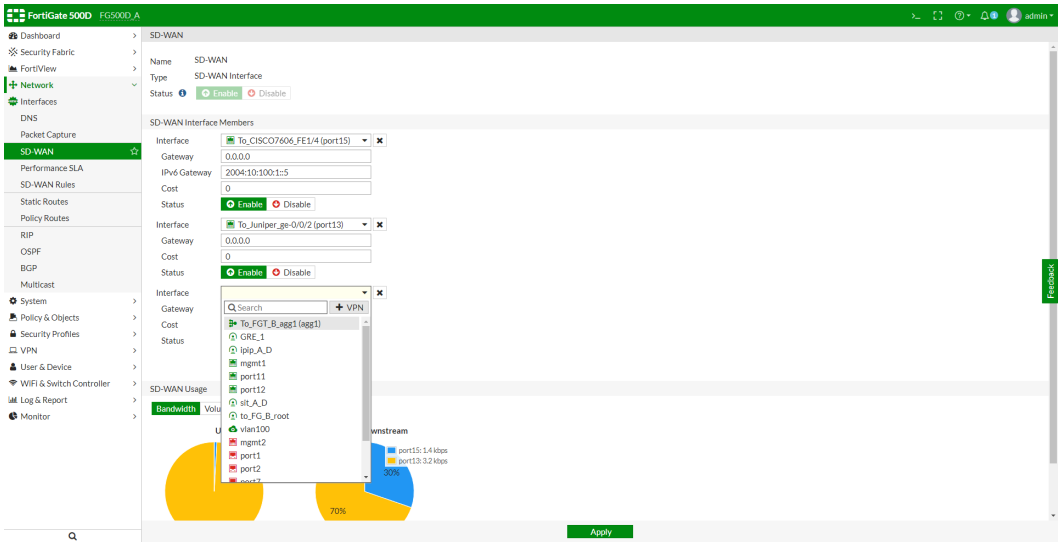
```
#diagnose sys ipsec-aggregate list
  agg1 algo=RR member=2 run_tally=2
  members:
    tunnel1
    tunnel2
```

Dual VPN Tunnel Wizard

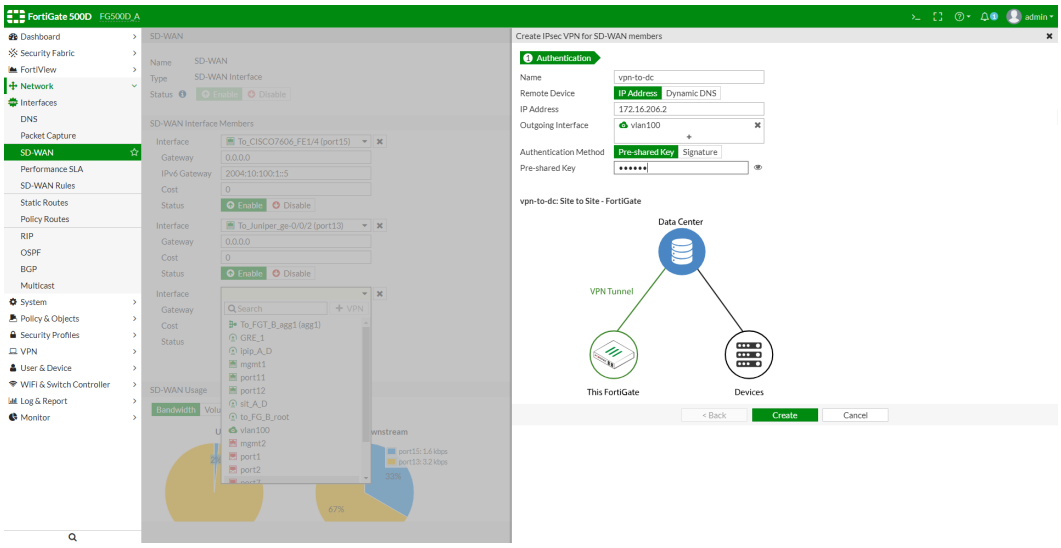
This new wizard is used to automatically set up multiple VPN tunnels to the same destination over multiple outgoing interfaces. This includes automatically configuring IPsec, Routing, and Firewall settings, avoiding cumbersome and error-prone configuration steps.

To create a new SD-WAN VPN interface using the tunnel wizard:

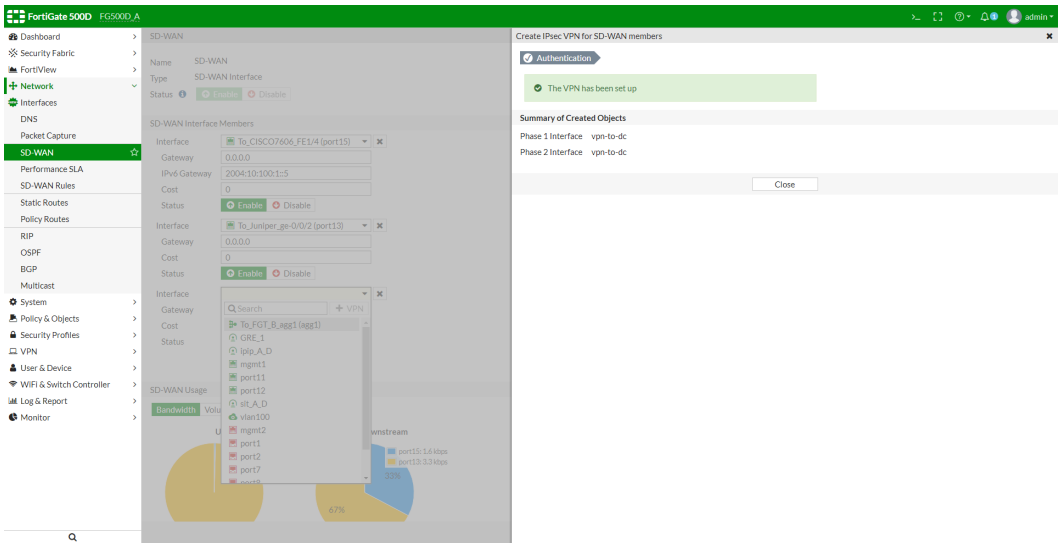
1. Go to *Network* > *SD-WAN*.
2. Add a new interface member.



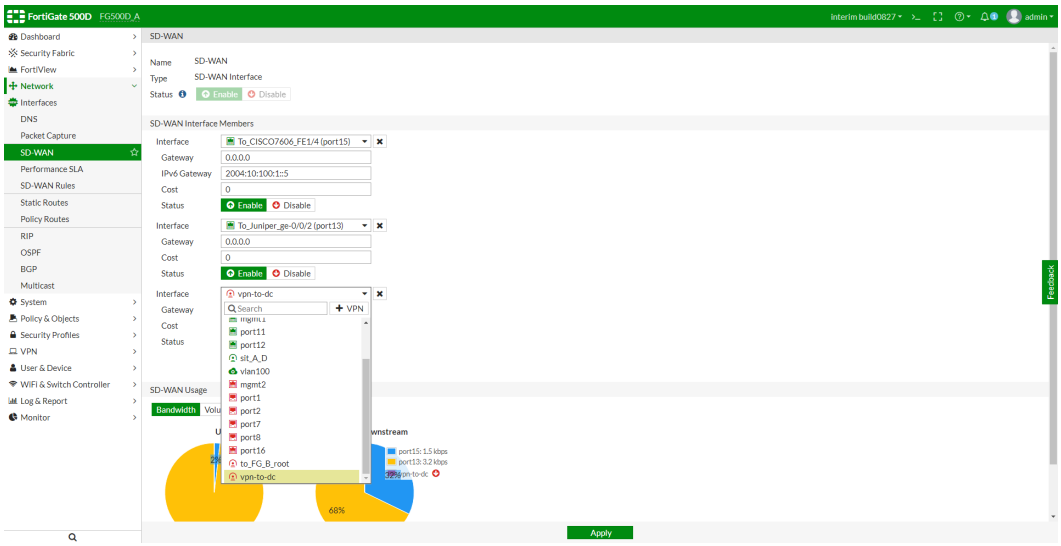
3. In the *Interface* drop-down, click *+VPN*. The *Create IPsec VPN for SD-WAN members* pane opens.



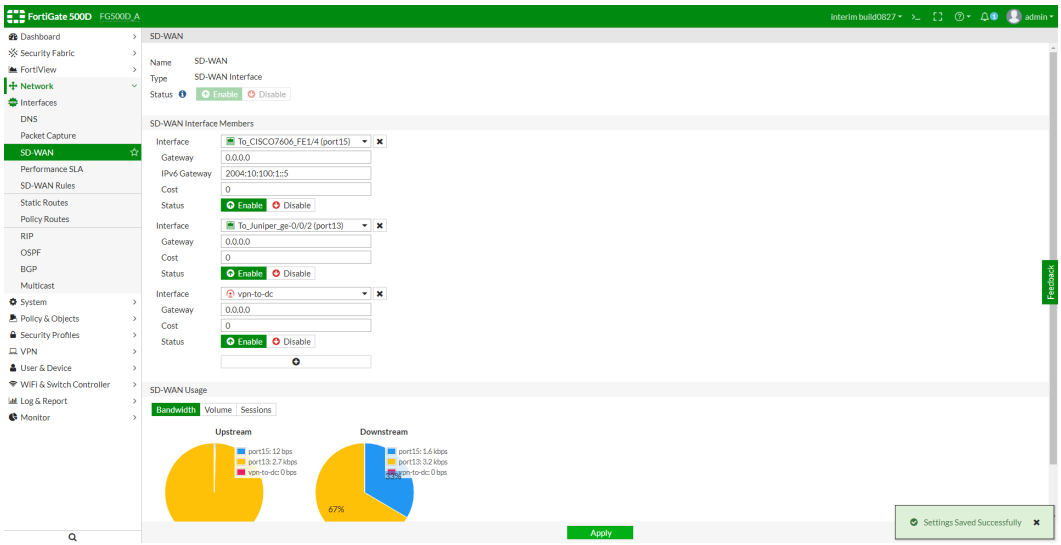
4. Enter the required information, then click *Create*.



5. Click *Close* to return to the SD-WAN page.
   The newly created VPN interface will be highlighted in the *Interface* drop-down list.



6. Select the VPN interface to add it as an SD-WAN member.
7. Click *Apply* to save the SD-WAN settings.



BGP Additional Path Support

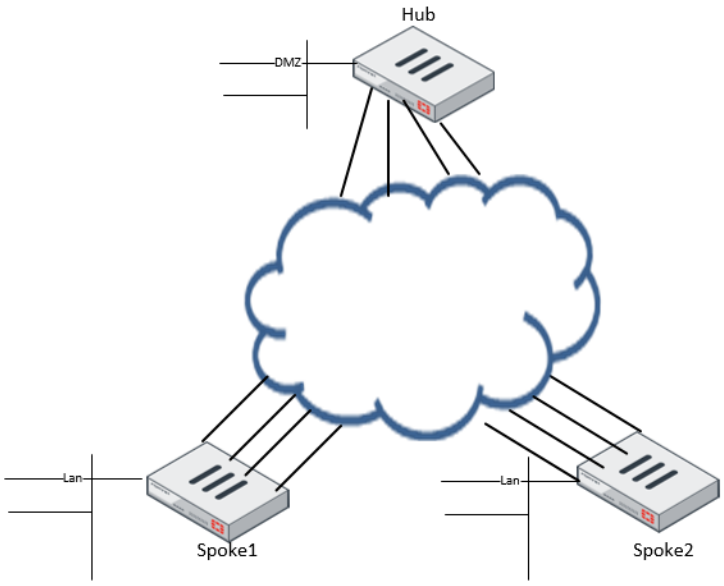
Currently, when deploying Auto-Discovery VPN (ADVPN) for Software-Defined Wide Area Networks (SD-WAN), a FortiGate deployed as the ADVPN hub is a route reflector. As such, it only advertises one path, which is the best path. Due to this, the branches receive different routes in their routing tables that point to the same next hop.

In 6.2, this is addressed by adding additional Border Gateway Protocol (BGP) path support, which allows the ADVPN hub to advertise multiple paths.

This feature allows BGP to extend and keep additional network paths according to RFC 7911.

Example

In the following example topology, each spoke has four VPN tunnels connected to the Hub with ADVPN. The Spoke-Hub has established four BGP neighbors on all four tunnels.



Spoke 1 and Spoke 2 can learn four different routes from each other.

Hub

```
config router bgp
   set as 65505
   set router-id 11.11.11.11
   set ibgp-multipath enable
   set additional-path enable  <<<<<<<<<< new
   set additional-path-select 4  <<<<<<<<<< new
   config neighbor-group
      edit "gr1"
            set capability-default-originate enable
            set remote-as 65505
            set additional-path both  <<<<<<<<<< new
            set adv-additional-path 4  <<<<<<<<<< new
            set route-reflector-client enable
      next
   end
   config neighbor-range
      edit 1
            set prefix 10.10.0.0 255.255.0.0
            set neighbor-group "gr1"
      next
   end
   config network
      edit 12
         set prefix 11.11.11.11 255.255.255.255
```

```
      next
   end
end
```

Spoke

```
config router bgp
   set as 65505
   set router-id 2.2.2.2
   set ibgp-multipath enable
   set additional-path enable <<<<<<<<<< new
   set additional-path-select 4 <<<<<<<<<< new
   config neighbor
      edit "10.10.100.254"
            set soft-reconfiguration enable
            set remote-as 65505
            set additional-path both <<<<<<<<<< new
            set adv-additional-path 4 <<<<<<<<<< new
      next
      edit "10.10.200.254"
         set soft-reconfiguration enable
         set remote-as 65505
         set additional-path both
         set adv-additional-path 4
      next
      edit "10.10.203.254"
         set soft-reconfiguration enable
         set remote-as 65505
         set additional-path both
         set adv-additional-path 4
      next
      edit "10.10.204.254"
         set soft-reconfiguration enable
         set remote-as 65505
         set additional-path both
         set adv-additional-path 4
      next
   end
   config network
      edit 3
         set prefix 22.1.1.0 255.255.255.0
      next
   end
end
Spoke1 # get router info routing-table bgp
Routing table for VRF=0
B*  0.0.0.0/0 [200/0] via 10.10.200.254, vd2-2, 03:57:26
      [200/0] via 10.10.203.254, vd2-3, 03:57:26
      [200/0] via 10.10.204.254, vd2-4, 03:57:26
      [200/0] via 10.10.100.254, vd2-1, 03:57:26
B  1.1.1.1/32 [200/0] via 11.1.1.1 (recursive via 12.1.1.1), 03:57:51
   [200/0] via 11.1.1.1 (recursive via 12.1.1.1), 03:57:51
   [200/0] via 11.1.1.1 (recursive via 12.1.1.1), 03:57:51
   [200/0] via 11.1.1.1 (recursive via 12.1.1.1), 03:57:51
B  11.11.11.11/32 [200/0] via 10.10.200.254, vd2-2, 03:57:51
   [200/0] via 10.10.203.254, vd2-3, 03:57:51
   [200/0] via 10.10.204.254, vd2-4, 03:57:51
```

```
   [200/0] via 10.10.100.254, vd2-1, 03:57:51
B  33.1.1.0/24 [200/0] via 10.10.204.3, vd2-4, 03:57:26
   [200/0] via 10.10.203.3, vd2-3, 03:57:26
   [200/0] via 10.10.200.3, vd2-2, 03:57:26
   [200/0] via 10.10.100.3, vd2-1, 03:57:26
   [200/0] via 10.10.204.3, vd2-4, 03:57:26
   [200/0] via 10.10.203.3, vd2-3, 03:57:26
   [200/0] via 10.10.200.3, vd2-2, 03:57:26
   [200/0] via 10.10.100.3, vd2-1, 03:57:26
   [200/0] via 10.10.204.3, vd2-4, 03:57:26
   [200/0] via 10.10.203.3, vd2-3, 03:57:26
   [200/0] via 10.10.200.3, vd2-2, 03:57:26
   [200/0] via 10.10.100.3, vd2-1, 03:57:26
   [200/0] via 10.10.204.3, vd2-4, 03:57:26
   [200/0] via 10.10.203.3, vd2-3, 03:57:26
   [200/0] via 10.10.200.3, vd2-2, 03:57:26
   [200/0] via 10.10.100.3, vd2-1, 03:57:26
Spoke1 #
```

SLA Logging

The features adds an SD-WAN daemon function to keep a short, 10 minute history of SLA that can be viewed in the CLI.

Performance SLA results related to interface selection, session failover, and other information, can be logged. These logs can then be used for long-term monitoring of traffic issues at remote sites, and for reports and views in FortiAnalyzer.

The time intervals that Performance SLA fail and pass logs are generated in can be configured.

To configure the fail and pass logs' generation time interval:

```
config system virtual-wan-link
    config health-check
        edit "ping"
            set sla-fail-log-period 30
            set sla-pass-log-period 60
        next
    end
end
```

To view the 10 minute Performance SLA link status history:

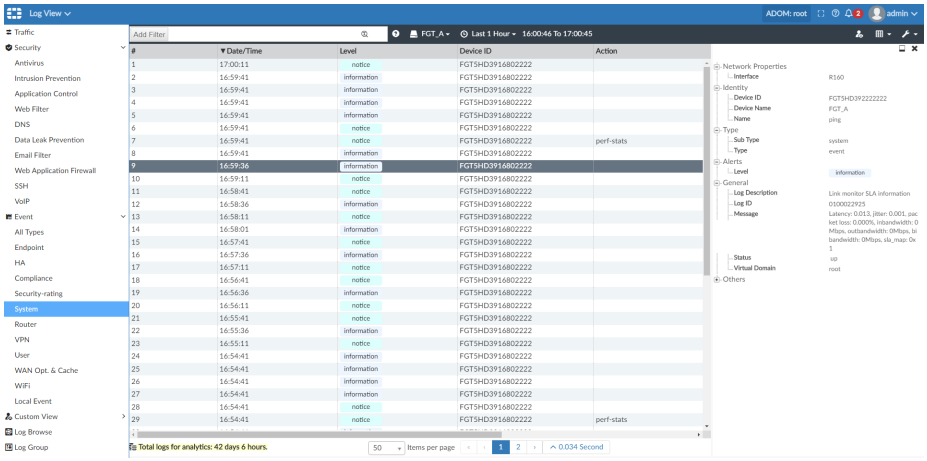
```
FGT_A (root) # diagnose sys virtual-wan-link sla-log ping 1
Timestamp: Thu Feb 28 10:58:24 2019, vdom root, health-check ping, interface: R150, status:
up, latency: 0.000, jitter: 0.000, packet loss: 0.000%.
Timestamp: Thu Feb 28 10:58:24 2019, vdom root, health-check ping, interface: R150, status:
up, latency: 0.097, jitter: 0.000, packet loss: 0.000%.
Timestamp: Thu Feb 28 10:58:25 2019, vdom root, health-check ping, interface: R150, status:
up, latency: 0.058, jitter: 0.040, packet loss: 0.000%.
Timestamp: Thu Feb 28 10:58:25 2019, vdom root, health-check ping, interface: R150, status:
up, latency: 0.044, jitter: 0.026, packet loss: 0.000%.
... ...
```

SLA pass logs

The FortiGate generates Performance SLA logs at the specified pass log interval (`sla-pass-log-period`) when SLA passes.

```
3: date=2019-02-28 time=11:53:26 logid="0100022925" type="event" subtype="system" level-
l="information" vd="root" eventtime=1551383604 logdesc="Link monitor SLA information" name-
e="ping" interface="R160" status="up" msg="Latency: 0.013, jitter: 0.001, packet loss: 0.000%,
inbandwidth: 0Mbps, outbandwidth: 0Mbps, bibandwidth: 0Mbps, sla_map: 0x1"
7: date=2019-02-28 time=11:52:26 logid="0100022925" type="event" subtype="system" level-
l="information" vd="root" eventtime=1551383545 logdesc="Link monitor SLA information" name-
e="ping" interface="R160" status="up" msg="Latency: 0.013, jitter: 0.002, packet loss: 0.000%,
inbandwidth: 0Mbps, outbandwidth: 0Mbps, bibandwidth: 0Mbps, sla_map: 0x1"
```

In the FortiAnalyzer GUI:

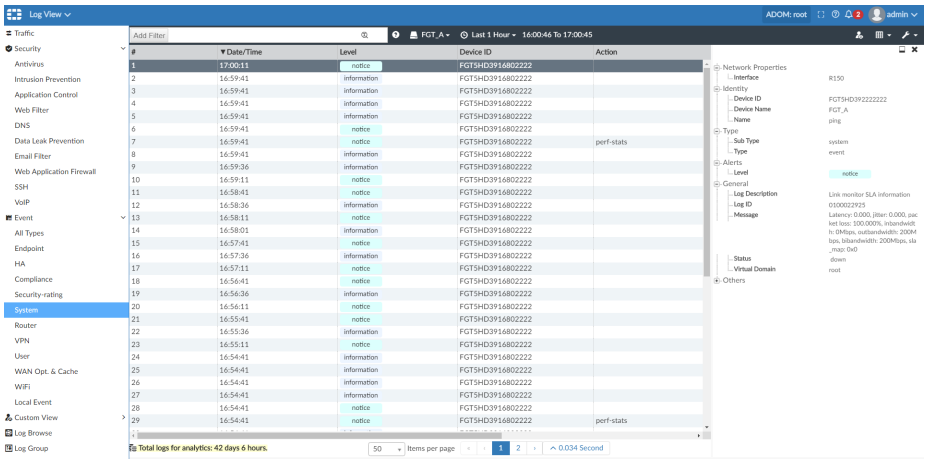


SLA fail logs

The FortiGate generates Performance SLA logs at the specified fail log interval (`sla-fail-log-period`) when SLA fails.

```
6: date=2019-02-28 time=11:52:32 logid="0100022925" type="event" subtype="system" level-
l="notice" vd="root" eventtime=1551383552 logdesc="Link monitor SLA information" name="ping"
interface="R150" status="down" msg="Latency: 0.000, jitter: 0.000, packet loss: 100.000%,
inbandwidth: 0Mbps, outbandwidth: 200Mbps, bibandwidth: 200Mbps, sla_map: 0x0"
8: date=2019-02-28 time=11:52:02 logid="0100022925" type="event" subtype="system" level-
l="notice" vd="root" eventtime=1551383522 logdesc="Link monitor SLA information" name="ping"
interface="R150" status="down" msg="Latency: 0.000, jitter: 0.000, packet loss: 100.000%,
inbandwidth: 0Mbps, outbandwidth: 200Mbps, bibandwidth: 200Mbps, sla_map: 0x0"
```

In the FortiAnalyzer GUI:



Internet Service Customization

This version introduces new flexibility to tune Internet Service DB (ISDB) entries for their environments. A new CLI option allows the admin to add custom port and port ranges into their predefined ISDB entries.

Use the new CLI `config firewall internet-service-addition` command in `system.global` to tune ISDB for your environment.

To add custom port range in global:

```
config firewall internet-service-addition
  edit 65646
      set comment "Add custom port-range:tcp/8080-8090 into 65646"
      config entry
          edit 1
              set protocol 6
              config port-range
                    edit 1
                          set start-port 8080
                          set end-port 8090
                    next
              end
          next
      end
  next
end
```

To execute internet-service refresh to apply the change:

```
 FGT-201E (65646) # end
 Warning: Configuration will only be applied after rebooting or using the 'execute internet-
service refresh' command.

 FGT-201E (global) # exec internet-service refresh
 Internet Service database is refreshed.
```

To verify that the change was applied:

```
FGT-201E (global) # diagnose internet-service info FG-traffic 6 8080 2.20.183.160
Internet Service: 65646(Google.Gmail)
FGT-201E (global) #
```

Multi-Cloud

This section lists the new features added to FortiOS for multi-cloud.

AWS Extensions

This section lists the new features added for AWS extensions.

Cross AZ High Availability Support

In 6.2, FortiGate High Availability (Active/Passive) can be deployed in AWS across Availability Zones (AZs).

With FortiGates of an HA pair in separate AZs, one FortiGate can remain operational if the other AZ fails.

This configuration supports the following HA features:

- Config synchronization
- IP failover
- Route failover

The following HA features are not supported with this configuration:

- Session pickup
- Session synchronization

Topology

FortiOS uses a normal HA configuration that uses unicast.

AWS uses the following configuration:

- 1 VPC 10.0.0.0/16 CIDR
  - 8 Subnets
    - 4 in Availability Zone A - Master FGTA has a NIC in each of these:
      - Public: 10.0.0.0/24 EIP
      - Internal: 10.0.1.0/24

        - Heartbeat: 10.0.2.0/24
        - Management: 10.0.3.0/24 EIP
    - 4 in Availability Zone B - Slave FGTB has a NIC in each of these:
        - Public 10.0.10.0/24
        - Internal 10.0.11.0/24
        - Heartbeat 10.0.12.0/24
        - Management 10.0.13.0/24 EIP
- 3 AWS UDR Routing Tables
    - For Public, add default route to Internet Gateway
    - For Internal, add default to Master FortiGate internal NIC
    - For all others, leave it default with AWS local address

Example

* Same as regular AWS HA unicast peering

```
##MASTER##
config system interface
edit "port1"
set vdom "root"
set ip 10.0.0.11 255.255.255.0
set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response cap
set type physical
set snmp-index 1
set mtu-override enable
set mtu 9001
next
edit "port2"
set vdom "root"
set ip 10.0.1.11 255.255.255.0
set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response cap
set type physical
set snmp-index 3
set mtu-override enable
set mtu 9001
next
edit "port3"
set ip 10.0.2.11 255.255.255.0
set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response cap
set type physical
set snmp-index 4
next
edit "port4"
set ip 10.0.3.11 255.255.255.0
set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response cap
set type physical
set snmp-index 5
next
edit "ssl.root"
set vdom "root"
set type tunnel
set alias "SSL VPN interface"
set snmp-index 2
```

```
next
end
config router static
edit 1
set gateway 10.0.0.1
set device "port1"
next
edit 2
set dst 10.0.11.0 255.255.255.0
set gateway 10.0.1.1
set device "port2"
next
end
config system ha
set group-name "test"
set mode a-p
set hbdev "port3" 50
set session-pickup enable
set ha-mgmt-status enable
config ha-mgmt-interfaces
edit 1
set interface "port4"
set gateway 10.0.3.1
next
end
set override disable
set priority 255
set unicast-hb enable
set unicast-hb-peerip 10.0.12.11
end

##SLAVE##
config system interface
edit "port1"
set vdom "root"
set ip 10.0.10.11 255.255.255.0
set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response cap
set type physical
set snmp-index 1
set mtu-override enable
set mtu 9001
next
edit "port2"
set vdom "root"
set ip 10.0.11.11 255.255.255.0
set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response cap
set type physical
set snmp-index 2
set mtu-override enable
set mtu 9001
next
edit "port3"
set ip 10.0.12.11 255.255.255.0
set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response cap
set type physical
set snmp-index 3
```

```
set mtu-override enable
set mtu 9001
next
edit "port4"
set ip 10.0.13.11 255.255.255.0
set allowaccess ping https ssh snmp http telnet fgfm radius-acct probe-response cap
set type physical
set snmp-index 4
set mtu-override enable
set mtu 9001
next
edit "ssl.root"
set vdom "root"
set type tunnel
set alias "SSL VPN interface"
set snmp-index 5
next
end
config router static
edit 1
set gateway 10.0.10.1
set device "port1"
next
edit 2
set dst 10.0.1.0 255.255.255.0
set gateway 10.0.11.1
set device "port2"
next
end
config system ha
set group-name "test"
set mode a-p
set hbdev "port3" 50
set session-pickup enable
set ha-mgmt-status enable
config ha-mgmt-interfaces
edit 1
set interface "port4"
set gateway 10.0.13.1
next
end
set override disable
set priority 1
set unicast-hb enable
set unicast-hb-peerip 10.0.2.11
end

##Trigger Failover##

slave # Become HA master
send_vip_arp: vd root master 1 intf port1 ip 10.0.10.11
send_vip_arp: vd root master 1 intf port2 ip 10.0.11.11
awsd get instance id i-0b29804fd38976af4
awsd get iam role WikiDemoHARole
awsd get region us-east-1
awsd get vpc id vpc-0ade7ea6e64befbfc
```

```
                    awsd doing ha failover for vdom root
                    awsd associate elastic ip for port1
                    awsd associate elastic ip allocation eipalloc-06b849dbb0f76555f to 10.0.10.11 of en
0ab045a4d6dce664a
                    awsd associate elastic ip successfully
                    awsd update route table rtb-0a7b4fec57feb1a21, replace route of dst 0.0.0.0/0 to en
0c4c085477aaff8c5
                    awsd update route successfully
```

Google Cloud Platform (GCP) Extensions

This section lists the new features added for GCP extensions.

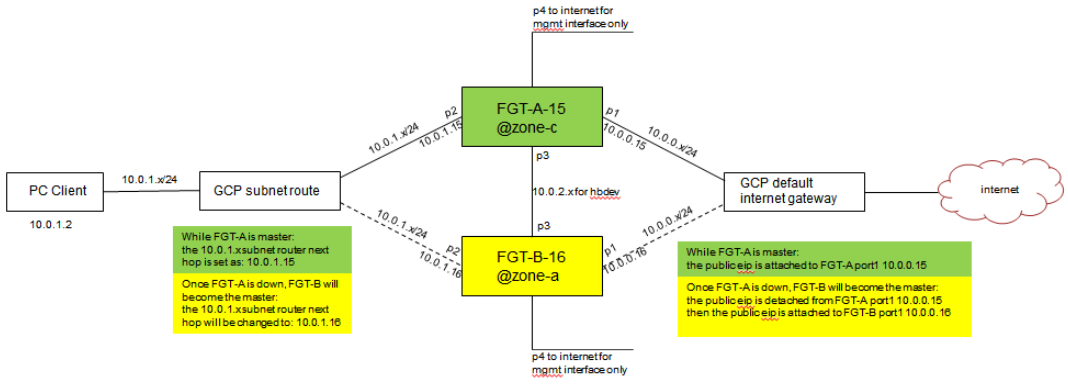
HA Between Zones

6.2 supports auto-scaling HA (High Availability) between Zones in Google Cloud environments.

Example

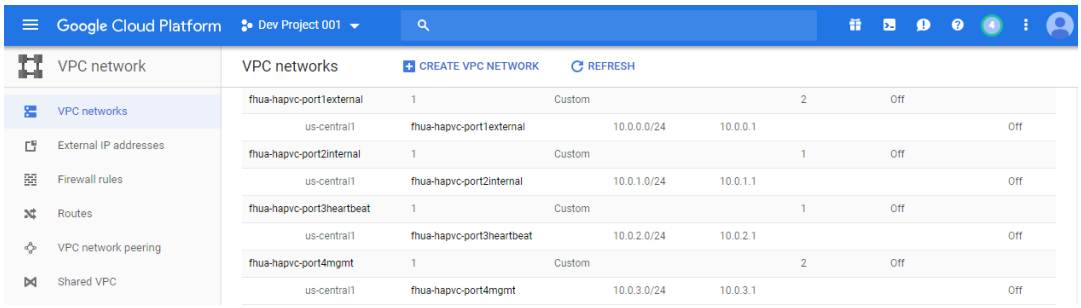
Following is an overview of how the feature works:

1. Create FGT-A as a master on one zone with metadata that has ha-master configuration.
2. Create FGT-B as a slave on another zone with metadata that has ha-slave configuration.
3. Create a PC that can access the Internet via FGT-HA.
4. Shut down FGT-A, and FGT-B become the master to handle traffic. The public EIP will attach to FGT-B.

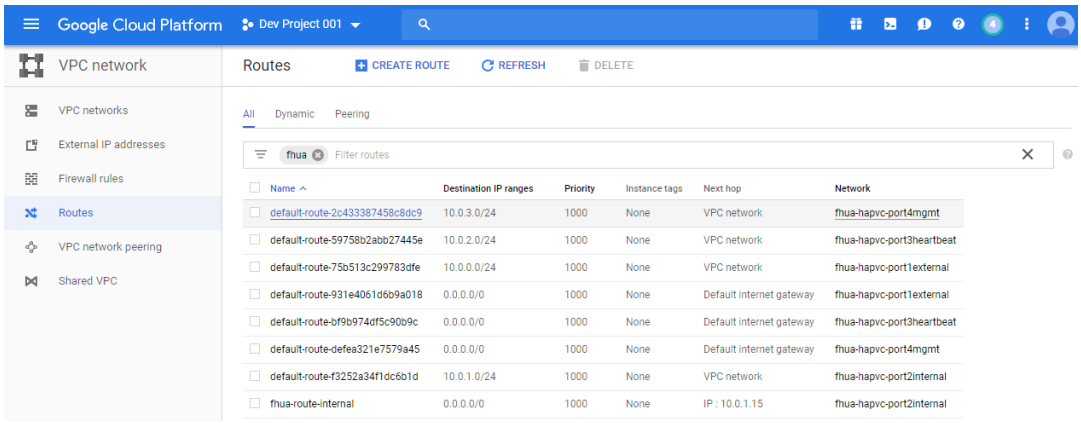


To configure HA between zones:

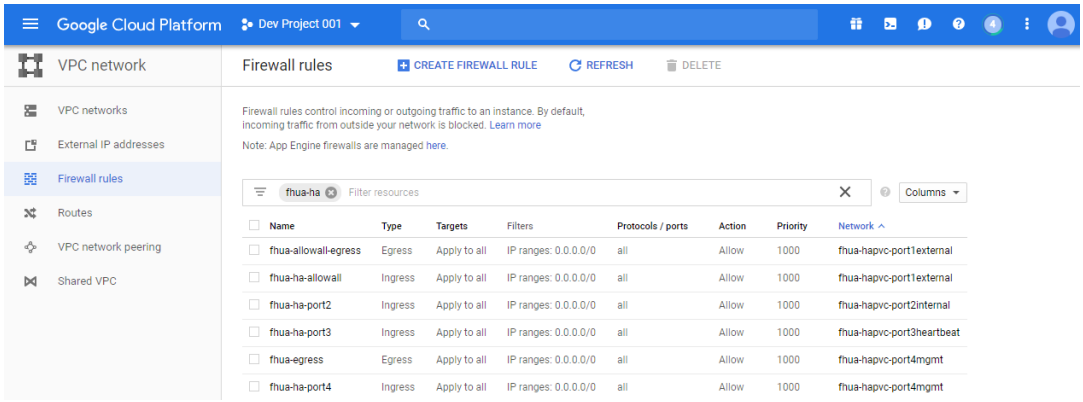
1. Create 4 VPC networks in region, such as us-central1.



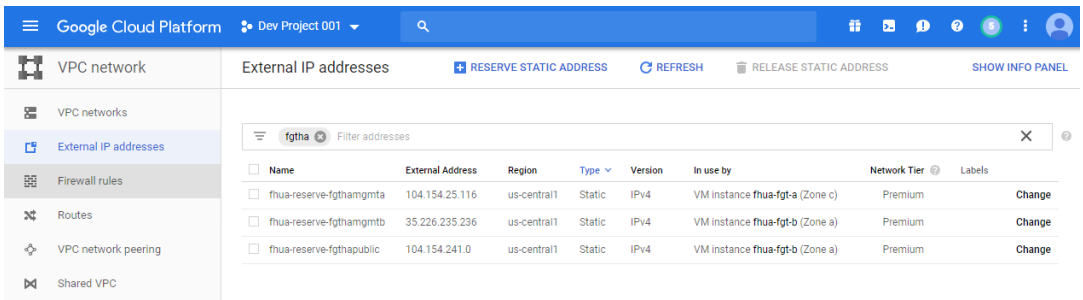
2. Create routes for each network.



3. Create firewall rules for each network.



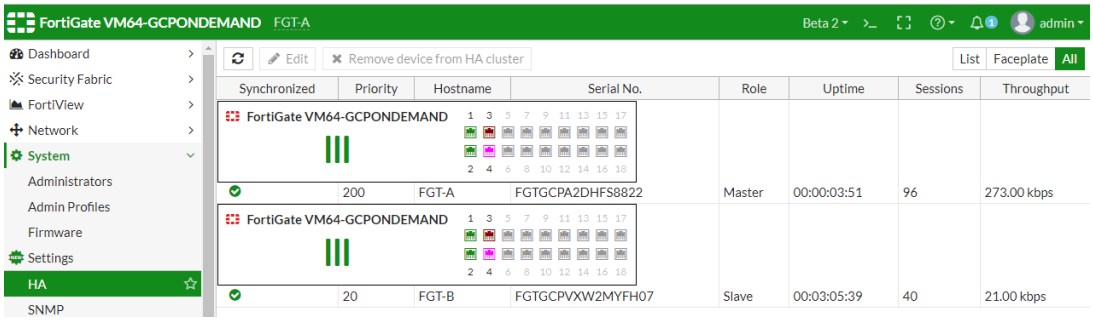
4. Reserve three external IP addresses for convenience.



5. Create both FGT-A and FGT-B in GCP:

```
gcloud beta compute --project=dev-project-001-166400 instances create fhua-fgt-a --zone=us-
      central1-c --machine-type=n1-standard-4 --network-tier=PREMIUM --can-ip-forward --
      maintenance-policy=MIGRATE --service-account=966517025500-
      compute@developer.gserviceaccount.com --scopes=https://www.googleapis.com/auth/cloud-
      platform --image=fhua-ond-0804 --image-project=dev-project-001-166400 --boot-disk-
      type=pd-standard --boot-disk-device-name=fhua-fgt-0804 --network-interface
      subnet=fhua-hapvc-port1external,private-network-ip=10.0.0.15,address=104.154.241.0 --
      network-interface subnet=fhua-hapvc-port2internal,private-network-ip=10.0.1.15,no-
      address --network-interface subnet=fhua-hapvc-port3heartbeat,private-network-
      ip=10.0.2.15,no-address --network-interface subnet=fhua-hapvc-port4mgmt,private-
      network-ip=10.0.3.15,address=104.154.25.116 --metadata-from-file user-
      data=/home/gcloud/config/master.conf
gcloud beta compute --project=dev-project-001-166400 instances create fhua-fgt-b --zone=us-
      central1-a --machine-type=n1-standard-4 --network-tier=PREMIUM --can-ip-forward --
      maintenance-policy=MIGRATE --service-account=966517025500-
      compute@developer.gserviceaccount.com --scopes=https://www.googleapis.com/auth/cloud-
      platform --image=fhua-ond-0804 --image-project=dev-project-001-166400 --boot-disk-
      type=pd-standard --boot-disk-device-name=fhua-fgt-0804 --network-interface
      subnet=fhua-hapvc-port1external,private-network-ip=10.0.0.16,no-address --network-
      interface subnet=fhua-hapvc-port2internal,private-network-ip=10.0.1.16,no-address --
      network-interface subnet=fhua-hapvc-port3heartbeat,private-network-ip=10.0.2.16,no-
      address --network-interface subnet=fhua-hapvc-port4mgmt,private-network-
      ip=10.0.3.16,address=35.226.235.236 --metadata-from-file user-
      data=/home/gcloud/config/slave.conf
```

After the FGT-VM-GCP is set up, you can view it in the FortiOS GUI:



6. Configure FGT-A:

```
config system ha
   set group-id 21
   set group-name "cluster1"
   set mode a-p
   set hbdev "port3" 50
   set session-pickup enable
   set session-pickup-connectionless enable
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
      edit 1
         set interface "port4"
         set gateway 10.0.3.1
      next
   end
   set override enable
   set priority 200
   set unicast-hb enable
   set unicast-hb-peerip 10.0.2.16
   set unicast-hb-netmask 255.255.255.0
```

```
end
config system sdn-connector
   edit "gcp_conn"
      set type gcp
      set ha-status enable
      config external-ip
         edit "fhua-reserve-fgthapublic"
         next
      end
      config route
         edit "fhua-route-internal"
         next
      end
         set use-metadata-iam disable
      set gcp-project "..."
      set service-account "..."
      set private-key "..."
   next
end
```

7. Configure FGT-B:

```
config system ha
   set group-id 21
   set group-name "cluster1"
   set mode a-p set hbdev "port3" 50
   set session-pickup enable
   set session-pickup-connectionless enable
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
      edit 1
         set interface "port4"
         set gateway 10.0.3.1
      next
   end
   set override enable
   set priority 20
   set unicast-hb enable
   set unicast-hb-peerip 10.0.2.15
   set unicast-hb-netmask 255.255.255.0
end
```

8. Create a PC that can access the Internet via FGT-HA.

Auto Scaling

This version supports auto scaling for Google Cloud environments.

Sample configuration

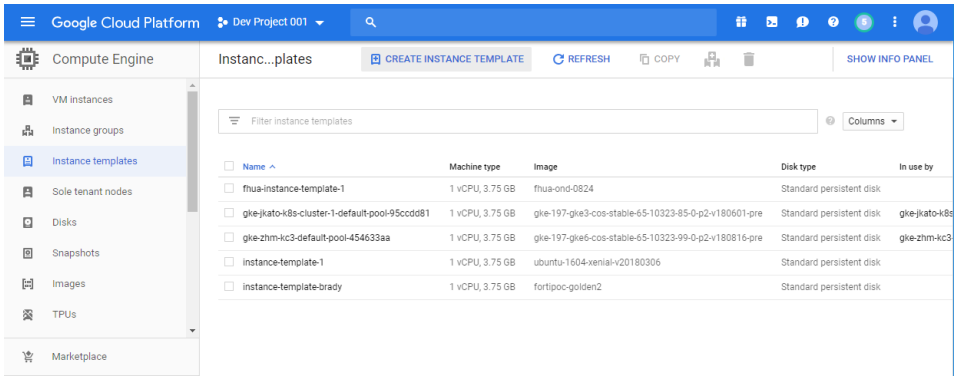
To set up auto scaling for a Google Cloud environment:

1. Create an instance template with Google Cloud Platform console.
2. Create an instance group with Google Cloud Platform console.
3. Set the first FortiGate VM in the auto scaling group as the master member.

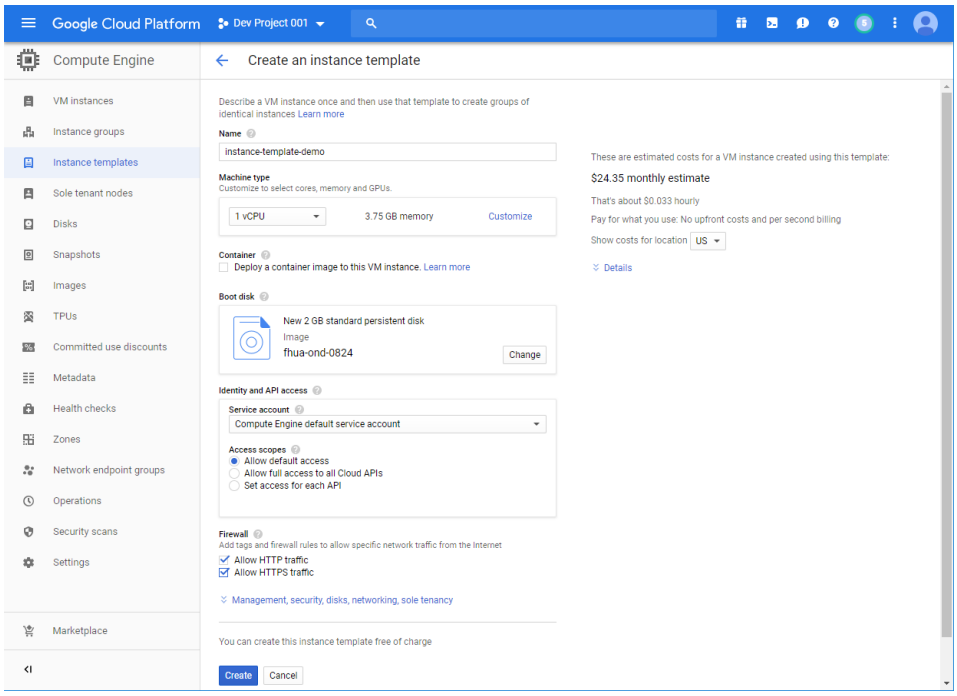
4. Scale out another FortiGate VM and set it as a slave member; and then synchronize configuration from master to slave.

To create an instance template with Google Cloud Platform console:

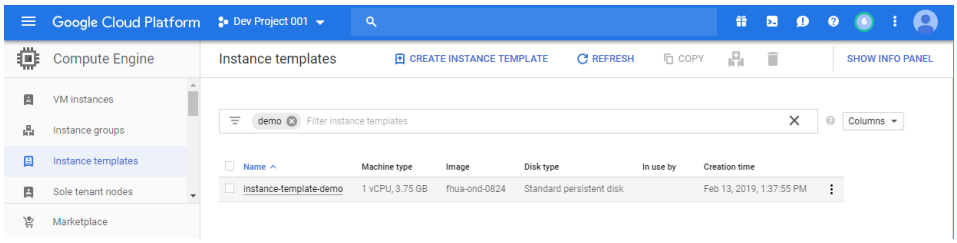
1. Go to *Instance templates* console and click *CREATE INSTANCE TEMPLATE*.



2. Configure the instance template.
   - Enter the instance template *Name*, for example *instance-template-demo*.
   - Select the *Machine type*.
   - Change *Boot disk* to your FortiGate VM image.
   - In the *Firewall* section, select *Allow HTTP traffic* and *Allow HTTPS traffic*.
   - Click *Create*.

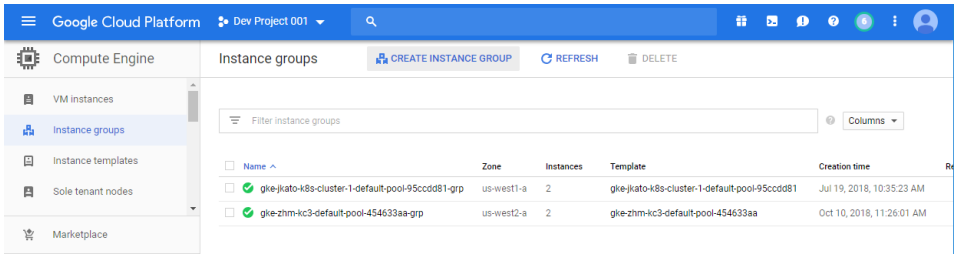


3. Go to *Instance templates* console and check that your instance template is created.

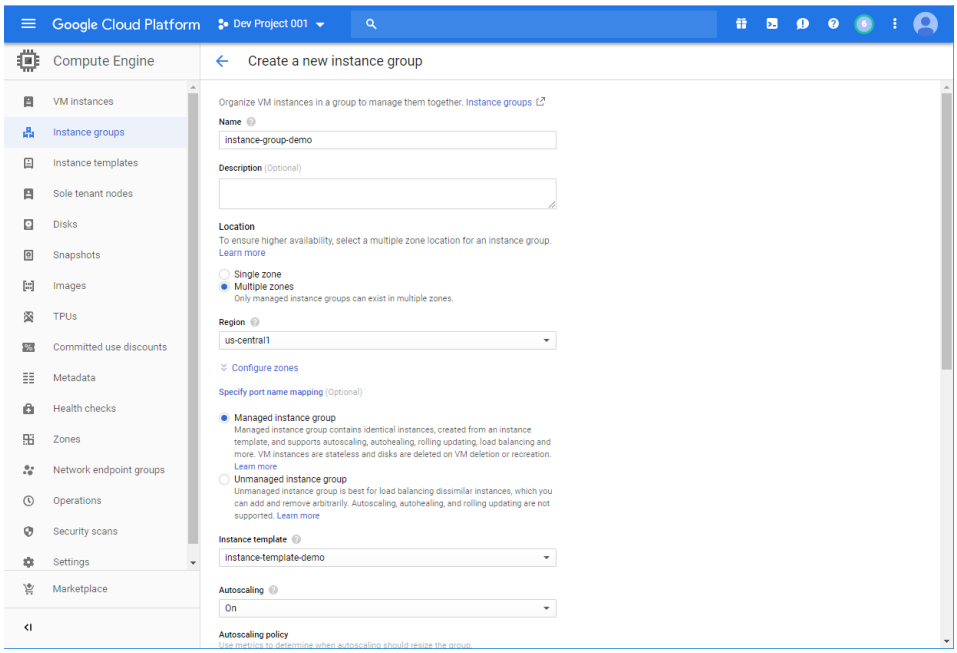


To create an instance group with Google Cloud Platform console:

1. Go to *Instance groups* console and click *CREATE INSTANCE GROUP*.

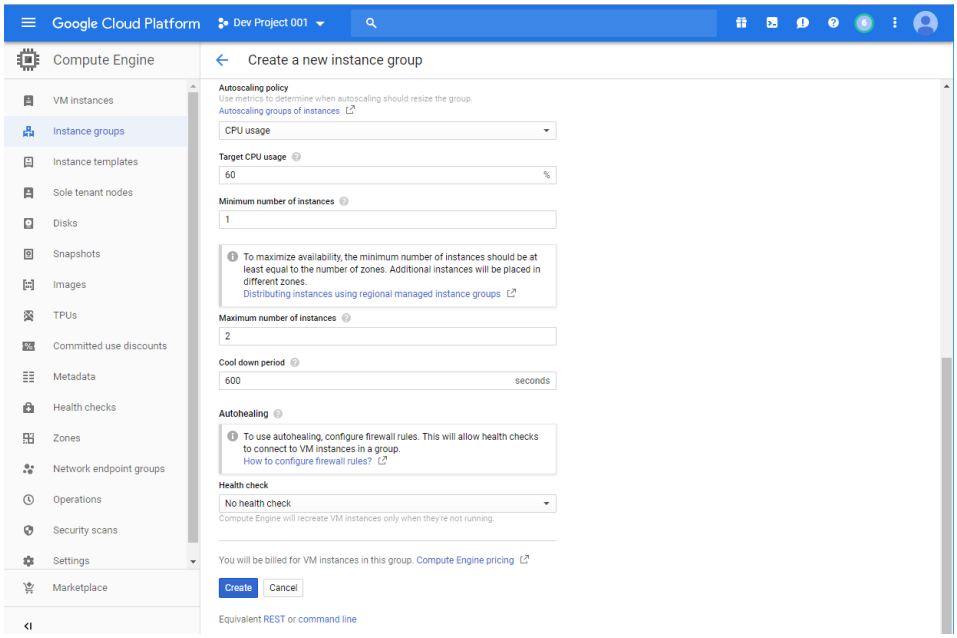


2. Configure the instance group.
   - Enter the instance group *Name*, for example *instance-group-demo*.
   - Select the *Instance template* you created.
   - For *Autoscaling*, select *On*.

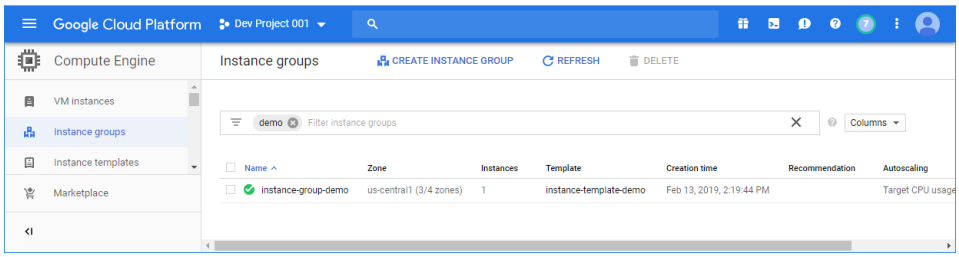


   - For *Autoscaling policy*, select *CPU usage*.
   - Enter the *Target CPU usage* percentage. For example, *60%*.
   - Enter the *Maximum number of instances* that you want for this instance group.

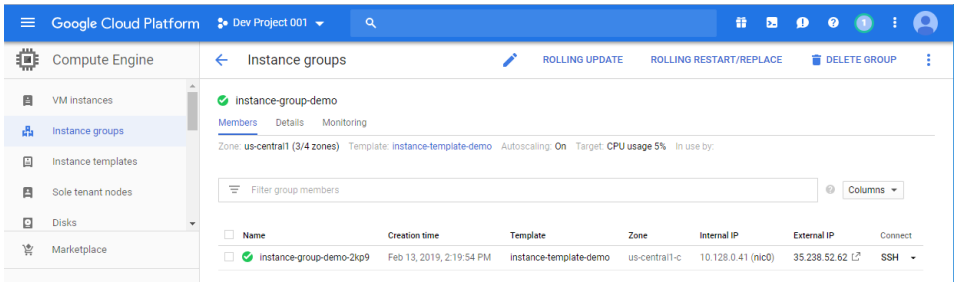
- If desired, enter the *Minimum number of instances* and *Cool down period*.
  The cool down period is the number of seconds auto scaling waits after a VM starts before collecting information from it. The time is typically the VM initialization time, when the collected usage is not reliable for auto scaling. The default cool down period is 60 seconds.
- Click *Create*.



3. Go to *Instance groups* console and check that your instance group is created.



4. Wait a few moments and click the instance group to check if an instance was launched automatically, since the minimum number of instances is set to 1.
   In this example, the first FortiGate VM instance name is *instance-group-demo-2kp9*.

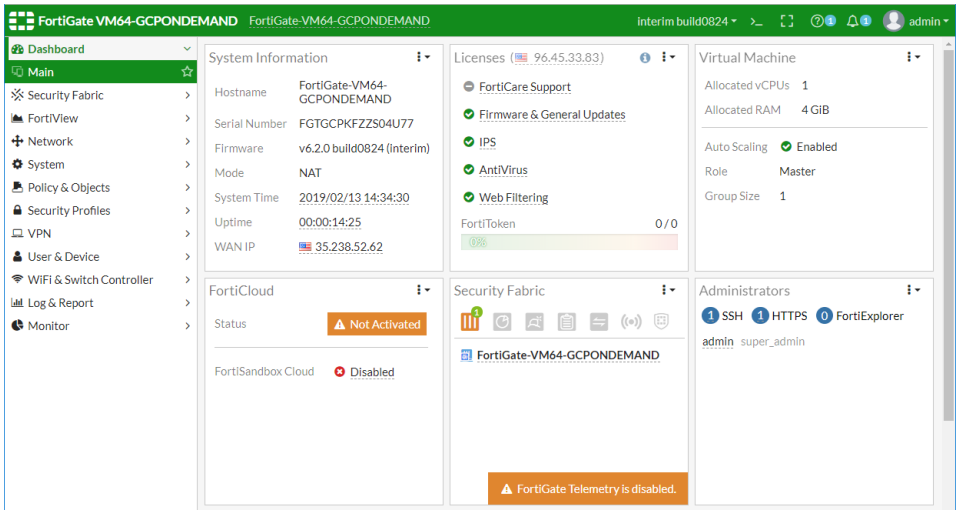


To set the first FortiGate VM in the auto scaling group as the master member:

1. Log into the FortiGate VM as administrator and the instance ID as the default password.
2. Use the CLI to enable auto scaling and set the role to master.

```
config system auto-scale
    set status enable
    set role master
    set sync-interface "port1"
    set psksecret xxxxxx
end
```

3. In the GUI, go to the *Dashboard Virtual Machine* widget to check that *Auto Scaling* is enabled and *Role* is *Master*.

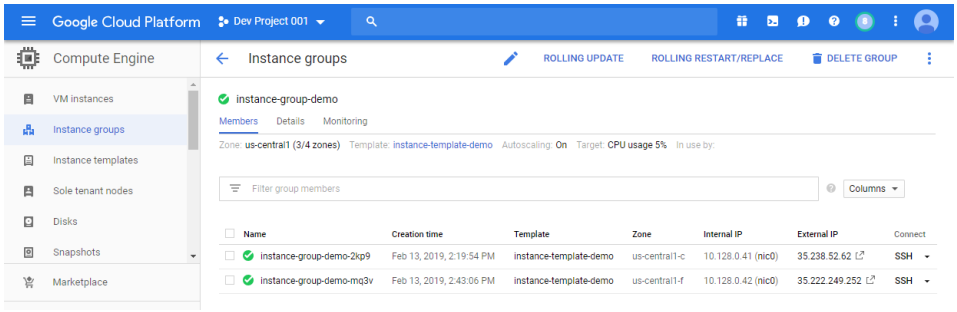


To scale out another FortiGate VM and set it as a slave member; and then synchronize configuration from master to slave:

1. Generate test traffic on the FortiGate VM where the CPU rate is higher than the instance group target CPU usage. For test purpose, you can also change the target CPU usage to a small value.

   The instance group will trigger to scale out an new FortiGate VM.

   In this example, the second FortiGate VM instance name is *instance-group-demo-mq3v*.



2. Log into the second FortiGate VM as administrator and the instance ID as the default password.
   Use the CLI to enable auto scaling and set the role to slave.

   For the `master-ip`, use the IP of the master member sync interface. The master IP should be the master side private IP address.

   Check that the configuration can be synced from the master member to the slave member.

```
config system auto-scale
    set status enable
    set role slave
    set sync-interface "port1"
    set master-ip 10.128.0.41
    set psksecret xxxxxx
end
```

3. Wait a few moments for the slave member to sync with the master member; and then the slave member can sync the FortiGate configuration from the master member.

```
FortiGate-VM64-GCPON~AND # diag deb app hasync -1
slave's configuration is not in sync with master's, sequence:0
slave's configuration is not in sync with master's, sequence:1
slave's configuration is not in sync with master's, sequence:2
slave's configuration is not in sync with master's, sequence:3
slave's configuration is not in sync with master's, sequence:4
slave starts to sync with master
logout all admin users
```

Oracle Cloud Extensions

This section lists the new features added for Oracle Cloud extensions.

IAM Authentication

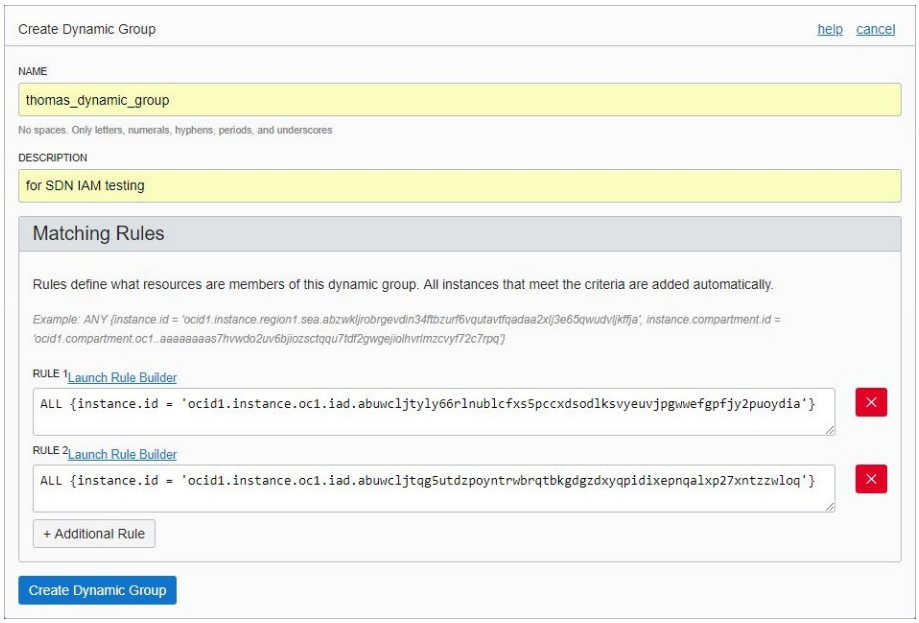
This feature adds the ability to use IAM credentials for Oracle Cloud Infrastructure (OCI) SDN connector functionality, including HA and dynamic address updating.

Prior to enabling IAM credentials for an SDN connector, a dynamic group and policy must configured on OCI. The SDN connector can then be configured using the FortiGate CLI or GUI.

To configure OCI:

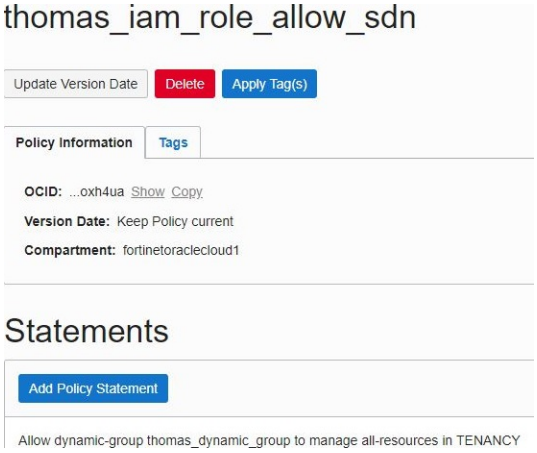
1. Create a *Dynamic Group* that includes rules to allow an instance that matches the FortiGate HA device's instance ID. For example:

```
ALL {instance.id =
     'ocid1.instance.oc1.iad.abuwcljtkqllbq6yxgxtowybgc4ht6sxqpfccckjj23p6pbfmvbl52uttb
     iq'}
ALL {instance.id =
     'ocid1.instance.oc1.iad.abuwcljttcylhekauqy42jzpsnu2dkalbhnlulqxfe2az24fktcuhtj65v
     nq'}
```



2. Create a policy that allows that group to manage all resources:

```
Allow dynamic-group API to manage all-resources in TENANCY
```



To Configure the FortiGate using the CLI:

1. Configure the SDN connector:

```
config system sdn-connector
   edit "oci-sdn"
      set status enable
      set type oci
      set ha-status enable
      set tenant-id
           "ocid1.tenancy.oc1..aaaaaaaambr3uzztoyhweohbzqqdo775h7d3t54zpmzkp4b2cf35vs55c
           k3a"
      set user-id
           "ocid1.user.oc1..aaaaaaaaq2lfspeo3uetzbzpiv2pqvzzevozccnys347stwssvizqlatfv7
           q"
      set compartment-id
           "ocid1.tenancy.oc1..aaaaaaaambr3uzztoyhweohbzqqdo775h7d3t54zpmzkp4b2cf35vs55c
           k3a"
```

```
        set oci-region ashburn
        set oci-cert ''
        set use-metadata-iam enable
        set update-interval 60
    next
  end
```

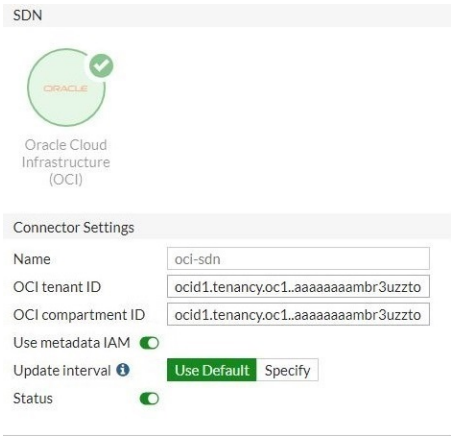
2. Confirm the HA failover succeeds on the secondary HA device:

```
# HA event
OCI sdn connector oci-sdn updating

Updating Compartment: fortinetoraclecloud1
VM FAZ-B1750
ip are 129.213.120.204:10.0.0.5
VM fmg-b1746
Become HA master mode 2
ocid collect vnics info for instance thomas-slave
vnic state: ATTACHED
vnic id(1/4):
ocid1.vnic.oc1.iad.abuwcljt5f2ehfi2zlkhqqbrewgrnpy7iqhsxuqyad7k6natuq42lsqo3hfq
ip are 129.213.138.127:10.0.0.5
VM fmg-b1781
vnic state: ATTACHED
vnic id(2/4):
ocid1.vnic.oc1.iad.abuwcljtk6t4glgvzjy5rwk3jywsthbyoxjdbojwouppnwdnbpadpnr3unra
vnic state: ATTACHED
vnic id(3/4):
ocid1.vnic.oc1.iad.abuwcljtipazqefscqeml15forvnzfmo5zh22zjaeahnbph67wjmm7gd6qha
ip are 132.145.170.31:10.0.0.14
VM instance-20180813-1141
vnic state: ATTACHED
vnic id(4/4):
ocid1.vnic.oc1.iad.abuwcljtyy3mvw7uqoefma6vx5y5g7bzjw4hycr37urncf53xyyzntzfeqza
ocid fail over private ip: 10.0.1.15
ip are 129.213.124.225:10.0.0.2
VM instance-20181024-1439
private ip 10.0.1.15 is attached in remote instance
attaching private ip 10.0.1.15 to local vnic
(ocid1.vnic.oc1.iad.abuwcljtk6t4glgvzjy5rwk3jywsthbyoxjdbojwouppnwdnbpadpnr3unra)
updating private ip with data: {"vnicId":
"ocid1.vnic.oc1.iad.abuwcljtk6t4glgvzjy5rwk3jywsthbyoxjdbojwouppnwdnbpadpnr3unra"}
ip are 132.145.173.187:10.0.0.11
ip are 132.145.173.187:10.0.10.2
VM instance-20181128-1505
ip are 132.145.162.119:10.0.0.3
VM instance-20181214-1616
moving private ip 10.0.1.15 to local successfully

ocid fail over private ip: 10.0.0.15
ip are 132.145.167.255:10.0.0.15
VM jkato-fgt603-dev005
private ip 10.0.0.15 is attached in remote instance
attaching private ip 10.0.0.15 to local vnic
(ocid1.vnic.oc1.iad.abuwcljtipazqefscqeml15forvnzfmo5zh22zjaeahnbph67wjmm7gd6qha)
updating private ip with data: {"vnicId":
```

```
"ocid1.vnic.oc1.iad.abuwcljtipazqefscqeml15forvnzfmo5zh22zjaeahnbph67wjmm7gd6qha"}
moving private ip 10.0.0.15 to local successfully
```

To Configure the FortiGate using the GUI:

1. Go to *Security Fabric* > *Fabric Connectors*.
2. Click *Create New*, then select *Oracle Cloud Infrastructure (OCI)* from the *SDN* category.
3. Fill in the *Name*, *User ID*, *OCI tenant ID*, and *OCI compartment ID*.
4. Enable *Use metadata IAM*.



5. Configure the *Update Interval* and *Status*, then click *OK*.
6. Go to *Policy and Objects* > *Addresses* to check that the dynamic address can update.

Paravirtualized Mode Support

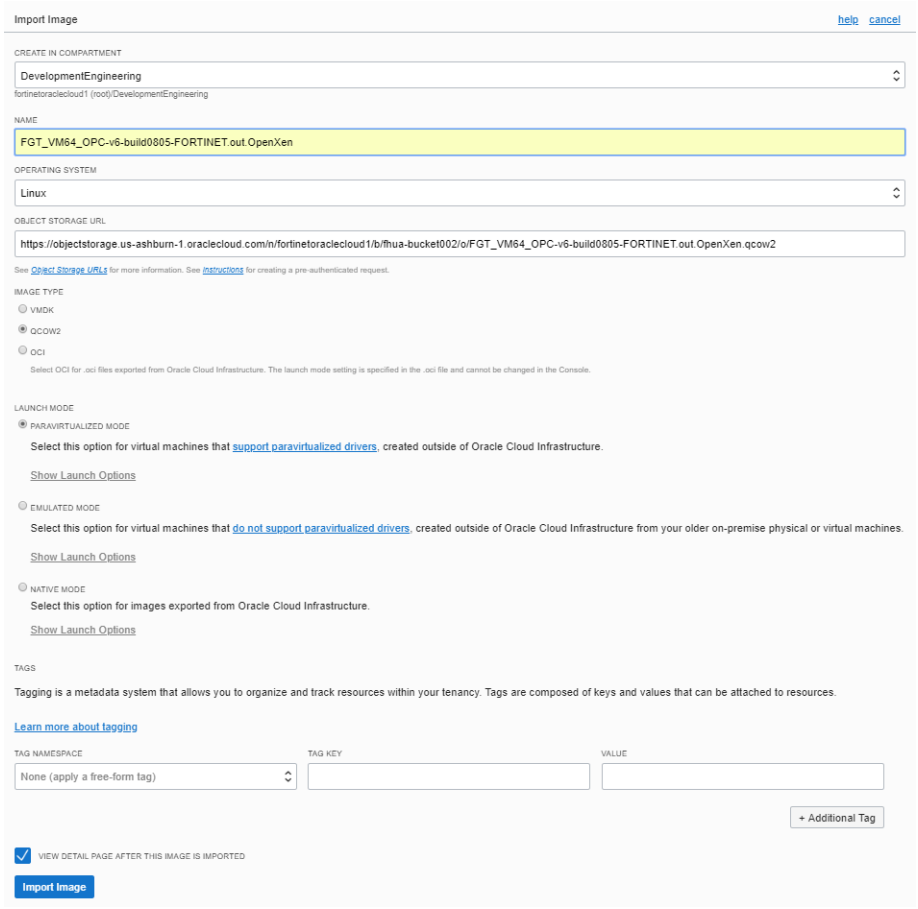
FGT_VM64_OPC now supports the new paravirtualized mode on Oracle Cloud Infrastructure (OCI).

The below instructions assume that the user already has an OCI account.

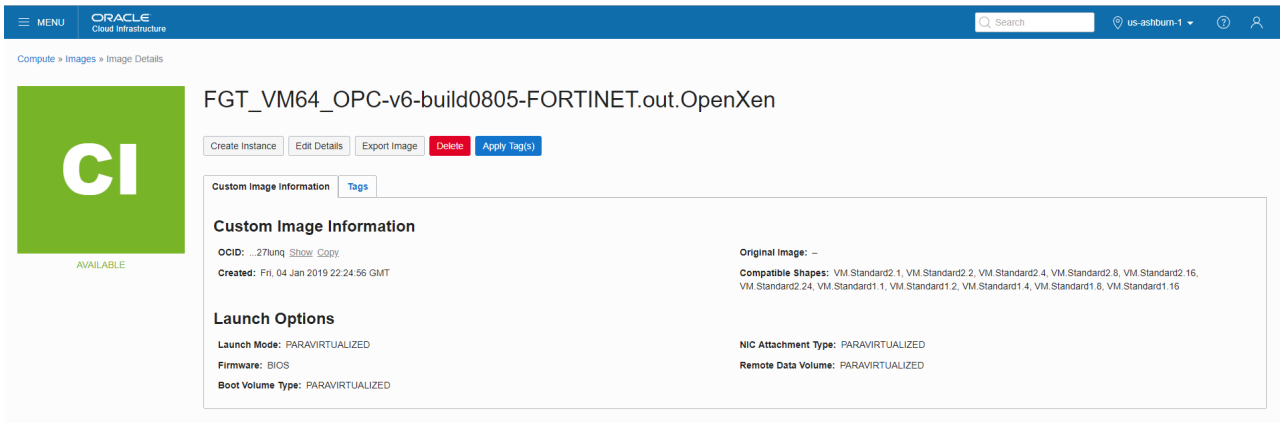
To launch a FortiGate-VM instance with paravirtualized mode:

1. Obtain the deployment image file:
   a. Go to Customer Service & Support. Navigate to *Download* > *VM Images* in the top menu.
   b. In the *Select Product* dropdown list, select *FortiGate*.
   c. In the *Select Platform* dropdown list, select *Oracle*.
   d. Obtain the FGT_VM64_OPC-vX-buildXXXX-FORTINET.out.OpenXen.zip file. XXXX is the build number. Ensure the file name includes OpenXen.
   e. After downloading, unzip the file. You will find the forties.qcow2 file, which is needed to deploy the FortiGate on OCI. Rename the file to FGT_VM64_OPC-v6-build0805-FORTINET.out.OpenXen.qcow2.
2. Upload the deployment image file:
   a. In OCI, go to *Storage* > *Object Storage*. Click an existing storage bucket or create a new bucket.
   b. Select the desired bucket, then upload the deployment image file FGT_VM64_OPC-v6-build0805-FORTINET.out.OpenXen.qcow2.
   c. Click *Upload Object*. The dialog shows the upload progress.

3. Copy the qcow2 file URL:
   a. From the *Storage* > *Object Storage* > *Bucket Details* page, click *Create Pre-Authenticated Requests*.
   b. Copy the URL under *PRE-AUTHENTICATED REQUEST URL*.
4. Create a FortiGate-VM image in paravirtualized mode:
   a. In OCI, go to *Compute* > *Custom Images*, then click *Import Image*.
   b. In the *OBJECT STORAGE URL* field, paste the URL copied in step 3.
   c. Under *IMAGE TYPE*, select *QCOW2*.
   d. Under *LAUNCH MODE*, select *PARAVIRTUALIZED MODE*.
   e. Configure other fields as desired, then click *Import Image*.



5. On the *Image Details* page, click *Create Instance* to create an instance with the newly created image.



The paravirtualized mode FortiGate-VM instance boots up and functions as expected.

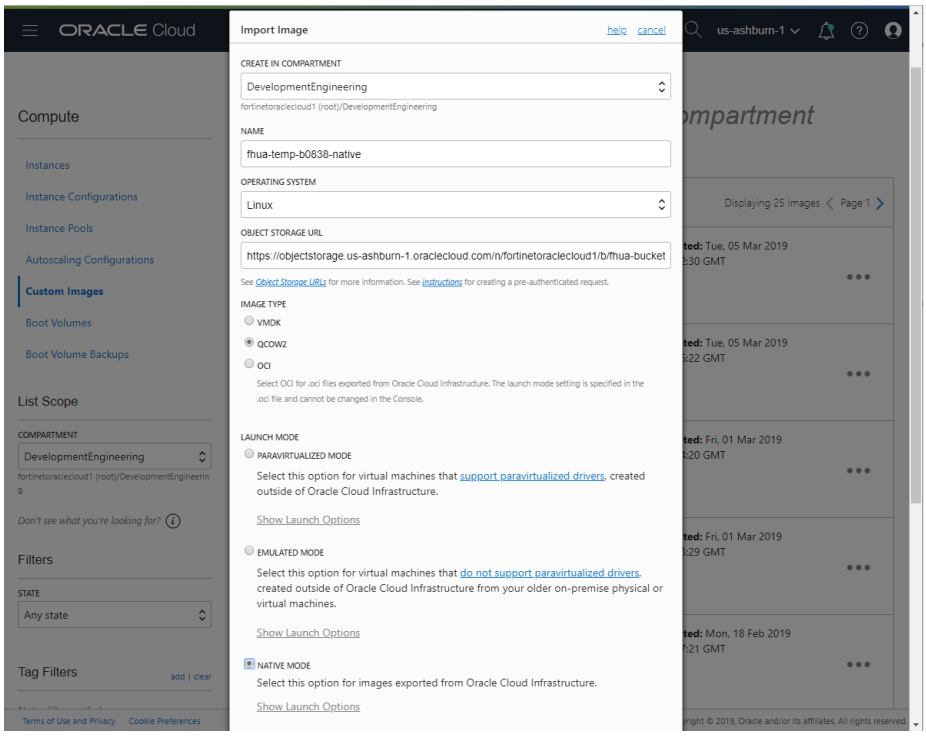
Native Mode Support for OCI

FGT_VM64_OPC now supports native mode on Oracle Cloud Infrastructure (OCI), in addition to emulation mode and paravirtualized mode. This version also supports iSCSI type hard disks.

To create a native mode FGT_VM64_OPC custom image:

1. Download the FGT image for OCI. The naming convention is: *FGT_VM64_OPC-v6-buildxxxx-FORTINET.out.OpenXen.zip*.
2. Unzip the file to get *fortios.qcow2*.
3. Upload *fortios.qcow2* to the OCI object storage and copy the file URL path (URI), for example, `https://objectstorage.us-ashburn-1.oraclecloud.com/n/fortinetoraclecloud1/b/fhua-bucket002/o/fortios.qcow2`.
4. Log into the Oracle Cloud web portal and go to *Compute* > *Custom Images* > *Import Image*.
5. Enter the image *NAME*, in this example, *fhua-temp-b0838-native*.
6. For *OPERATING SYSTEM*, select *Linux*.
7. For the *OBJECT STORAGE URL*, paste the URI you copied when you uploaded *fortios.qcow2*.
8. For *IMAGE TYPE*, select *QCOW2*.
9. For *LAUNCH MODE*, select *NATIVE MODE*.

10. Click *Import Image*.

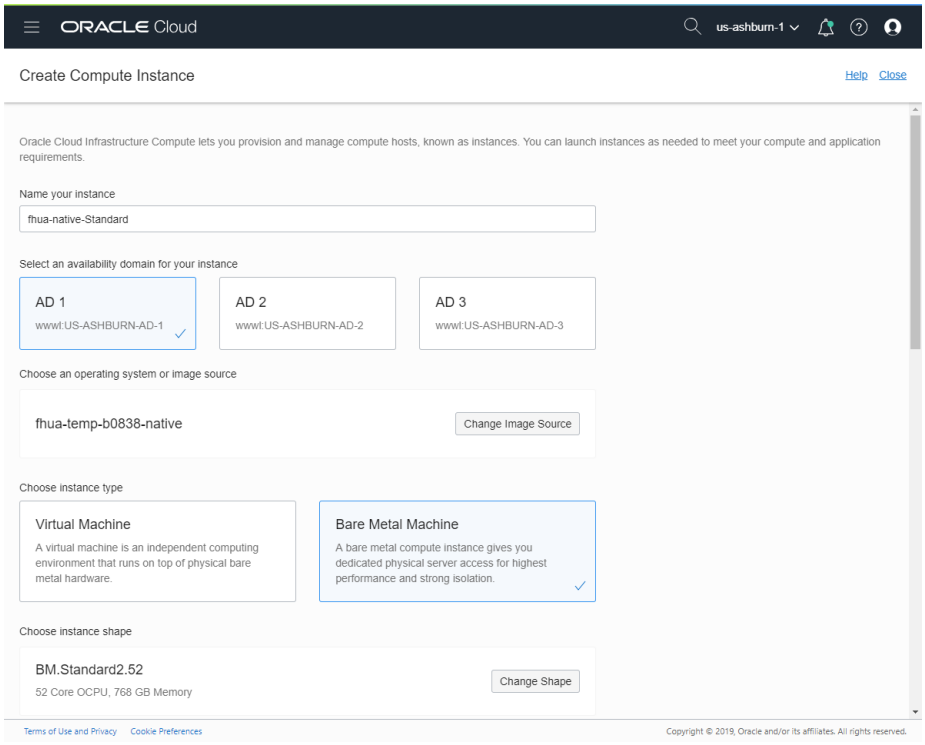


When the import is complete, the FortiGate for OCI custom image is available. In this example, the custom image name is *fhua-temp-b0838-native*.

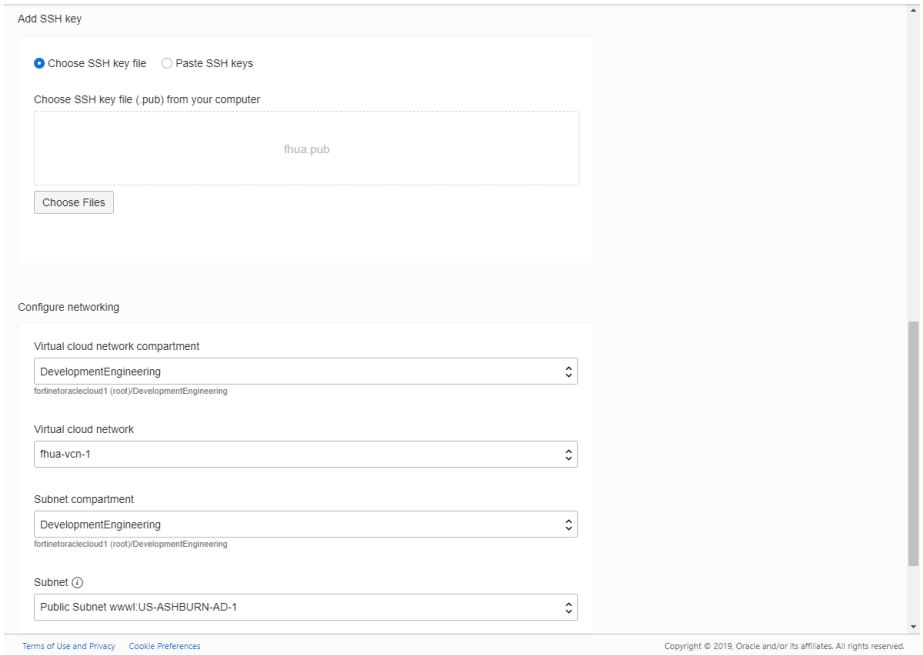
To create a FGT_VM64_OPC instance with the native mode custom image:

1. Log into the Oracle Cloud web portal and go to *Compute* > *Instances* > *Create Instance*.
2. In *Name your instance*, enter your FGT-VM instance name.
3. Select an availability domain for your instance.
4. Select the image source *fhua-temp-b0838-native* that you configured in the previous procedure.
5. For *Choose instance type*, select *Bare Metal Machine*.

6. Click *Change Shape* and select your instance shape, for example, *BM.Standard2.52*.

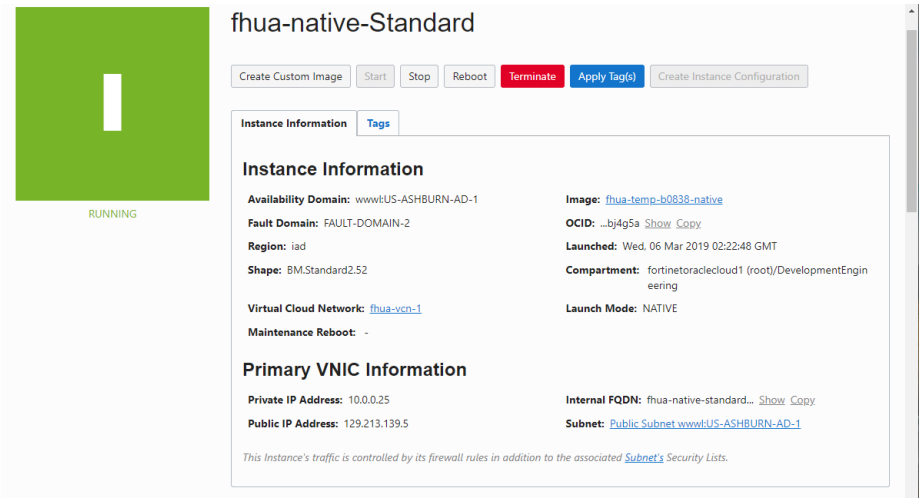


7. Leave *Configure boot volume* as default.
8. If necessary, add your SSH key file.
9. Select your *Virtual cloud network* and *Subnet*.
10. Click *Create*.



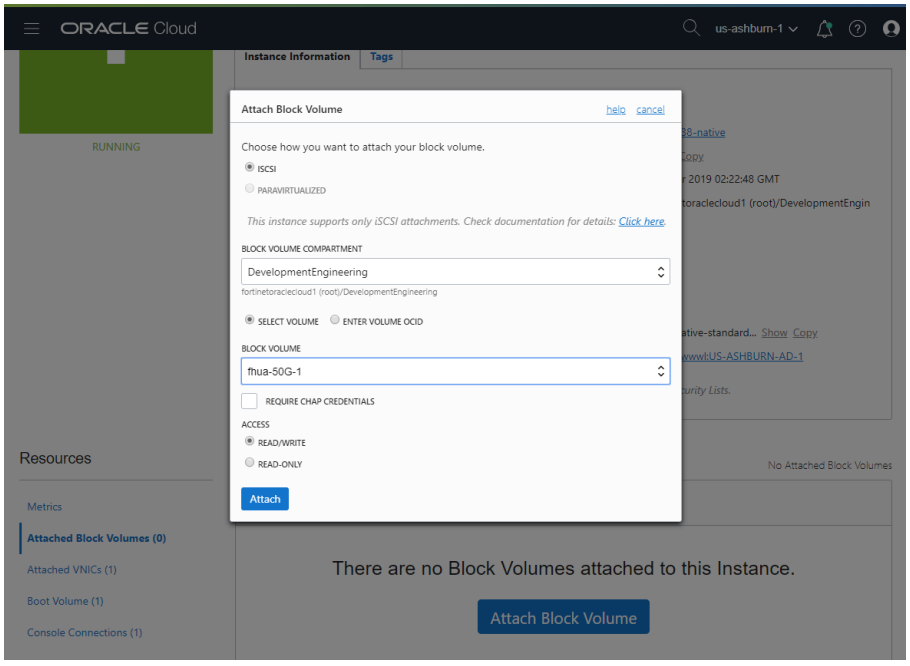
11. Wait for the instance to run.
    You can access the FGT-VM using your SSH key or the default username/password of admin/ocid.

12. Hover your pointer over the … to the right of the FGT-VM and click *View Instance Details*.
The *Instance Information* tab shows that *Launch Mode* is *NATIVE*.



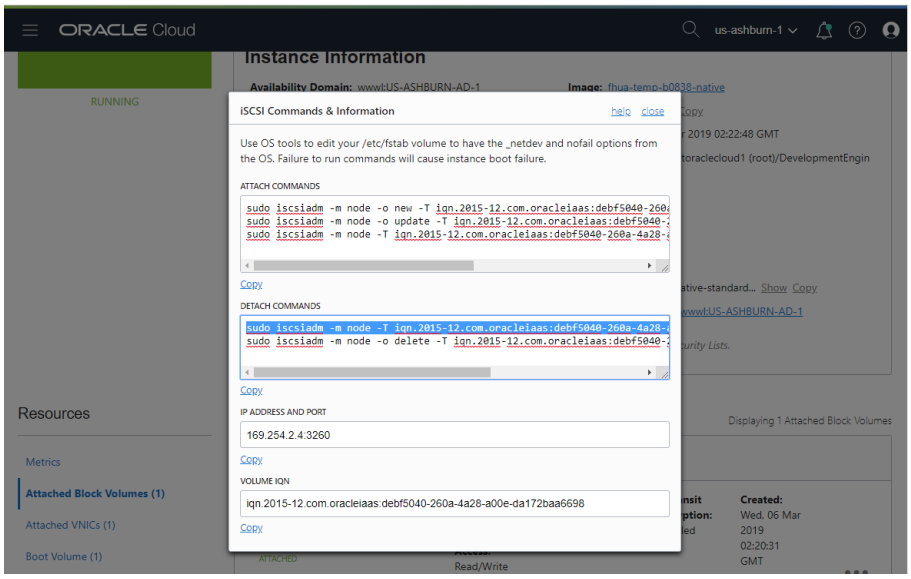
To attach a hard disk to the FGT_VM64_OPC with iSCSI mode:

1. On the *Instance Details* page navigation bar, click *Attached Block Volumes* and then click *Attach Block Volume*.
2. In the Attach Block Volume dialog box, select *ISCSI*.
3. Select the *BLOCK VOLUME COMPARTMENT*.
4. Select the *BLOCK VOLUME*.
5. Leave *ACCESS* as default.
6. Click *Attach*.



7. Wait for the block volume to be attached.
8. In the *Instance Details* page, hover your pointer over the … to the right of the block volume entry and click *iSCSI Commands & Information*.

This dialog box shows this iSCSI's IP address and IQN.



To configure the iSCSI hard disk in FortiGate using CLI:

```
config system iscsi
    edit "i1"
        set ip <class_ip>
        set iqn <string>
    next
end
```

For example:

```
config system iscsi
    edit "Demo-iSCSI-HD"
        set ip 169.254.2.4
        set iqn "iqn.2015-12.com.oracleiaas:debf5040-260a-4a28-a00e-da172baa6698"
    next
end
```

To connect an iSCSI hard disk in FortiGate using CLI:

```
execute iscsi login <iscis-disk-name>
```

To disconnect an iSCSI hard disk in FortiGate using CLI:

```
execute iscsi logout <iscis-disk-name>
```

To check the hard disk in FortiGate and the second HD (50.0GiB) is attached:

```
fhua-native-Standard # d hardware deviceinfo disk

Disk SYSTEM(boot)              46.6GiB    type: ISCSI [IET Controller] dev: /dev/sda
  partition          123.0MiB,  62.0MiB free  mounted: Y  label:  dev: /dev/sda1(boot) start:
2048
  partition            1.7GiB,   1.7GiB free  mounted: Y  label:  dev: /dev/sda2(boot) start:
```

```
264192
  partition ref:   3 127.0MiB,  86.0MiB free  mounted: N  label:  dev: /dev/sda3 start:
3932160

Disk Virtual-Disk    ref:  32  50.0GiB    type: ISCSI [IET Controller] dev: /dev/sdc
  partition ref:  33  49.2GiB,  48.9GiB free  mounted: N  label: LOGUSEDX6FFE3A65 dev:
/dev/sdc1 start: 2048

Total available disks: 2
Max SSD disks: 8  Available storage disks: 1
```

AliCloud Extensions

This section lists the new features added for GCP extensions.

Auto Scaling

This version supports auto scaling for AliCloud or Aliyun environments.

Sample configuration

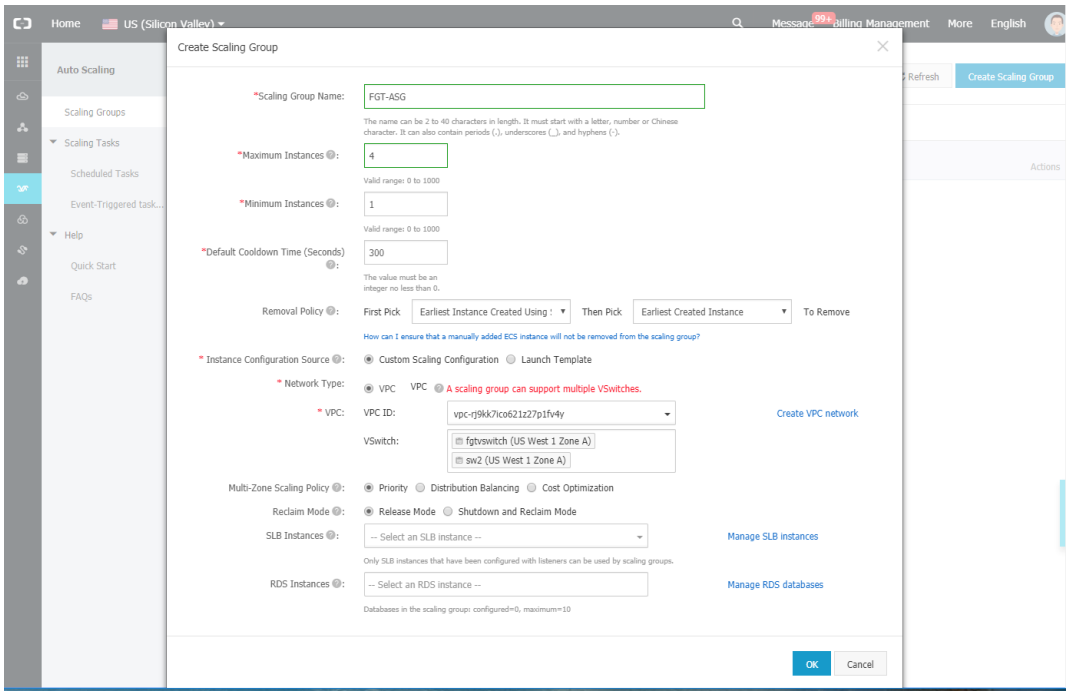
To set up auto scaling for a an AliCloud environment:

1. Create a scaling group in AliCloud console.
2. Create a scaling configuration in AliCloud console.
3. Create scaling rules in AliCloud console.
4. Set the first FortiGate VM in the auto scaling group as the master member.
5. Scale out another FortiGate VM and set it as a slave member; and then synchronize configuration from master to slave.

To create a scaling group in AliCloud console:

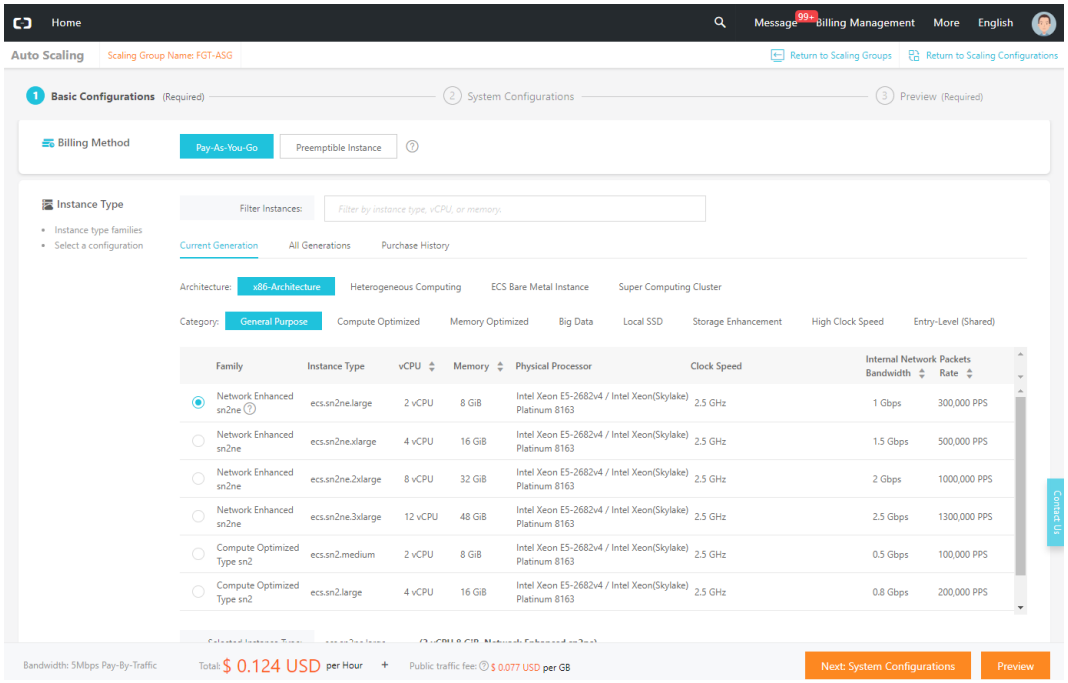
1. In AliCloud, go to *Auto Scaling* > *Scaling Groups*, click *Create Scaling Group*.
2. Configure the scaling group parameters:

Scaling Group Name	Enter a name. In this example: *FGT-ASG*.
Maximum Instances	In this example: *4*.
Minimum Instances	In this example: *1*.
Instance Configuration Source	Use the default.
Network Type	Use the default of *VPC*.
VPC ID	Select the *VPC ID*.
VSwitch	Select the *VSwitch*.



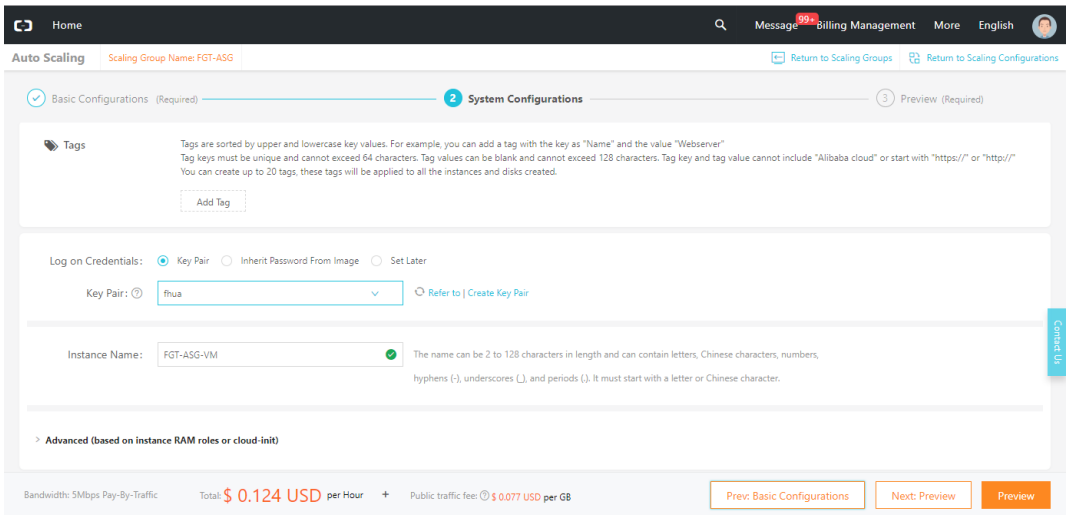
To create a scaling configuration in AliCloud console:

1. In the scaling group pop-up window, click *Create Now* to create a new scaling configuration.
2. Select the *Instance Type* and *FortiGate image*.
3. Select *Assign Public IP* and the *Security Group*.
4. Click *Next: System Configurations*.

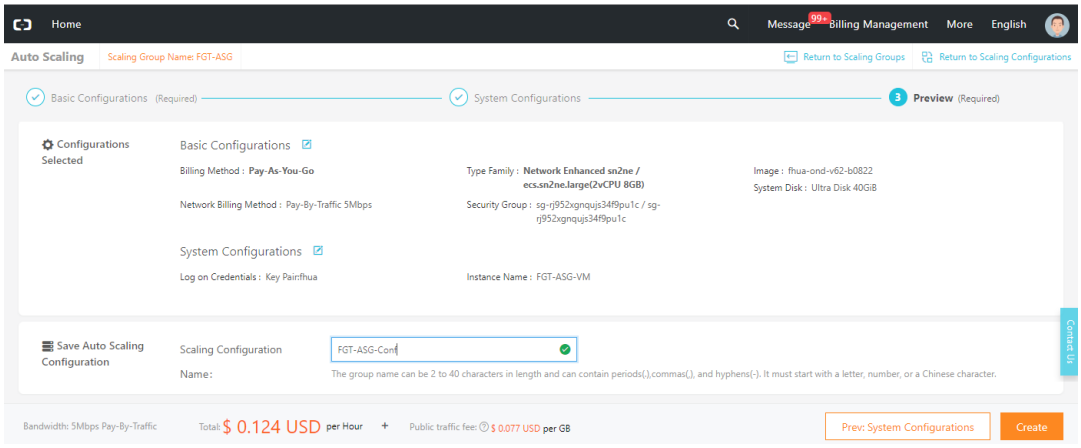


5. If desired, select a *Key Pair*.

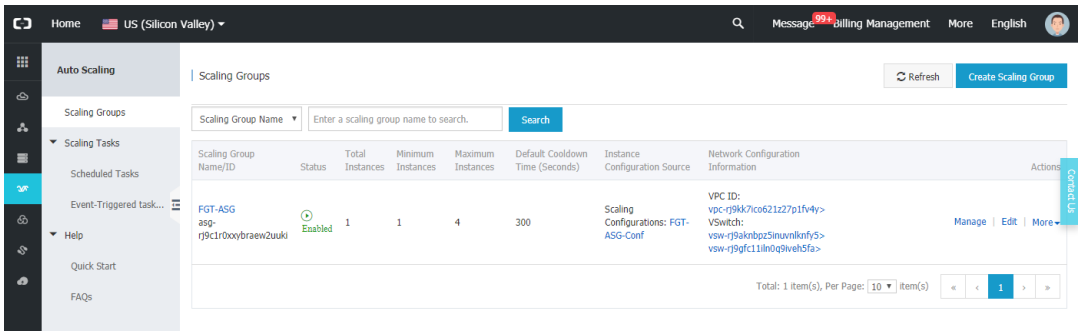
6. Click *Preview*.



7. If the configuration is correct, click *Create* and then click *Enable Configuration*.



8. Check that the auto scaling group is created and the first FortiGate VM is launched automatically.

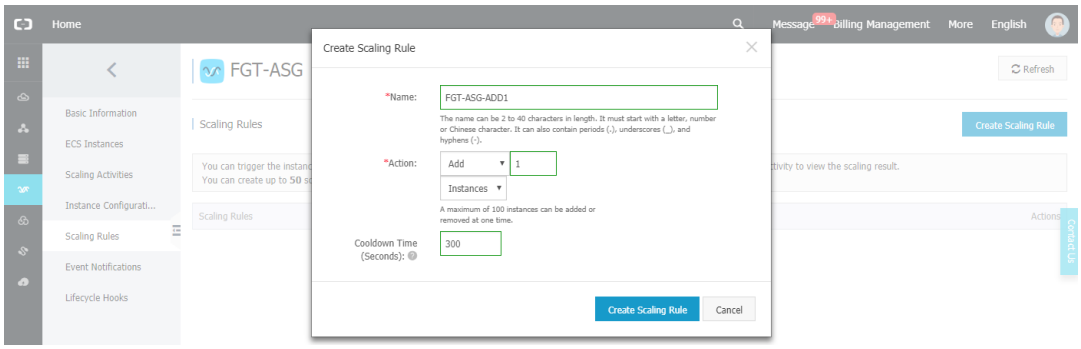


To create scaling rules in AliCloud console:

1. In the *Auto Scaling* console *Scaling Groups* page, click *FGT-ASG* to edit it.
2. In the left menu, click *Scaling Rules*.

3. Configure the scaling rule parameters:

Name	Enter a scaling rule name. In this example: *FGT-ASG-ADD1*.
Action	Select the *Action*. In this example, *1*.
Cooldown Time	In this example: *300* seconds.



The scaling rule *FGT-ASG-ADD1* is created and it can be executed to add one *FGT-ASG* instance.

Use the same procedure to create another scaling rule named *FGT-ASG-REMOVE1* to remove one FortiGate VM instance.

To set the first FortiGate VM in the auto scaling group as the master member:

1. Log into the FortiGate VM as administrator.
2. Use the CLI to enable auto scaling and set the role to master.

```
config system auto-scale
    set status enable
    set role master
    set sync-interface "port1"
    set psksecret xxxxxx
end
```

To scale out another FortiGate VM and set it as a slave member; and then synchronize configuration from master to slave:

1. In the *Auto Scaling* console *FGT-ASG* scaling rules page, execute the scaling rule policy *FGT-ASG-ADD1*. A new FortiGate VM instance is created.
2. Log into the new FortiGate VM as administrator and use the CLI to enable auto scaling and set the role to slave. For the `master-ip`, use the master side private IP address.

```
config system auto-scale
    set status enable
    set role slave
    set sync-interface "port1"
    set master-ip 192.168.1.204
    set psksecret xxxxxx
end
```

3. Wait a few moments for the slave member to sync with the master member; and then the slave member can sync the FortiGate configuration from the master member.

```
FortiGate-VM64-ALION~AND # diag deb app hasync -1
slave's configuration is not in sync with master's, sequence:0
slave's configuration is not in sync with master's, sequence:1
slave's configuration is not in sync with master's, sequence:2
slave's configuration is not in sync with master's, sequence:3
slave's configuration is not in sync with master's, sequence:4
slave starts to sync with master
logout all admin users
```

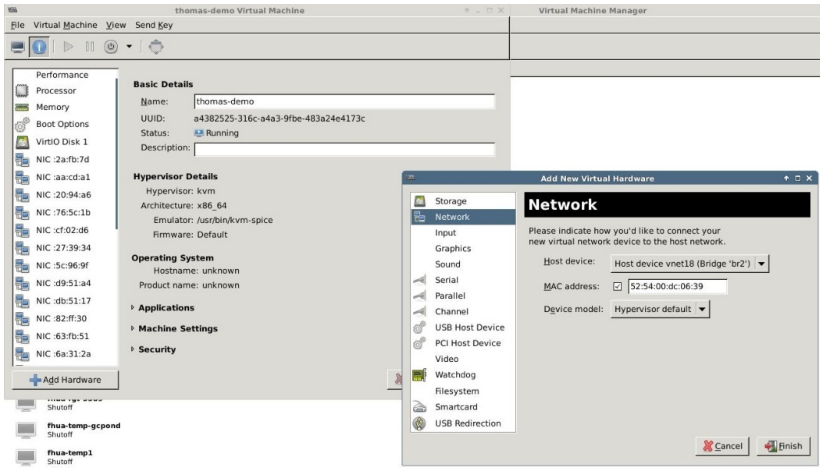
Support up to 18 Interfaces

The number of network interfaces that can be supported by FortiGate-VM has been increased. Currently, FortiGate-VM supports up to a maximum of 10 interfaces. This new feature expands this support to a maximum of 18 interfaces (16 traffic ports, 1 management port, 1 HA port).

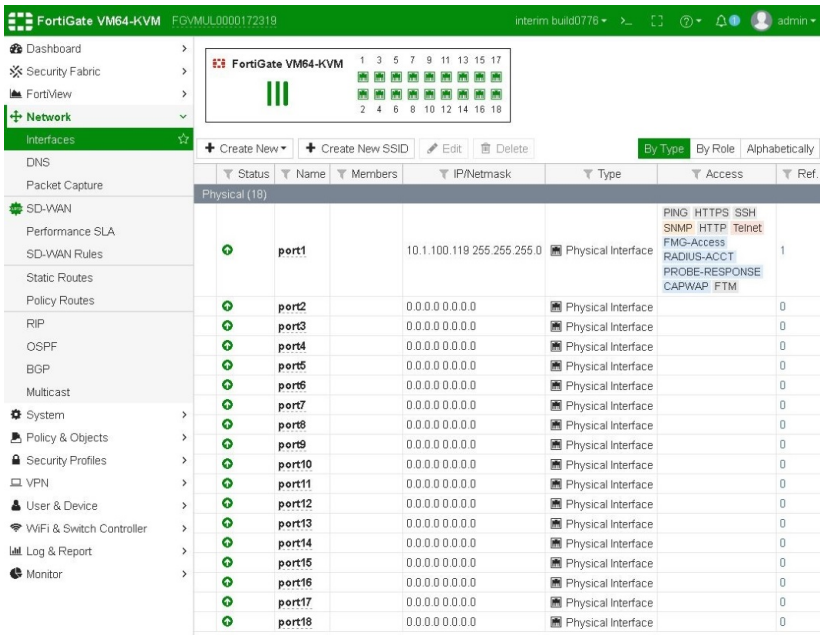
This change applies to all FortiGate-VM models except VMX and SVM, as VMX does not use interfaces to process traffic.

To configure the maximum number of interfaces:

1. In your hypervisor, create a new VM or open an existing VM.
2. Create up to a maximum of 18 interfaces.



3. Once created, the interfaces will be displayed in the FortiGate GUI under *Network* > *Interfaces*.



Limitations

Certain cloud service providers and hypervisors have their own limitations on the maximum number of interfaces supported, for example:

Cloud Service Provider	Maximum Interfaces Supported
AWS	15
Azure	8
Google Cloud Platform	8
Oracle	16
Aliyun	8

Physical Hypervisor	Maximum Interfaces Supported
VMware	10
Hyper-V	12
OpenStack	28
XenServer	7

The maximum number of interfaces supported per cloud provider/hypervisor is subject to change without notice. The lists above are not inclusive of all cloud providers and hypervisors.

OpenStack — Network Service Header (NSH) Chaining Support

This version provides NSH chaining support for virtual wire pair, TP mode networks. FortiOS receives and unwraps the NSH packets and re-encapsulates them before sending them out. The inner packet is processed by firewall policies.

NSH support in FortiGate is basically unwrapping the packet on Ingress and putting the NSH header back on before sending it out. Other parts of NSH aren't supported yet (SI is currently left unchanged).

There's no CLI/GUI change. The only change is to show `ext_header=nsh` in NSH session info when listing sessions.

Sample configuration

To configure virtual wire pair and firewall policy using the CLI:

```
config system virtual-wire-pair
    edit "test-vw"
        set member "port1" "mgmt2"
    next
end
config firewall policy
    edit 99
        set uuid 241710a0-3ac6-51e9-10e9-9dd3eb65e708
        set srcintf "mgmt2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
end
```

Sample results of configuring a wire pair and policy between port1 and mgmt2. Packets with NSH are processed and the session list shows `ext_header=nsh`.

```
A (vdom1) # diag sys session list

session info: proto=6 proto_state=01 duration=10 expire=3595 timeout=3600 flags=00000000 sock-
flag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=log may_dirty br src-vis dst-vis f00
statistic(bytes/packets/allow_err): org=112/2/1 reply=60/1/1 tuples=2
tx speed(Bps/kbps): 10/0 rx speed(Bps/kbps): 5/0
orgin->sink: org pre->post, reply pre->post dev=4->9/9->4 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 172.16.200.11:46739->172.16.200.55:23(0.0.0.0:0)
hook=post dir=reply act=noop 172.16.200.55:23->172.16.200.11:46739(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
src_mac=00:00:11:11:11:11  dst_mac=00:00:22:22:22:22
misc=0 policy_id=99 auth_info=0 chk_client_info=0 vd=1
serial=0000094d tos=ff/ff app_list=0 app=0 url_cat=0
```

```
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x040001 no_offload
no_ofld_reason:  mac-host-check disabled-by-policy non-npu-intf
ext_header_type=nsh
total session 1
```

Physical Function (PF) SR-IOV Driver Support

This feature adds Physical Function (PF) SR-IOV drivers for i40e and ixgbe interfaces in virtual environments.

PF adds the ability for PCI Passthrough, but requires an entire Network Interface Card (NIC) for a VM. It can usually achieve greater performance than a Virtual Function (VF) based SR-IOV. PF is also expensive; while VF allows one NIC to be shared among multiple guests VMs, PF is allocated to one port on a VM.

The now supported driver versions are:

- ixgbe: 5.3.7
- ixgbevf: 4.3.5
- i40e: 2.4.10
- i40evfL 3.5.13

All tools and software utilities for UEFI 1.X have been removed from this release. Update to UEFI 2.x to use the UEFI tools or software utilities.

Configuration to use PF or VF is done on the hypervisor, and is not configured on the FortiGate.

The following CLI command can be used to check what driver is being used on the FortiGate:

```
FGVM0800000000 # diagnose hardware deviceinfo nic port2
Name:        port2
Driver:      i40e
Version:     2.4.10
Bus:         0000:03:00.0
Hwaddr:      3c:fd:fe:1e:98:02
Permanent Hwaddr:3c:fd:fe:1e:98:02
State:       up
Link:        up
Mtu:         1500
Supported:   auto 1000full 10000full
Advertised:  auto 1000full 10000full
Auto:        disabled
Rx packets:      0
Rx bytes:        0
Rx compressed:       0
...
```

FortiMeter Extensions

This section lists the new features added for FortiMeter extensions.

FortiMeter - Microsoft Hyper-V Instances

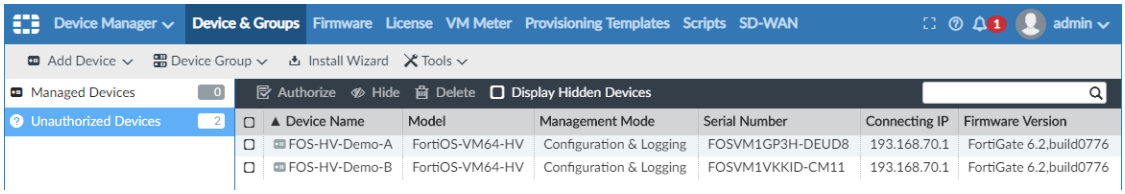
FortiMeter now supports Microsoft Hyper-V in addition to support for VMware, KVM, and Xen.

The Microsoft Hyper-V FortiOS-VM must be added to the FortiManager system before authorization. Once the Microsoft Hyper-V FortiOS-VM is authorized, it can receive updates from FortiManager and process traffic. An unauthorized Microsoft Hyper-V FortiOS-VM cannot receive updates from FortiManager or process traffic.

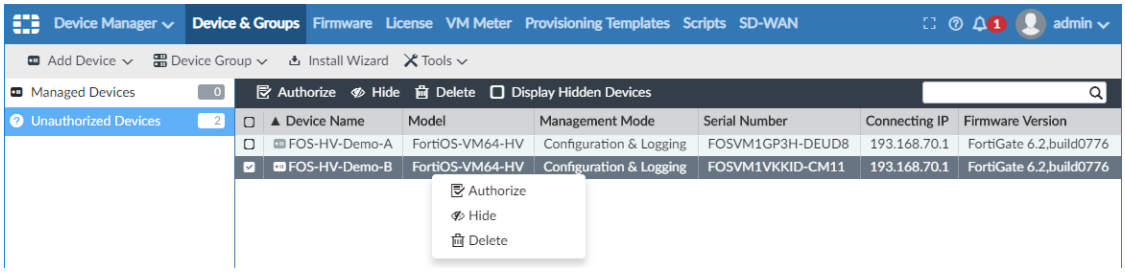
Microsoft Hyper-V FortiOS-VM support requires FortiManager 6.2.0 or a later version.

To authorize a Microsoft Hyper-V FortiOS-VM on FortiManager using the GUI:

1. Ensure that the VM is registered to the FortiManager. See the *FortiManager 6.2.0 Administration Guide*.
2. Ensure that you are in the correct ADOM.
3. Go to *Device Manager* > *Device & Groups* > *Unauthorized Devices*.



4. Select the Microsoft Hyper-V FortiOS-VM, then click *Authorize* in the toolbar, right-click on a device then select *Authorize*, or double-click on a device. The *Authorize Device(s)* dialog box opens. An unauthorized device can use firewall services for up to 48 hours.



5. Select the *License Type*:

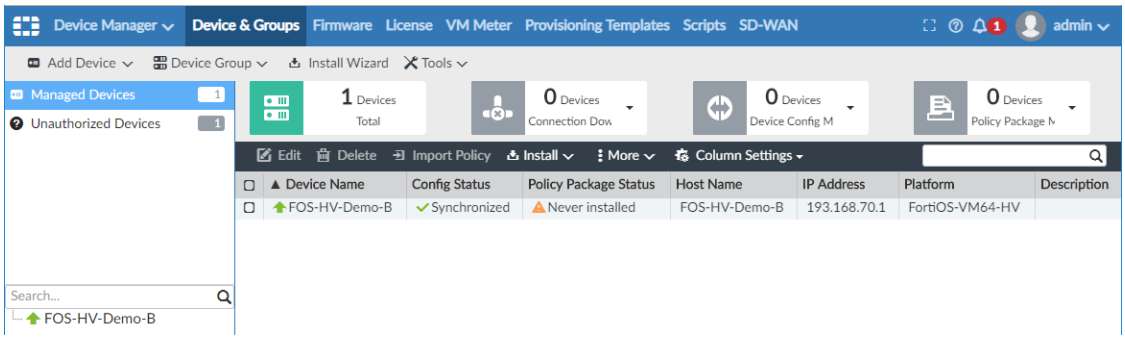
Trial	Maximum of two devices can have a trial license at any one time. No traffic data are sent to FortiGuard, so no points are used. Can be used for up to 30 days.

Regular	Regular license. Points used based on the service level and volume of traffic going to FortiGuard.

6. Select the *Services*:

Firewall	Firewall only. This option cannot be deselected.
IPS	IPS services.
Web Filter	Web filtering services.
AntiVirus	Antivirus services.
App Control	Application control services.
Full UTM	All services are selected.

7. Click *OK* to authorize the device. The device now shows as authorized on the FortiManager GUI.



To authorize a Microsoft Hyper-V FortiOS-VM on FortiManager using CLI commands:

In the example below, the FortiManager IP address is 172.18.3.72. Run the following commands in the FortiOS CLI :

```
config system central-management
   set type fortimanager
   set fmg "172.18.3.72"
   config server-list
      edit 1
         set server-type update rating
         set server-address 172.18.3.72
      next
   end
end
```

FortiMeter - Fallback to Public FortiGuard

In previous releases, FortiOS-VM (FortiMeter) instances needed to get services from FortiManager that facilitated updates by tracking service entitlements based on serial numbers starting with FOSVM1. However, if the FortiMeter instance connected directly to Fortinet Distribution Network (FDN), updates were not available since FDN was not aware of serial numbers with prefix FOSVM1.

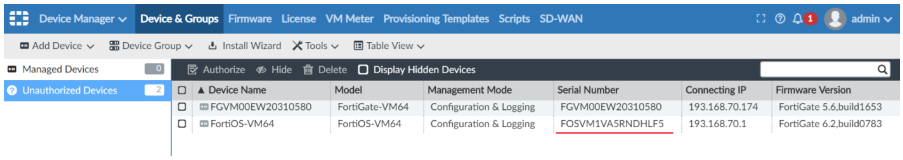
In the current release, the serial number prefix FOSVM2 was added to FortiOS-VM. When the FortiMeter instance connects directly to FDN, it is now able to receive the updates.

The same serial number will have two different prefixes depending on the situation:

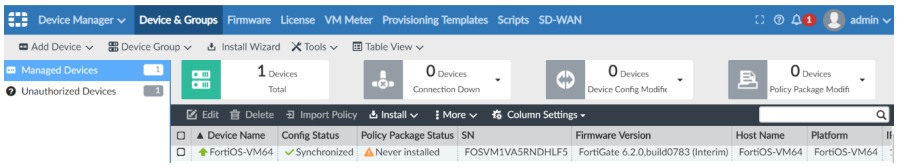
- FortiOS-VM sends the serial numbers with prefix FOSVM2 to FortiManager or FortiGuard for updates and rating service. FOSVM2 is not visible on the FortiManager GUI.
- FortiOS-VM sends the serial numbers with prefix FOSVM1 to FortiManager for management. FOSVM1 is shown on the FortiManager GUI.

FortiGate Serial Numbers shown in FortiManager

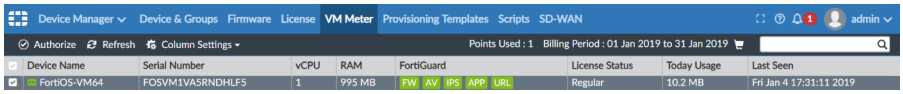
- FortiOS-VM in FortiOS *Unauthorized Devices* list with the serial number prefix FOSVM1



- Authorized FortiOS-VM in FortiOS



- Authorize FortiGuard service to FortiOS-VM. FortiOS checks service license with serial number prefix FOSVM1 while providing service to FOSVM2.



Automation and Dev-Ops

This section lists the new features added to FortiOS for automation and dev-ops.

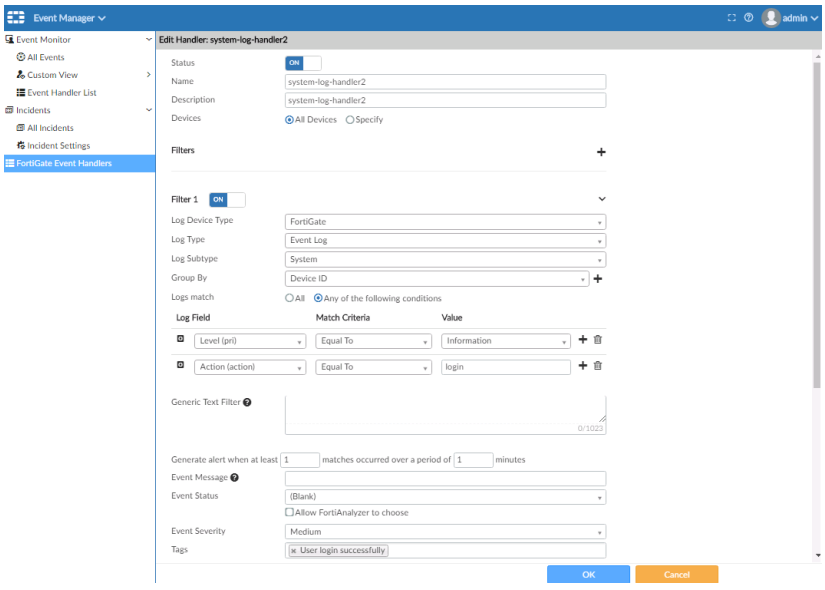
Trigger — FortiAnalyzer Event Handler

This version adds FortiAnalyzer event handler as an Automation Stitch trigger. You can trigger automation rules based on FortiAnalyzer event handlers giving you the ability to define rules based on complex correlation across devices, log types, frequency, and other criteria.

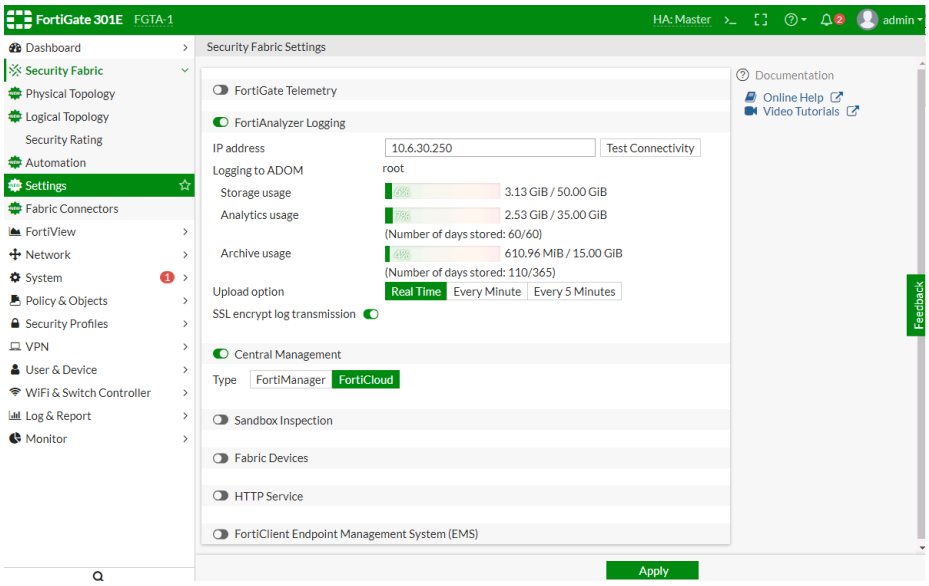
When FortiAnalyzer event handler triggers, it sends a notification to the FortiGate automation framework, which generates a log and triggers the automation stitch.

Sample configuration

In FortiAnalyzer *Event Manager* > *FortiGate Event Handlers*, configure the FortiAnalyzer event handler that will be triggered when FortiGate logs in.



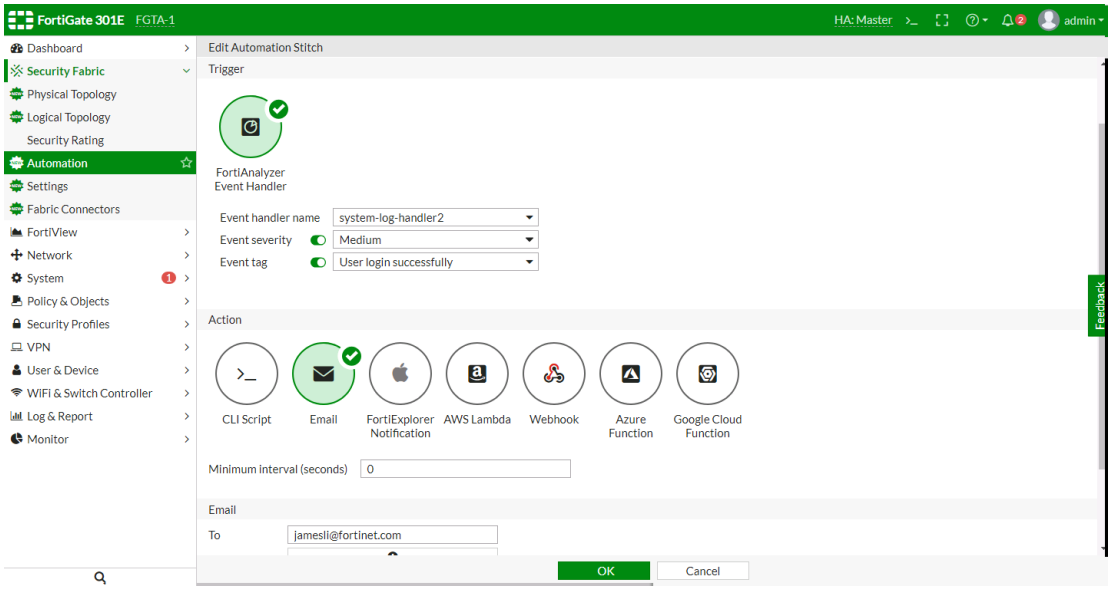
In FortiGate *Security Fabric* > *Settings*, configure FortiAnalyzer and get authorized.



To configure Security Fabric Settings using the CLI:

```
config log fortianalyzer setting
    set status enable
    set server "10.6.30.250"
    set serial "FL-4HET318900407"
    set upload-option realtime
    set reliable enable
end
```

To configure Security Fabric Automation Stitch with trigger of FortiAnalyzer Event Handler in the GUI:

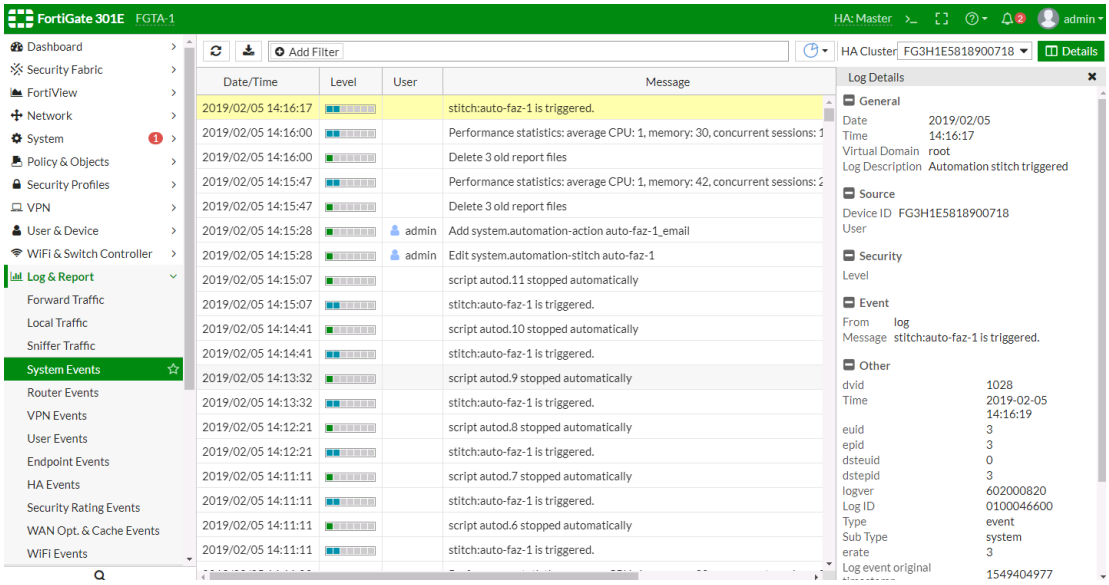


To configure Security Fabric Automation Stitch with trigger of FortiAnalyzer Event Handler in the CLI:

```
config system automation-action
    edit "auto-faz-1_email"
        set action-type email
        set email-to "jamesli@fortinet.com"
        set email-subject "CSF stitch alert"
        set email-body "User login FortiGate successfully."
    next
end

config system automation-trigger
    edit "auto-faz-1"
        set event-type faz-event
        set faz-event-name "system-log-handler2"
        set faz-event-severity "medium"
        set faz-event-tags "User login successfully"
    next
end

config system automation-stitch
    edit "auto-faz-1"
        set trigger "auto-faz-1"
        set action "auto-faz-1_email"
    next
end
```

To see the trigger event log in the GUI:

1. Log into FortiGate to trigger the FortiAnalyzer event so that FortiAnalyzer sends notification to the FortiGate automation framework and generates an event log in FortiGate and triggers the automation stitch.

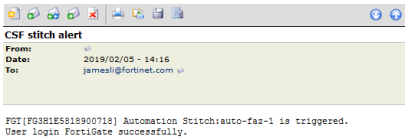


Sample of the trigger event log in the CLI

```
date=2019-02-05 time=14:16:17 logid="0100046600" type="event" subtype="system" level="notice"
vd="root" eventtime=1549404977 logdesc="Automation stitch triggered" stitch="auto-faz-1"
```

```
trigger="auto-faz-1" from="log" msg="stitch:auto-faz-1 is triggered."
```

Sample of email sent when automation stitch is triggered



Action — NSX Quarantine

This version adds a new *Security Fabric* > *Automation* > *Action*: *Assign VMware NSX Security Tag* to the NSX endpoint instance. This action is only available when the *Trigger* is *Compromised Host*.

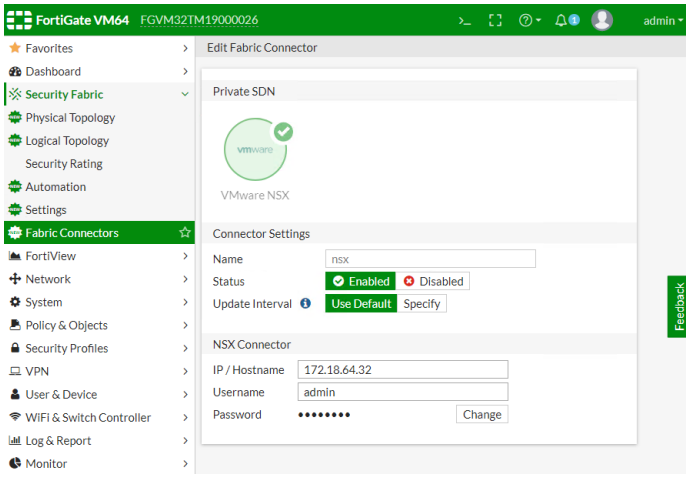
First configure NSX type SDN connector in FortiGate. Then FortiGate can retrieve security tags from VMware NSX server through the NSX connector.

Configure an automation stitch with the trigger *Compromised Host* and the *Action Assign VMware NSX Security Tag*, then choose a *Security tag* in the security tags retrieved from VMware NSX server through NSX connector.

If an endpoint instance in the VMware NSX environment is compromised which triggers the automation stitch in FortiGate, FortiGate will then assign the configured security tag to the compromised NSX endpoint instance.

To configure a VMware NSX SDN connector in the GUI:

1. Go to *Security Fabric* > *Fabric Connectors* and click *Create New*.
2. Select *VMware NSX* and configure its settings.



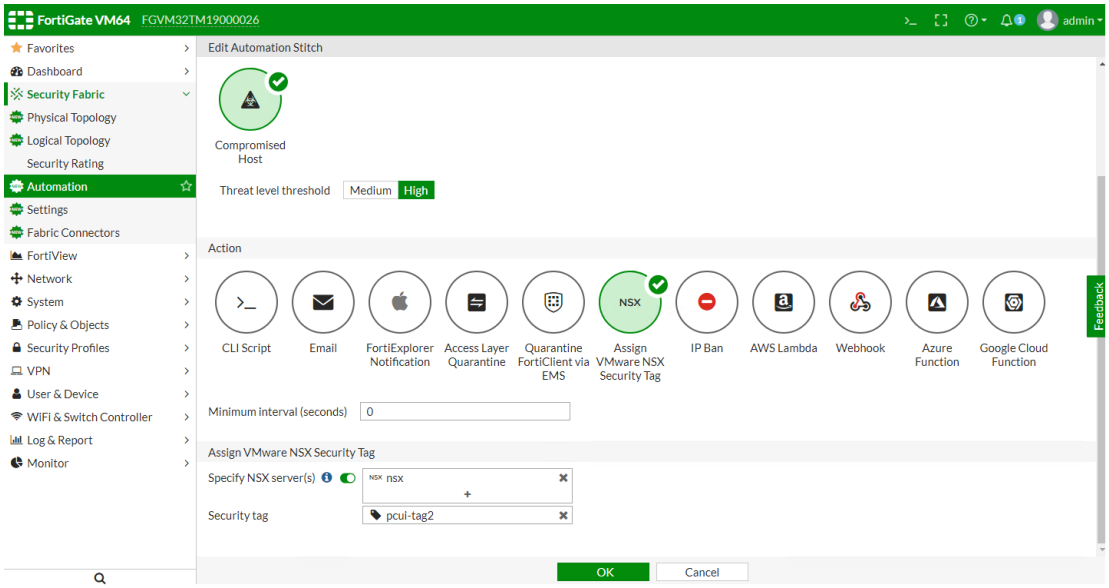
To configure a VMware NSX SDN connector in the CLI:

```
config system sdn-connector
    edit "nsx"
        set type nsx
        set server "172.18.64.32"
        set username "admin"
```

```
        set password xxxxx
    next
end
```

To configure an automation stitch with a *Trigger Compromised Host* and *Action Assign VMware NSX Security Tag* using the GUI:

1. Go to *Security Fabric* > *Automation* and click *Create New*.
2. In the *Trigger* section, select *Compromised Host*.
3. In the *Action* section, select *Assign VMware NSX Security Tag* and configure its settings.

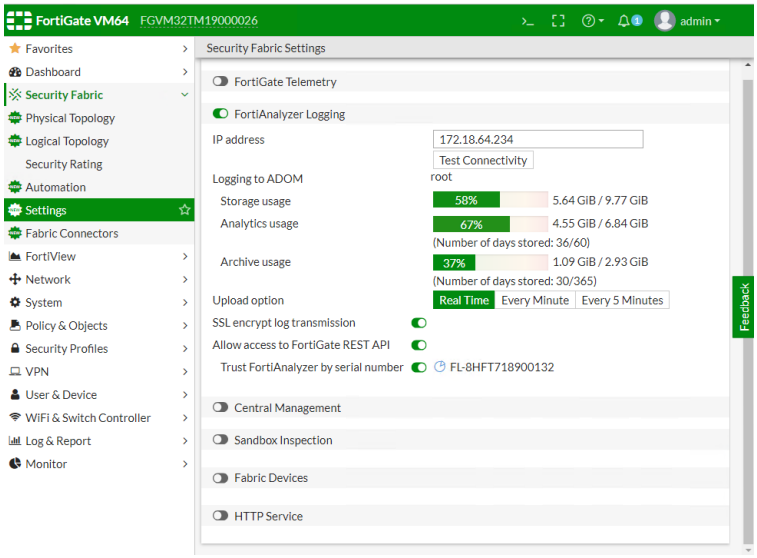


To configure an automation stitch with a *Trigger Compromised Host* and *Action Assign VMware NSX Security Tag* using the CLI:

```
config system automation-action
    edit "pcui-test_quarantine-nsx"
        set action-type quarantine-nsx
        set security-tag "pcui-tag2"
        set sdn-connector "nsx"
    next
end

config system automation-trigger
    edit "pcui-test"
        set ioc-level high
    next
end

config system automation-stitch
    edit "pcui-test"
        set trigger "pcui-test"
        set action "pcui-test_quarantine-nsx"
    next
end
```

To configure FortiAnalyzer in FortiGate which is used to send endpoint compromise notifications to FortiGate using the GUI:

1. Go to *Security Fabric* > *Settings*.
2. Enable *FortiAnalyzer Logging* and configure its settings.

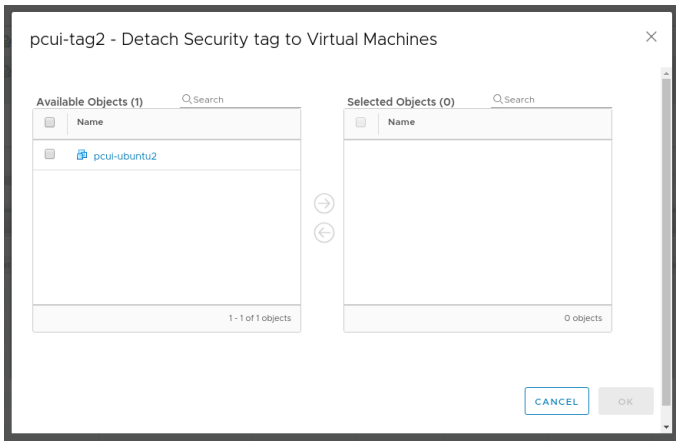


To configure FortiAnalyzer in FortiGate which is used to send endpoint compromise notifications to FortiGate using the CLI:

```
config log fortianalyzer setting
    set status enable
    set server "172.18.64.234"
    set serial "FL-8HFT718900132"
    set upload-option realtime
    set reliable enable
end
```

When an endpoint instance is compromised

When an endpoint instance, for example, *pcui-ubuntu2*, in the VMware NSX environment is compromised, the automation stitch in FortiGate is triggered. FortiGate then assigns the security tag, in this example, *pcui-tag2*, to the compromised NSX endpoint instance.



Action — CLI Script

This version adds a new automation action to run a CLI script. You can use this feature to add CLI script actions for Security Fabric automation.

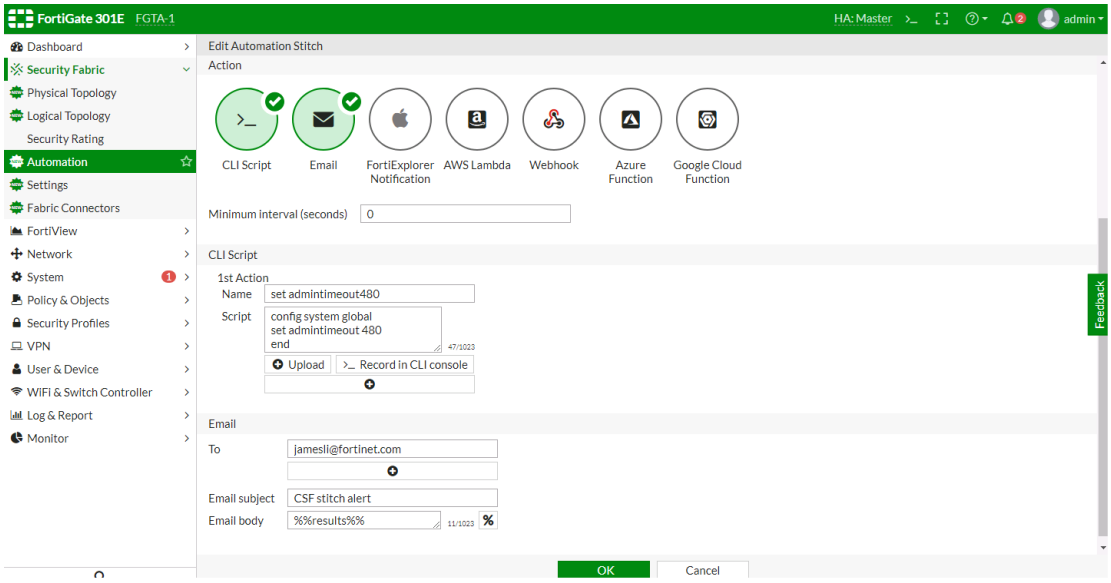
CLI scripts can be manually entered, uploaded as a file, or recorded in CLI console. The CLI script output can be sent in an Automation Action email.

Sample configuration

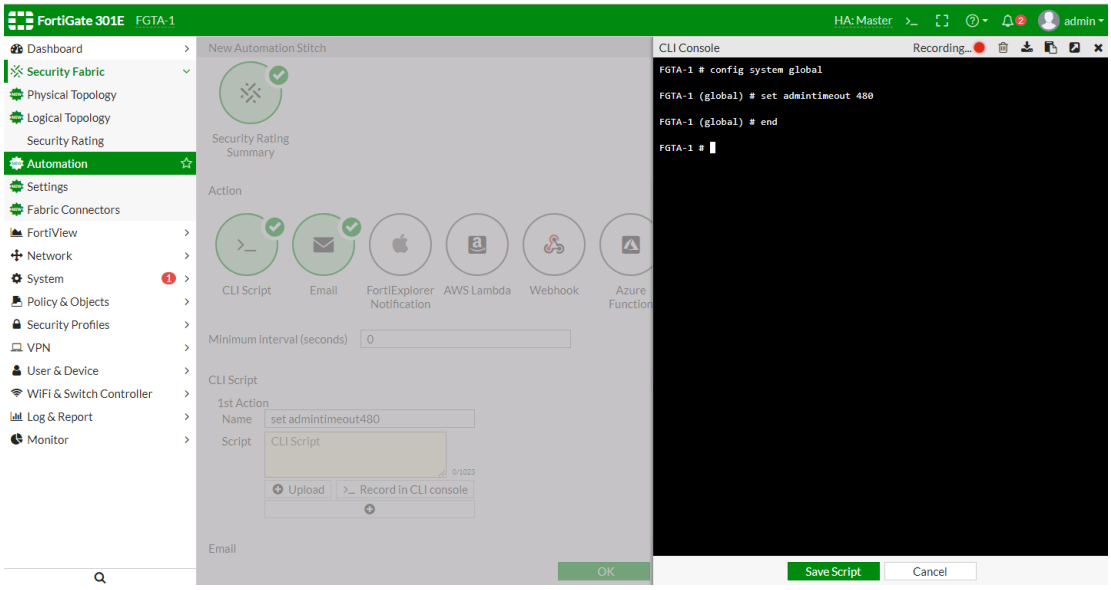
To configure a Security Fabric *Automation Stitch* using the GUI:

1. Go to *Security Fabric* > *Automation*.
2. In the *Action* section, select *CLI Script* and *Email*.

3. Configure a CLI script.
   - To manually enter a CLI script, enter the script in the *Script* box.
   - To upload a script file, click *Upload* and specify the script file.



   - To record a script in CLI console, click *>_Record in CLI console* and then save the script.



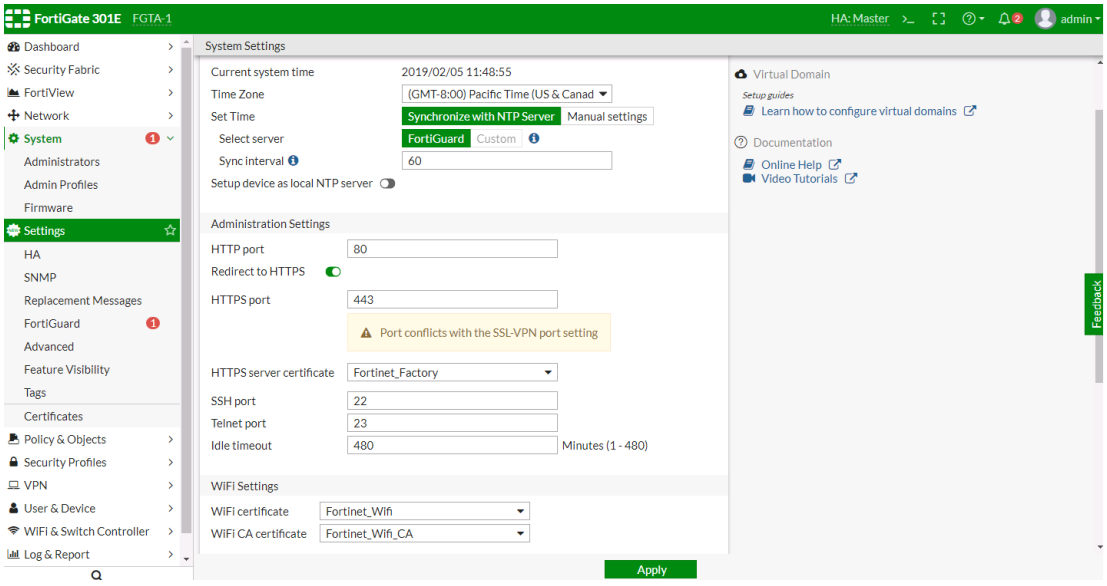
4. Enter the other fields as required and click *OK*.

To configure a Security Fabric *Automation Stitch* using the CLI:

```
config system automation-trigger
    edit "auto-cli-1"
        set trigger-type event-based
        set event-type security-rating-summary
    next
end
```

```
config system automation-action
    edit "set admintimeout480"
        set action-type cli-script
        set minimum-interval 0
        set delay 0
        set required enable
        set script "config system global
            set admintimeout 480
            end"
    next
    edit "auto-cli-1_email"
        set action-type email
        set email-to "jamesli@fortinet.com"
        set email-subject "CSF stitch alert"
        set email-body "%%results%%"
        set minimum-interval 0
    next
end

config system automation-stitch
    edit "auto-cli-1"
        set status enable
        set trigger "auto-cli-1"
        set action "set admintimeout480" "auto-cli-1_email"
    next
end
```

To execute the CLI script automatically after the *Automation Stitch* is triggered:



To execute the CLI script automatically after the *Automation Stitch* is triggered:

```
FGTA-1 # show system global
config system global
    set admintimeout 480
```

```
...
end
```

Sample of script output sent in automation action email

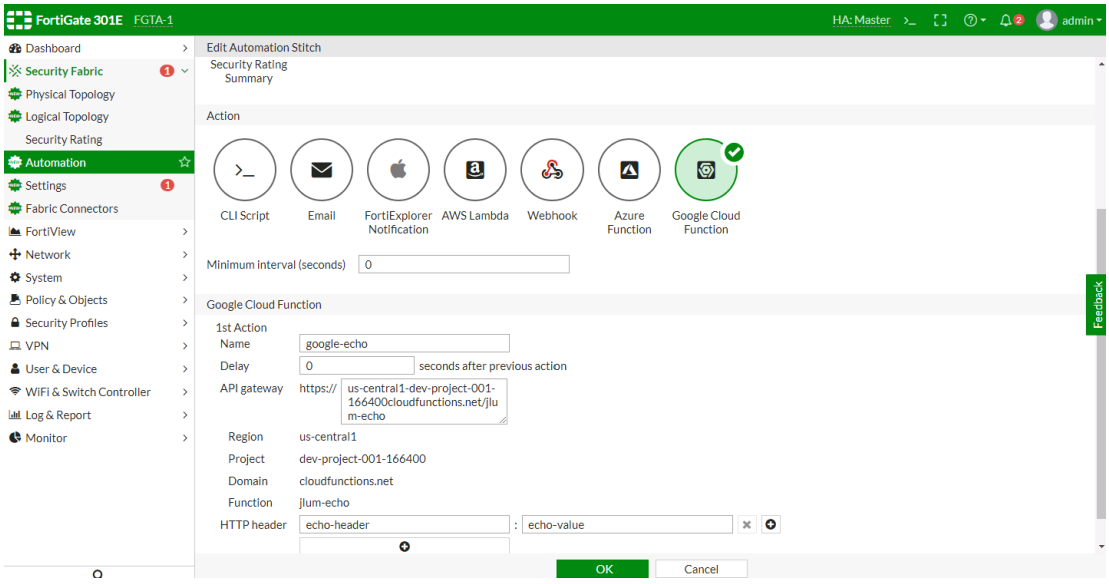
Action — Google Cloud Function

This version adds support to Automation Action to call Google Cloud Function when the *Automation Stitch* is triggered. This is a new quarantine action to call Google Cloud Function.

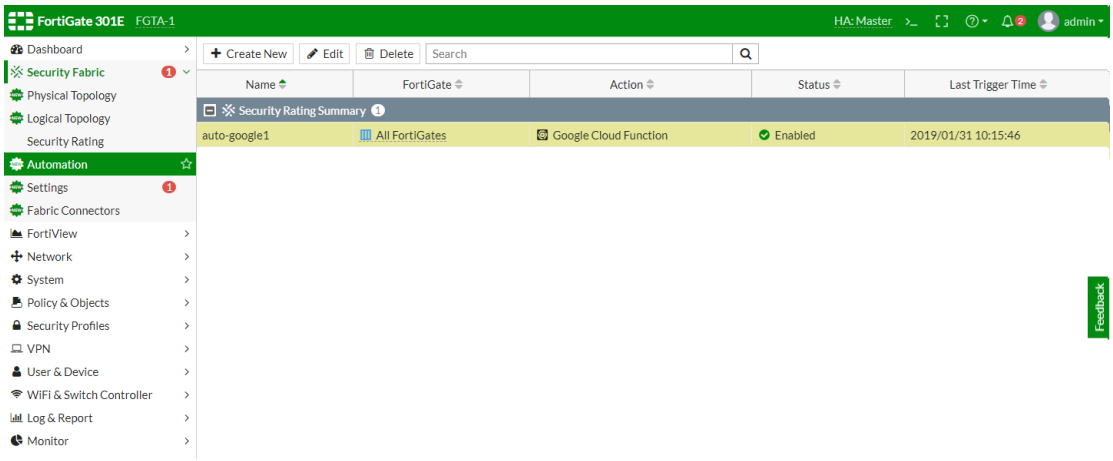
Sample configuration

To configure Google Cloud Function using the GUI:

1. Go to *Security Fabric* > *Automation*.
2. Configure an *Automation Stitch* and set the *Action* to *Google Cloud Function*.



When the automation stitch is triggered, FortiGate shows the stitch trigger time.

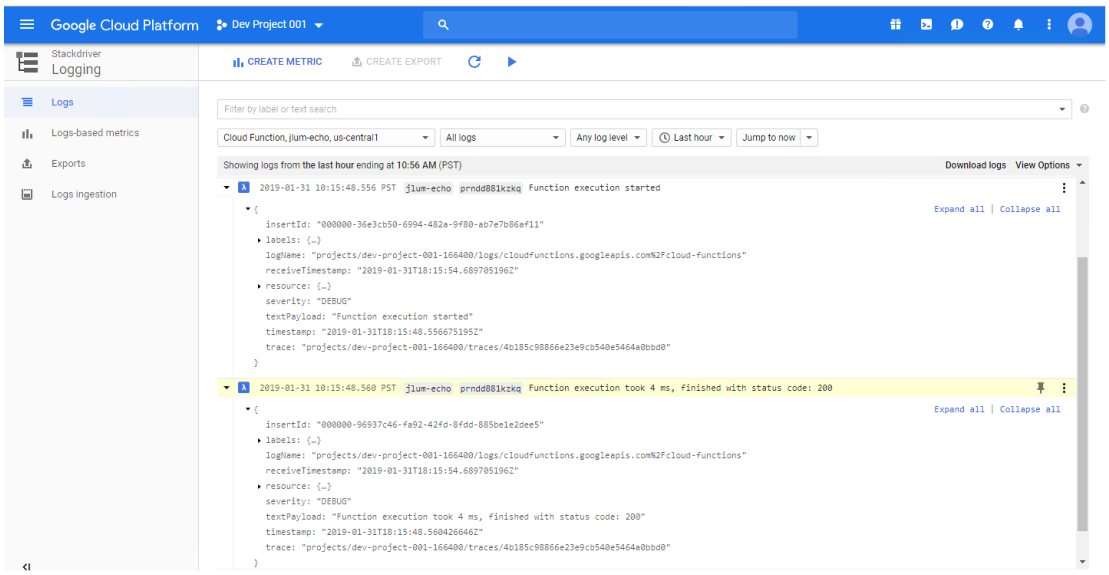


To configure Google Cloud Function using the CLI:

```
config system automation-action
    edit "google-echo"
        set action-type google-cloud-function
        set gcp-function-region "us-central1"
        set gcp-project "dev-project-001-166400"
        set gcp-function-domain "cloudfunctions.net"
        set gcp-function "jlum-echo"
        set headers "echo-header:echo-value"
    next
end
config system automation-trigger
    edit "auto-google1"
        set event-type security-rating-summary
    next
end
config system automation-stitch
    edit "auto-google1"
        set trigger "auto-google1"
        set action "google-echo"
    next
end
```

To see the function log in Google Cloud using the GUI:

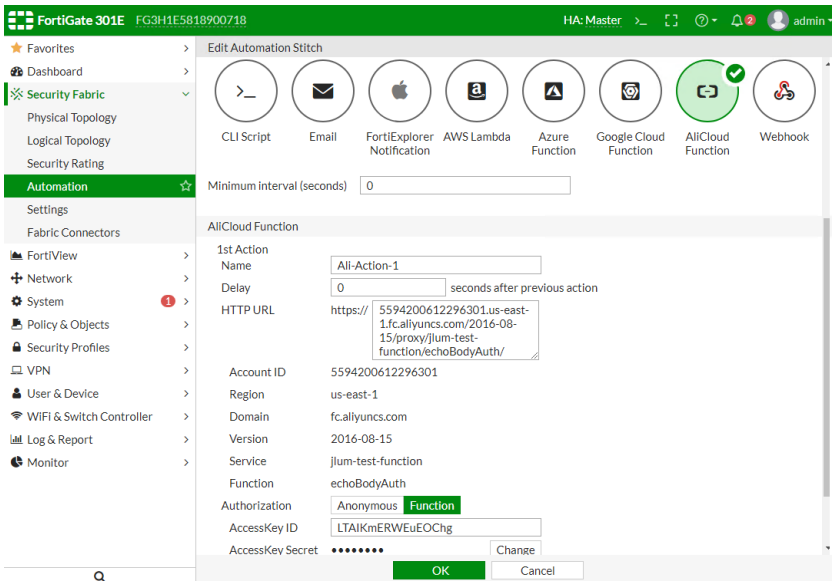
1. Go to *Google Cloud Platform* > *Logs*.
   The function log shows that the configured function is called, executed, and finished.



Action - AliCloud Function

This version adds support to *Automation* action of calling AliCloud Functions when the automation stitch is triggered.

To configure an *AliCloud Function* automation stitch in the GUI, go to *Security Fabric* > *Automation*, select *AliCloud Function* and configure its settings.

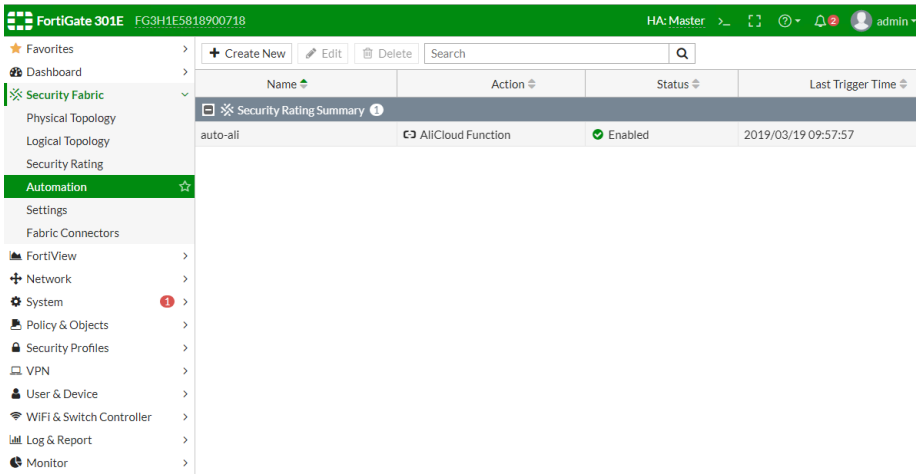


To configure an AliCloud Function automation stitch in the CLI, use the following commands.

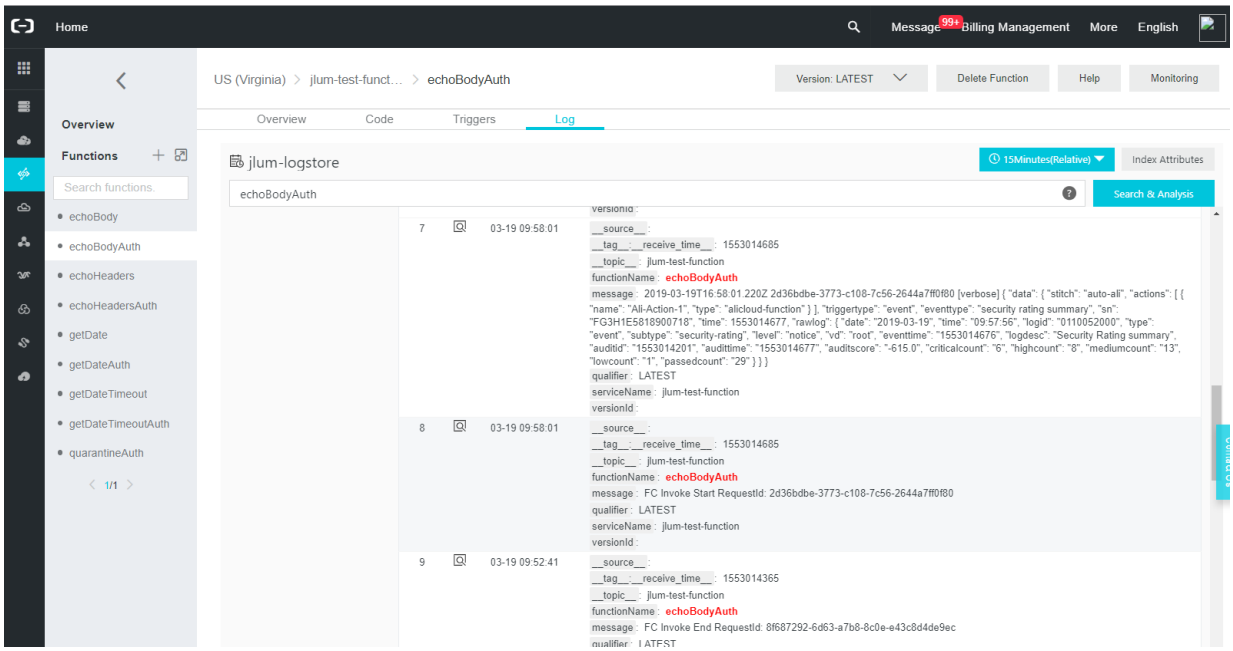
```
config system automation-action
    edit "Ali-Action-1"
        set action-type alicloud-function
        set alicloud-account-id "5594200612296301"
        set alicloud-region "us-east-1"
```

```
        set alicloud-version "2016-08-15"
        set alicloud-service "jlum-test-function"
        set alicloud-function "echoBodyAuth"
        set alicloud-function-authorization function
        set alicloud-access-key-id "LTAIKmERWEuEOChg"
        set alicloud-access-key-secret xxxxxx
    next
end

config system automation-trigger
    edit "auto-ali"
        set event-type security-rating-summary
    next
end

config system automation-stitch
    edit "auto-ali"
        set trigger "auto-ali"
        set action "Ali-Action-1"
    next
end
```

When the automation stitch is triggered, FortiGate shows the stitch trigger time.



In AliCloud, the function log shows the function is called, executed, and finished.



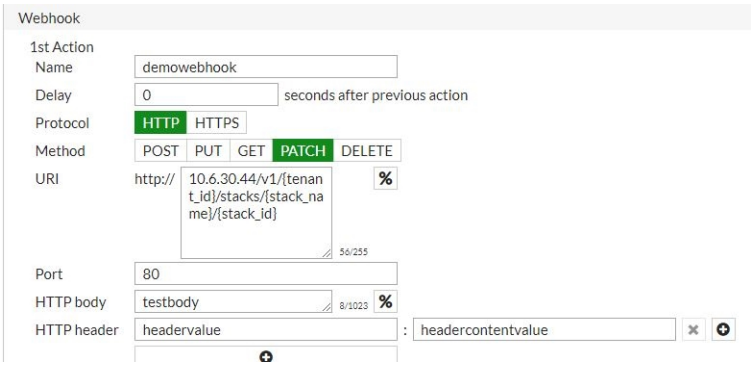
Action — Webhook Extensions

This version introduces the *PATCH* and *DELETE* methods in the *Webhook* section in *Security Fabric* > *Automation*.

The following shows examples of *PATCH* and *DELETE* methods using the GUI and CLI.

To set the Patch method using the GUI:

1. Go to *Security Fabric* > *Automation* and click *Create New*.
2. In the *Action* section, click *Webhook* to display the *Webhook* section.
3. For the *Method*, select *PATCH*.



4. Fill in the other fields and click *OK*.

On the server, check that FortiGate sends the header, body, and method correctly:

```
--22e0822b-A--
[17/Jan/2019:14:26:34 --0800] XEEBGqwQyCwAAEDNKxIAAAAC 10.6.30.5 6163 10.6.30.44 80
--22e0822b-B--
PATCH /v1/{tenant_id}/stacks/{stack_name}/{stack_id} HTTP/1.1
Host: 10.6.30.44
Accept: */*
headervalue: headercontentvalue
Content-Length: 8
Content-Type: application/x-www-form-urlencoded

--22e0822b-C--
testbody
--22e0822b-F--
HTTP/1.1 200 OK
Content-Length: 570
Content-Type: text/html; charset=iso-8859-1

--22e0822b-E--
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>200 OK</title>
```

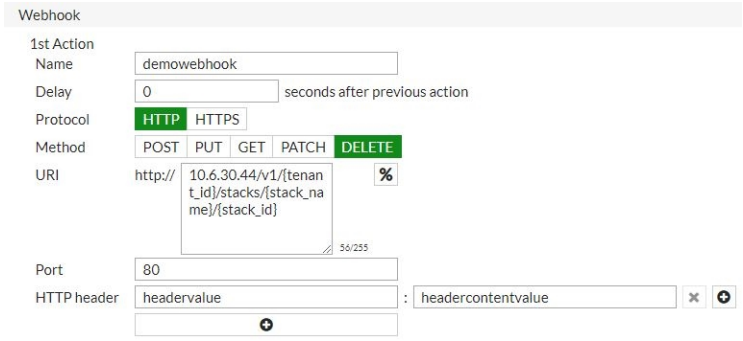
To set the Patch method using the CLI, see the following example:

In the CLI, `set method patch` is added.

```
config system automation-action
   edit "demowebhook"
      set action-type webhook
      set method patch
      set uri "10.6.30.44/v1/{tenant_id}/stacks/{stack_name}/{stack_id}"
      set http-body "testbody"
      set port 80
      set headers "headervalue:headercontentvalue"
   next
end
```

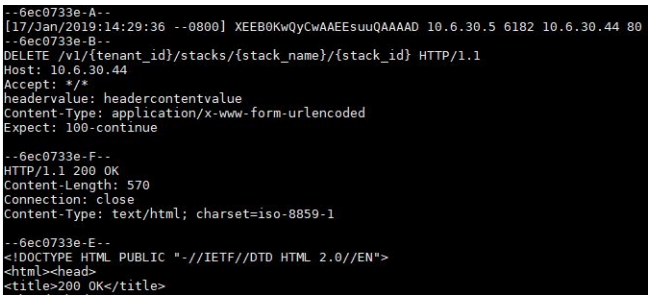
To set the Delete method using the GUI:

1. Go to *Security Fabric* > *Automation* and click *Create New*.
2. In the *Action* section, click *Webhook* to display the *Webhook* section.
3. For the *Method*, select *DELETE*.



4. Fill in the other fields and click *OK*.

On the server, check that FortiGate sends the header, body, and method correctly:



To set the Delete method using the CLI, see the following example:

In the CLI, `set method delete` is added.

```
config system automation-action
   edit "demowebhook"
      set action-type webhook
      set method delete
      set uri "10.6.30.44/v1/{tenant_id}/stacks/{stack_name}/{stack_id}"
      set http-body "/v1/{tenant_id}/stacks/{stack_name}/{stack_id}/preview"
      set port 80
      set headers "headervalue:headercontentvalue"
   next
end
```

Advanced Threats

This section lists the new features added to FortiOS for advanced threats.

Flow-based Inspection

This section lists new flow-based inspection features added to FortiOS.

Web Filtering

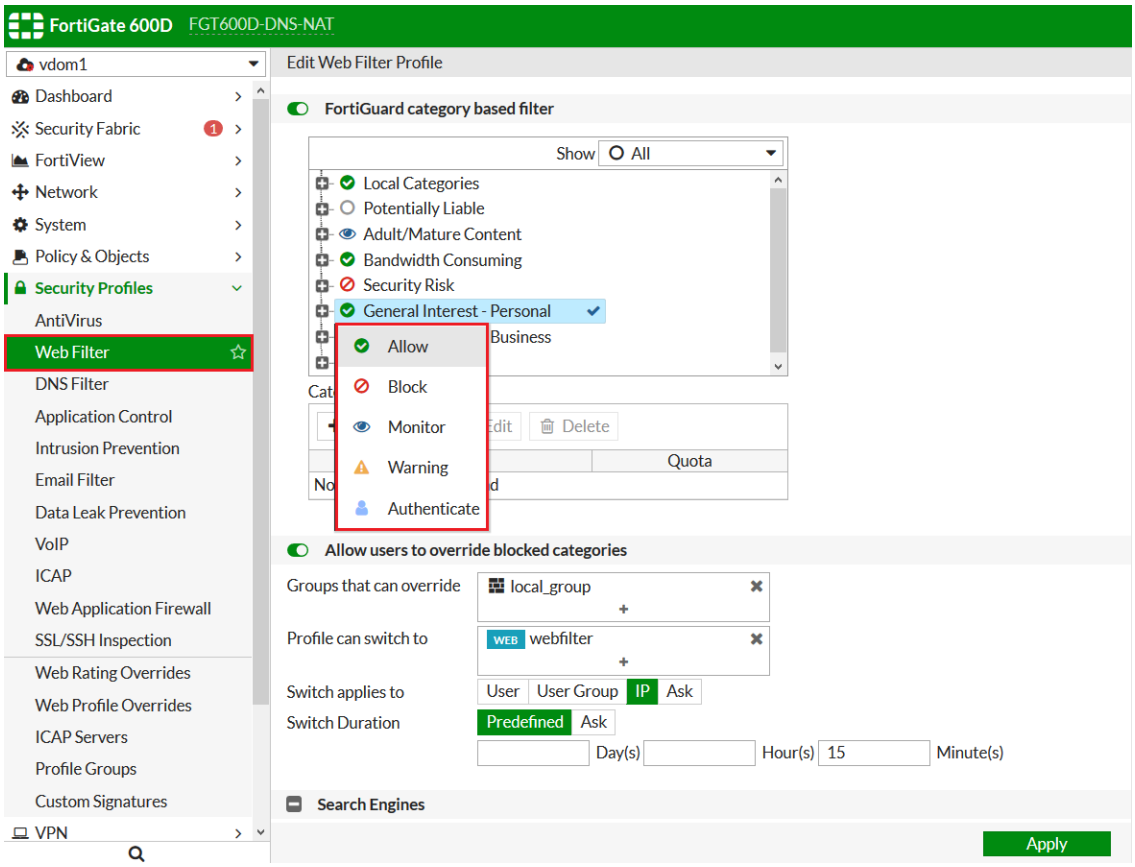
Flow-based web filtering support has been extended to allow for the following options:

- *Authenticate*: Require authentication for specific website categories.
- *Warn*: Display a warning message but allow users to continue to the website.
- *Override*: Allow users with valid credentials to override their web filter profile.

To enable Authenticate and Warning web filters:

1. Go to *Security Profiles* > *Web Filter* in the FortiGate web GUI.
2. Right-click on a selected category to view the context menu.

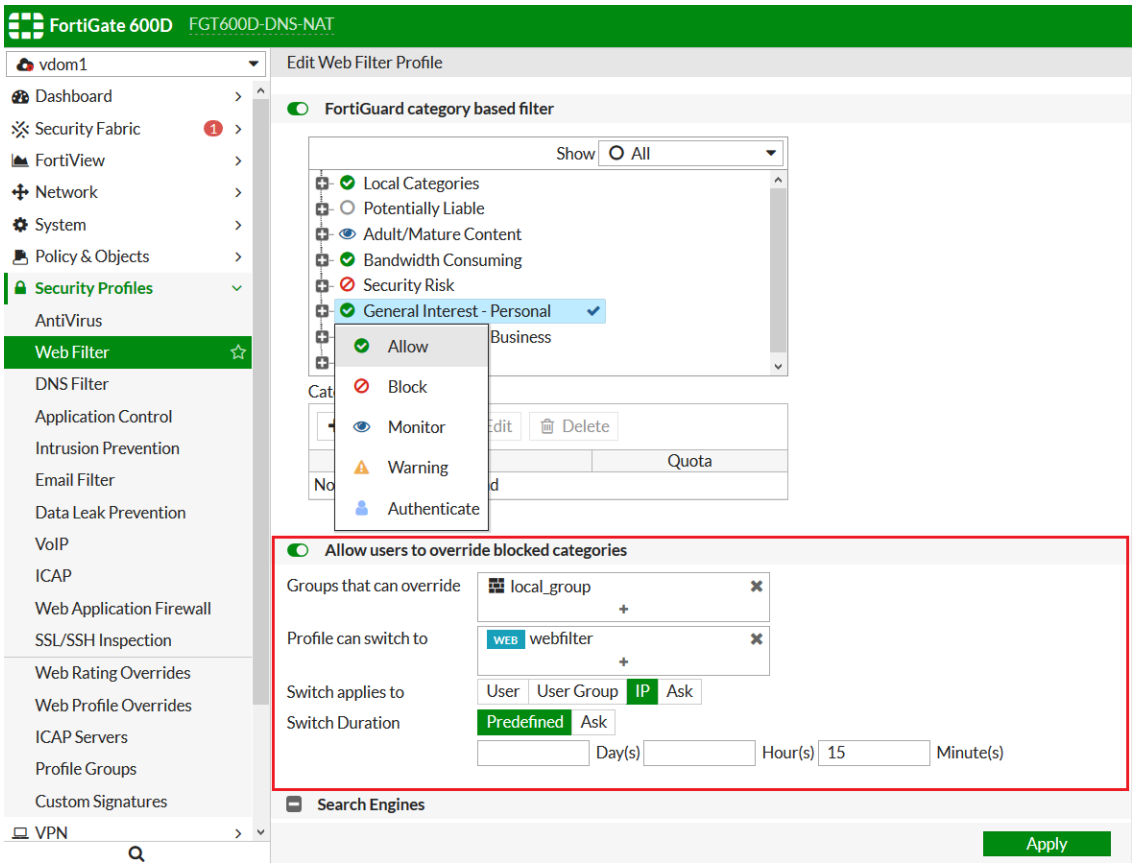
3. Select the *Authenticate* or *Warning* web filter.



4. Select *Apply*.

To allow users to override blocked categories:

1. Select *Allow users to override blocked categories*.



2. Enter the following information:
   - Groups that can override
   - Profile can switch to
   - Switch applies to
   - Switch duration
3. Select *Apply*.

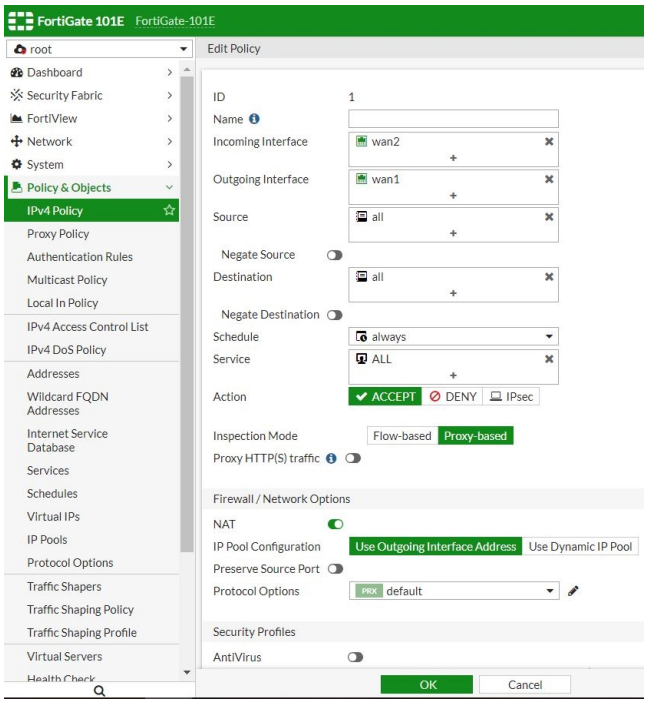
Inspection Mode Per Policy

In this version, in NGFW Mode, the Inspection Mode is moved to per-policy, enabling more flexible setup for different policies.

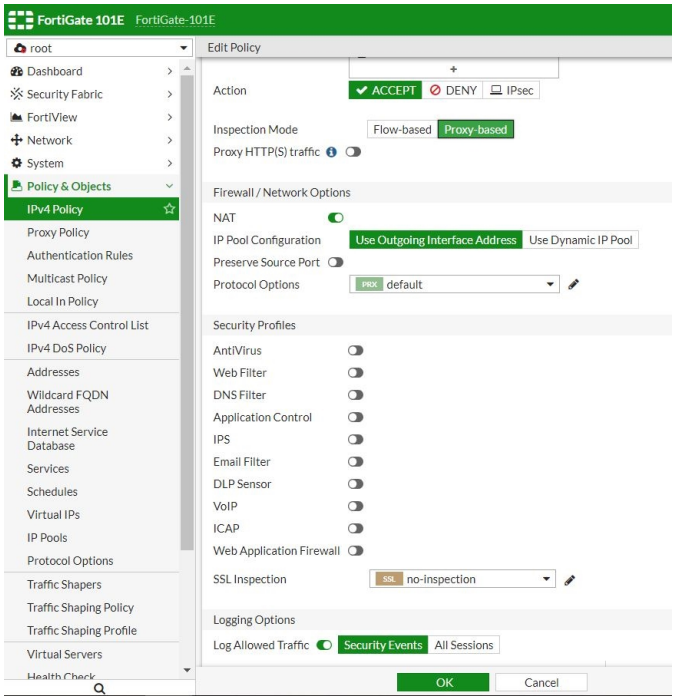
In *System* > *VDOM*, the *NGFW Mode* option has been removed.

When you configure a policy, you can select a *Flow-based* or *Proxy-based Inspection Mode*. Default is *Flow-based*.

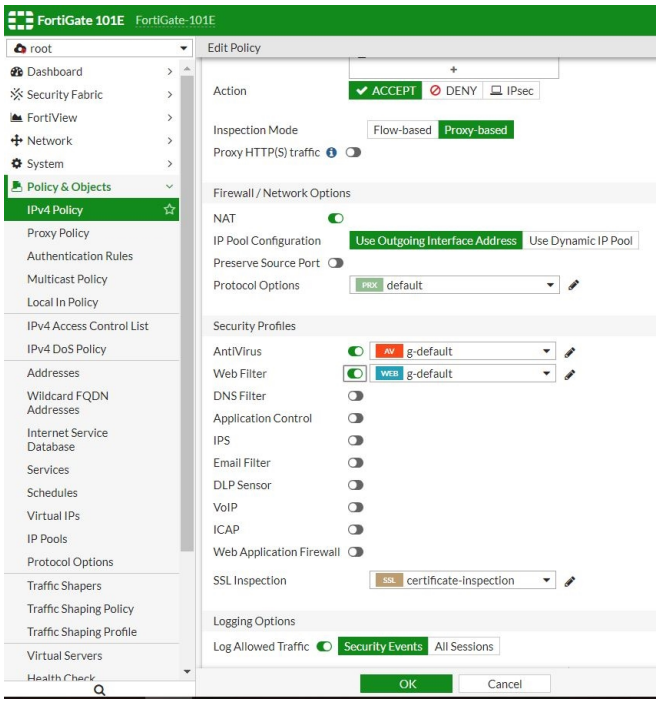
If you change to *Proxy-based*, the *Proxy HTTP(S) traffic* option displays.



In the *Security Profiles* section, if no security profiles are enabled, the default *SSL Inspection* is *no-inspection*.



In the *Security Profiles* section, if you enable any security profile, the *SSL Inspection* changes to *certificate-inspection*.



To see the inspection mode changes in the CLI:

```
FortiGate-101E (root) # config firewall policy

FortiGate-101E (policy) # edit 1

FortiGate-101E (1) # set utm-status disable

FortiGate-101E (1) # set inspection-mode
proxy     Proxy based inspection.
flow      Flow based inspection.

FortiGate-101E (1) # set inspection-mode proxy

FortiGate-101E (1) # end

FortiGate-101E (root) # sh firewall policy
config firewall policy
    edit 1
        set uuid 05d88354-4817-51e9-7494-06cb70accbf0
        set srcintf "wan2"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set nat enable
    next
end
```

To see http-policy-redirect/ssh-policy-redirect setting when inspection mode is set to proxy:

```
FortiGate-101E (root) # config firewall policy

FortiGate-101E (policy) # end

FortiGate-101E (root) # config firewall policy

FortiGate-101E (policy) # edit 1

FortiGate-101E (1) # set inspection-mode proxy

FortiGate-101E (1) # set http-policy-redirect
enable     Enable HTTP(S) policy redirect.
disable    Disable HTTP(S) policy redirect.

FortiGate-101E (1) # set ssh-policy-redirect
enable     Enable SSH policy redirect.
disable    Disable SSH policy redirect.

FortiGate-101E (1) # set http-policy-redirect enable

FortiGate-101E (1) # set ssh-policy-redirect enable

FortiGate-101E (1) # end

FortiGate-101E (root) # sh firewall policy 1
config firewall policy
    edit 1
        set uuid 05d88354-4817-51e9-7494-06cb70accbf0
        set srcintf "wan2"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set http-policy-redirect enable
        set ssh-policy-redirect enable
        set nat enable
    next
end
```

To see the default ssl-ssh-policy set to no inspection:

```
FortiGate-101E (root) # config firewall policy

FortiGate-101E (policy) # edit 1

FortiGate-101E (1) # sh
config firewall policy
    edit 1
        set uuid 05d88354-4817-51e9-7494-06cb70accbf0
        set srcintf "wan2"
        set dstintf "wan1"
```

```
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set inspection-mode proxy
        set http-policy-redirect enable
        set ssh-policy-redirect enable
        set nat enable
    next
end

FortiGate-101E (1) # sh fu | grep ssl-ssh-profile
        set ssl-ssh-profile "no-inspection"

FortiGate-101E (1) # end
```

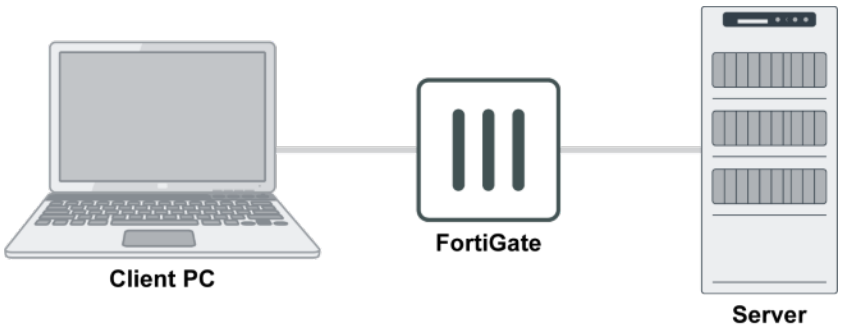
Statistics

This feature adds a flow AV statistics check, and provides an API for SNMP to get AV statistics.

Two CLI commands are added to show and clear the AV statistics:

```
diagnose ips av stats show
diagnose ips av stats clear
```

This example uses the following topology:



To check flow AV statistics:

1. Create an AV profile:
```
config antivirus profile
   edit "av-test"
      config http
         set options scan avmonitor
      end
      config ftp
         set options scan quarantine
      end
   next
end
```
2. Enable the profile on a firewall policy:
```
config firewall policy
   edit 1
```

```
        set name "policy1"
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set fsso disable
        set av-profile "av-test"
        set ssl-ssh-profile "custom-deep-inspection"
        set nat enable
    next
end
```

3. On the client PC, download the EICAR Standard Anti-Virus Test File via HTTP.
4. Check the AV statistics on the FortiGate. As the action is set to monitor for HTTP, `HTTP virus detected` is increased by 1:

```
diagnose ips av stats show
    AV stats:
    HTTP virus detected: 1
    HTTP virus blocked: 0
    SMTP virus detected: 0
    SMTP virus blocked: 0
    POP3 virus detected: 0
    POP3 virus blocked: 0
    IMAP virus detected: 0
    IMAP virus blocked: 0
    NNTP virus detected: 0
    NNTP virus blocked: 0
    FTP virus detected: 0
    FTP virus blocked: 0
    SMB virus detected: 0
    SMB virus blocked: 0
```

5. On the client PC, download the EICAR file via FTP.
6. Check the AV statistics on the FortiGate. As the action is set to quarantine for FTP, `FTP virus detected` and `FTP virus blocked` are both increased by 1:

```
diagnose ips av stats show
    AV stats:
    HTTP virus detected: 1
    HTTP virus blocked: 0
    SMTP virus detected: 0
    SMTP virus blocked: 0
    POP3 virus detected: 0
    POP3 virus blocked: 0
    IMAP virus detected: 0
    IMAP virus blocked: 0
    NNTP virus detected: 0
    NNTP virus blocked: 0
    FTP virus detected: 1
    FTP virus blocked: 1
    SMB virus detected: 0
    SMB virus blocked: 0
```

7. Check the AV statistics using snmpwalk:

```
root:~# snmpwalk -c public -v 1 10.1.100.6 1.3.6.1.4.1.12356.101.8.2.1.1
```

```
iso.3.6.1.4.1.12356.101.8.2.1.1.1.1 = Counter32: 2 (fgAvVirusDetected)
iso.3.6.1.4.1.12356.101.8.2.1.1.2.1 = Counter32: 1 (fgAvVirusBlocked)
iso.3.6.1.4.1.12356.101.8.2.1.1.3.1 = Counter32: 1 (fgAvHTTPVirusDetected)
iso.3.6.1.4.1.12356.101.8.2.1.1.4.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.5.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.6.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.7.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.8.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.9.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.10.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.11.1 = Counter32: 1 (fgAvFTPVirusDetected)
iso.3.6.1.4.1.12356.101.8.2.1.1.12.1 = Counter32: 1 (fgAvFTPVirusBlocked)
iso.3.6.1.4.1.12356.101.8.2.1.1.13.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.14.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.15.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.16.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.17.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.18.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.19.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.20.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.21.1 = Counter32: 0
iso.3.6.1.4.1.12356.101.8.2.1.1.22.1 = Counter32: 0
```

8. Optionally, reset the AV statistics to zero:

```
diagnose ips av stats clear
```

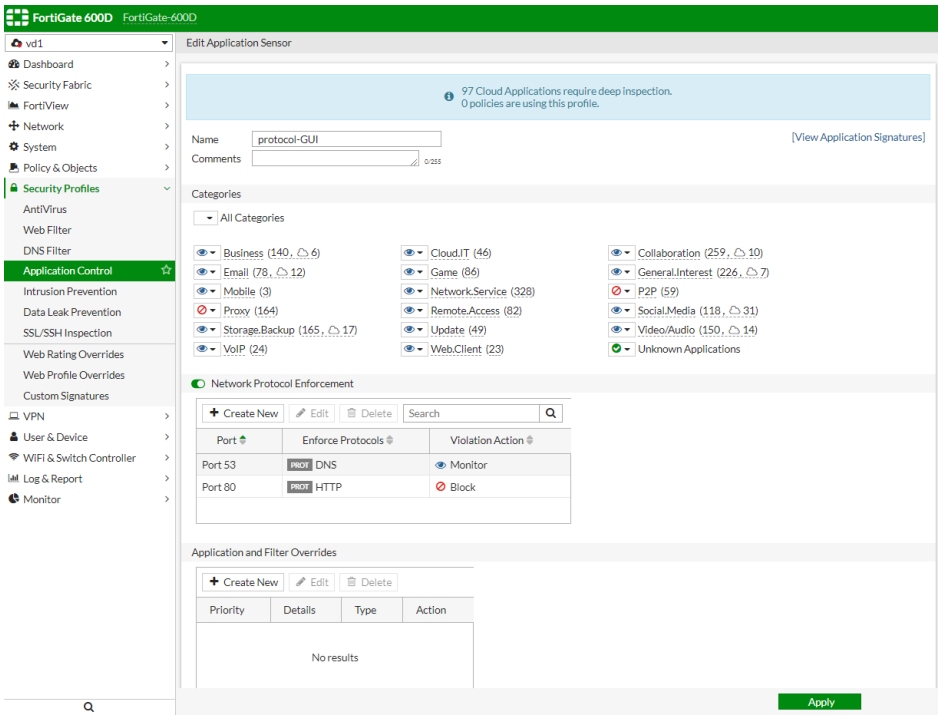
Protocol Port Enforcement

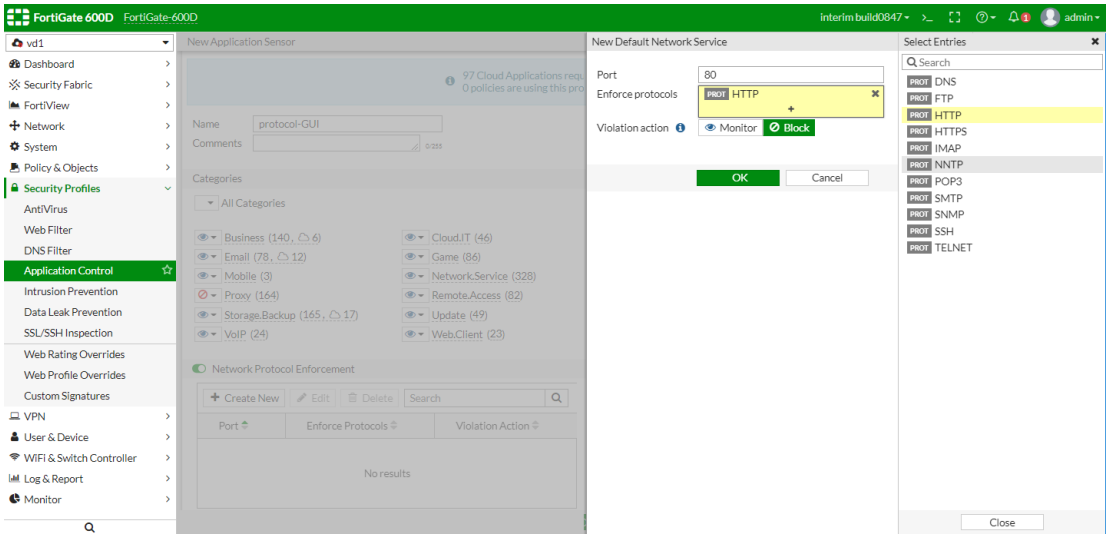
Protocol enforcement is added to the Application Control Profile, allowing the admin to configure network services (e.g., FTP, HTTP, HTTPS) on known ports (e.g., 21, 80, 443), while blocking those services on other ports.

The feature takes action in the following scenarios:

- When one protocol dissector confirms the service of network traffic, protocol enforcement can check whether the confirmed service is whitelisted under the server port. If it is not, then the traffic is considered a violation and IPS can take action (e.g., block) specified in the configuration.
- There is no confirmed service for the network traffic. It would be considered a service violation if IPS dissectors rule out all the services enforced under its server port.

In *Security Profiles* > *Application Control*, a new Network Protocol Enforcement pane lets you create and configure network services on specific ports and set violation action.





To configure the application profile default network service list using CLI:

```
config application list
    edit "protocol-GUI"
        set other-application-log enable
        set control-default-network-services enable     # Enable enforcement of protocols over
select ports.
        config default-network-services                 # Default network service entries
            edit 1
                set port 80                             # Port number, port Enter an integer
value from <0> to <65535>
                set services http                       # Network protocols: http, ssh, telnet,
ftp, dns, smtp, pop3, imap, snmp, nntp and https
```

```
            next
            edit 2
                set port 53
                set services dns
                set violation-action monitor           # Set action for protocols not whitel-
isted under select port: block/pass/monitor
            next
        end
    next
end
```

IP Reputation Filtering

This features adds support for reputation filtering in the firewall policies.

Currently, there are five reputation levels in the internet-service database (ISDB), and custom reputation levels can be defined in a custom internet-service. This features allows firewall policies to filter traffic according to the configured reputation level. If the reputation level of either the source or destination IP address is equal to or greater than the level set in the policy, then the packet is forwarded, otherwise, the packet is dropped.

The five default reputation levels are:

1	Known malicious sites related to botnet servers, phishing sites, etc.
2	Sites providing high risk services, such as TOR, proxy, P2P, etc.
3	Unverified sites.
4	Reputable sites from social media, such as Facebook, Twitter, etc.
5	Known and verified safe sites, such as Gmail, Amazon, eBay, etc.

The default minimum reputation level in a policy is zero, meaning that the reputation filter is disabled.

For IP addresses that are not included in the ISDB, the default reputation level is three.

The default reputation direction is `destination`.

To set the reputation level and direction in a policy:

```
config firewall policy
    edit 1
        set uuid dfcaec9c-e925-51e8-cf3e-fed9a1d42a1c
        set srcintf "wan2"
        set dstintf "wan1"
        set dstaddr "all"
        set reputation-minimum 3
        set reputation-direction source
        set action accept
```

```
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set auto-asic-offload disable
        set nat enable
    next
end
```

Packets from the source IP address with reputation levels three, four, or five will be forwarded by this policy.

In a policy, if `reputation-minimum` is set, and the `reputation-direction` is `destination`, then the `dstaddr`, `service`, and `internet-service` options are removed from the policy.

If `reputation-minimum` is set, and the `reputation-direction` is `source`, then the `srcaddr`, and `internet-service-src` options are removed from the policy.

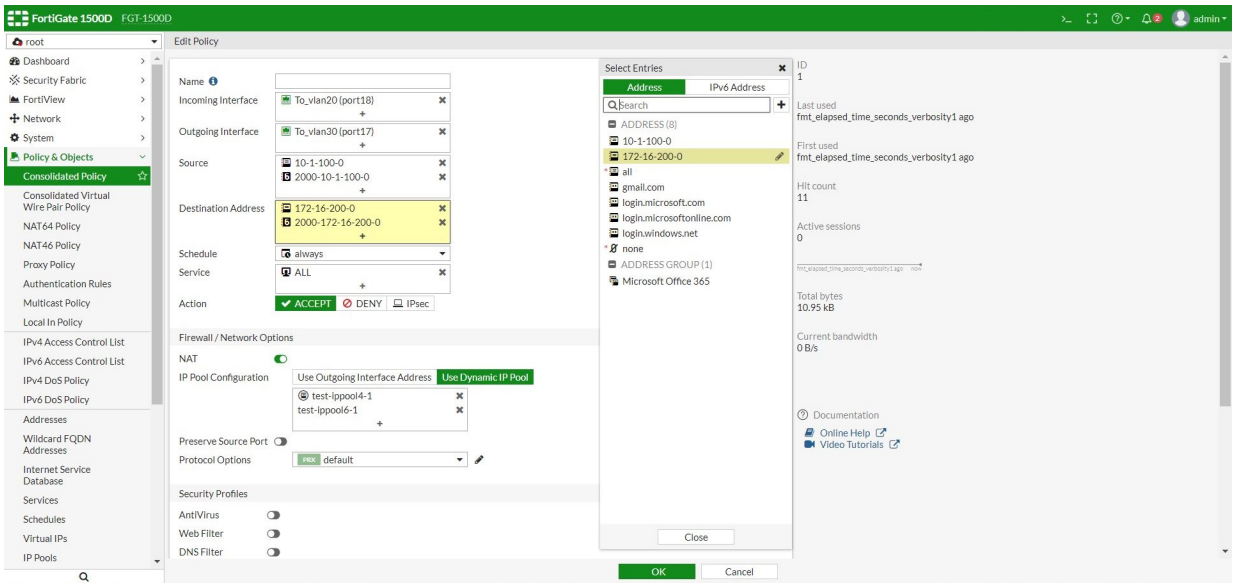
IPv6

This section lists new IPv6 features added to FortiOS.

Combined IPv4 and IPv6 Policy

This feature introduces a new, consolidated policy mode. In this mode, IPv4 and IPv6 policies are combined into a single, consolidated policy. This means that a single policy can be defined that includes both IPv4 and IPv6, instead of defining separate policies.

In consolidated policy mode, there is a single policy table for the GUI. The same source interface, destination interface, service, user, and schedule are shared for both IPv4 and IPv6, while there are different IP addresses and IP pool settings.



Consolidated policy mode can be enabled with the following CLI command:

```
config system settings
   set consolidated-firewall-mode enable
      Enabling consolidated-firewall-mode will delete all firewall policy/policy6. Do you
           want to continue? (y/n) y
end
```

Enabling consolidated policy mode will delete all existing IPv4 and IPv6 policies.

To configure a consolidated policy in the CLI:

```
config firewall consolidated policy
   edit 1
      set uuid 754a86b6-2507-51e9-ef0d-13a6e4bf2e9d
      set srcintf "port18"
      set dstintf "port17"
      set srcaddr4 "10-1-100-0" <-------- IPv4 srcaddr
      set dstaddr4 "172-16-200-0" <-------- IPv4 dstaddr
      set srcaddr6 "2000-10-1-100-0" <-------- IPv6 srcaddr
      set dstaddr6 "2000-172-16-200-0" <-------- IPv6 dstaddr
      set action accept set schedule "always"
      set service "ALL"
      set logtraffic all
      set ippool enable
      set poolname4 "test-ippool4-1" <-------- IPv4 poolname
      set poolname6 "test-ippool6-1" <-------- IPv6 poolname
      set nat enable
   next
end
```

Limitations

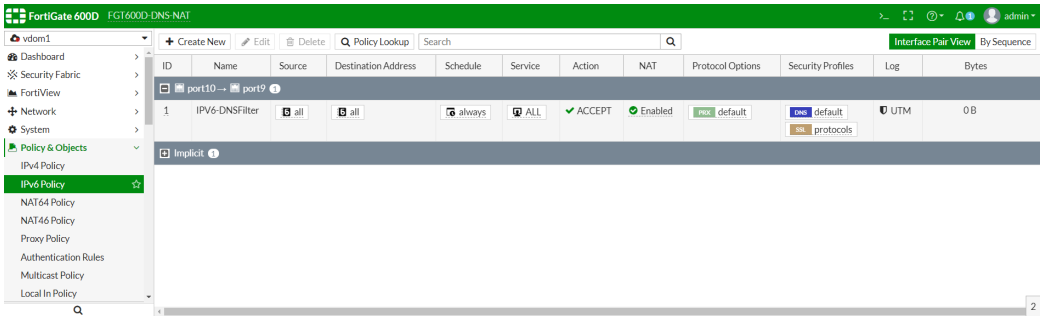
The following features are not currently supported by consolidated policy mode:

- Policy-learning mode
- Internet-services in policy
- Address-negate and service-negate
- DSCP-match/Tos
- Traffic shaper in policy
- Capture-packet in policy
- External IP list in policy
- schedule-timeout, block-notification, disclaimer, custom-log-fields, or reputation in policy
- timeout-send-rst, tcp-session-without-syn, or anti-replay in policy;
- Policy Interface Pair View
- Policy lookup function on page.

The session/iprope tables for IPv4 and IPv6 are still displayed separately.

FortiGuard DNS Filter

This feature adds DNS profile inspection to IPv6 policies. This includes FortiGuard DNS filtering (with a web filtering license), and portal replacement message redirect.



To apply a DNS Filter profile to an IPv6 policy using the CLI:

```
config firewall policy6
   edit 1
      set name "IPV6-DNSFilter"
      set uuid b1adb096-1919-51e9-05c7-87813d4e2b2a
      set srcintf "port10"
      set dstintf "port9"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set utm-status enable
      set dnsfilter-profile "default"
      set ssl-ssh-profile "protocols"
      set nat enable
   next
end
```

A new CLI variable is added to the DNS filter profile for the IPv6 address of the SDNS redirect portal: `redirect-portal6`

```
config dnsfilter profile
   edit "default"
      set comment "Default dns filtering."
      config domain-filter
         unset domain-filter-table
      end
      config ftgd-dns
         unset options
         config filters
            edit 1
               set category 2
               set action monitor
            next
            edit 2
               set category 7
               set action monitor
            next
         ......
      end
      set log-all-domain disable
      set sdns-ftgd-err-log enable
      set sdns-domain-log enable
      set block-action redirect
      set block-botnet enable
      set safe-search disable
      set redirect-portal 0.0.0.0
      set redirect-portal6 ::
   next
end
```

After the FortiGate has successfully initialized communication with the SDNS server (for domain rating service), the following CLI command will show the default redirect portal IPv6 address:

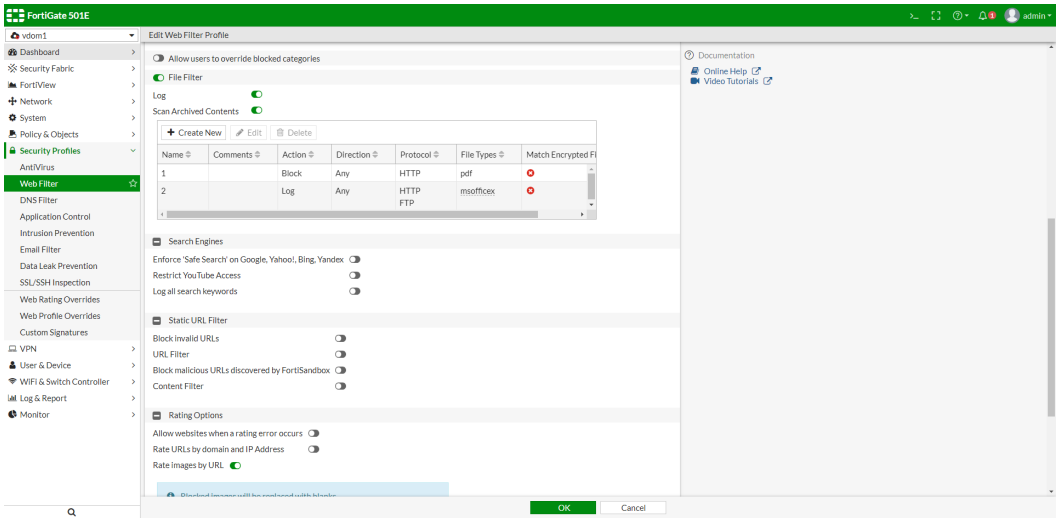
```
(global) # diag test app dnsproxy 3
   ......
   FGD_REDIR_V4:208.91.112.55 FGD_REDIR_V6:[2001:cdba::3257:9652]
```

File Filtering for Web and Email Filter Profiles

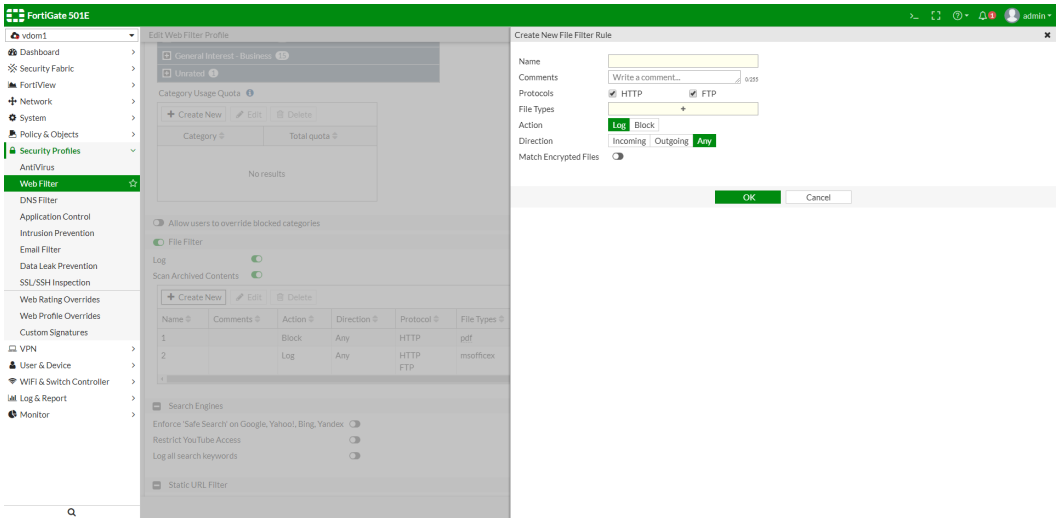
This feature adds file filtering capabilities to web and email filter profiles. The web filters will cover the detection of HTTP and FTP traffic, while the email filters cover SMTP, POP3, and IMAP. New logs and replacement messages are also added.

To add a file filter to a web filter profile in the GUI:

1. On the FortiGate, go to *Security Profiles* > *Web Filter*.
2. Edit an existing profile, or create a new one.



3. Enable *File Filter*, if not already enabled, then click *Create New* in the filter table. The *Create New File Filter Rule* pane opens.



4. Configure the filter as required, then click *OK*.

To add a file filter to a web filter profile using the CLI:

```
config webfilter profile
  edit "webfilter-file-filter"
    config file-filter
      set status {enable | disable}
      set log {enable | disable}
      set scan-archive-contents {enable | disable}
        config entries
        edit "filter1"
          set comment "Block files"
          set protocol [http | ftp]
```

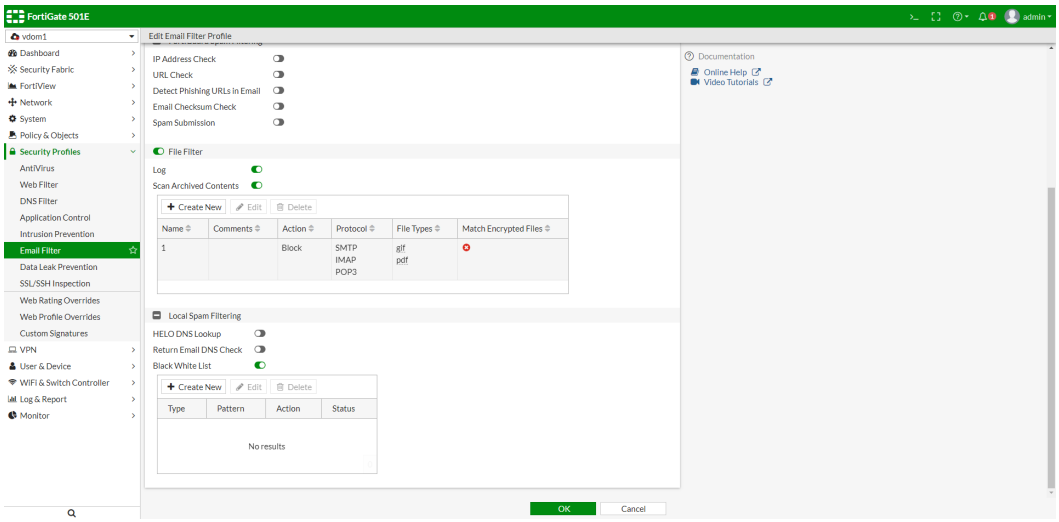
```
          set action {block | log}
          set direction {any | incoming | outgoing}
          set encryption {any | yes}
          set file-type "pdf" "msofficex"
        next
      end
    end
  next
end
```

Web filter profiles handle HTTP and FTP protocols, and can configure the traffic direction.

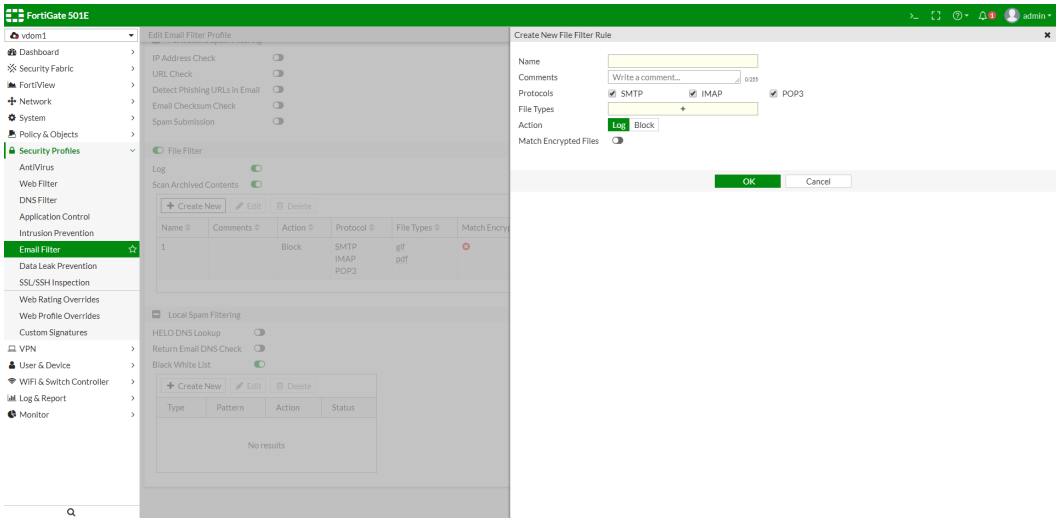
Variable	Description
status {enable | disable}	Enable/disable file filtering (default = enable).
log {enable | disable}	Enable/disable file filter logging (default = enable).
scan-archive-contents {enable | disable}	Enable/disable file filter archive contents scan (default = enable).
comment <string>	Optional comments.
protocol [http | ftp]	Protocols to use (default = http ftp).
action {block | log}	The action taken for matched file (default = log).
direction {any | incoming | outgoing}	Match files transmitted in the session's originating direction (incoming), reply direction (outgoing), or either (any) (default = any).
encryption {any | yes}	Match encrypted files or not: • `any` - match any file (default). • `yes` - match only encrypted files.
file-type <string>	Select the file types to match.

To add a file filter to an email filter profile in the GUI:

1. On the FortiGate, go to *Security Profiles* > *Email Filter*.
2. Edit an existing profile, or create a new one.



3. Enable *Enable Spam Detection and Filtering*, if not already enabled.
4. Enable *File Filter*, if not already enabled, then click *Create New* in the filter table. The *Create New File Filter Rule* pane opens.



5. Configure the filter as required, then click *OK*.

To add a file filter to an email filter profile with the CLI:

```
config emailfilter profile
  edit "emailfilter-file-filter"
    config file-filter
      set status {enable | disable}
      set log {enable | disable}
      set scan-archive-contents {enable | disable}
      config entries
        edit "filter1"
```

```
          set comment "Block files"
          set protocol [smtp | imap | pop3]
          set action {block | log}
          set encryption {any | yes}
          set file-type "exe"
        next
      end
    end
  next
end
```

Email filter profiles handle SMTP, IMAP, and POP3 protocols. The traffic direction cannot be configured, as it is implied by the protocol.

Variable	Description
status {enable | disable}	Enable/disable file filtering (default = enable).
log {enable | disable}	Enable/disable file filter logging (default = enable).
scan-archive-contents {enable | disable}	Enable/disable file filter archive contents scan (default = enable).
comment <string>	Optional comments.
protocol [smtp | imap | pop3]	Protocols to use (default = smtp imap pop3).
action {block | log}	The action taken for matched file (default = log).
encryption {any | yes}	Match encrypted files or not: • `any` - match any file (default). • `yes` - match only encrypted files.
file-type <string>	Select the file types to match.

New logs

A new `file_filter` event type is added to both web and email filter log categories.

Log samples

Web Filter File Filter action as *Block*:

```
1: date=2019-03-19 time=09:42:15 logid="0346012673" type="utm" subtype="webfilter" event-
type="file_filter" level="warning" vd="vd1" eventtime=1548438135 policyid=1 sessionid=29449
srcip=10.1.100.22 srcport=52816 srcintf="dmz" srcintfrole="undefined" dstip=172.16.200.55
dstport=80 dstintf="wan1" dstintfrole="undefined" proto=6 service="HTTP" host-
name="172.16.200.55" profile="webfilter-filefilter" action="blocked" reqtype="direct" url-
l="/app_data/test1.pdf" sentbyte=0 rcvdbyte=0 direction="incoming" filename="test1.pdf"
filtername="filter1" filetype="pdf" msg="File was blocked by file filter."
```

Web Filter File Filter action as *Log*:

```
2: date=2019-03-19 time=10:48:23 logid="0346012672" type="utm" subtype="webfilter" event-
type="file_filter" level="notice" vd="vd1" eventtime=1548442102 policyid=1 sessionid=521
srcip=10.1.100.22 srcport=52894 srcintf="dmz" srcintfrole="undefined" dstip=172.16.200.55
dstport=80 dstintf="wan1" dstintfrole="undefined" proto=6 service="HTTP" host-
name="172.16.200.55" profile="webfilter-filefilter" action="passthrough" reqtype="direct"
url="/app_data/park.jpg" sentbyte=0 rcvdbyte=0 direction="incoming" filename="park.jpg" fil-
tername="filter2" filetype="jpeg" msg="File was detected by file filter."
```

Email Filter File Filter action as *Block*:

```
1: date=2019-01-25 time=15:20:16 logid="0554020511" type="utm" subtype="emailfilter" event-
type="file_filter" level="warning" vd="vdom1" eventtime=1548458416 policyid=1 ses-
sionid=2881 srcip=10.1.100.12 srcport=45974 srcintf="port2" srcintfrole="undefined"
dstip=172.16.200.56 dstport=143 dstintf="port1" dstintfrole="undefined" proto=6 ser-
vice="IMAP" action="blocked" from="emailuser1@qa.fortinet.com" to="-
"emailuser2@qa.fortinet.com" recipient="emailuser2" direction="incoming" subject="EXE file
block" size="622346" attachment="yes" filename="putty.exe" filtername="filter1" file-
type="exe"
```

Email Filter File Filter action as *Log*:

```
1: date=2019-01-25 time=15:23:16 logid="0554020510" type="utm" subtype="emailfilter" event-
type="file_filter" level="notice" vd="vdom1" eventtime=1548458596 policyid=1 sessionid=3205
srcip=10.1.100.12 srcport=55664 srcintf="port2" srcintfrole="undefined" dstip=172.16.200.56
dstport=25 dstintf="port1" dstintfrole="undefined" proto=6 service="SMTP" pro-
file="emailfilter-file-filter" action="detected" from="emailuser1@qa.fortinet.com" to="-
"emailuser2@qa.fortinet.com" sender="emailuser1@qa.fortinet.com"
recipient="emailuser2@qa.fortinet.com" direction="outgoing" subject="PDF file log" size-
e="390804" attachment="yes" filename="fortiauto.pdf" filtername="filter2" filetype="pdf"
```

New replacement messages

Web Filter File Filter blocking upload:

You are not permitted to upload the file "%%FILE%%".

Web Filter File Filter blocking download:

Your attempt to access the file "%%FILE%%" has been blocked by your system administrator.

Email Filter File Filter blocking emails:

This email has been blocked. The file %%FILE%% was blocked due to its file type or properties.

IOT & OT

This section lists the new features added to FortiOS for IOT & OT.

MAC Addressed-Based Policies

This version adds a new address type — range of MAC addresses for IPv4 policies, including:

- IPv4 Firewall Policy.
- IPv4 Virtual Wire Pair Policy.
- IPv4 ACL Policy.
- IPv4 Central SNAT Policy.
- IPv4 DoS Policy.

The MAC address is a link layer-based address type and the MAC address cannot be forwarded across different IP segments.

For policies in NAT mode VDOM, we only support this new MAC address type as source address.

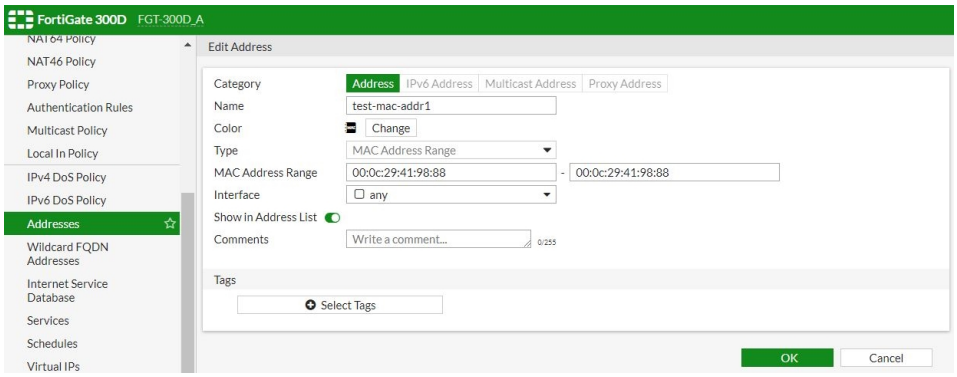
For policies in Transparent mode or Virtual Wire Pair interface, you can use this address type as source or destination address.

When you use this address type in a policy as source address in NAT mode VDOM, IP address translation (NAT) is still performed according to the rules defined in the policy. This new address type only works for source address matching. It does not have any association with NAT actions.

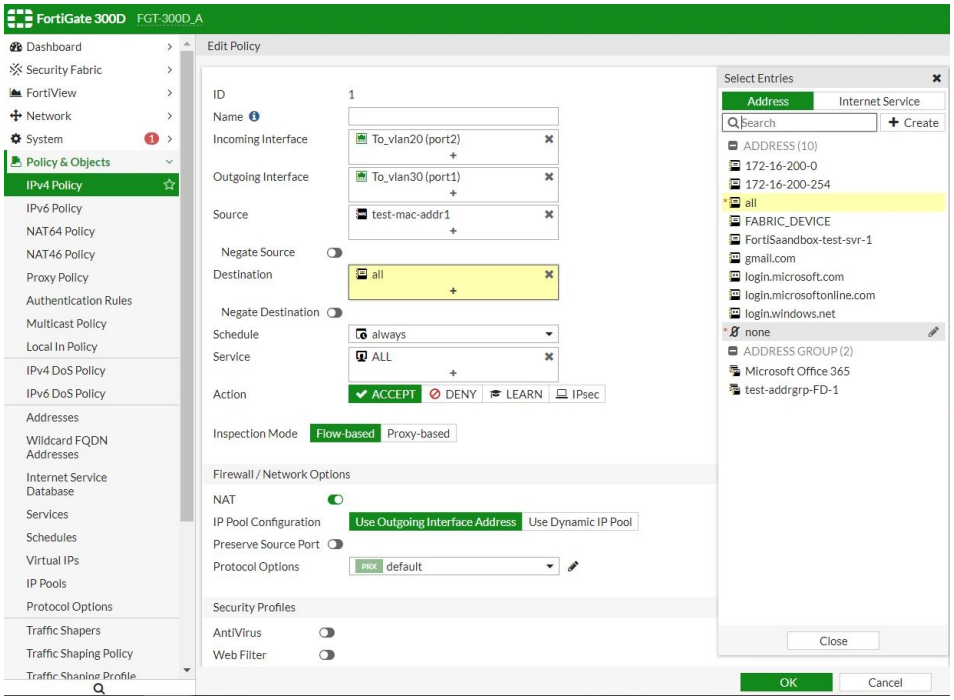
Sample configuration

To configure a MAC address range using the GUI:

1. Go to *Policy & Objects* > *Addresses* to create or edit an address.
   - For *Category*, select *Address*.
   - For *Type*, select *MAC Address Range* and enter the address range.
   - Enter the other fields and click *OK*.



2. Go to *Policy & Objects* > *IPv4 Policy* to apply the address type to a policy in NAT mode VDOM. In NAT mode VDOM, this address type cannot be used as destination address.



To configure a MAC address range using the CLI:

1. Create a new MAC address range type.

```
config firewall address
    edit <object_name>
        set type mac
        set start-mac <mac_address_start #>
        set end-mac <mac_address_end #>
    next
end
```

2. Apply the address type to a policy. In Transparent mode or Virtual Wire Pair interface, this address type can be mixed with other address types in the policy.

```
config firewall address
    edit "test-mac-addr1"
```

```
            set type mac
            set start-mac 00:0c:29:41:98:88
            set end-mac 00:0c:29:41:98:88
        next
    end
    config firewall policy
        edit 1
            set srcintf "port2"
            set dstintf "port1"
            set srcaddr "test-mac-addr1" "10-1-100-42"
            set dstaddr "all"
            set action accept
            set schedule "always"
            set service "ALL"
            set logtraffic all
            set nat enable
        next
    end
```

SOC Adoption

This section lists the new features added to FortiOS for SOC adoption.

Topology View — Consolidated Risk

The new Consolidated Risk View in the Security Fabric Topology displays different risks within the topology view. The filter considers threats originating from different components including:

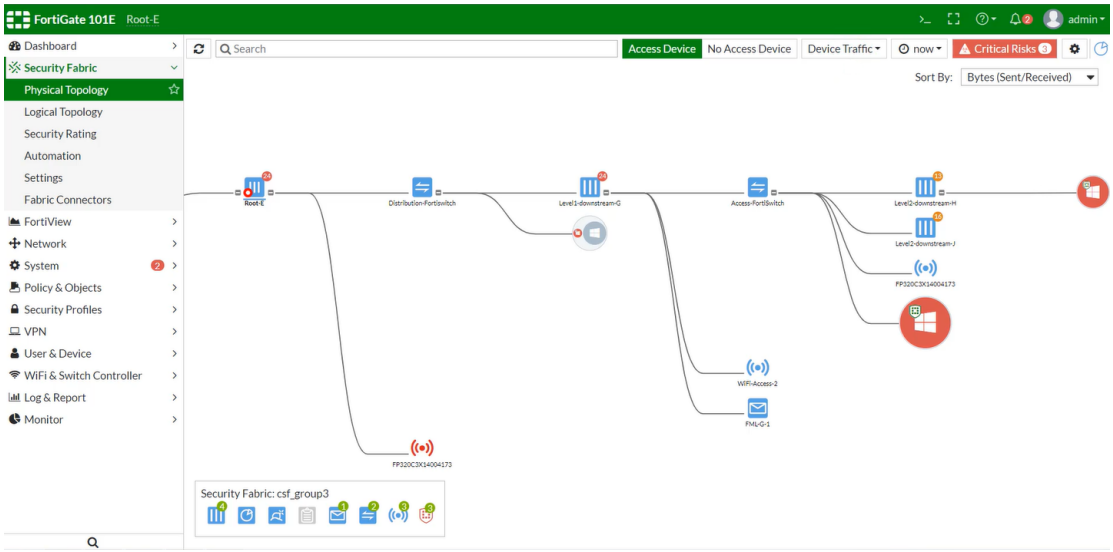
- IOC Detections
- Vulnerabilities
- Threat Score

The topology shows endpoints based on their highest severity event. Details are available in the tooltips. Administrators can also filter by risk type or severity.

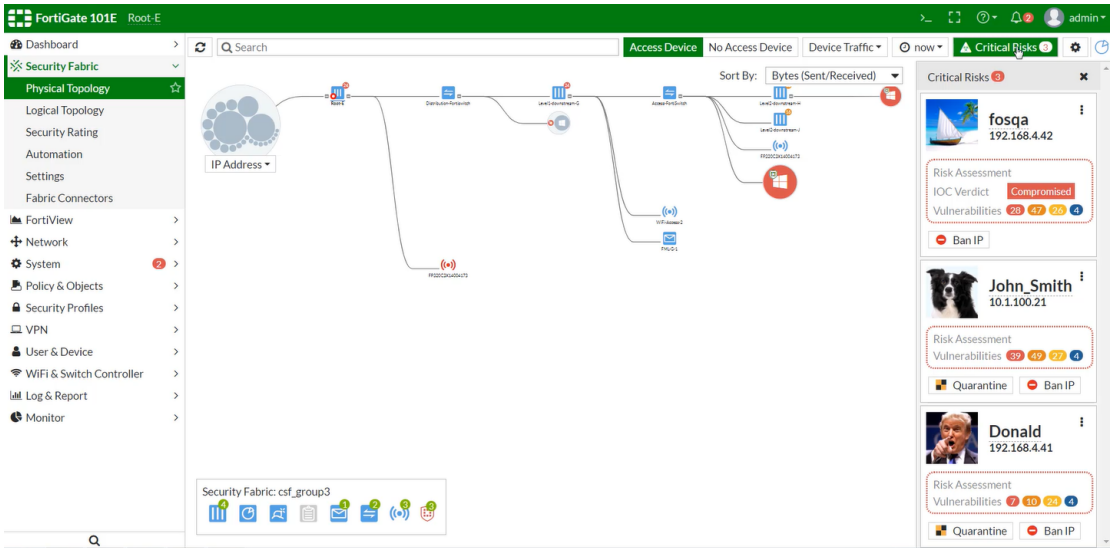
This version addes two improvements for topology pages:

- Add the ability to highlight hosts with critical vulnerabilities along with compromised hosts as Critical Risks in the default topology view. You can also view Critical Risk devices in the right pane.
- Consolidate the *Vulnerability*, *Threat Score*, and '*IOC Score* view into a new view mode called *Risk* view.

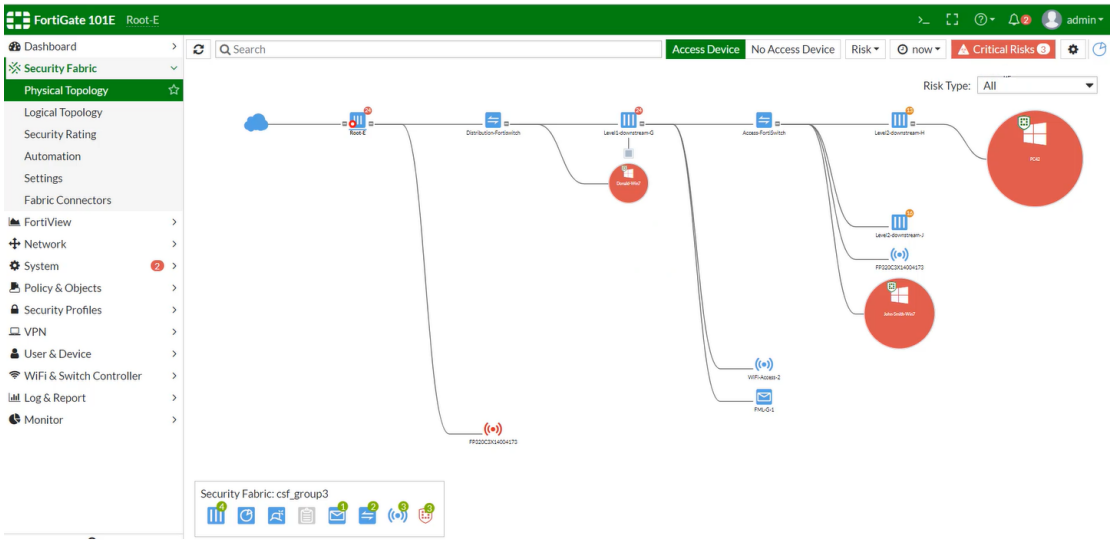
In *Security Fabric* > *Physical Topology*, the default topology view highlights hosts with critical vulnerabilities along with compromised hosts as *Critical Risks*.



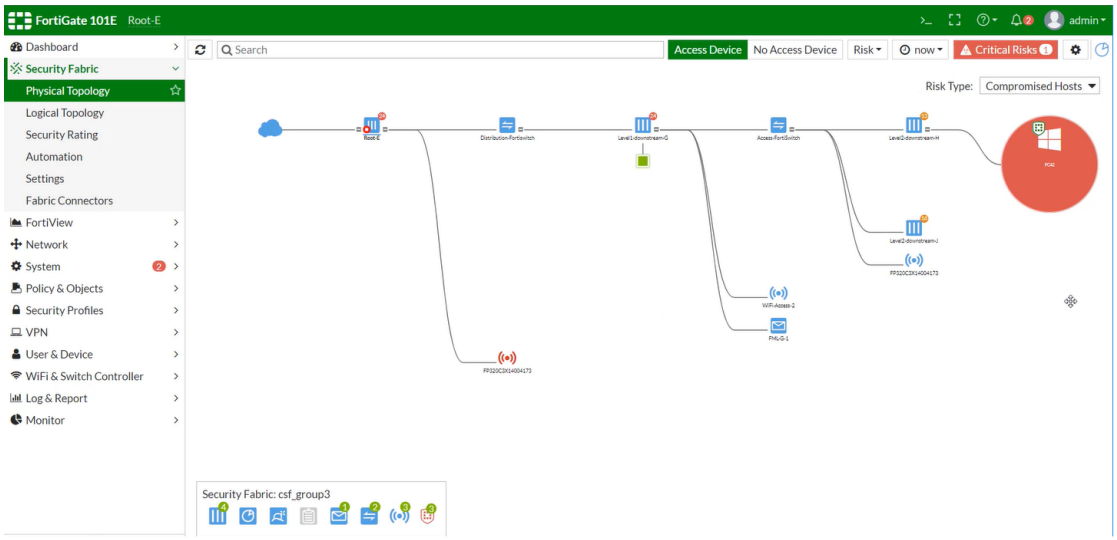
Click *Critical Risks* to view critical risk devices in the right pane.



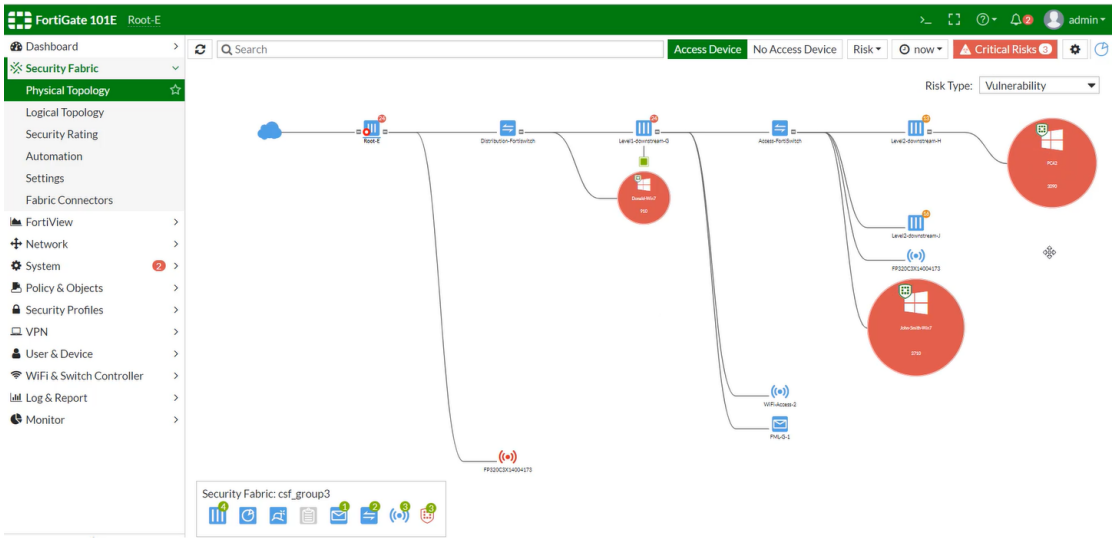
Using View mode *Risk* with *Risk Type All*.



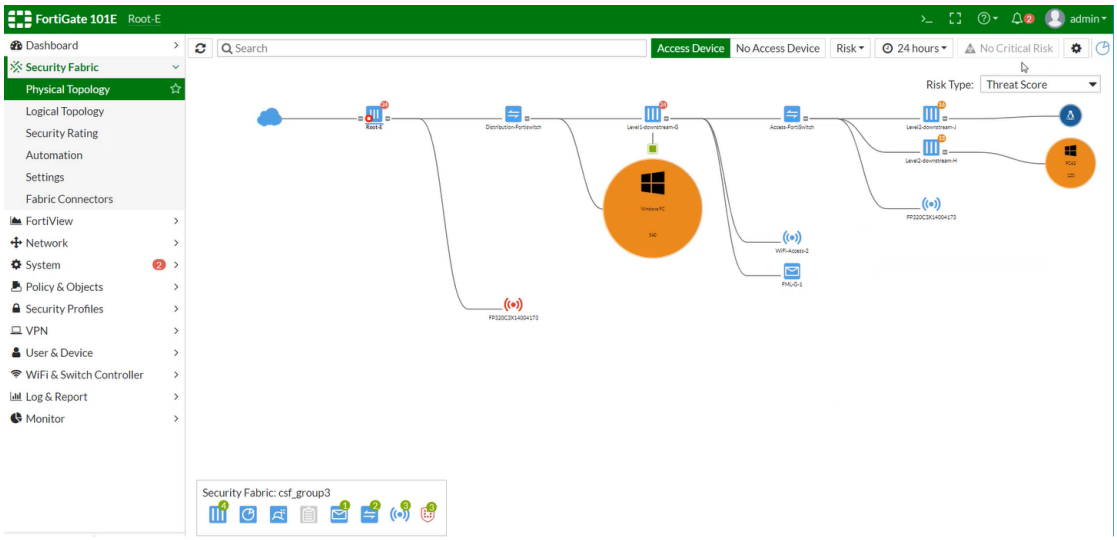
Using View mode *Risk* with *Risk Type Compromised Hosts*.



Using View mode *Risk* with *Risk Type Vulnerability*.



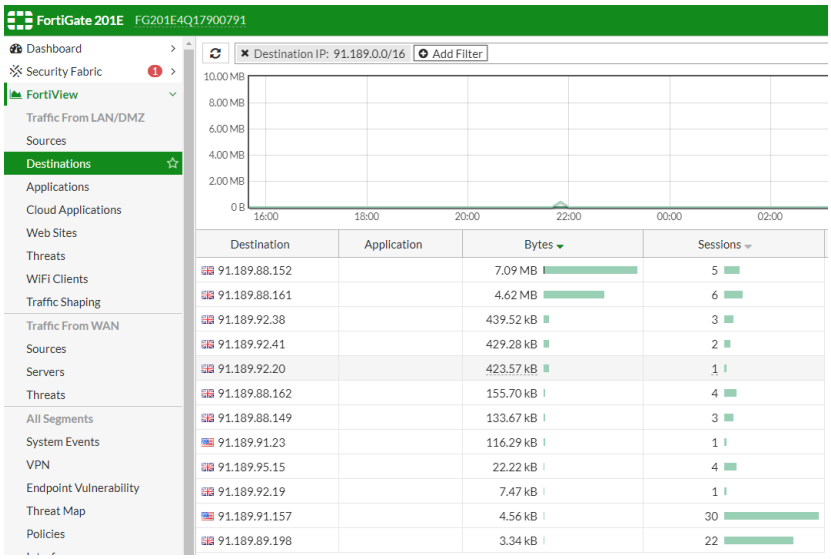
Using View mode *Risk* with *Risk Type Threat Score*.



FortiView — Subnet Filters

This version supports filtering source IPs or destination IPs with subnet mask in the format of x.x.x.x/x in both real-time and historical modes. Both logging from disk and logging from FortiAnalyzer are supported.

Sample configuration



Sample results in the backend subnet filter

```
FG201E4Q17900791 # di de application miglogd 0x70000
Debug messages will be on for unlimited time.
```

```
FG201E4Q17900791 # fortiview_add_filter_field_ex()-1559: fortiview add filter field:"des-
tination"=>"dstip" type:4 negate:0
fortiview_add_filter_field_ex()-1560: values:
fortiview_add_filter_field_ex()-1562: value[0]=91.189.0.0/16
fortiview_add_filter_field_ex()-1559: fortiview add filter field:"srcintfrole"=>"srcintfrole"
type:4 negate:0
fortiview_add_filter_field_ex()-1560: values:
fortiview_add_filter_field_ex()-1562: value[0]=lan
fortiview_add_filter_field_ex()-1562: value[1]=dmz
fortiview_add_filter_field_ex()-1562: value[2]=undefined
__params_from_filter()-583: filter field:dstip  91.189.0.0/16
__params_from_filter()-583: filter field:srcintfrole  lan
__params_from_filter()-583: filter field:srcintfrole  dmz
__params_from_filter()-583: filter field:srcintfrole  undefined
fortiview_request_data()-896: dataset:fv.dest.group tabid:0
_dump_sql()-829: dataset=fv.dest.group, sql:select dstip, max(dstintf) dst_intf,max(dstdev-
type) dst_devtype,max(dstmac) dst_mac,group_concat(distinct appid) appid,group_concat(distinct
appservice||case when subapp is null then '' else '_'||subapp end) appname,sum(sessioncount)
session_count, sum(case when passthrough<>'block' then sessioncount else 0 end) session_allow,
sum(case when passthrough='block' then sessioncount else 0 end) session_block, sum(rcvdbyte)
r, sum(sentbyte) s, sum(rcvdbyte + sentbyte) bandwidth ,sum(crscore) score, sum(case when
passthrough<>'block' then crscore else 0 end) score_allow, sum(case when passthrough='block'
then crscore else 0 end) score_block  from grp_traffic_all_dst  where timestamp between
1551397800 and 1551484200 and 1=1 AND ( ft_ipmask(dstip, 0, '91.189.0.0/16') )  AND srcint-
frole  in ('lan','dmz','undefined')  group by dstip   order by bandwidth desc   limit 100;
 takes 10(ms), agggr:0(ms)

fortiview_request_data()-933: total:12 start:1551397800 end:1551484200
__params_from_filter()-583: filter field:dstip  91.189.0.0/16
__params_from_filter()-583: filter field:srcintfrole  lan
__params_from_filter()-583: filter field:srcintfrole  dmz
__params_from_filter()-583: filter field:srcintfrole  undefined
fortiview_request_data()-896: dataset:fv.general.chart tabid:0
_dump_sql()-829: dataset=fv.general.chart, sql:select a.timestamp1,ses_al,ses_bk,r,s,ifnull
(sc_l,0),ifnull(sc_m,0),ifnull(sc_h,0),ifnull(sc_c,0) from (select timestamp-(timestamp%600)
timestamp1 ,sum(case when passthrough<>'block' then sessioncount else 0 end) ses_al,sum(case
when passthrough='block' then sessioncount else 0 end) ses_bk,sum(rcvdbyte) r,sum(sentbyte) s
from grp_traffic_all_dst where  timestamp BETWEEN 1551397800 and 1551484199  and 1=1 AND ( ft_
ipmask(dstip, 0, '91.189.0.0/16') )  AND srcintfrole  in ('lan','dmz','undefined')  group by
timestamp1 ) a left join (select timestamp-(timestamp%600) timestamp1 ,sum(case when threat_
level=1 then crscore else 0 end) sc_l,sum(case when threat_level=2 then crscore else 0 end)
sc_m,sum(case when threat_level=3 then crscore else 0 end) sc_h,sum(case when threat_level=4
then crscore else 0 end) sc_c  from grp_threat where  timestamp BETWEEN 1551397800 and
1551484199  and 1=1 AND ( ft_ipmask(dstip, 0, '91.189.0.0/16') )  AND srcintfrole  in
('lan','dmz','undefined')  group by timestamp1 ) b on a.timestamp1 = b.timestamp1;
 takes 30(ms), agggr:0(ms)

fortiview_request_data()-933: total:47 start:1551397800 end:1551484199
```

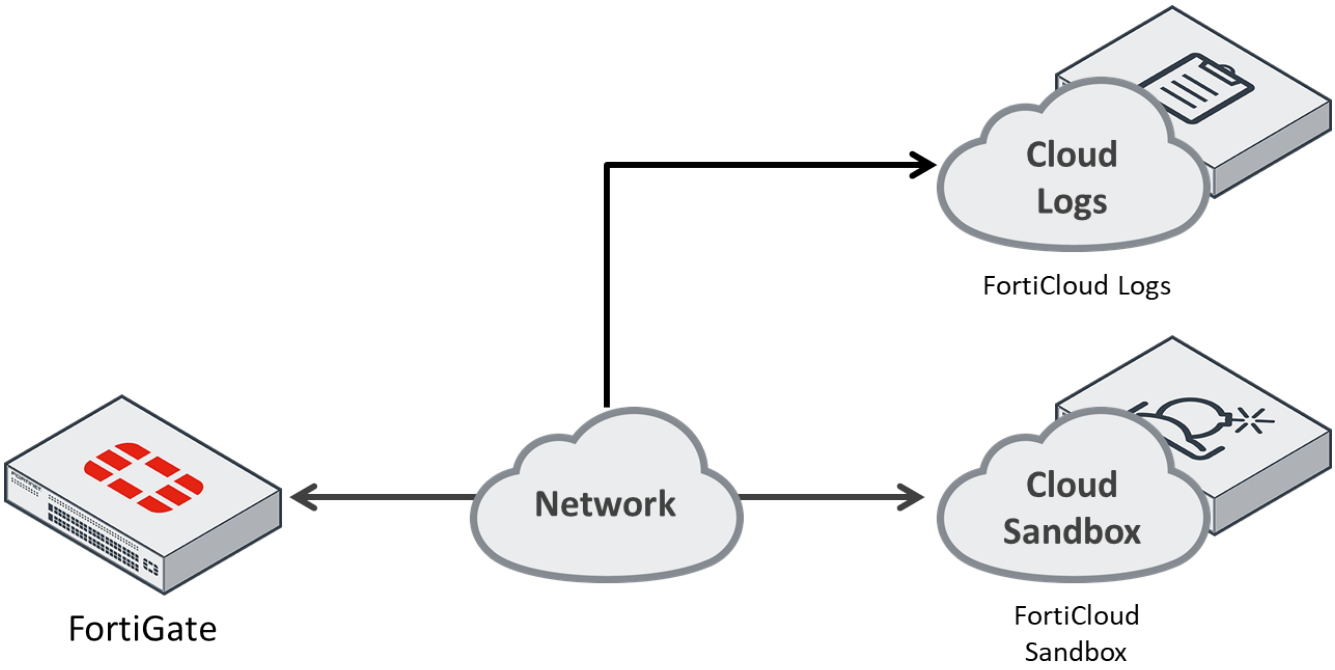
Compliance

This section lists the new features added to FortiOS for Compliance.

FortiSandbox Cloud Region Selection

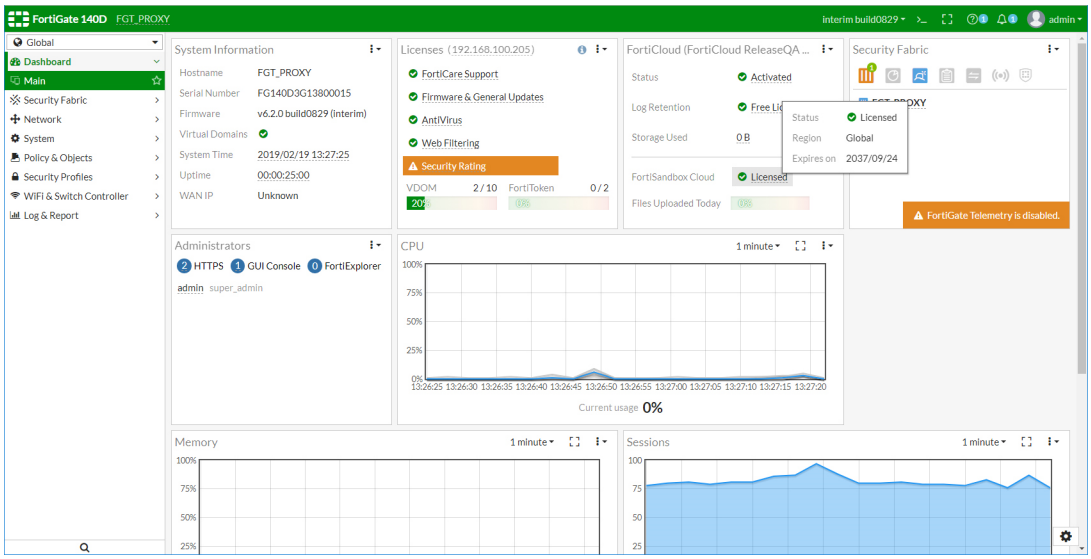
In FortiOS 6.2, FortiSandbox Cloud services, also referred to as FortiCloud Sandbox services, are decoupled from the FortiCloud license, allowing users to specify a FortiSandbox Cloud region as well as take advantage of FortiSandbox features without a FortiCloud account.

The topology below demonstrates how FortiCloud Logs and FortiSandbox Cloud are separated in FOS 6.2.

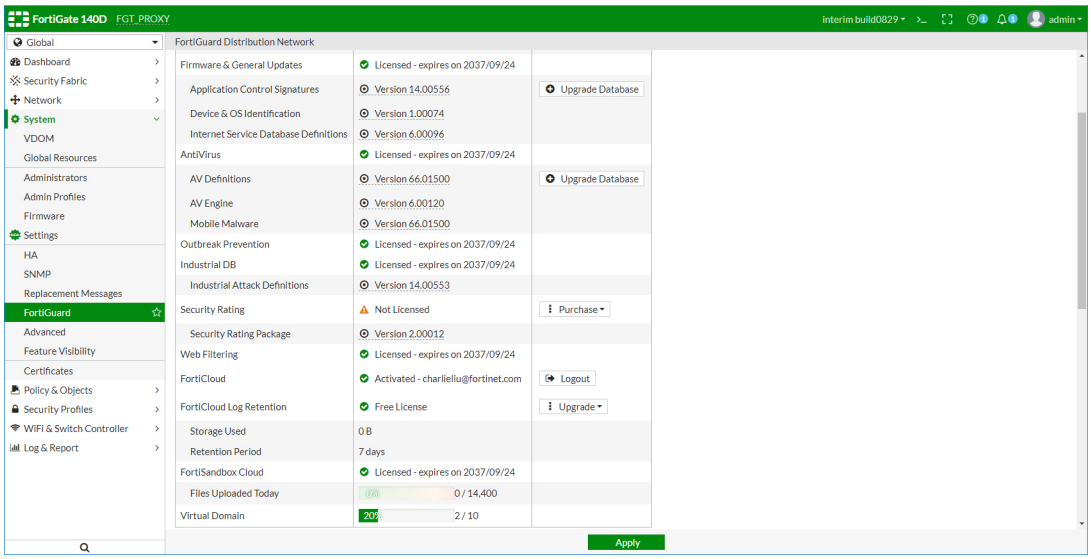


FortiCloud Log and Sandbox licenses shown in FortiOS

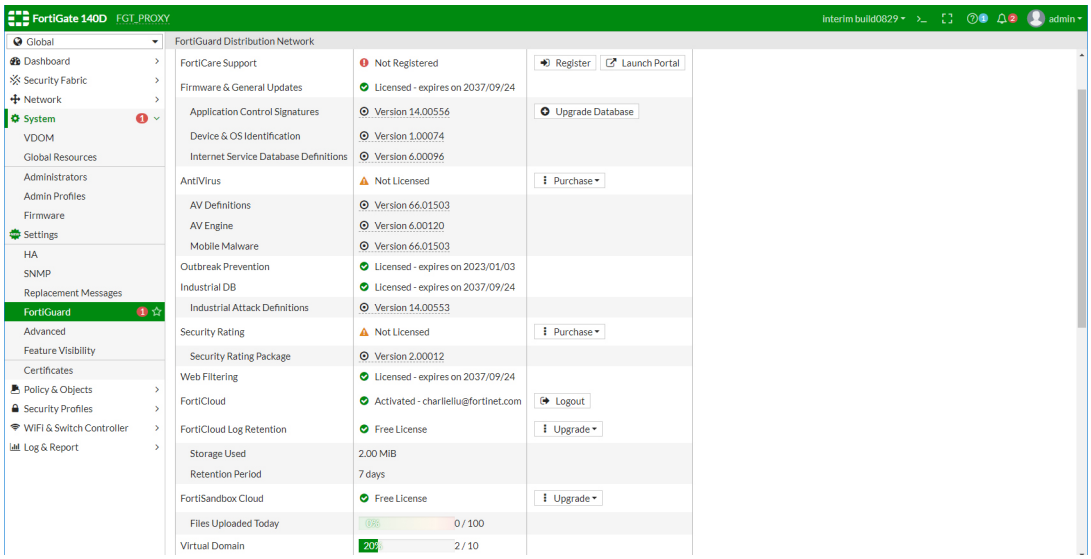
- FortiGate's *Main Dashboard* displays separated *FortiSandbox Cloud* and *FortiCloud Log* license statuses within the *FortiCloud* widget.
  In the example below, the FortiCloud account is using a free license while FortiSandbox Cloud is using a paid license.



- To obtain a FortiSandbox Cloud license, register the FortiGate with a paid *FortiGuard AntiVirus* license. As the FortiSandbox Cloud license is linked to the user's AntiVirus license, it will expire when the AntiVirus license expires.



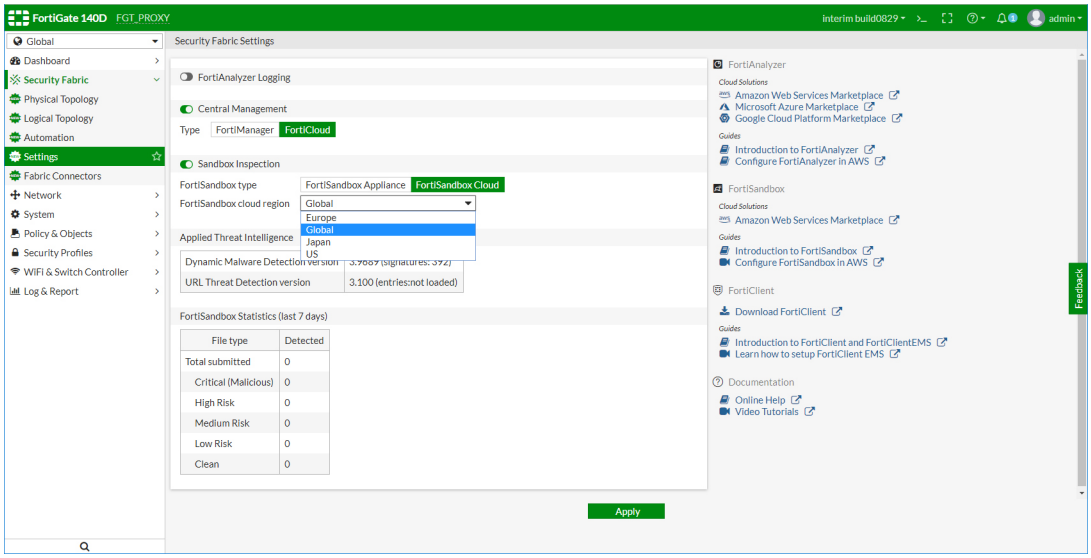
- If the FortiGate is not registered with a paid AntiVirus license, the FortiGate will use the free FortiCloud license. This license limits the FortiGate to 100 FortiSandbox Cloud submissions per day.



FortiSandbox Cloud region selection

To set the FortiSandbox Cloud region in the GUI:

1. Go to *Security Fabric* > *Settings*.
2. In the *Sandbox Inspection* section, select a region from the *FortiSandbox cloud region* dropdown. The following regions are available:
   - Europe
   - Global
   - Japan
   - US



3. Select *Apply*.

To set the FortiSandbox Cloud region in the CLI:

- In the FortiOS CLI, enter the command: `forticloud-sandbox region` and select a region.

```
FGT_PROXY (global) # exec forticloud-sandbox region
0  Europe
1  Global
2  Japan
3  US
Please select cloud sandbox region[0-3]:3
Cloud sandbox region is selected: US

FGT_PROXY (global) #
```

- The separation of the FortiCloud Log and Sandbox services can be seen in the example below:

```
FGT_PROXY (global) # diagnose test application forticldd 3
Debug zone info:
    Domain:FortiCloud ReleaseQA Global - 172.16.95.16
    Home log server: 172.16.95.93:514
    Alt log server: 172.16.95.27:514
    Active Server IP:      172.16.95.93
    Active Server status:  up
    Log quota:      102400MB
    Log used:       0MB
    Daily volume:   20480MB
    fams archive pause: 0
    APTContract : 1
    APT server: 172.16.102.52:514
    APT Altserver: 172.16.102.51:514
    Active APTServer IP:      172.16.102.52
    Active APTServer status:  up

FGT_PROXY (global) #
```

FortiGate-VM Unique Certificate

To safeguard against certificate compromise, FortiGate VM and FortiAnalyzer VM allow the same deployment model as FortiManager VM whereby the license file contains a unique certificate tied to the virtual device's serial number.

A hardware appliance usually comes with a BIOS certificate with a unify serial number that identifies the hardware appliance. This built-in BIOS certificate is different from a firmware certificate. A firmware certificate is distributed in all appliances with the same firmware version.

Using a BIOS certificate with a built-in serial number provides a high trust level for the other side in X.509 authentication.

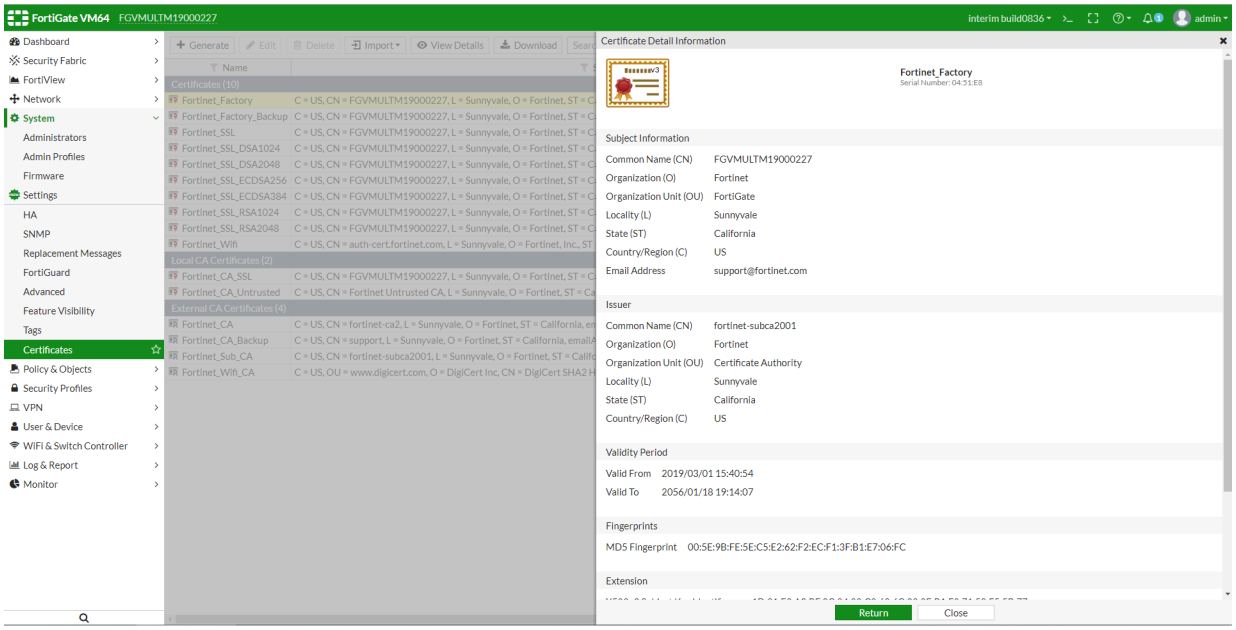
Since a VM appliance has no BIOS certificate, a signed VM license can provide an equivalent of a BIOS certificate. The VM license assigns a serial number in the BIOS equivalent certificate, which gives the certificate with an abstract access ability, i.e., the same as a BIOS certificate with the same high trust level.

Only new registered VM licenses support this feature.

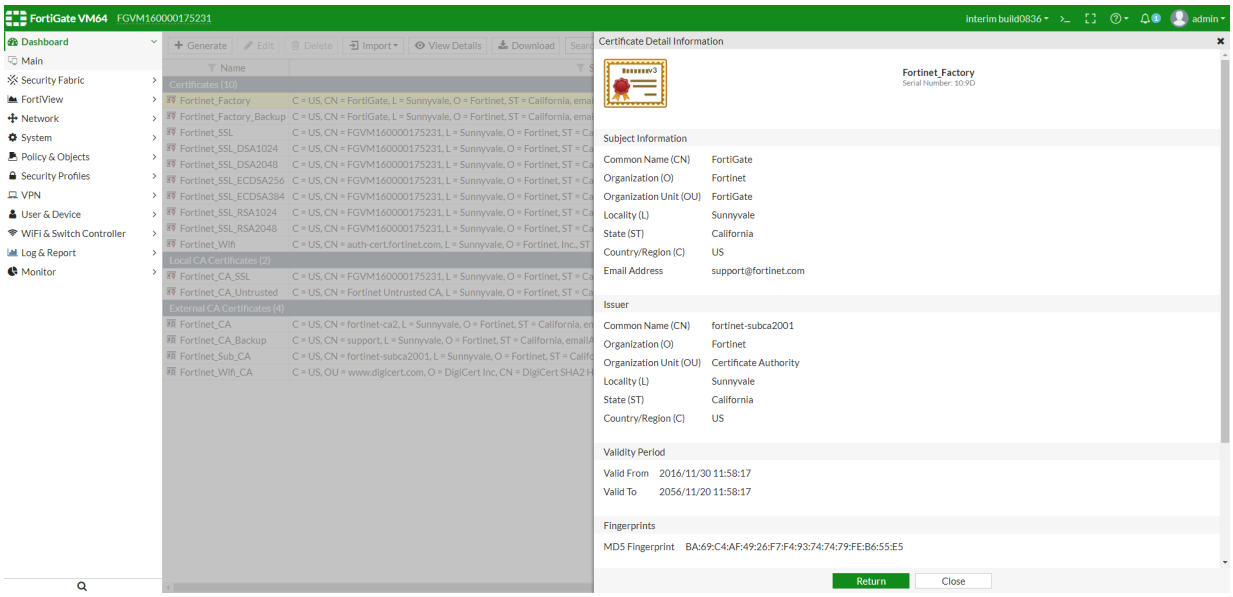
Sample configuration

Depending on the firmware version and VM license, check the following sample configurations.

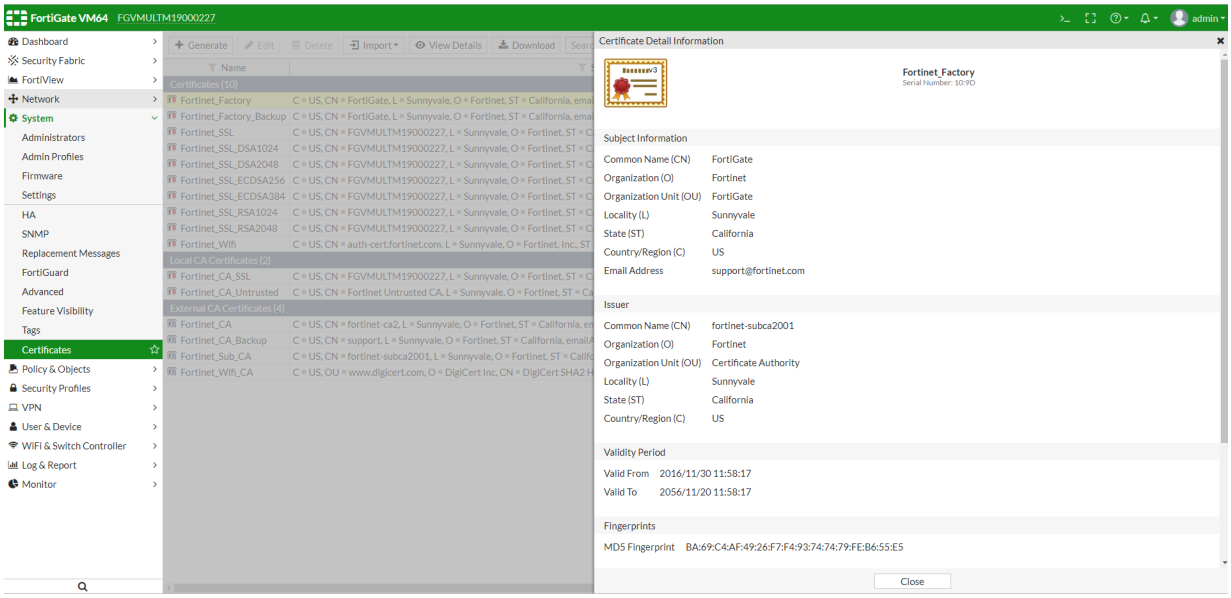
If you are using new firmware (v6.2.0 build0836) with a new VM license, verify VM license can be validated and the certificates `Fortinet_Factory` and `Fortinet_Factory_Backup` CN are changed to the FortiGate VM serial number.



If you are using new firmware (v6.2.0 build0836) with an old VM license, verify VM license can be validated and the certificates `Fortinet_Factory` and `Fortinet_Factory_Backup` CN are kept as `CN = FortiGate` and **not** changed to serial number.



UsiIf you are using old firmware (v6.0.2 build0231) with a new VM license, verify VM license can be validated and the certificates `Fortinet_Factory` and `Fortinet_Factory_Backup` CN are kept as `CN = FortiGate` and **not** changed to serial number.

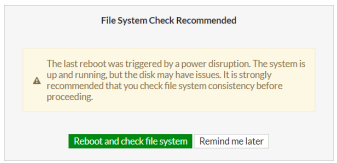


Run a File System Check Automatically

This feature adds the option to perform an automatic file system check if the FortiGate shuts down ungracefully.

By default, automatic file system check is disabled. When disabled, the next time an administrator logs in after an ungraceful shutdown, a warning message will advise them to manually run a file system check.

GUI warning:



CLI warning:

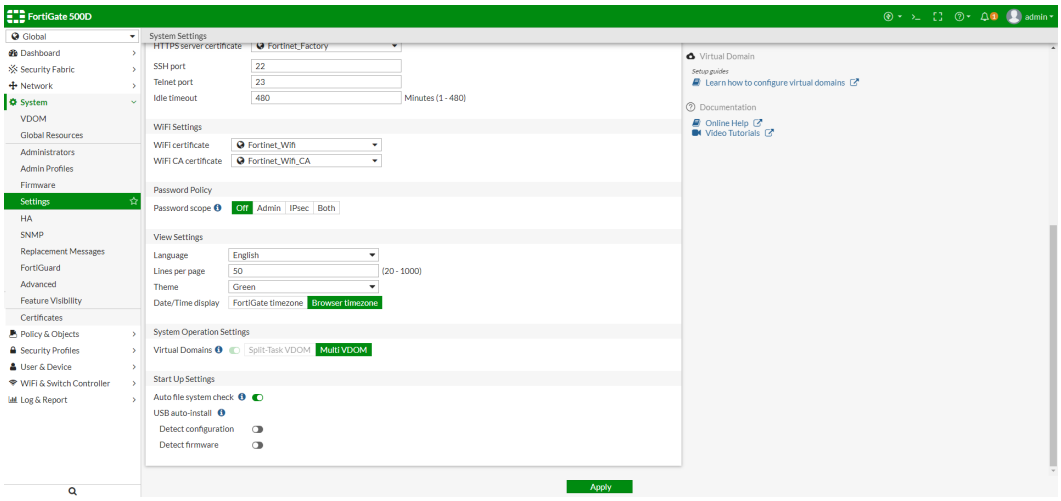
```
WARNING: File System Check Recommended! Unsafe reboot may have caused inconsistency in disk
drive.
It is strongly recommended that you check file system consistency before proceeding.
Please run 'execute disk scan 17'
Note: The device will reboot and scan during startup. This may take up to an hour
```

Enable automatic file system checks

Automatic file system checking can be enabled using both the GUI and the CLI.

To enable automatic file system checks in the GUI:

1. On the FortiGate, go to *System* > *Settings*.
2. In the *Start Up Settings* section, enable *Auto file system check*.



3. Click *Apply*.

To enable automatic file system checks using the CLI:

```
config system global
   set autorun-log-fsck enable
end
```

UX / Usability

This section lists the new features added to FortiOS for usability.

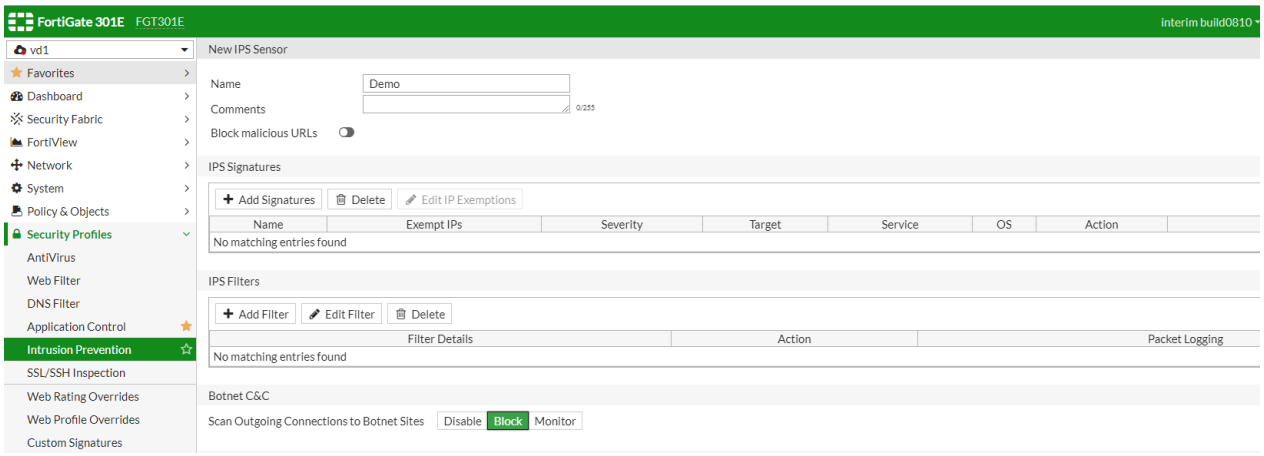
Move Botnet C&C into IPS Profile

Security Profiles > *Intrusion Prevention* has a new *Botnet C&C* option. This option consolidates multiple botnet options into a single option in the IPS Profile so that in one place, you can enable botnet blocking across all traffic that match the policy.

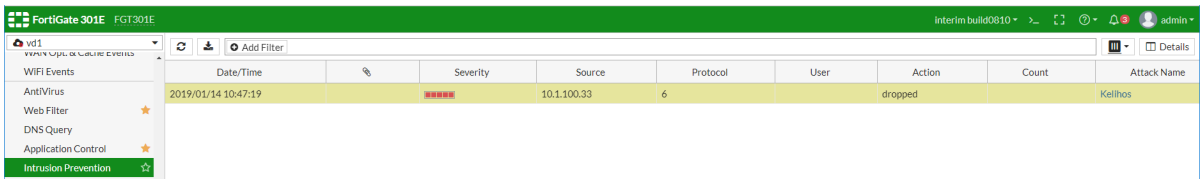
The new *Security Profiles* > *Intrusion Prevention* > *Botnet C&C* option replaces and enhances the old *Network Interfaces* > *Scan Outgoing Connections to Botnet Sites* option.

To configure Botnet C&C IP blocking using the GUI:

1. Go to *Security Profiles* > *Intrusion Prevention* and enable *Botnet C&C* by setting *Scan Outgoing Connections to Botnet Sites* to *Block* or *Monitor*.



2. Add the above sensor to the firewall policy and the IPS engine will start to scan outgoing connections to botnet sites.
   For example, visit a botnet IP and an IPS log is generated for this attack.



To configure Botnet C&C IP blocking using the CLI:

`config ips sensor` now has a new `scan-botnet-connections` option.

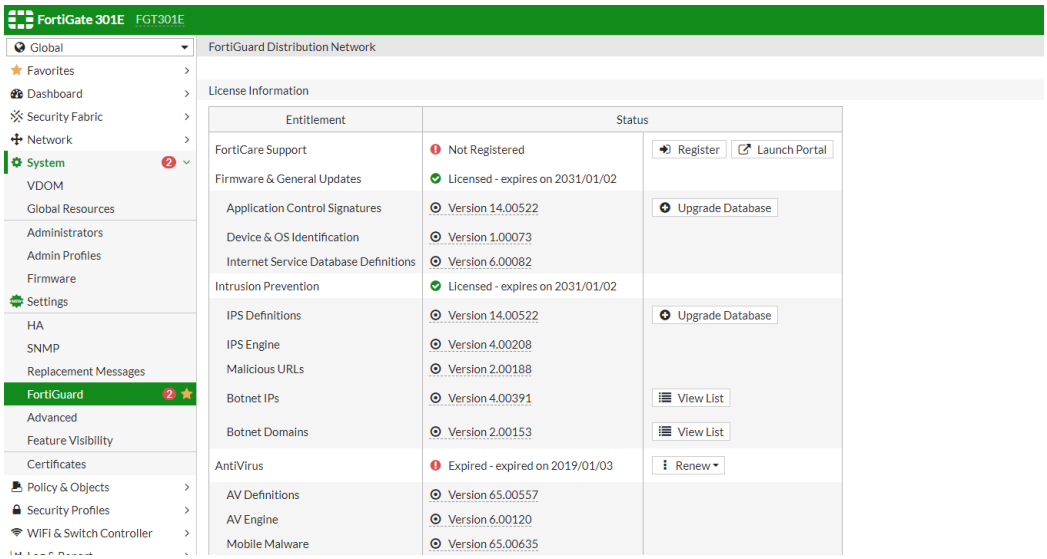
```
config ips sensor
   edit "Demo"
      set scan-botnet-connections <disable | block | monitor>
   next
end
```

The `scan-botnet-connections` option is no longer available in the following CLI commands:

- `config firewall policy`
- `config firewall interface-policy`
- `config firewall proxy-policy`
- `config firewall sniffer`

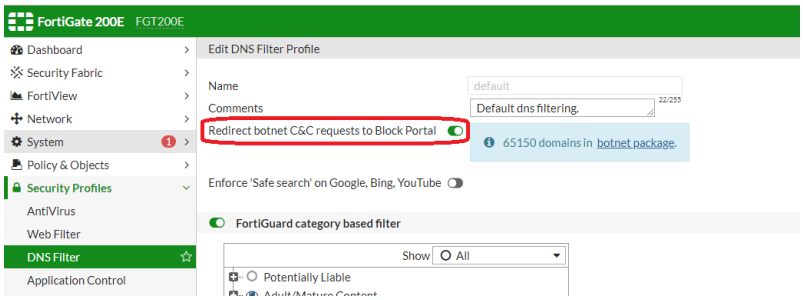
Botnet IPs and Botnet Domains moved to Intrusion Prevention section

In *System* > *FortiGuard* , *Botnet IPs* and *Botnet Domains* are now in the *Intrusion Prevention* section.



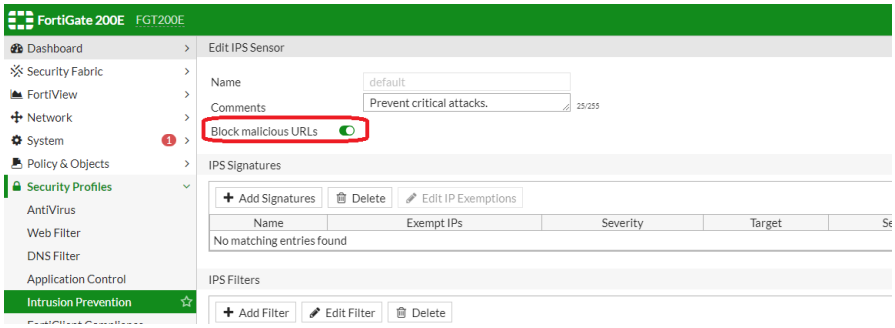
Botnet C&C Domain Blocking

There are no changes from version 6.0.4 in configuring *Security Profiles* > *DNS Filter* > *Redirect botnet C&C requests to Block Portal*. Add the profile to a firewall policy to block connections to Botnet domains.



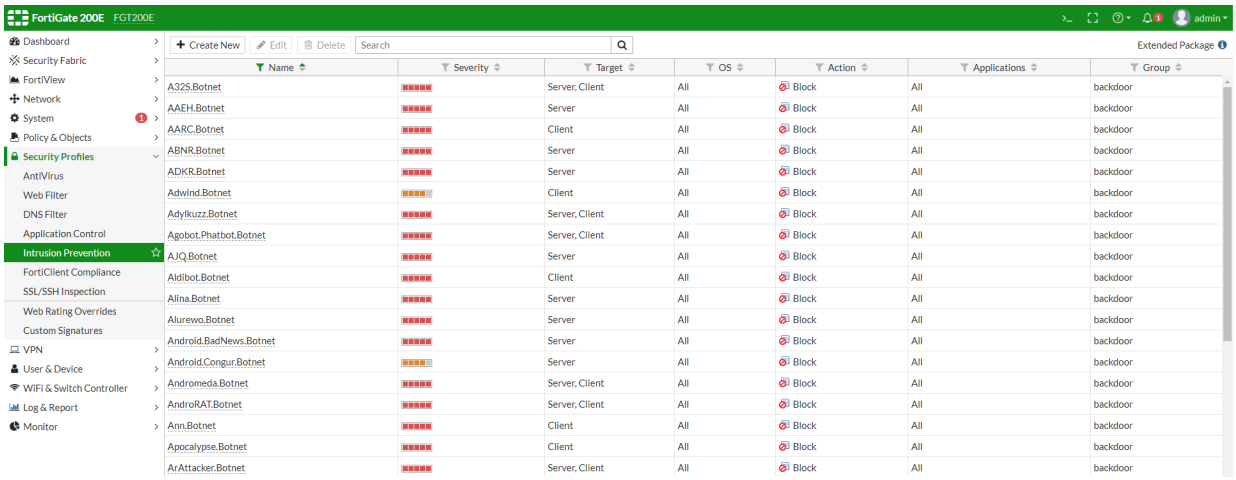
Botnet C&C URL Blocking

There are no changes from version 6.0.4 in configuring *Security Profiles* > *Intrusion Prevention* > *Block malicious URLs*. Enable *Block malicious URLs* in IPS Sensor and then add the sensor to a firewall policy.



Botnet C&C Signature Blocking

In this version and version 6.0.4, there are IPS signatures for botnet attacks. Include these signatures in IPS Sensor and then add the sensor to a firewall policy to detect or block attacks matching the IPS signatures.

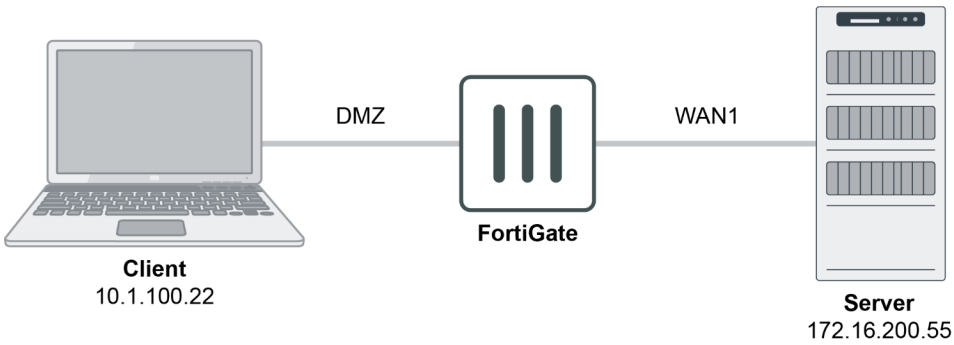


Logging - Session versus Attack Direction

IPS logs have been updated to record source and destination information based on session direction instead of attack direction. This update allows for better alignment between IPS and traffic logs, as traffic logs also record source and destination information based on session direction. FortiOS can use this information to present a more accurate summary and drill-down path.

IPS logs also include a new `direction` field to indicate attack direction when applicable.

The following scenarios show examples of traffic and IPS logs for server-side and client-side attacks. Both scenarios use the topology illustrated below. The session direction is from the client to the server.



In both scenarios, note that both the traffic and IPS log record the source and destination IP addresses using the session direction, treating the client as the source and the server as the destination. The source fields (`srcip`, `srcport`, and `srcintf`) use client data. The destination fields (`dstip`, `dstport`, and `dstinf`) use server data. The IPS log examples also include the `direction` field to show the attack direction.

Server-side attack traffic and IPS logs

In this scenario, the client attempts to download malware from the server. The attack direction therefore is incoming (from the server to the client). The table below shows the traffic and IPS logs for this scenario:

Traffic log	IPS log
date=2018-12-29 time=14:50:47 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="vdom1" eventtime=1540849847 **srcip=10.1.100.22 srcport=46552 srcintf="dmz"** srcintfrole="lan" **dstip=172.16.200.55 dstport=80 dstintf="wan1"** dstintfrole="wan" poluuid="c939f294-d6ff-51e8-3988-c628cfa2a346" sessionid=2979 proto=6 action="server-rst" policyid=1 policytype="policy" service="HTTP" dstcountry="Reserved" srccountry="Reserved" trandisp="snat" transip=172.16.200.6 transport=46552 duration=0 sentbyte=296 rcvdbyte=152 sentpkt=4 rcvdpkt=3 appcat="unscanned" utmaction="reset" countips=1 devtype="Linux PC" devcategory="None" osname="Linux" osversion="Debian" mastersrcmac="00:0c:29:6c:43:21" srcmac="00:0c:29:6c:43:21" srcserver=0 utmref=65522-42	date=2018-12-29 time=14:50:47 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" vd="vdom1" eventtime=1540849847 severity="info" **srcip=10.1.100.22** srccountry="Reserved" **dstip=172.16.200.55 srcintf="dmz"** srcintfrole="lan" **dstintf="wan1"** dstintfrole="wan" sessionid=2979 action="reset" proto=6 service="HTTP" policyid=1 attack="Virus.File" **srcport=46552 dstport=80** hostname="172.16.200.55" url="/virus/example.com" **direction="incoming"** attackid=29844 profile="ips-test" ref="http://www.fortinet.com/ids/VID29844" incidentserialno=122164746 msg="file_ transfer: Virus.File,"

Client-side attack traffic and IPS logs

In this scenario, the client attempts to post malware to the server. The attack direction therefore is outgoing (from the client to the server). The table below shows the traffic and IPS logs for this scenario:

Traffic log	IPS log
date=2018-12-29 time=15:30:25 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="vdom1" eventtime=1540852225 **srcip=10.1.100.22 srcport=53330 srcintf="dmz"** srcintfrole="lan" **dstip=172.16.200.55 dstport=80 dstintf="wan1"** dstintfrole="wan" poluuid="c939f294-d6ff-51e8-3988-c628cfa2a346" sessionid=4205 proto=6 action="server-rst" policyid=1 policytype="policy" service="HTTP" dstcountry="Reserved" srccountry="Reserved" trandisp="snat" transip=172.16.200.6 transport=53330 duration=0 sentbyte=692 rcvdbyte=318 sentpkt=6 rcvdpkt=5 appcat="unscanned" utmaction="reset" countips=1 devtype="Linux PC" devcategory="None" osname="Linux" osversion="Debian" mastersrcmac="00:0c:29:6c:43:21" srcmac="00:0c:29:6c:43:21" srcserver=0 utmref=65522-96	date=2018-12-29 time=15:30:25 logid="0419016384" type="utm" subtype="ips" eventtype="signature" level="alert" vd="vdom1" eventtime=1540852225 severity="info" **srcip=10.1.100.22** srccountry="Reserved" **dstip=172.16.200.55 srcintf="dmz"** srcintfrole="lan" **dstintf="wan1"** dstintfrole="wan" sessionid=4205 action="reset" proto=6 service="HTTP" policyid=1 attack="Virus.File" **srcport=53330dstport=80** hostname="172.16.200.55" url="/cgi-bin/upload.py?root" **direction="outgoing"** attackid=29844 profile="ips-test" ref="http://www.fortinet.com/ids/VID29844" incidentserialno=2111356281 msg="file_ transfer: Virus.File,"

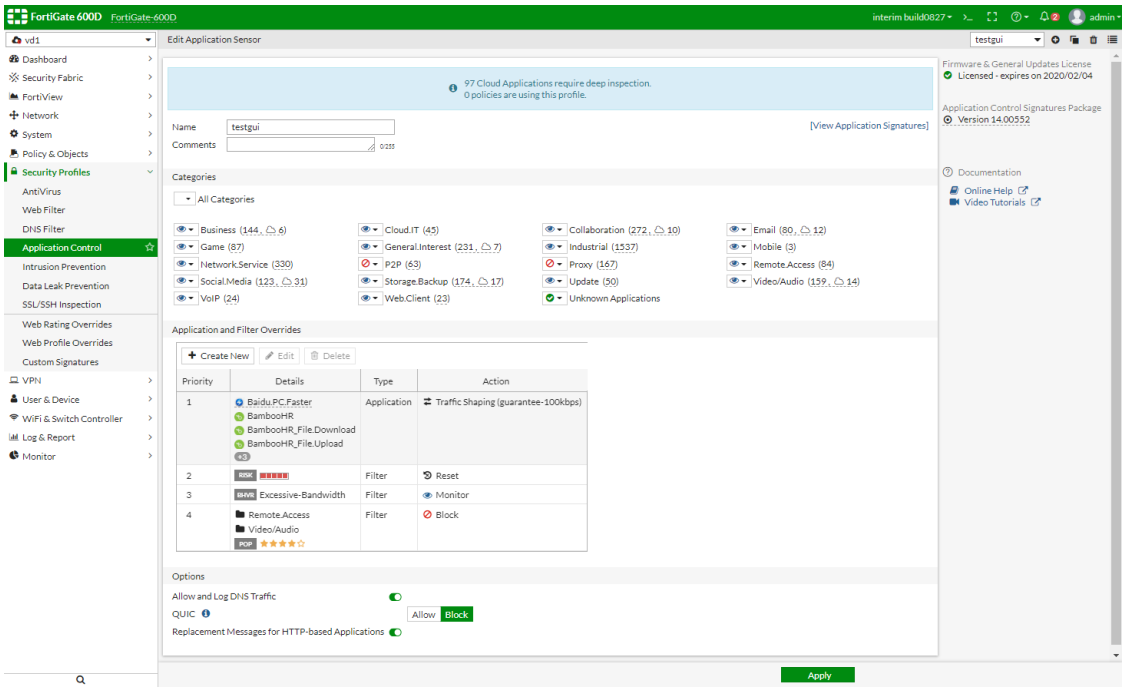
Application Control Profile GUI Improvements

This version adds multiple GUI enhancements to the Application Control Profile including:

- A right-sided pane in the sensor page to display FortiGuard help links.
- Individual application overrides and filter overrides tables are combined into one override table. The two types are combined when adding a new override.
- Override entries in the table display sequence numbers and can be reordered by dragging and dropping.

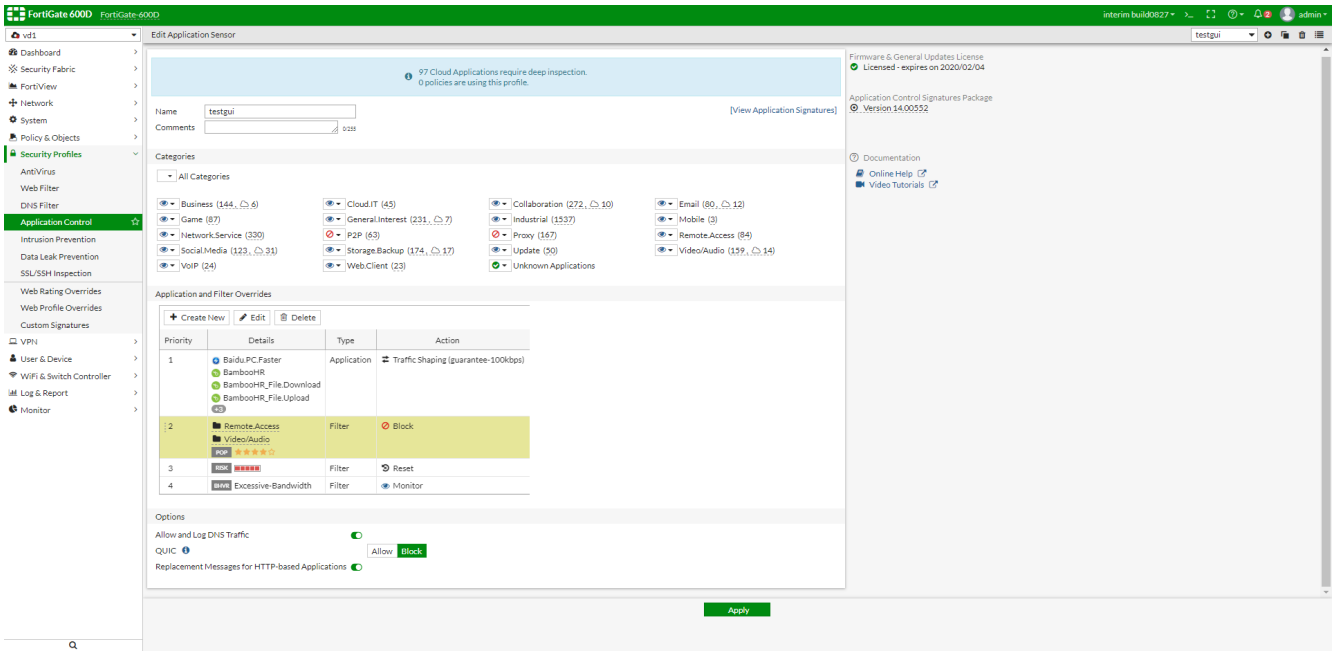
Specific application overrides and filter overrides tables are combined into one override table, where signature and filter entries are mixed together. A right-sided gutter has been added to sensor page to display FortiGuard help links.

For specific applications, parent/child application structures are removed.



Override entries in the table display sequence numbers that can be reordered by dragging and dropping.

Entries in the *Application and Filter Overrides* table can be reordered by dragging the priority number to the desired position. The priority number and the selected entries are reordered.



In the *Application and Filter Overrides* section, the pane to add and edit overrides entries has two tabs: *Application* and *Filter*.

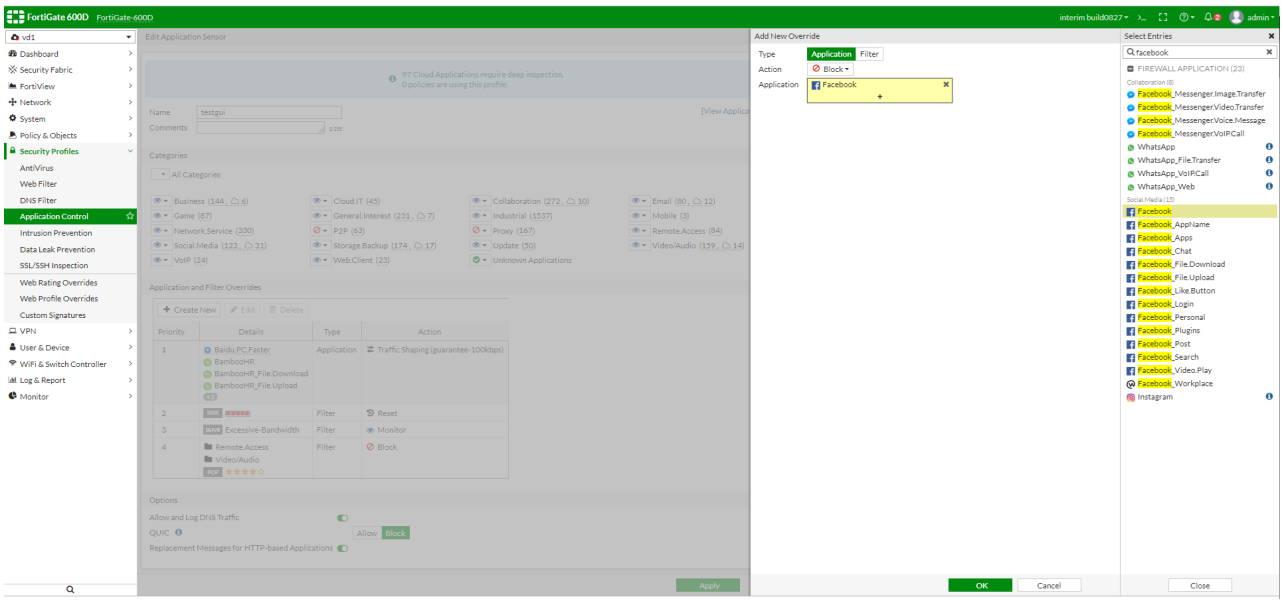
For each entry in the override table, you can only configure one type: for *Application* or *Filter* option.

Type	Select *Application* for application override. Select *Filter* for filter override.
Action	No change from previous version. Can be set to *Monitor/Allow/Block/Quarantine*.
Application	Available if you select *Application Type*. Use the pane to add one or more application signatures for an entry. Use the search box to filter signatures.
Filter	Available if you select *Filter Type*. You can select filters by behavior/application category/technology/popularity/protocol/risk/vendor subtypes. Filters can be accumulated to filter a set of signatures that match all selected filters. The Search box can be use to find if input signature is included in selected filters, where matched applications are shown at the bottom.

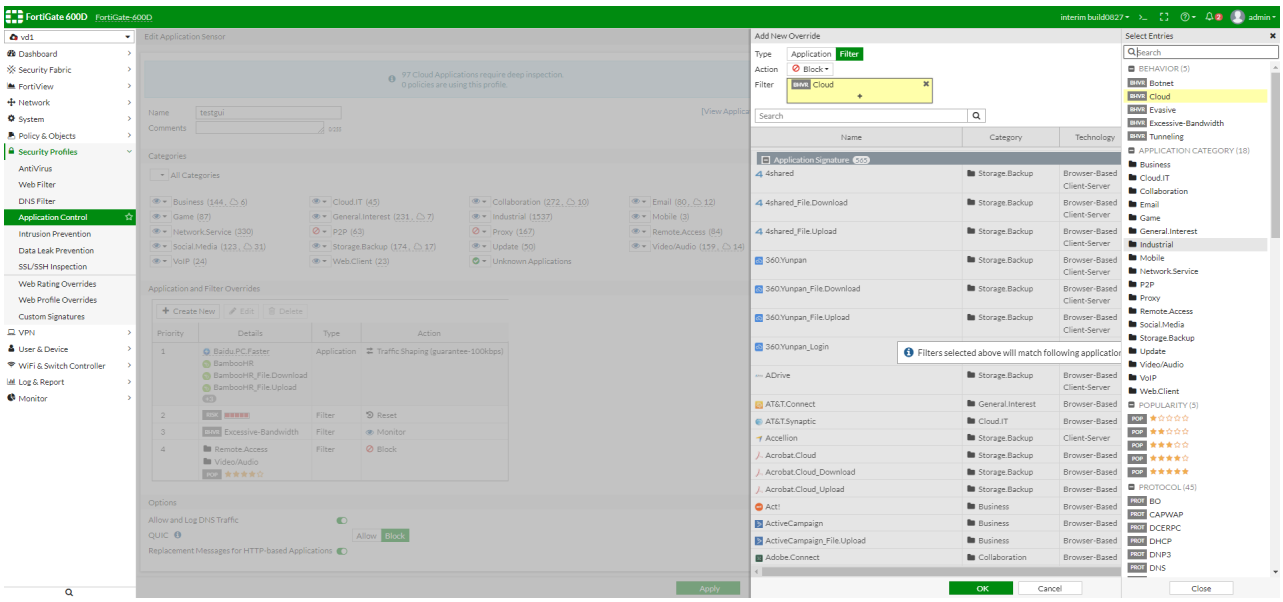
To create a new Application Control Profile with the Application Type:

1. In *Security Profiles* > *Application Control* in the *Application and Filter Overrides* section, click *Create New*.
2. For *Type*, select *Application*. For *Action*, select *Block*.
3. For *Application*, click **+**.
   All application signatures are listed.

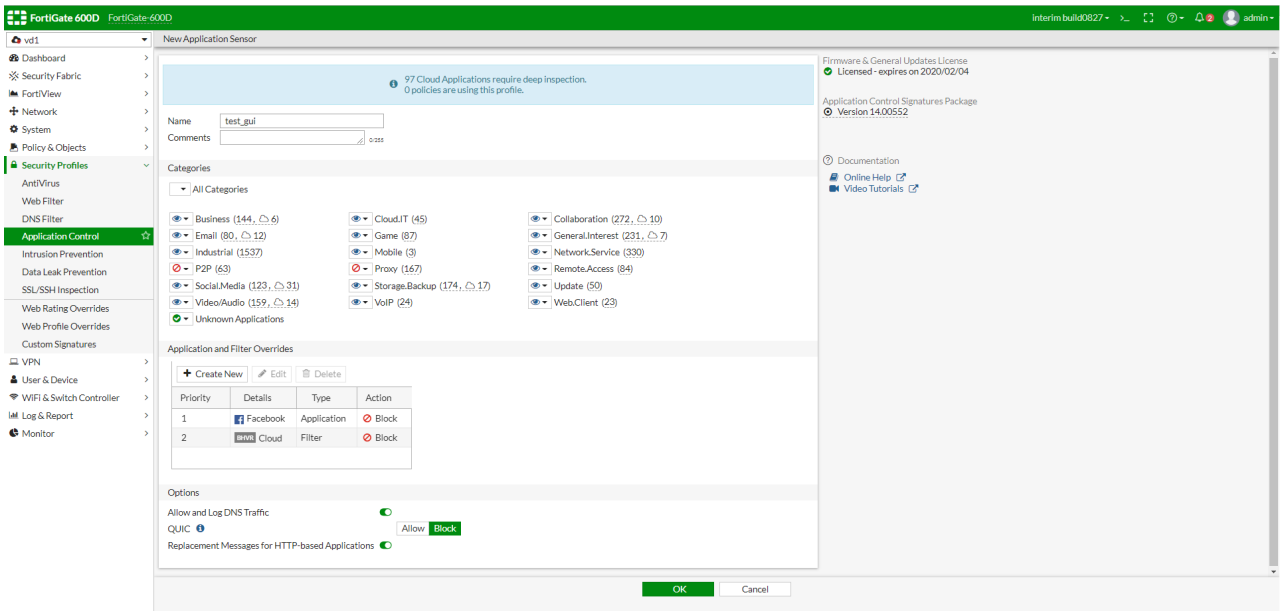
4. In the Search box, enter *Facebook* and select *Facebook*.



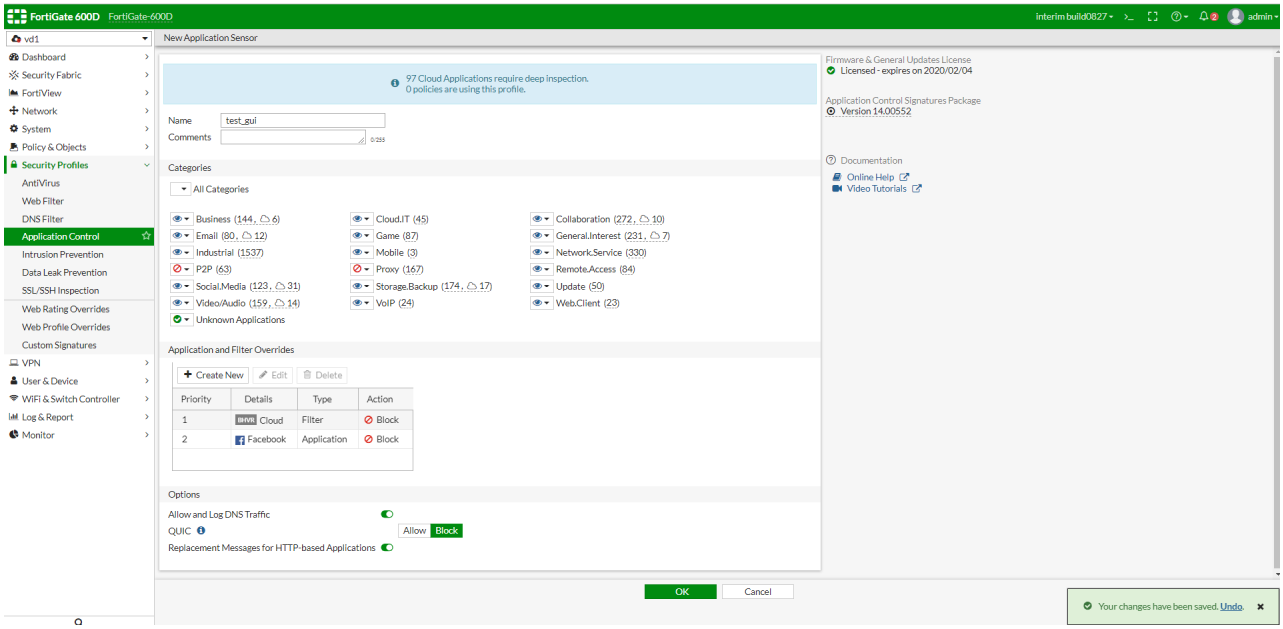
5. Click *OK* to apply this entry.
6. Click *Create New* to create another entry.
7. For *Type*, select *Filter*. For *Action*, select *Block*.
8. For *Filter*, click **+**.
9. In the *Select Entries* list under *BEHAVIOR*, select *Cloud*.
   All matching signatures are listed.



10. Click *OK* to apply this entry.
    The *Application and Filter Overrides* section shows two entries.



11. Drag the second entry to the top, and click *OK* to save this profile.



Authentication Policy Extensions

In 6.0, if you defined an authentication policy for specific traffic, then you might need to exclude the destination from the default *implicit policy*, otherwise, the implicit rule might allow unauthenticated users go to through. This new option forces the authentication to take precedence over subsequent rules without having to create additional policies.

By default, unauthenticated traffic is permitted to fall through to the next policy. FortiGate only forces unauthenticated users to authenticate against the authentication policy when there are no other matching policies. In this version, administrators can force the authentication to always take place.

To set authentication requirement:

```
config user setting

    set auth-on-demand <always|implicitly>

end
```

`always`	Always trigger firewall authentication on demand.
`implicitly` (default)	Implicitly trigger firewall authentication on demand. This is the default setting and the original behavior.

You can only use CLI to configure this feature. See the following example.

```
config user setting
    set auth-on-demand always
end


config firewall policy
    edit 1
        set name "QA to Database"
        set srcintf "port10"
        set dstintf "port9"
        set srcaddr "QA_subnet"
        set dstaddr "Database"
        set action accept
        set schedule "always"
        set service "ALL"
        set fsso disable
        set groups "qa_group"
        set nat enable
    next
    edit 2
        set name "QA to Internet"
        set srcintf "port10"
        set dstintf "port9"
        set srcaddr "QA_subnet"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set fsso disable
        set nat enable
    next
end
```

Workspace Mode

This feature adds a workspace mode to FortiOS, allowing administrators to make a batch of changes that are not implemented until the transaction is committed. Prior to committing, the changes can be reverted or edited as needed without impacting current operations.

When an object is edited in workspace mode it is locked, preventing other administrators from editing that object. A warning message will be shown to let the administrator know that the object is currently being configured in another transaction.

All administrators can use workspace mode; their permissions in workspace mode are the same as defined in their account profile.

A workspace mode transaction times out in five minutes if there is no activity. When a transaction times out, all changes are discarded. A warning message will be shown to let the administrator know that a timeout is imminent, or has already happened:

```
config transaction id=1 will expire in 30 seconds
config transaction id=1 will expire in 20 seconds
config transaction id=1 will expire in 10 seconds
config transaction id=1 has expired
```

The following configurations are not changeable in a workspace transaction:

```
system.console
system.resource-limits
system.elbc
config system global
   set split-port
   set vdom-admin
   set management-vdom
   set wireless-mode
   set internal-switch-mode
end
config system settings
   set opmode
end
system.npu
system.np6
config system wireless
   set mode
end
system.vdom-property
system.storage
```

The `execute batch` command cannot be used in or to start workspace mode.

To use workspace mode:

1. Start workspace mode:
   ```
   execute config-transaction
   ```
   Once in workspace mode, the administrator can make configuration changes, all of which are made in a local CLI process that is not viewable by other processes.
2. Commit configuration changes:
   ```
   execute config-transaction commit
   ```
   After performing the commit, the changes are available for all other processes, and are also made in the kernel.
3. Abort configuration changes:
   ```
   execute config-transaction abort
   ```
   If changes are aborted, no changes are made to the current configuration or the kernel.

Diagnose commands

```
diagnose sys config-transaction show txn-meta
```

Show config transaction meta information. For example:

```
# diagnose sys config-transaction show txn-meta
txn_next_id=8, txn_nr=2
```

```
diagnose sys config-transaction show txn-info
```

Show config transaction information. For example:

```
# diagnose sys config-transaction show txn-info
current_jiffies=680372

txn_id=6, expire_jiffies=706104, clicmd_fpath='/dev/cmdb/txn/6_EiLl9G.conf'
txn_id=7, expire_jiffies=707427, clicmd_fpath='/dev/cmdb/txn/7_UXK6wY.conf'
```

```
diagnose sys config-transaction show txn-entity
```

Show config transaction entity. For example:

```
# diagnose sys config-transaction show txn-entity
vd='global', cli-node-oid=37(system.vdom), txn_id=7. location: fileid=0, storeid=0,
     pgnr=0, pgidx=0
vd='global', cli-node-oid=46(system.interface), txn_id=7. location: fileid=3, storeid=0,
     pgnr=0, pgidx=0
```

```
diagnose sys config-transaction show txn-lock
```

Show transaction lock status. For example:

```
# diagnose sys config-transaction show txn-lock
type=-1, refcnt=0, value=256, pid=128
```

```
diagnose sys config-transaction status
```

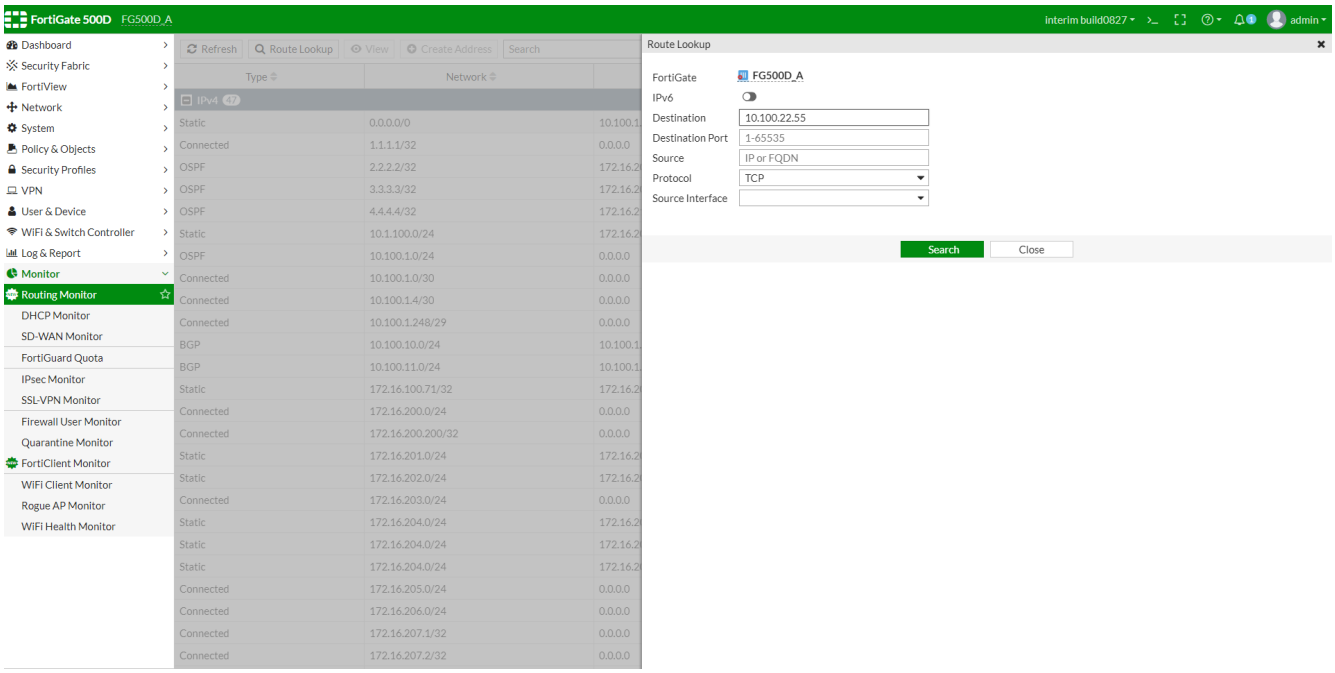
Show the transaction status in the current CLI.

Extend Policy/Route Check to Policy Routing

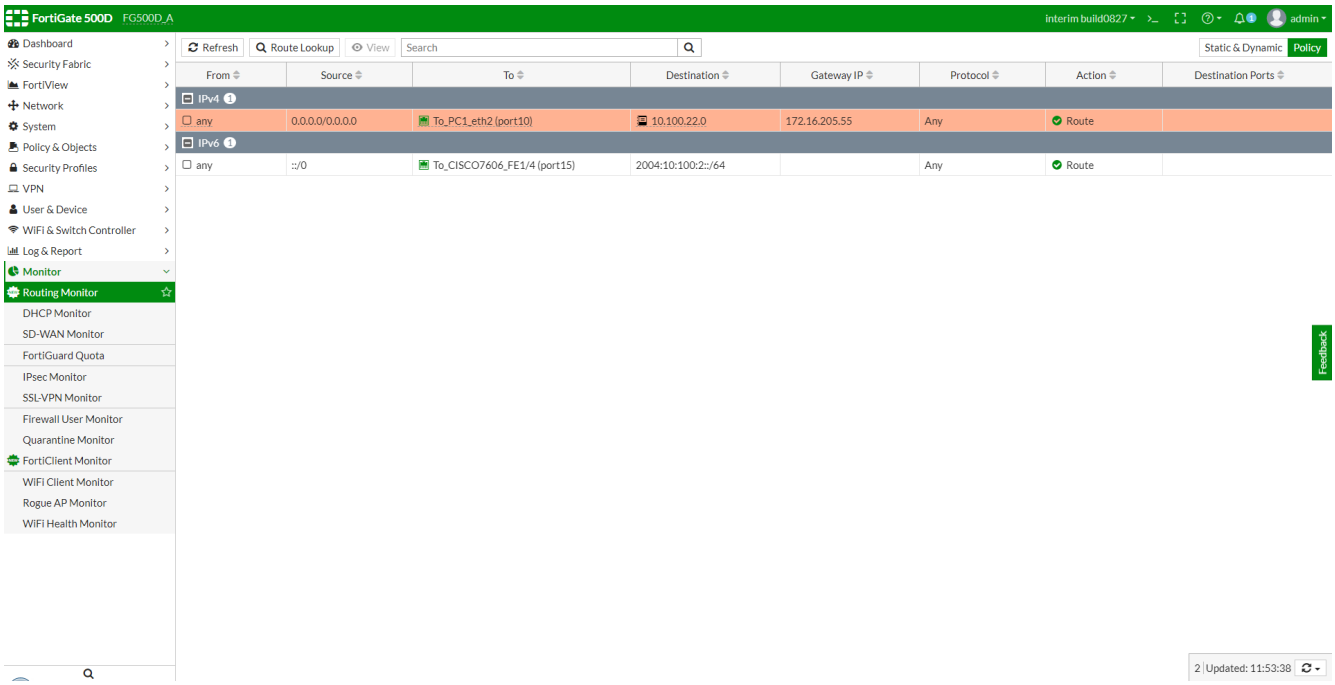
The existing Policy Check and Route Check features in FortiOS 6.0 exclude checking against the Policy Routing engine. In 6.2, this is added, and new options are available in the GUI to support further testing scenarios.

This version adds policy route look up support and prioritizes it over static/dynamic (normal) routes when doing route lookup in the GUI.

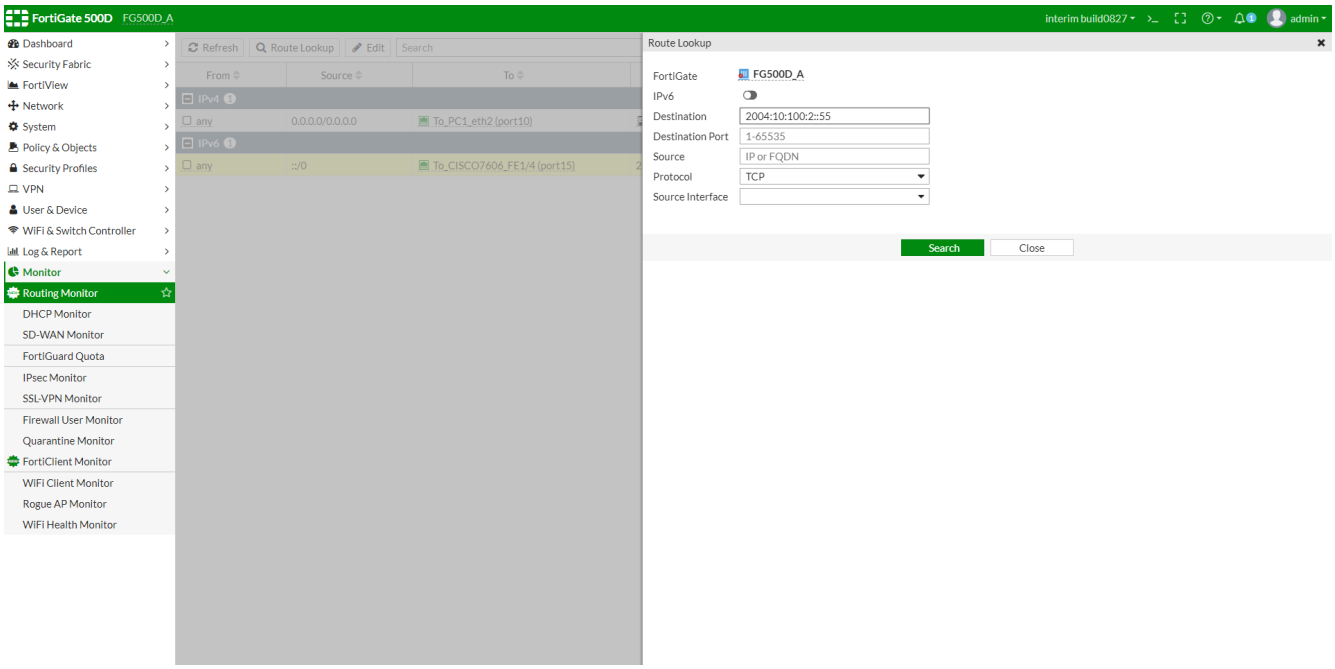
In *Monitor* > *Routing Monitor*, click *Route Lookup* to look up an address. If it matches the policy route first, the policy route is highlighted.



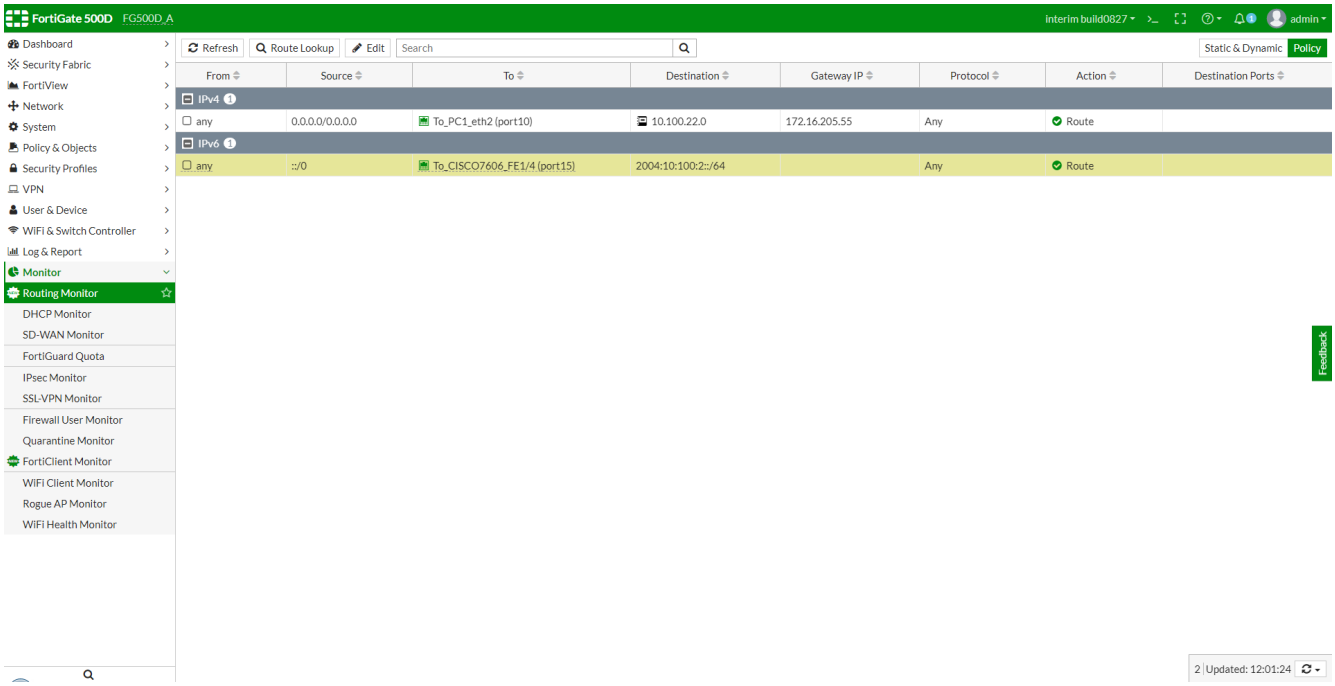
The result of the matching policy route is highlighted in the *Route Monitor* page. Below is an example of IPv4 lookup.



Below is an example of IPv6 lookup.



The result of the matching IPv6 policy route is highlighted in the *Route Monitor* page.



IPv4 policy route match CLI command:

```
diag ip proute match <IPv6 destination address> <IPv6 source address> <interface name>
      <protocol> <destination port>

proute                                  IPv6 policy routing.
match                                   Match IPv6 route to policy routes.
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx  IPv6 destination address.
```

```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx   IPv6 source address.
intf-name                                 Interface Name.
<1-255>                                   Protocol.
<0-65535>                                 Destination port.
```

IPv6 policy route match CLI command:

```
diag ipv6 proute match <destination ip addres> <source ip address> <interface name> <protocol>
     <destination port>
```

```
proute              Policy routing.
match               Match policy route
XXX.XXX.XXX.XXX     Destination IP address.
XXX.XXX.XXX.XXX     Source IP address.
intf-name           Interface Name.
<1-255>             Protocol.
<0-65535>           Destination port.
```

To configure IP policy route match using the CLI — example 1:

```
FGT (root) # diagnose ip proute match 10.100.21.44 2.2.2.2 port2 6 2
dst=10.100.21.44 src=2.2.2.2 iif=24 protocol=6 dport=2
id=7f00000c type=VWL
seq-num=12
```

To configure IP policy route match using the CLI — example 2:

```
FGT (root) # diagnose ip proute match 10.100.20.44 2.2.2.2 port2 6 2
dst=10.100.20.44 src=2.2.2.2 iif=24 protocol=6 dport=2
id=00000016 type=Policy Route
seq-num=22
```

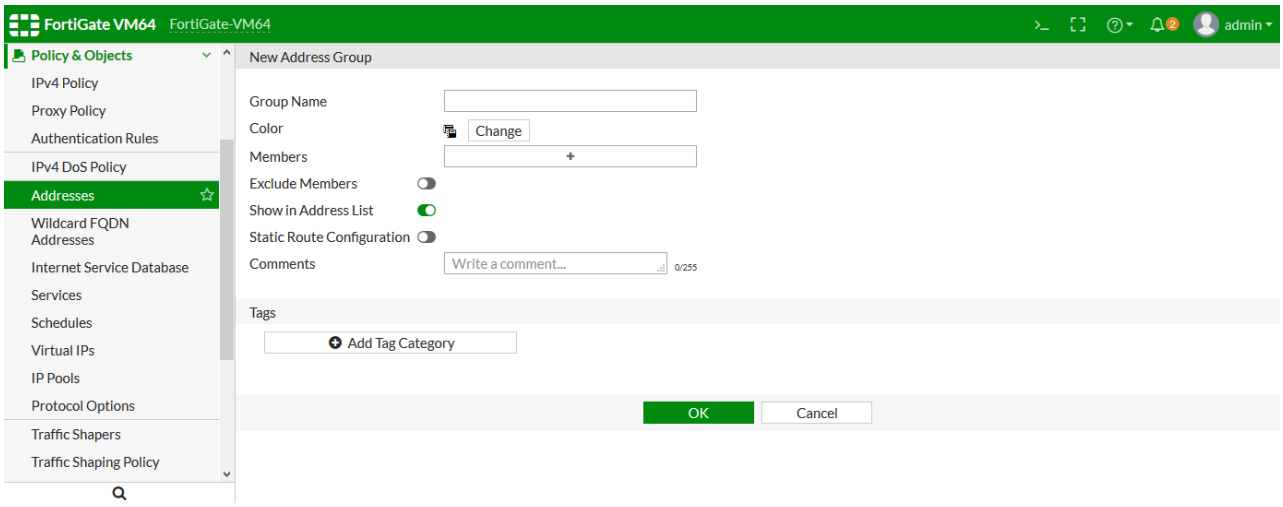
Address Group - Exclusions

This feature introduces the *Exclude Members* setting in IPv4 address groups. The specified IP addresses or ranges are subtracted from the address group.

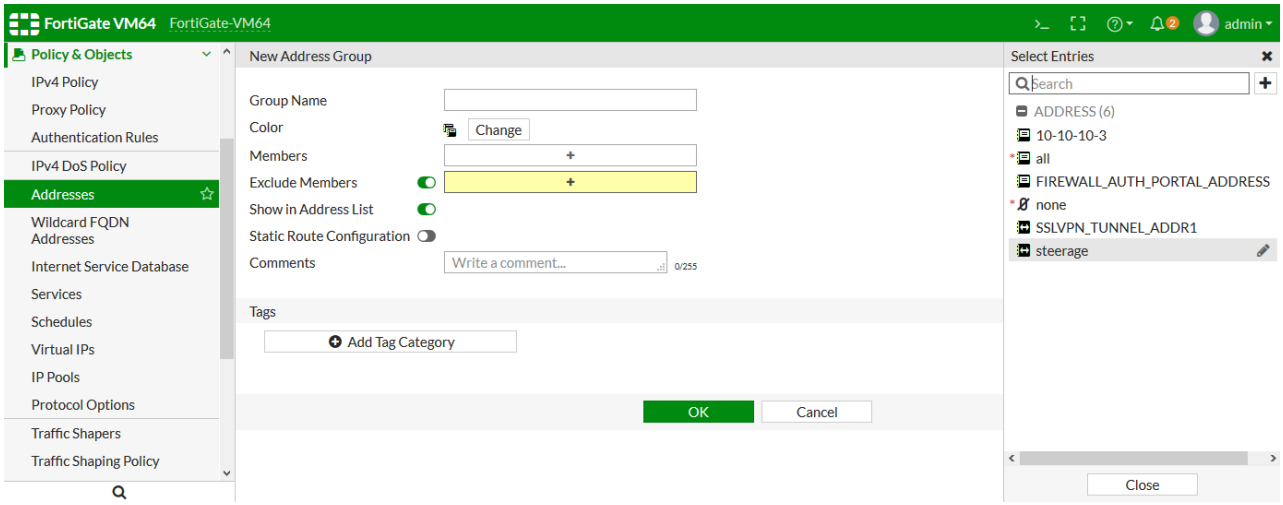
This feature is only supported for IPv4 address groups, and only for addresses with a *Type* of *IP Range* or *Subnet*.

To exclude an address or addresses from an address group using the GUI:

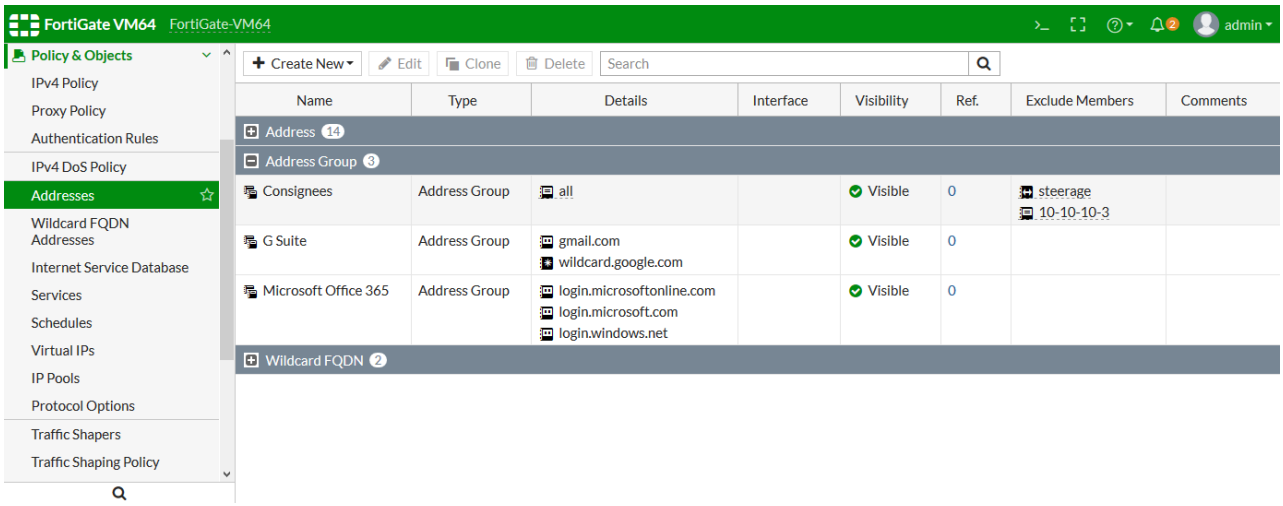
1. Go to *Policy & Objects* > *Addresses*.
2. Create a new address group, or edit an existing group.



3. Enable Exclude Members, and select the addresses that will be excluded from the group.



4. Click OK.
   The excluded members are listed in the Exclude Member column.



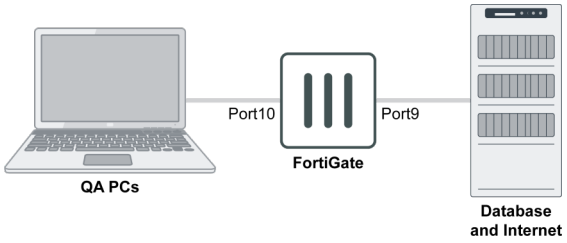
To exclude an address or addresses from an address group using CLI commands:

```
config firewall addrgrp
   edit <address group>
      set exclude enable
      set exclude-member <address> <address> ... <address>
   next
end
```

Traffic Shaping GUI Update

This feature adds GUI support for interface based traffic shaping.

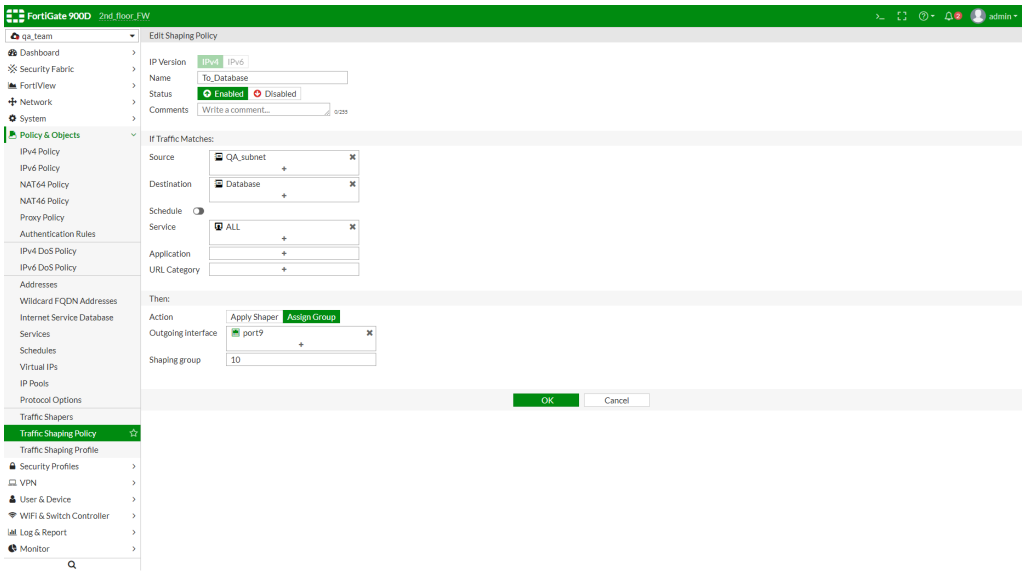
Example



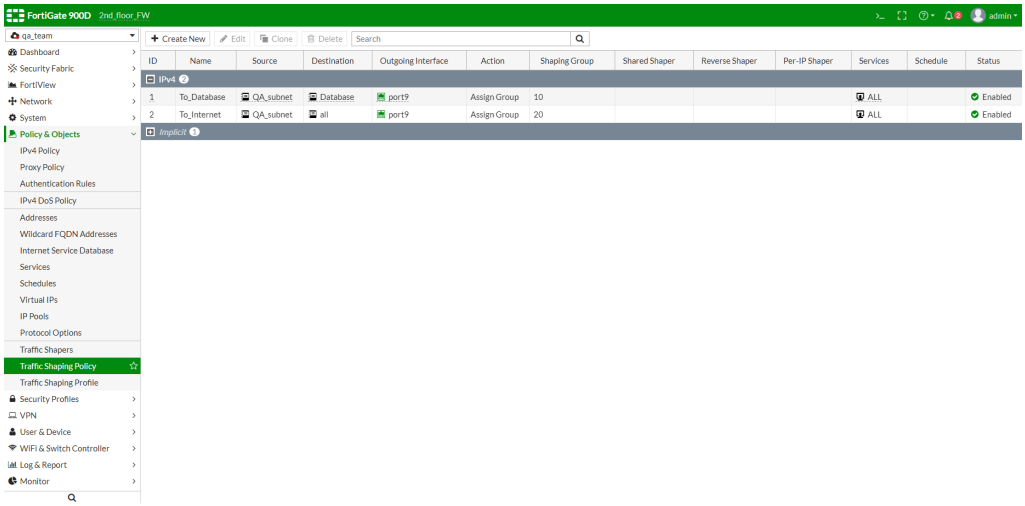
In this example, QA traffic to the database is put into shaping group 10 and is guaranteed to have 60% of the interface bandwidth, which is 6Mbps. Other QA traffic is put into shaping group 20 and is guaranteed to have 40% of the interface bandwidth, which is 4Mbps.

To configure interface based traffic shaping in the GUI:

1. On the FortiGate, create a firewall policy for the traffic.
2. Create the shaping policy for QA to access the database:
   a. Go to *Policy & Objects* > *Traffic Shaping Policy*.
   b. Click *Create New*. The *New Shaping Policy page* opens.

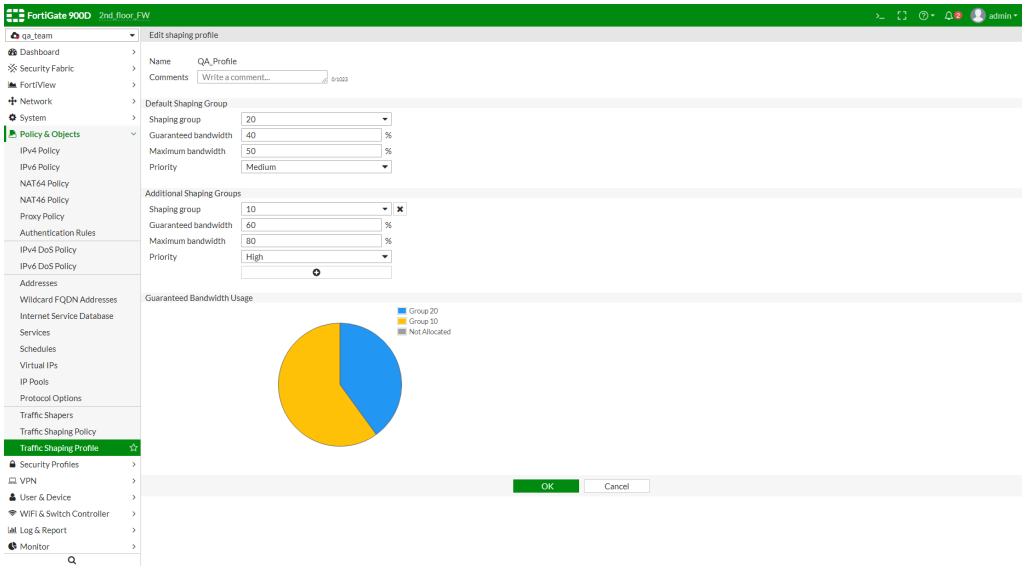


   c. Configure the settings as needed, setting the *Destination* to the database, the *Outgoing interface* to port9, and the *Shaping group* to 10.
   d. Click *OK*.
3. Create the shaping policy for all other QA traffic:
   a. Go to *Policy & Objects* > *Traffic Shaping Policy*.
   b. Click *Create New*. The *New Shaping Policy page* opens.
   c. Configure the settings as needed, setting the *Shaping group* to 20.
   d. Click *OK*.



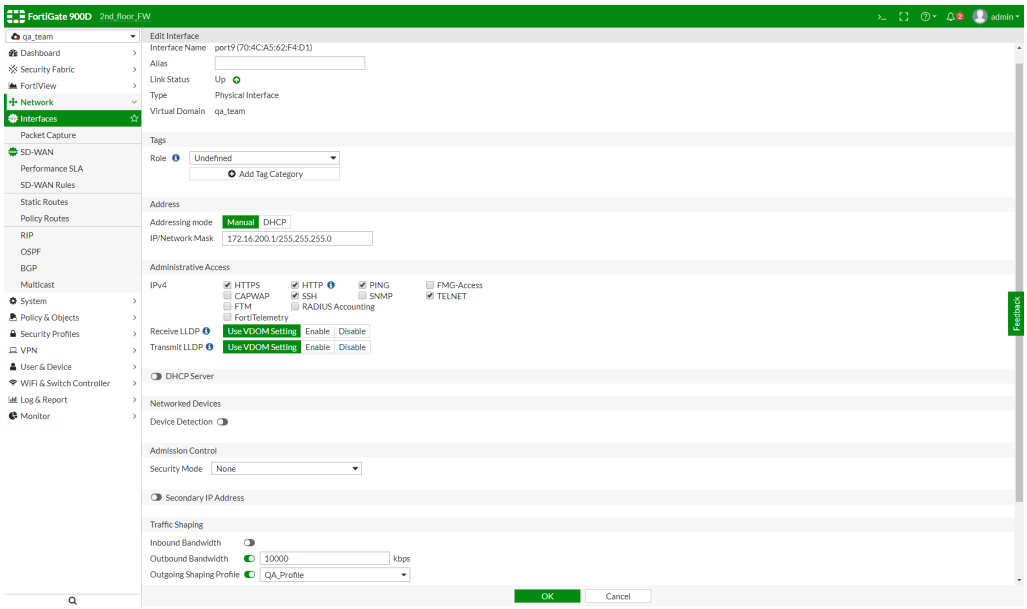
Traffic from QA to the database is put into shaping group 10, and all other QA traffic is put into shaping group 20.

4. Configure a traffic shaping profile:
   a. Go to *Policy & Objects* > *Traffic Shaping Profile*.
   b. Click *Create New*. The *Create shaping profile* page opens.
   c. Set the *Default Shaping Group* to *Shaping group* 20 with a *Guaranteed bandwidth* of 40.
   d. Add an *Additional Shaping Group*, and set the *Shaping group* to 10 and *Guaranteed bandwidth* to 60.



   e. Configure the remaining settings as needed.
   f. Click *OK*.

5. Enable interface based traffic shaping on an interface (port9 in this example):
   a. Go to *Network* > *Interfaces* and double-click on port9. The *Edit Interface* page opens.
   b. Set the *Outbound Bandwidth* to 10000 Kbps.
   c. Set the *Outgoing Shaping Profile* to the just created profile.



   d. Configure the remaining settings as needed.
   e. Click *OK*.

To configure interface based traffic shaping in the CLI:

1. On the FortiGate, create a firewall policy for the traffic:

```
config firewall policy
    edit 2
        set name "QA to Internet"
        set srcintf "port10"
        set dstintf "port9"
        set srcaddr "QA_subnet"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set auto-asic-offload disable
        set nat enable
    next
end
```

2. Create shaping policies for QA to access the database and the Internet:

```
config firewall shaping-policy
    edit 1
        set name "To_Database"
        set service "ALL"
        set dstintf "port9"
        set class-id 10
        set srcaddr "QA_subnet"
        set dstaddr "Database"
    next
    edit 2
        set name "To_Internet"
        set service "ALL"
        set dstintf "port9"
        set class-id 20
        set srcaddr "QA_subnet"
        set dstaddr "all"
    next
end
```

3. Configure a firewall shaping profile:

```
config firewall shaping-profile
    edit "QA_Profile"
        set default-class-id 20
        config shaping-entries
            edit 1
                set class-id 20
                set priority medium
                set guaranteed-bandwidth-percentage 40
                set maximum-bandwidth-percentage 50
            next
            edit 2
                set class-id 10
                set guaranteed-bandwidth-percentage 60
                set maximum-bandwidth-percentage 80
            next
        end
```

```
    next
end
```

4. Enable interface based traffic shaping on an interface (port9 in this example):

```
config system interface
    edit "port9"
        set vdom "qa_team"
        set ip 172.16.200.1 255.255.255.0
        set allowaccess ping https ssh http telnet
        set type physical
        set outbandwidth 10000
        set egress-shaping-profile "QA_Profile"
        set snmp-index 11
    next
end
```

Interface based traffic shaping cannot be used when traffic is offloaded.

Centralized Web Filtering Statistics

This version adds a new, centralized set of counters for the combined results for explicit proxy, Flow mode, and Proxy mode web filtering. The Proxy mode web filter counter is not new. This version adds the results from Flow mode.

Sample usage

You must use the CLI to use this feature.

The Proxy mode web filter counter is not new to this version.

To use Proxy mode web filtering:

```
(vdom)# diag wad stats filter list
......

filtering of all accessible vdoms
  dlp          = 0
  content-type = 0
  urls:
     examined = 181
     allowed = 16
     blocked = 1
     logged = 95
     overridden = 6

(global)#diag wad stats filter list
......

filtering of all accessible vdoms
```

```
  dlp          = 0
  content-type = 0
  urls:
     examined = 181
     allowed = 16
     blocked = 1
     logged = 95
     overridden = 6
```

To use Flow mode web filtering to display global Flow URL filter statistics counter:

```
(global)#diag test app ipsmonitor 29
Global URLF states:
request: 116
response: 116
pending: 1
request error: 0
response timeout: 0
blocked: 24
allowed: 92
```

To reset global Flow URL filter statistics counter:

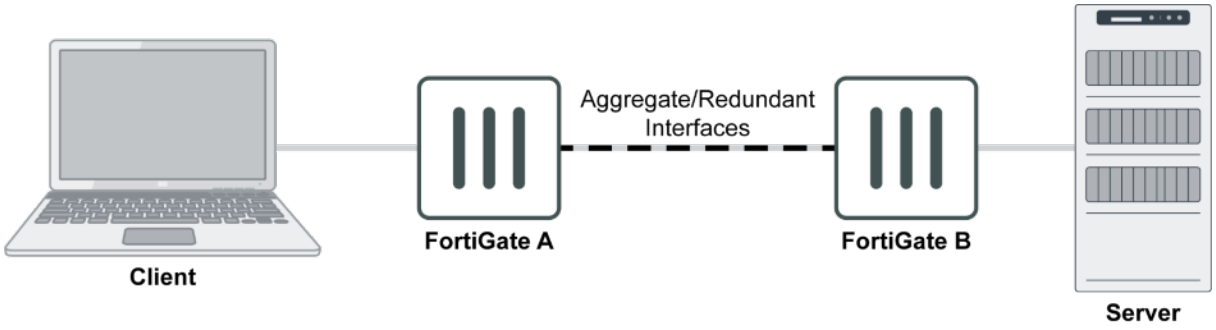
```
(global)#diag test app ipsmonitor 30
```

Other

This section lists other new features added to FortiOS.

Extend Interface Failure Detection to Aggregate Interfaces

This feature extends fail-detect to aggregate and redundant interfaces. When an aggregate or a redundant interface goes down, the corresponding fail-alert-interface will be changed to down. When the aggregate or redundant interface comes up, the corresponding fail-alert-interface will be changed to up.



Fail-detect on aggregate and redundant interfaces can be configured using the CLI.

To configure an aggregate interface so that port3 goes down with it:

```
config system interface
   edit "agg1"
      set vdom "root"
      set fail-detect enable
      set fail-alert-method link-down
      set fail-alert-interfaces "port3"
      set type aggregate
      set member "port1" "port2"
   next
end
```

To configure a redundant interface so that port4 goes down with it:

```
config system interface
   edit "red1"
      set vdom "root"
      set fail-detect enable
      set fail-alert-method link-down
      set fail-alert-interfaces "port4"
      set type redundant
      set member "port1" "port2"
   next
end
```

Source & Destination UUID Logging

This feature has two parts:

- The `log-uuid` setting in `system global` is split into two settings: `log-uuid-address` and `log-uuid policy`.
- Two `internet-service` name fields are added to the traffic log: *Source Internet Service* (`srcinetsvc`) and *Destination Internet Service* (`dstinetsvc`).

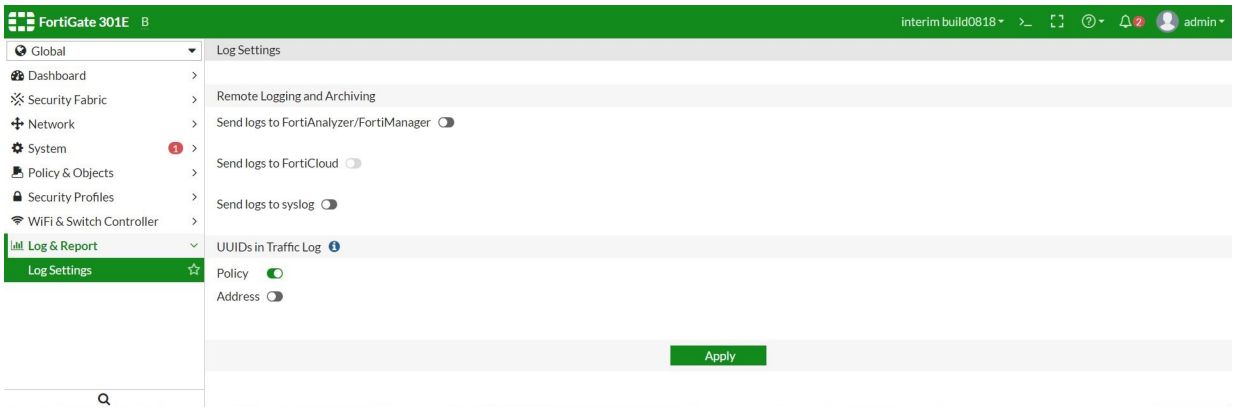
Log UUIDs

This feature allows matching UUIDs for each source and destination that match a policy to be added to the traffic log. This allows the address objects to be referenced in log analysis and reporting.

As this may consume a significant amount of storage space, this feature is optional. By default, policy UUID insertion is enabled and address UUID insertion is disabled.

To enable insertion of address and policy UUIDs to traffic logs in the GUI:

1. Go to *Log Settings*.



2. Under *UUIDs in Traffic Log*, enable *Policy* and/or *Address*.
3. Click *Apply*.

To enable insertion of address and policy UUIDs to traffic logs in the CLI:

Enter the following CLI commands:

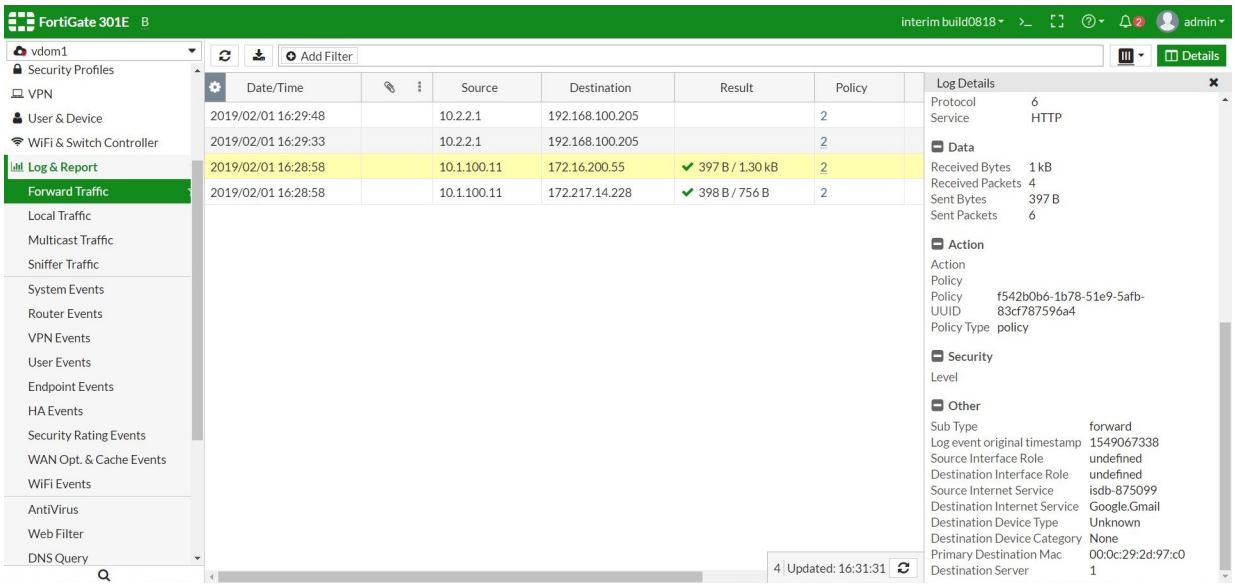
```
config system global
   set log-uuid-address enable
   set log-uuid-policy enable
end
```

Example forward traffic log:

```
# date=2019-01-25 time=11:32:55 logid="0000000013" type="traffic" subtype="forward"
      level="notice" vd="vdom1" eventtime=1528223575 srcip=192.168.1.183 srcname="PC24"
      srcport=33709 srcintf="lan" srcintfrole="lan" dstip=192.168.70.184 dstport=80
      dstintf="wan1" dstintfrole="wan" srcuuid="27dd503e-883c-51e7-ade1-7e015d46494f"
      dstuuid="27dd503e-883c-51e7-ade1-7e015d46494f"
      poluuid="9e0fe24c-1808-51e8-1257-68ce4245572c" sessionid=5181 proto=6 action="client-
      rst" policyid=4 policytype="policy" service="HTTP" trandisp="snat"
      transip=192.168.70.228 transport=33709 appid=38783 app="Wget"
      appcat="General.Interest" apprisk="low" applist="default" duration=5 sentbyte=450
      rcvdbyte=2305 sentpkt=6 wanin=368 wanout=130 lanin=130 lanout=130 utmaction="block"
      countav=2 countapp=1 crscore=50 craction=2 devtype="Linux PC" devcategory="None"
      osname="Linux" mastersrcmac="00:0c:29:36:5c:c3" srcmac="00:0c:29:36:5c:c3" srcserver=0
      utmref=65523-1018
```

Internet service name fields

The forward traffic log for internet-service has two new fields: *Source Internet Service* and *Destination Internet Service*.



Example internet-service name fields in forward traffic log:

```
# date=2019-01-25 time=14:17:04 logid="0000000013" type="traffic" subtype="forward"
      level="notice" vd="vdom1" eventtime=1548454622 srcip=10.1.100.11 srcport=51112
      srcintf="port3" srcintfrole="undefined" dstip=172.217.14.228 dstport=80
      dstintf="port1" dstintfrole="undefined" poluuid="af519380-2094-51e9-391c-b78e8edbddfc"
      srcinetsvc="isdb-875099" dstinetsvc="Google.Gmail" sessionid=6930 proto=6
      action="close" policyid=2 policytype="policy" service="HTTP" dstcountry="United
      States" srccountry="Reserved" trandisp="snat" transip=172.16.200.2 transport=51112
      duration=11 sentbyte=398 rcvdbyte=756 sentpkt=6 rcvdpkt=4 appcat="unscanned"
      devtype="Router/NAT Device" devcategory="Fortinet Device"
      mastersrcmac="90:6c:ac:41:7a:24" srcmac="90:6c:ac:41:7a:24" srcserver=0
      dstdevtype="Unknown" dstdevcategory="Fortinet Device" masterdstmac="08:5b:0e:1f:ed:ed"
      dstmac="08:5b:0e:1f:ed:ed" dstserver=0
```

DNS - Multiple Domain List

DNS settings have been expanded to support a list of up to eight domains. When a client requests a URL that does not include a FQDN, FortiOS resolves the URL by traversing through the DNS domain list and performing a query for each domain until the first match is found.

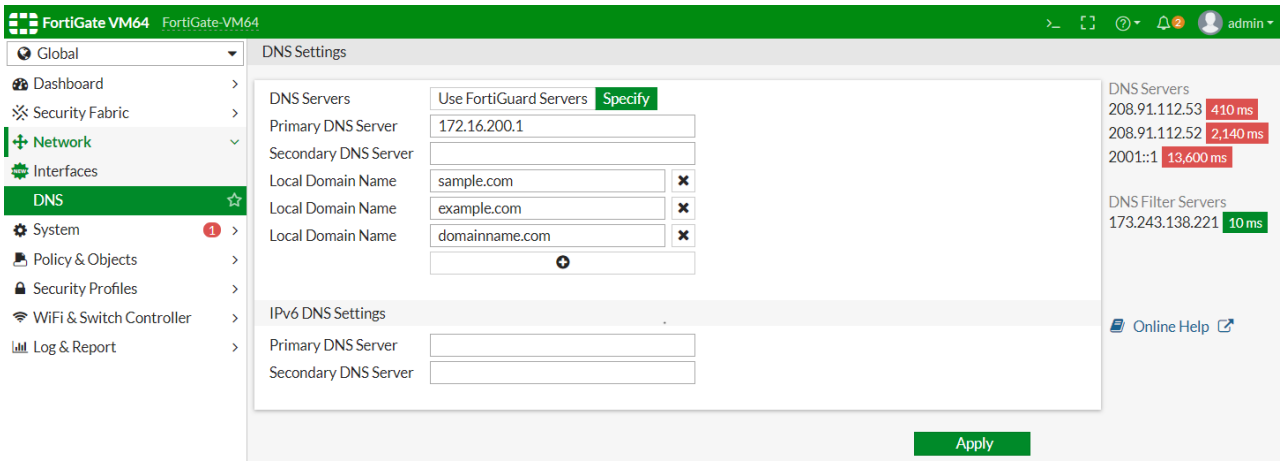
You can configure a DNS domain list using the GUI or the CLI.

CLI options have been added to allow customization of the DNS `timeout` and `retry` settings.

To configure a DNS domain list using the GUI:

1. In FortiOS, go to *Network* > *DNS*.
2. You can click the + button to add multiple domains. Configure up to eight domains as required. In the example below, the DNS domain list is configured to include three domains: sample.com, example.com, and domainname.com.

3. Configure additional DNS settings as required, then click *Apply*.



To configure a DNS domain list using the CLI:

The example below shows the CLI commands for setting the primary DNS server IP address to 172.16.200.1 and configuring multiple domains: sample.com, example.com, and domainname.com.

```
config system dns
   set primary 172.16.200.1
   set domain "sample.com" "example.com" "domainname.com"
end
```

To configure the DNS timeout and retry settings using the CLI:

You may want to customize the DNS timeout and retry settings. For example, if you have eight domains configured, you may want to decrease the DNS timeout value to avoid delays. The following table defines the timeout and retry settings:

CLI option	Description
timeout	DNS query timeout interval in seconds. Enter an integer value between 1 and 10. The default value is 5 seconds.
retry	Number of times to retry the DNS query. Enter an integer value between 0 and 5. The default value is 2 tries.

The example below increases the timeout to 7 seconds and the number of retries to 3:

```
config system dns
   set timeout 7
   set retry 3
end
```

To confirm the DNS domain list was configured:

Once configuration is complete, you can verify that the DNS domain list was configured as desired.

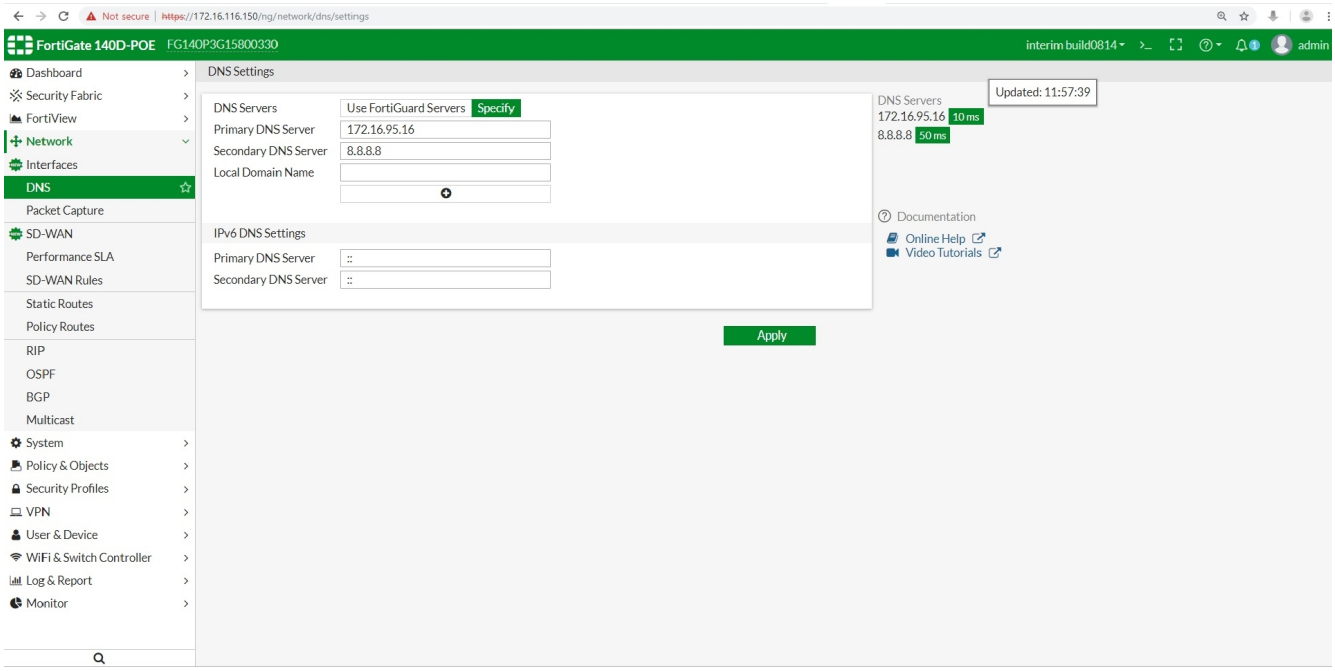
In the example below, the local DNS server has the entry for host1 mapped to the FQDN of host1.sample.com, while the entry for host2 is mapped to the FQDN of host2.example.com. The example shows pinging host1 and host2 to verify that the domain list was configured as desired.

1. In Command Prompt, enter `ping host1`. The system returns the following response:
   `PING host1.sample.com (1.1.1.1): 56 data bytes`
   Since the request does not include a FQDN, FortiOS traverses the configured DNS domain list to find a match. Since host1 is mapped to the host1.sample.com, FortiOS resolves host1 to sample.com, the first entry in the domain list.
2. Enter `ping host2`. The system returns the following response:
   `PING host2.example.com (2.2.2.2): 56 data bytes`
   Again, FortiOS traverses the domain list to find a match. It first queries sample.com, the first entry in the domain list, but does not find a match. It then queries the second entry in the domain list, example.com. Since host2 is mapped to the FQDN of host2.example.com, FortiOS resolves host2 to example.com.

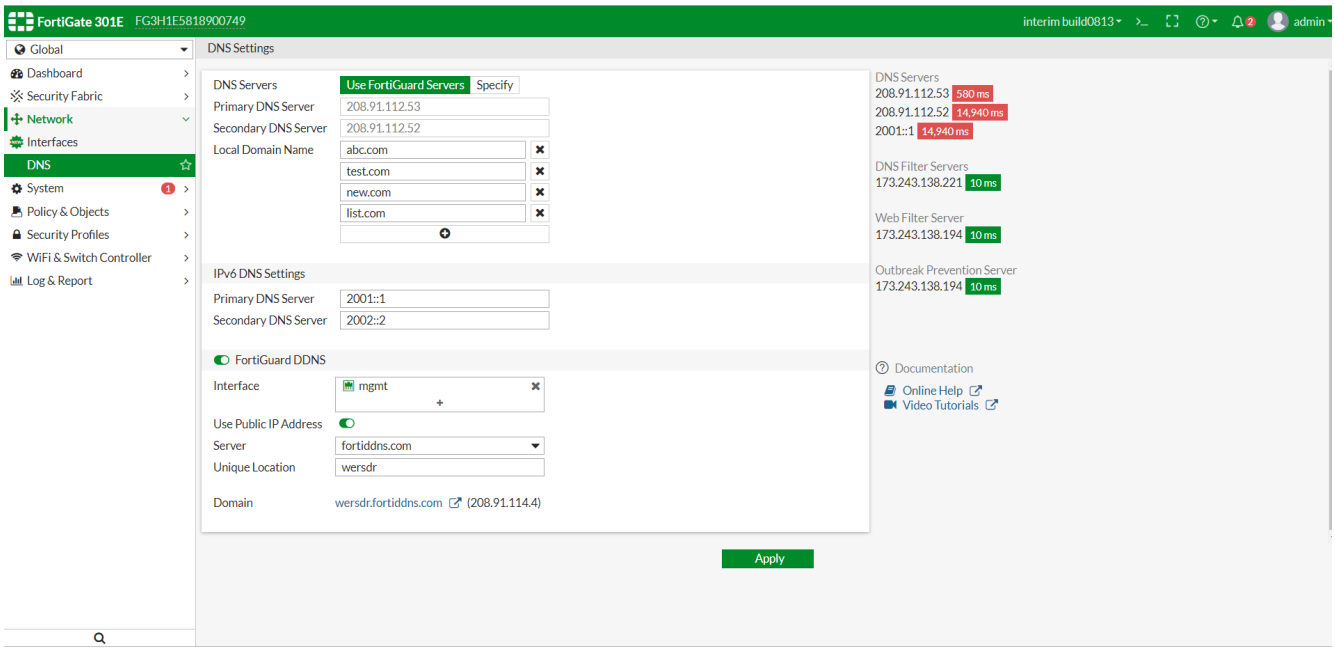
DNS - Latency Info

When there is high latency in DNS traffic, it might result in sluggish overall experience for end users. This new feature helps administrators quickly identify DNS latency issues in their configuration.

The *Interfaces* > *DNS* page shows additional details about DNS latency.



If you use FortiGuard DNS, the information includes latency for regular DNS, DNS filter servers, web filter server, and outbreak prevention servers.



Hover your pointer over a latency value to see the last updated time.

There are no new CLI commands for this feature. DNS latency information is extracted from the CLI data below. See the following examples.

```
diagnose test application dnsproxy 2
worker idx: 0
worker: count=1 idx=0
retry_interval=500 query_timeout=1495
DNS latency info:
vfid=0 server=2001::1 latency=1494 updated=73311
vfid=0 server=208.91.112.52 latency=1405 updated=2547
vfid=0 server=208.91.112.53 latency=19 updated=91
SDNS latency info:
vfid=0 server=173.243.138.221 latency=1 updated=707681
DNS_CACHE: alloc=35, hit=26
RATING_CACHE: alloc=1, hit=49
DNS UDP: req=66769 res=63438 fwd=83526 alloc=0 cmp=0 retrans=16855 to=3233
   cur=111 switched=8823467 num_switched=294 v6_cur=80 v6_switched=7689041 num_v6_switched=6
   ftg_res=8 ftg_fwd=8 ftg_retrans=0
DNS TCP: req=0, res=0, fwd=0, retrans=0 alloc=0, to=0
FQDN: alloc=45 nl_write_cnt=9498 nl_send_cnt=21606 nl_cur_cnt=0
Botnet: searched=57 hit=0 filtered=57 false_positive=0
```

To see the latency from web filter server and outbreak protection server, use the `diagnose debug rating` command, for example:

```
diagnose debug rating
Locale   : english

Service  : Web-filter
Status   : Enable
License  : Contract
```

```
Service  : Antispam
Status   : Disable

Service  : Virus Outbreak Prevention
Status   : Disable

-=- Server List (Tue Jan 22 08:03:14 2019) -=-

IP               Weight RTT Flags  TZ  Packets  Curr Lost Total Lost  Updated Time
173.243.138.194  10     0 DI       -8  700      0         2           Tue Jan 22 08:02:44 2019
173.243.138.195  10     0          -8  698      0         4           Tue Jan 22 08:02:44 2019
173.243.138.198  10     0          -8  698      0         4           Tue Jan 22 08:02:44 2019
173.243.138.196  10     0          -8  697      0         3           Tue Jan 22 08:02:44 2019
173.243.138.197  10     1          -8  694      0         0           Tue Jan 22 08:02:44 2019
96.45.33.64      10     22 D       -8  701      0         6           Tue Jan 22 08:02:44 2019
64.26.151.36     40     62         -5  704      0         10          Tue Jan 22 08:02:44 2019
64.26.151.35     40     62         -5  703      0         9           Tue Jan 22 08:02:44 2019
209.222.147.43   40     70 D       -5  696      0         1           Tue Jan 22 08:02:44 2019
66.117.56.42     40     70         -5  697      0         3           Tue Jan 22 08:02:44 2019
66.117.56.37     40     71         -5  702      0         9           Tue Jan 22 08:02:44 2019
65.210.95.239    40     74         -5  695      0         1           Tue Jan 22 08:02:44 2019
65.210.95.240    40     74         -5  695      0         1           Tue Jan 22 08:02:44 2019
45.75.200.88     90     142        0   706      0         12          Tue Jan 22 08:02:44 2019
45.75.200.87     90     155        0   714      0         20          Tue Jan 22 08:02:44 2019
45.75.200.85     90     156        0   711      0         17          Tue Jan 22 08:02:44 2019
45.75.200.86     90     159        0   704      0         10          Tue Jan 22 08:02:44 2019
62.209.40.72     100    157        1   701      0         7           Tue Jan 22 08:02:44 2019
62.209.40.74     100    173        1   705      0         11          Tue Jan 22 08:02:44 2019
62.209.40.73     100    173        1   699      0         5           Tue Jan 22 08:02:44 2019
121.111.236.179  180    138        9   706      0         12          Tue Jan 22 08:02:44 2019
121.111.236.180  180    138        9   704      0         10          Tue Jan 22 08:02:44 2019
```

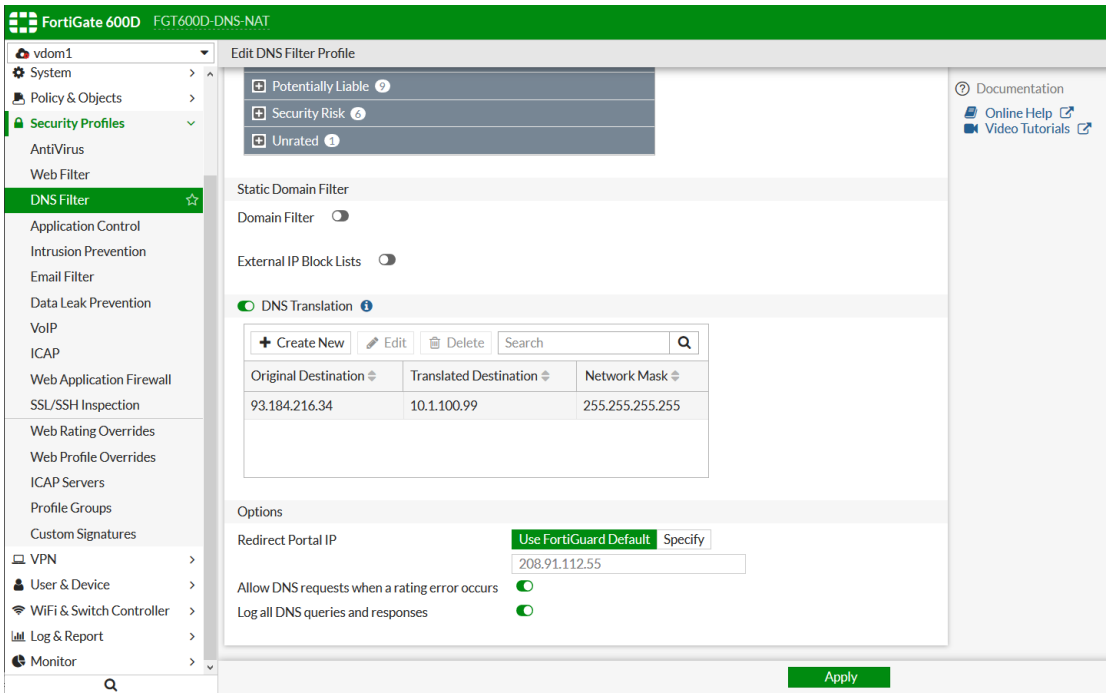
DNS - Add DNS Translation to DNS Profile

DNS translation has moved to the DNS profile configuration, allowing different translations to be applied on a per-policy basis. Prior to 6.2, this was a single table outside of the profile.

DNS filter dns-translation enforces what 'a record' (IP address) in a DNS reply will be translated into another IP address, which allows you to control the DNS resolve result.

To configure a DNS filter using the GUI:

1. Go to *Security Profiles* > *DNS Filter*.
2. Enable *DNS Translation*, configure as follows, and click *Appy*:



3. Apply the DNS filter profile to the firewall policy.

To configure a DNS filter using the CLI:

1. Enable `dns-translation`:

```
config dnsfilter profile
   edit "<dns-filter-profile>"
   ......
      config dns-translation
         edit 1
            set src 93.184.216.34
            set dst 10.1.100.99
            set netmask 255.255.255.255
         next
      end
end
```

Multiple FortiAnalyzer (or Syslog) Per VDOM

Under VDOM, support has been added for multiple FortiAnalyzer and Syslog servers as follows:

- Support for up to three override FortiAnalyzer servers.
- Support for up to four override Syslog servers.

If the VDOM `faz-override` and/or `syslog-override` setting is enabled or disabled (default) before upgrading, the setting remains the same after upgrading.

In the GUI, if the override setting is disabled, the GUI displays the global FortiAnalyzer1 or syslog1 setting. If the override setting is enabled, the GUI displays the VDOM override FortiAnalyzer1 or syslog1 setting.

You can only use CLI to enable the override to support multiple log servers.

To enable FortiAnalyzer and Syslog server override under VDOM:

```
config log setting
   set faz-override enable
   set syslog-override enable
end
```

When `faz-override` and/or `syslog-override` is enabled, the following CLI commands are available to config VDOM override:

To configure VDOM override for FortiAnalyzer:

```
config log fortianalyzer/fortianalyzer2/fortianalyzer3 override-setting
   set status enable
   set server "123.12.123.123"
   set reliable enable
end
config log fortianalyzer/fortianalyzer2/fortianalyzer3 override-filter
   set severity information
   set forward-traffic enable
   set local-traffic enable
   set multicast-traffic enable
   set sniffer-traffic enable
   set anomaly enable
   set voip enable
   set dlp-archive enable
   set dns enable
   set ssh enable
   set ssl enable
end
```

To configure VDOM override for Syslog server:

```
config log syslogd/syslogd2/syslogd3/syslogd4 override-setting
   set status enable
   set server "123.12.123.12"
   set facility local1
end
config log syslogd/syslogd2/syslogd3/syslogd4 override-filter
   set severity information
   set forward-traffic enable
   set local-traffic enable
   set multicast-traffic enable
   set sniffer-traffic enable
   set anomaly enable
   set voip enable
   set dns enable
   set ssh enable
   set ssl enable
```

```
end
```

Web Proxy

This section lists other new features added to FortiOS related to web proxy.

Transparent Web Proxy Forwarding

This feature enables the proxy forwarding option for Transparent Web Proxy policies and Regular Firewall for HTTP and HTTPS.

In previous versions of FortiOS, explicit proxy allowed the user to forward proxy traffic to another proxy server (proxy chaining). With this new implementation, web traffic can be forwarded to the upstream proxy without requiring the users to reconfigure their browsers or publish a proxy auto-reconfiguration (PAC) file.

Once configured, traffic generated by a client is forwarded by the FortiGate to the upstream proxy, then the upstream proxy forwards it to the server.

Example configuration:

1. Configure the web proxy forwarding server:

```
config web-proxy forward-server
    edit "PC_03"
        set ip 172.16.200.46
        set healthcheck enable
        set monitor "http://www.google.ca"
    next
end
```

2. Append the web proxy forwarding server to a firewall policy:

```
config firewall policy
    edit 1
        set name "LAN to WAN"
        set uuid b89f6184-2a6b-51e9-5e2d-9b877903a308
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set logtraffic all
        set webproxy-forward-server "PC_03"
        set fsso disable
        set av-profile "av"
```

```
        set ssl-ssh-profile "deep-custom"
        set nat enable
    next
end
```

Multiple Dynamic Header Count

This feature adds support for dynamic headers for web proxy profiles, as well as base64 encoding and append/new options. Previously, web proxy profiles supported dynamic (or user defined) header content for filtering, but the format was fixed and could not support multiple patterns in one header. With this features, multiple patterns are supported.

With the implementation of dynamic headers, an administrator only has to select the dynamic header, and the FortiGate will automatically display the corresponding static value. For example, if the administrator selects the $client-ip header in the profile, the FortiGate will display the actual client IP address.

The supported headers are:

$client-ip	Client IP address
$user	Authentication user name
$domain	User domain name
$local_grp	Firewall group name
$remote_grp	Group name from authentication server
$proxy_name	Proxy realm name

Example configuration:

As authentication is required, FSSO NTLM authentication is configured for this example.

1. Configure LDAP:

```
config user ldap
    edit "ldap-kerberos"
        set server "172.18.62.220"
        set cnid "cn"a
        set dn "dc=fortinetqa,dc=local"
        set type regular
        set username "CN=root,CN=Users,DC=fortinetqa,DC=local"
        set password ENC
k9AF5nj3NInc11qORQ+WHUmNbCKGX/4d6MkzdBwPSnJQHNCEJBnVSiiMwQ1FKHIQFZVDFK3ACD/mCfJWyENnWBE6M3/
Qk3DweaRhlLjxSLSXs6H/R5oTCl3nrj5yFZEjDMZtbWwjwC7MtgxzXZ0ztLqFeVPhy8jzmxBJLwvan2nUnu/Xe5ujkK
XdOxRm1cAI7q/shg==
    next
end
```

2. Configure FSSO:

```
config user fsso
    edit "1"
        set server "172.18.62.220"
        set password ENC
I4b2VpJAM5AZsbqGsIJ/EfvYgbN3hmEU7O2PXU9YK0AbmpTiX7Evlo5xy74bkgPniWJrHJ49Gtx8mGb4HcGa2XKdD9b
```

```
STvgQqfCcZuLANBSrJg/Qy4V7RyrkKp8B3Zsbj7nN+Rzg5FAoNhnw1Hrf0ZvdSTKvAGN5e+OtILz7lR9jaudydIOpy6
0qq4I7RHeGiVQiXA==
    next
end
```

3. Configure a user group:

```
config user group
    edit "NTLM-FSSO"
        set group-type fsso-service
        set member "FORTINETQA/FSSO"
    next
end
```

4. Configure an authentication scheme:

```
config authentication scheme
    edit "au-sch-ntlm"
        set method ntlm
    next
end
```

5. Configure an authentication rule:

```
config authentication rule
    edit "au-rule-fsso"
        set srcaddr "all"
        set active-auth-method "au-sch-ntlm"
    next
end
```

6. Create a web proxy profile, adding the new dynamic and custom via header

```
config web-proxy profile
    edit "test"
        set log-header-change enable
        config headers
            edit 1
                set name "client-ip"
                set content "$client-ip"
            next
            edit 2
                set name "Proxy-Name"
                set content "$proxy_name"
            next
            edit 3
                set name "user"
                set content "$user"
            next
            edit 4
                set name "domain"
                set content "$domain"
            next
            edit 5
                set name "local_grp"
                set content "$local_grp"
            next
            edit 6
                set name "remote_grp"
```

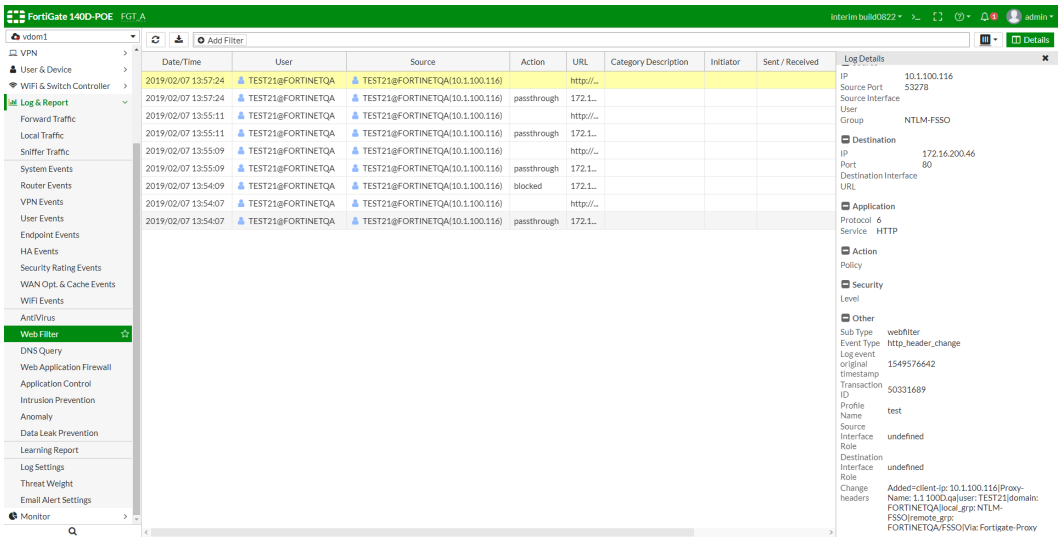
```
                set content "$remote_grp"
            next
            edit 7
                set name "Via"
                set content "Fortigate-Proxy"
            next
        end
    next
end
```

7. In the proxy policy, append the web proxy profile create in the previous step:

```
config firewall proxy-policy
    edit 1
        set uuid bb7488ee-2a6b-51e9-45c6-1715bdc271d8
        set proxy explicit-web
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set service "web"
        set action accept
        set schedule "always"
        set logtraffic all
        set groups "NTLM-FSSO"
        set webproxy-profile "test"
        set utm-status enable
        set av-profile "av"
        set webfilter-profile "content"
        set ssl-ssh-profile "deep-custom"
    next
end
```

8. Once traffic is being generated from the client, look at the web filter logs to verify that it is working.
All the added header fields display their corresponding value in the *Change headers* section at the bottom of the *Log Details* screen.

```
1: date=2019-02-07 time=13:57:24 logid="0344013632" type="utm" subtype="webfilter"
eventtype="http_header_change" level="notice" vd="vdom1" eventtime=1549576642 policyid=1
transid=50331689 sessionid=1712788383 user="TEST21@FORTINETQA" group="NTLM-FSSO"
profile="test" srcip=10.1.100.116 srcport=53278 dstip=172.16.200.46 dstport=80
srcintf="port2" srcintfrole="undefined" dstintf="port1" dstintfrole="undefined" proto=6
service="HTTP" url="http://172.16.200.46/" agent="curl/7.22.0" chgheaders="Added=client-ip:
10.1.100.116|Proxy-Name: 1.1 100D.qa|user: TEST21|domain: FORTINETQA|local_grp: NTLM-
FSSO|remote_grp: FORTINETQA/FSSO|Via: Fortigate-Proxy"
```



Restricted SaaS Access (0365, G-Suite, Dropbox)

This feature extends the web-proxy profile to allow for specifying access permissions for Microsoft Office 365, Google G Suite, and Dropbox. It works by inserting vendor defined headers that restrict access to the specific accounts. Custom headers for any destination can also be inserted.

The web-proxy profile can be configured with the required headers for the specific destinations, and then applied directly into a policy to control the header's insertion.

To implement Office 365 tenant restriction, Dropbox network access control, and Google G Suite account access control on FortiGate, you need to:

1. Configure a web-proxy profile according to the vendors' specifications:
   a. Define the traffic destination (service provider).
   b. Define the header name, defined by the service provider.
   c. Define the value that will be inserted into the traffic, defined by your settings.
2. Apply the web-proxy profile to a policy.

The following example creates a web-proxy profile for Office 365, G Suite, and Dropbox access control. Note that, due to vendors' changing requirements, this example may no longer be in compliance with the vendors' official guidelines.

1. Configure the web-proxy profile:

```
config web-proxy profile
   edit "SaaS-Tenant-Restriction"
        set header-client-ip pass
        set header-via-request pass
        set header-via-response pass
        set header-x-forwarded-for pass
        set header-front-end-https pass
        set header-x-authenticated-user pass
        set header-x-authenticated-groups pass
        set strip-encoding disable
        set log-header-change disable
        config headers
            edit 1
```

```
                set name "Restrict-Access-To-Tenants"  <---header name defined by Office365
spec. input EXACTLY as it is
                set dstaddr "Microsoft Office 365" <----built-in destination address for
Office365
                set action add-to-request
                set base64-encoding disable
                set add-option new
                set protocol https http
                set content "contoso.onmicrosoft.com,fabrikam.onmicrosoft.com"  <----your
tenants restriction configuration
            next
            edit 2
                set name "Restrict-Access-Context"  <----header name defined by Office365
spec. input EXACTLY as it is
                set dstaddr "Microsoft Office 365"  <----build-in destination address for
Office365
                set action add-to-request
                set base64-encoding disable
                set add-option new
                set protocol https http
                set content "456ff232-35l2-5h23-b3b3-3236w0826f3d" <----your directory ID
can find in Azure portal
            next
            edit 3
                set name "X-GooGApps-Allowed-Domains"  <----header name defined by Google G
suite.
                set dstaddr "G Suite"  <---- built-in G Suite destination address
                set action add-to-request
                set base64-encoding disable
                set add-option new
                set protocol https http
                set content "abcd.com"    <----your domain restriction when you create G
Suite account
            next

            edit 4
                set name "X-Dropbox-allowed-Team-Ids" <----header defined by Dropbox
                set dstaddr "wildcard.dropbox.com"  <----build-in destination address for
Dropbox
                set action add-to-request
                set base64-encoding disable
                set add-option new
                set protocol https http
                set content "dbmid:FDFSVF-DFSDF"  <----your team-Id in Dropbox
            next
        end
    next
end
```

2. Apply the web-proxy profile to a firewall policy:

```
config firewall policy
     edit 1
               set name "WF"
               set uuid 09928b08-ce46-51e7-bd95-422d8fe4f200
               set srcintf "port10" "wifi"
               set dstintf "port9"
```

```
                set srcaddr "all"
                set dstaddr "all"
                set action accept
                set schedule "always"
                set service "ALL"
                set webproxy-profile "SaaS-Tenant-Restriction"
                set utm-status enable
                set utm-inspection-mode proxy
                set logtraffic all
                set webfilter-profile "blocktest2"
            set application-list "g-default"
                set profile-protocol-options "protocol"
                set ssl-ssh-profile "protocols"
                set nat enable
            next
    end
```

References:

Office 365 - Use Tenant Restrictions to manage access to SaaS cloud applications

G Suite - Block access to consumer accounts

Dropbox - Network Control

Protocols

This section lists other new features added to FortiOS related to protocols.

TLS 1.3 Support

SSL VPN

TLS 1.3 support has been added for SSL VPN. The following steps are required for a client to establish an SSL VPN connection with TLS 1.3 to the FortiGate:

1. Configure TLS 1.3 support using the FortiOS CLI.
2. Configure the SSL VPN and firewall policy.
3. For Linux clients, ensure OpenSSL 1.1.1a is installed.
4. Use OpenSSL with the TLS 1.3 option to connect to SSL VPN.
5. Ensure that the SSL VPN connection has been established with TLS 1.3.

This feature can only be used with endpoints that have FortiClient 6.2.0 or a later version installed. Earlier FortiClient versions do not support TLS 1.3.

To configure TLS 1.3 support using the FortiOS CLI:

A new command for TLS 1.3 has been added under `config vpn ssl setting`. By default, TLS 1.3 support is enabled. You can enable TLS 1.3 support using the following FortiOS CLI command:

```
config vpn ssl setting
   set tlsv1-3 enable
end
```

To configure SSL VPN and the firewall policy:

Configure the SSL VPN settings and firewall policy as required. Refer to the FortiOS Handbook for details.

To ensure OpenSSL 1.1.1a is installed on the Linux client:

Run the following commands in the terminal on the Linux client:

```
root@PC1:~/tools# openssl
OpenSSL> version
```

If OpenSSL 1.1.1a is installed, the system displays a response like the following:

```
OpenSSL 1.1.1a  20 Nov 2018
```

To connect to SSL VPN using OpenSSL with TLS 1.3:

On the Linux client, use OpenSSL to connect to FortiGate SSL VPN with TLS 1.3 by running the following command:

```
#openssl s_client -connect 10.1.100.10:10443 -tls1_3
```

To ensure that SSL VPN connection is established with TLS 1.3:

Run the following commands in the FortiOS CLI to ensure that the SSL VPN connection has been established with TLS 1.3:

```
# diagnose debug application sslvpn -1
# diagnose debug enable
```

The system should display a response like the following:

```
[207:root:1d]SSL established: TLSv1.3 TLS_AES_256_GCM_SHA384
```

Deep Inspection (Flow Based)

FortiOS now supports TLS 1.3 for policies that have the following security profiles applied:

- Web Filter profile with flow-based inspection mode enabled
- Deep inspection SSL/SSH Inspection profile

Consider that a policy with the above Web Filter and SSL/SSH Inspection profiles applied is enabled. A client attempts to access a website that supports TLS 1.3. FortiOS sends the traffic to the IPS engine. The IPS engine then decodes TLS 1.3, and the client is able to access the website.

TLS 1.3 support is only available for IPS engine 4.205 and later versions.

PTPv2 (Slave Mode)

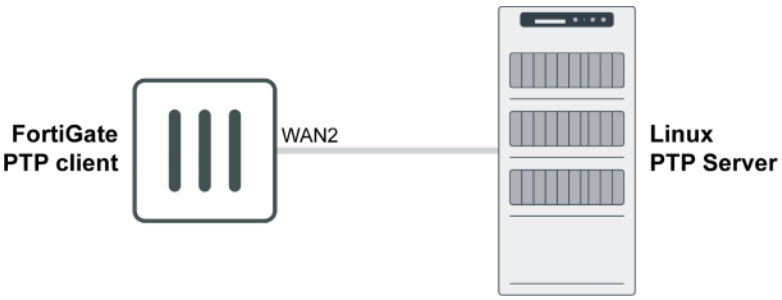
Precision Time Protocol (PTP) is used to synchronize network clocks. It is best suited to situations where time accuracy is of the utmost importance, as it supports accuracy in the sub-microsecond range. Conversely, NTP accuracy is in the range of milliseconds or tens of milliseconds.

The following CLI commands have been added:

```
config system ptp
   set status {enable | disable}
   set mode {multicast | hybrid}
   set delay-mechanism {E2E | P2P}
   set request-interval <integer>
   set interface <interface>
end
```

Command	Description
status {enable | disable}	Enable/disable setting the FortiGate system time by synchronizing with an PTP server (default = disable).
mode {multicast | hybrid}	Use multicast or hybrid transmission (default = multicast).
delay-mechanism {E2E | P2P}	Use End to End (E2E) or Peer to Peer (P2P) delay detection (default = E2E).
request-interval <integer>	The logarithmic mean interval between the delay request messages sent by the client to the server, in seconds (default = 1).
interface <interface>	The interface that the PTP client will reply through.

This example uses the following topology:



To configure a FortiGate to act as a PTP client that synchronizes itself with a Linux PTP server:

1. Enable debug messages:
   ```
   diagnose debug application ptpd -1
   ```
   This command will provide details to debug the PTP communication with the server.
2. Check the system date:
   ```
   execute date
   ```

```
   current date is: 2019-01-01
```

3. Configure PTP in global mode:

```
config system ptp
   set status enable
   set interface wan2
end
```

The following, or similar, debug message will be shown:

```
FGT_A (global) # [notice]PTPDv2 started successfully on wan2 using "slaveonly" preset
      (PID 5958)
[info]TimingService.PTP0: PTP service init
[info]Observed_drift loaded from kernel: 0 ppb
[notice]Now in state: PTP_LISTENING
[warning]TimingService: No TimingService available for clock sync
[info]New best master selected: 000c29fffe236b0c(unknown)/1
[notice]Now in state: PTP_SLAVE, Best master: 000c29fffe236b0c(unknown)/1
      (IPv4:172.16.200.55)
[notice]Received first Sync from Master
[critical]Offset above 1 second. Clock will step.
[warning]Change time from Tue Jan 1 00:00:28 2019 to Mon Jan 14 15:11:10 2019.
      [notice]Now in state: PTP_LISTENING
[info]New best master selected: 000c29fffe236b0c(unknown)/1
[notice]Now in state: PTP_SLAVE, Best master: 000c29fffe236b0c(unknown)/1
      (IPv4:172.16.200.55)
[notice]Received first Sync from Master
[info]TimingService.PTP0: now available
[notice]Received first Delay Response from Master
[notice]Received new Delay Request interval 0 from Master (was: 1)
[notice]TimingService.PTP0: elected best TimingService
[info]TimingService.PTP0: acquired clock control
```

4. Check the system date again after synchronization with the PTP server

```
execute date
   current date is: 3/27/2019
```

Telnet Disabled Option

A new CLI option has been added that completely disables Telnet, removing the GUI options per interface and disabling the Telnet daemon.

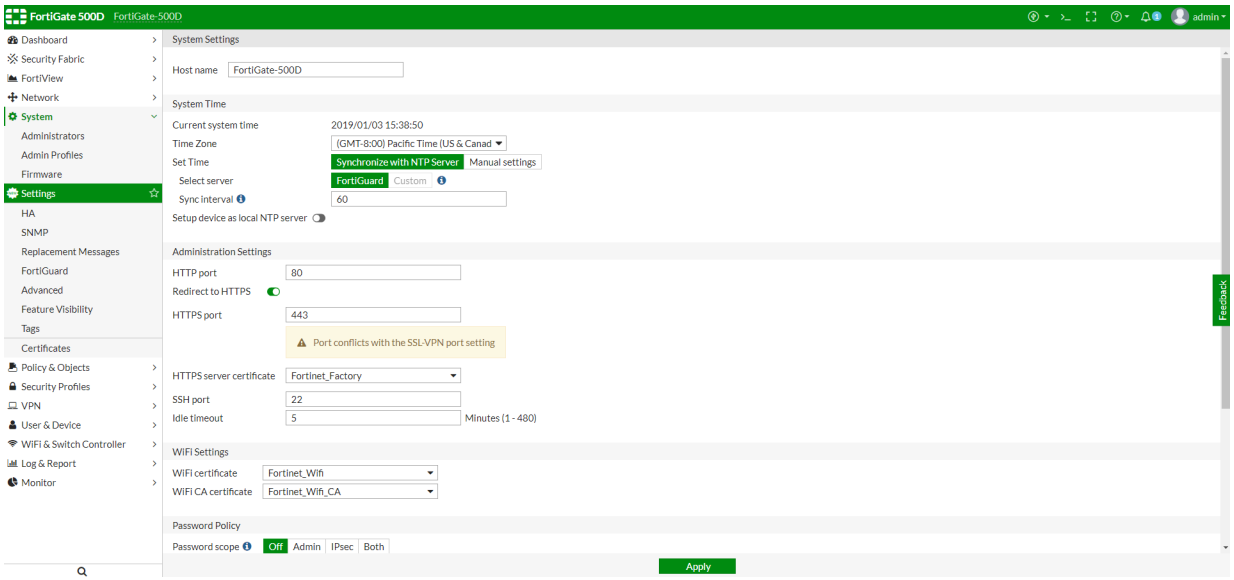
When Telnet is disabled, the Telnet port cannot be configured and access cannot be enabled on interfaces.

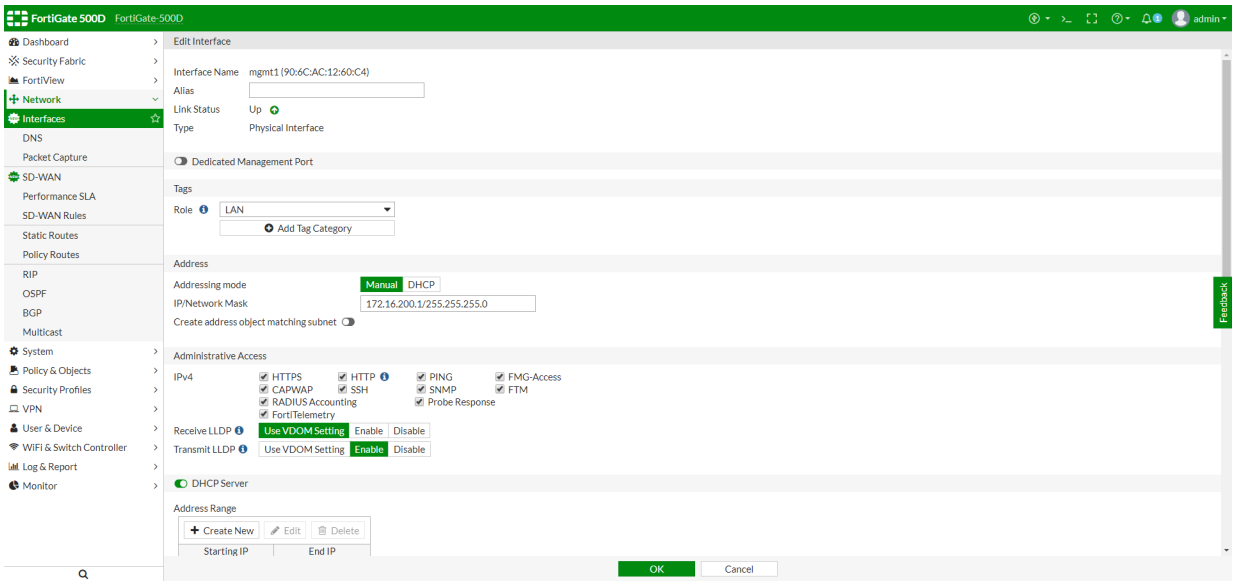
Telnet is enabled by default.

To disable Telnet:

```
config system global
   set admin-telnet disable
end
```

When disabled, the Telnet port is removed from the *System* > *Settings* page, and *TELNET* is no longer an administrative access option on the *Network* > *Interfaces* page.

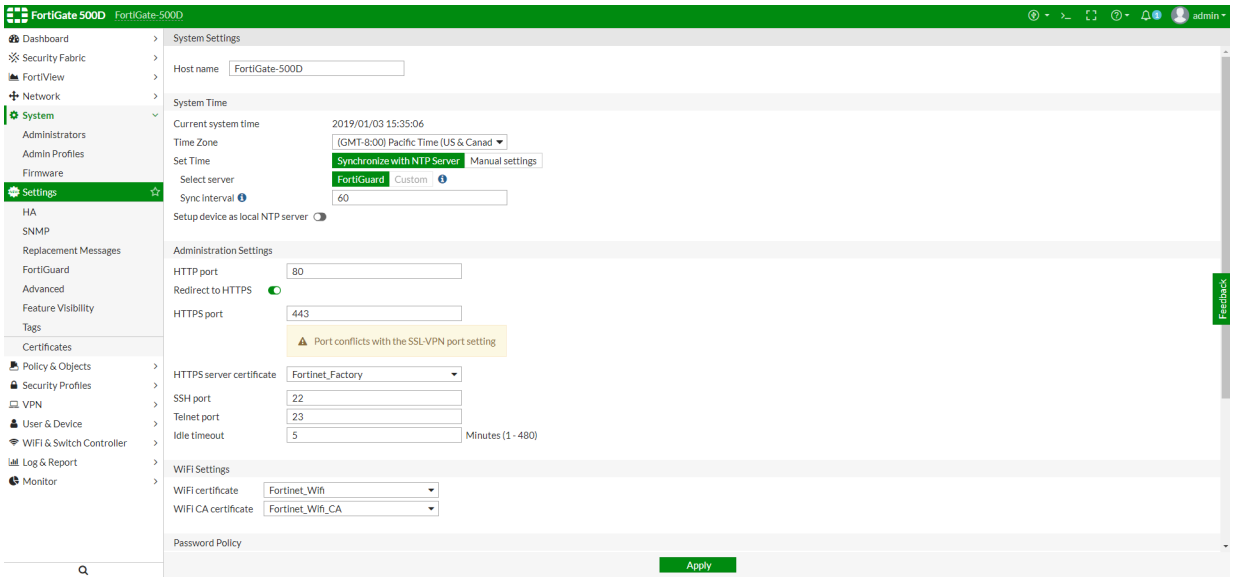


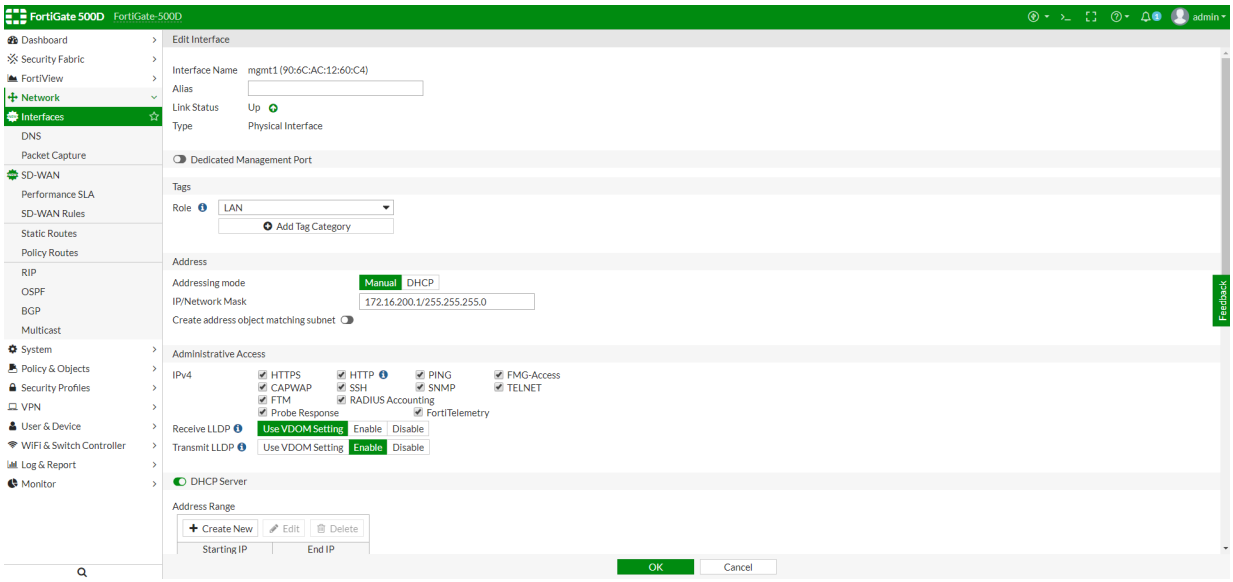


To enable Telnet:

```
config system global
   set admin-telnet enable
   set admin-telnet-port <port>
end
```

When Telnet is enabled, the port can be configured on the *System* > *Settings* page, and TELNET can be selected can be selected as an administrative access option on the *Network* > *Interfaces* page.

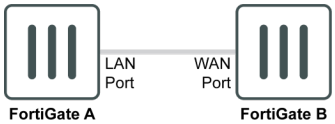




LLDP Reception (Arista Connector)

This feature enables LLDP reception on WAN interfaces, and prompts FortiGates that are joining the Security Fabric if the upstream FortiGate asks.

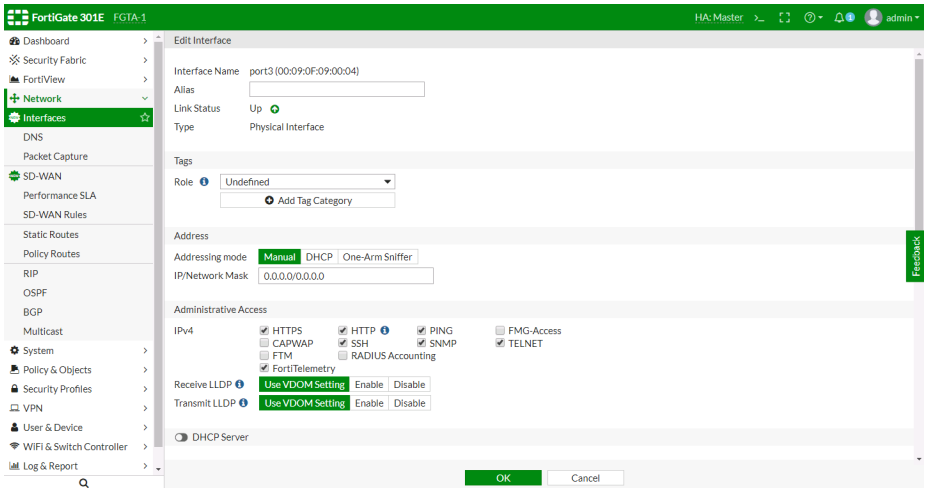
- If an interface's role is undefined, LLDP reception and transmission inherit settings from the VDOM.
- If an interface's role is WAN, LLDP reception is enabled.
- If an interface's role is LAN, LLDP transmission is enabled.



When a FortiGate B's WAN interface detects that FortiGate A's LAN interface is immediately upstream (through the default gateway), and FortiGate A has Security Fabric enabled, FortiGate B will show a notification on the GUI asking to join the Security Fabric.

To configure LLDP reception and join a Security Fabric:

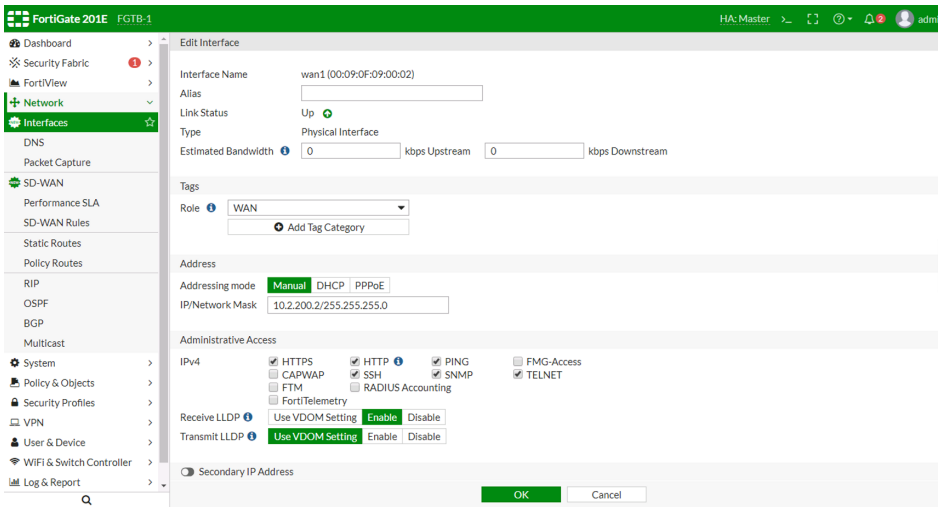
1. Go To *Network* > *Interfaces*.
2. Configure an interface:
   - If the interface's role is undefined, under *Administrative Access*, set *Receive LLDP* and *Transmit LLDP* to *Use VDOM Setting*.



Using the CLI:

```
config system interface
    edit "port3"
        set lldp-reception vdom
        set lldp-transmission vdom
        set role undefined
        ...
    next
end
```

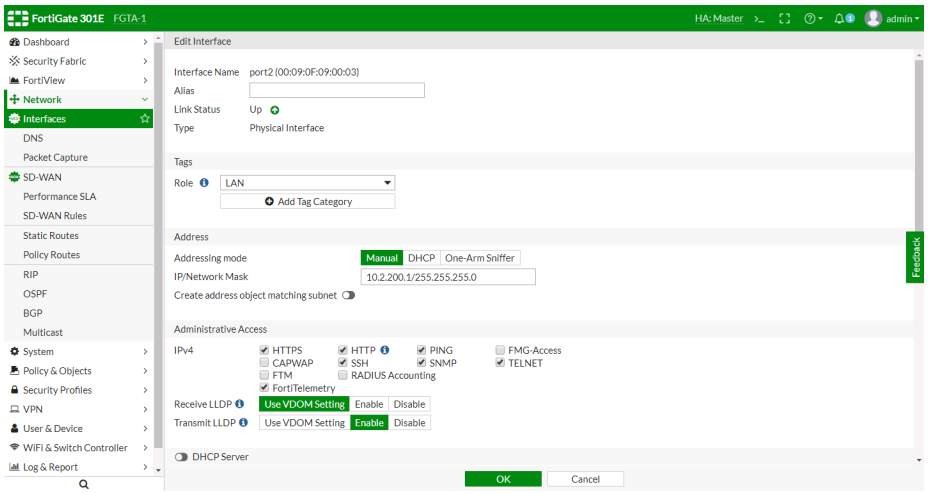
   - If the interface's role is WAN, under *Administrative Access*, set *Receive LLDP* to *Enable* and *Transmit LLDP* to *Use VDOM Setting*.



Using the CLI:

```
config system interface
    edit "wan1"
        set lldp-reception enable
        set lldp-transmission vdom
        set role wan
        ...
    next
end
```

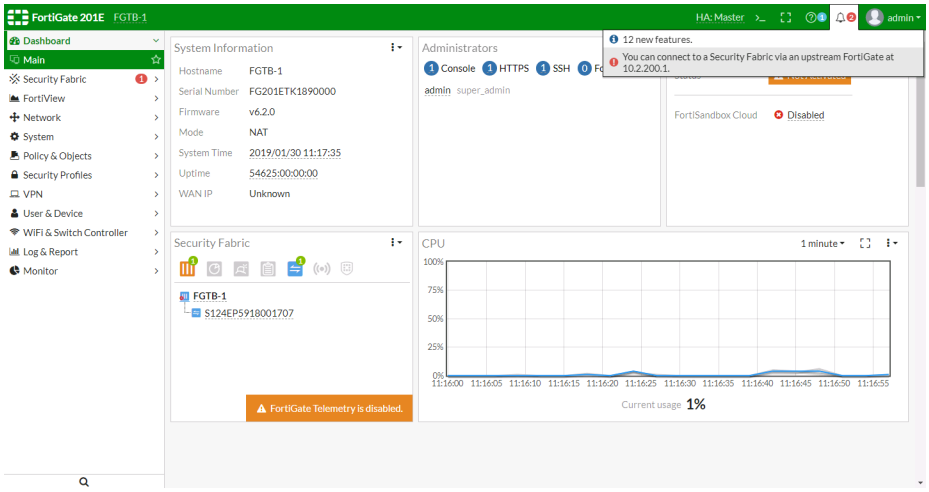
- If the interface's role is LAN, under *Administrative Access*, set *Receive LLDP* to *Use VDOM Setting* and *Transmit LLDP* to *Enable*.



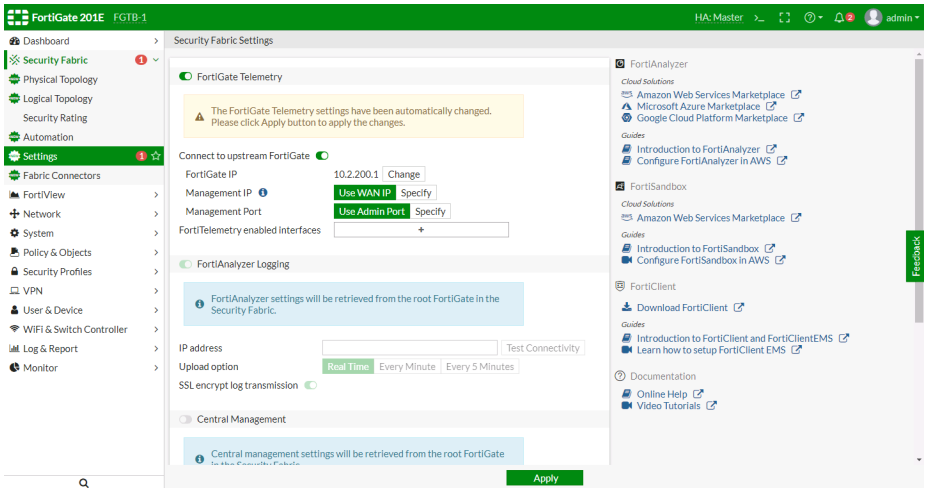
Using the CLI:

```
config system interface
    edit "port2"
        set lldp-reception vdom
        set lldp-transmission enable
        set role lan
        ...
    next
end
```

A notification will be shown on FortiGate B.



3. Click the notification. The *Security Fabric Settings* page opens with all the required settings automatically configured.



4. Click *Apply* to apply the settings, or use the following CLI commands:

```
config system csf
    set status enable
    set upstream-ip 10.2.200.1
end
```

SHA-1 Authentication Support (for NTPv4)

SHA-1 authentication support allows the NTP client to verify that severs are known and trusted and not intruders masquerading (accidentally or intentionally) as legitimate servers. In cryptography, SHA-1 is a cryptographic hash algorithmic function.

In this version, SHA-1 authentication support is only available for NTP clients, not NTP servers.

The following CLI commands have been added to `config ntpserver`:

Command	Description
authentication <*enable* | *disable*>	Enable/disable MD5/SHA1 authentication (default = disable).
key <*passwd*>	Key for MD5/SHA1 authentication. Enter a password value.
key-id	Key ID for authentication. Enter an integer value from <0> to <4294967295>.

For example, to configure authentication on a FortiGate NTP client:

```
config system ntp
   set ntpsync enable
   set type custom
   set syncinterval 1
   config ntpserver
      edit 883502
         set server "10.1.100.11"
         set authentication enable
         set key
               ENCi9NmcqsV3xBJvOkgIL3lFxA8mnNs2XKfB7spOQoUw4cm8FOOP0nrCbqx6rJ+om95+hVUHpaVZmepdd
               4KznPlAHNiuliPgPOk
         set key-id 1
      next
   end
end
```

If NTP authentication is set up correctly, `diag sys ntp status` shows `server-version=4`. For example:

```
diag sys ntp status

synchronized: yes, ntpsync: enabled, server-mode: disabled
ipv4 server(10.1.100.11) 10.1.100.11 -- reachable(0xff) S:4 T:6 selected
server-version=4, stratum=3
```

DNS over TLS

A new option is added to DNS Profile, forcing DNS over TLS for added security.

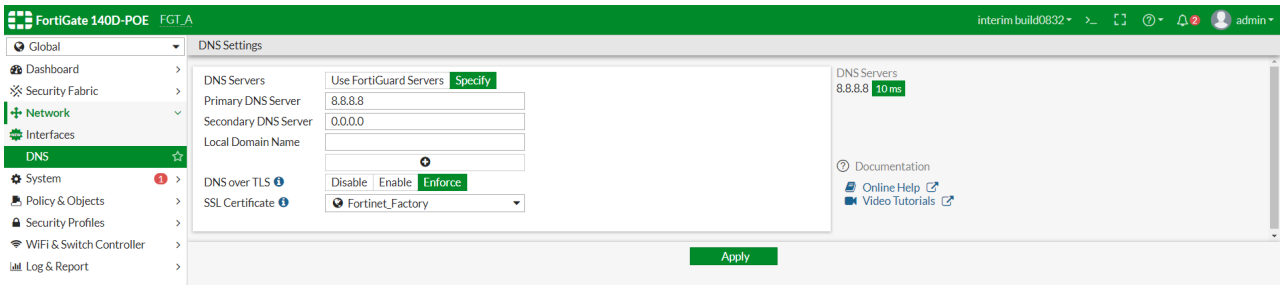
DNS over TLS (DoT) is a security protocol for encrypting and wrapping Domain Name System (DNS) queries and answers via the Transport Layer Security (TLS) protocol. The goal of the method is to increase user privacy and security by preventing eavesdropping and manipulation of DNS data via man-in-the-middle attacks.

Below is a typical topology.

FortiGate (client/server)<-----(DNS over TLS)<----------> DNS server/client

To configure DNS over TLS using the GUI:

1. Go to *Network* > *DNS*.
2. In *DNS over TLS*, select *Enforce*.



To configure DNS over TLS using the CLI:

```
FGT_A (global) # config system dns

FGT_A (dns) # show
config system dns
    set primary 8.8.8.8
    set dns-over-tls enforce
end

FGT_A (dns) # set dns-over-tls
disable    Disable DNS over TLS.
enable     Use TLS for DNS queries if TLS is available.
enforce    Use only TLS for DNS queries. Does not fall back to unencrypted DNS queries if TLS
is unavailable.

FGT_A (dns) # set dns-over-tls enforce
 <Enter>

FGT_A (dns) # set dns-over-tls enforce

FGT_A (dns) # set ssl-certificate
<string>    please input string value
Fortinet_CA_SSL    local
Fortinet_CA_Untrusted    local
Fortinet_Factory    local
Fortinet_SSL    local
Fortinet_SSL_DSA1024    local
Fortinet_SSL_DSA2048    local
Fortinet_SSL_ECDSA256    local
Fortinet_SSL_ECDSA384    local
Fortinet_SSL_RSA1024    local
Fortinet_SSL_RSA2048    local
Server    local
testercert    local

FGT_A (dns) # set ssl-certificate
```

Recognize AnyCast Address in Geo-IP Blocking

An AnyCast IP can be advertised from multiple locations and the router selects a path based on latency, distance, cost, number of hops, etc. This technique is widely used by providers to route users to the closest server. Since the IP is hosted in multiple geographic locations, there is no way to specify one single location to that IP.

This version introduces an option to bypass AnyCast IP ranges in Geo-IP blocking. ISDB contains a list of confirmed AnyCast IP ranges that can be used for this purpose.

When source/destination is set to `geoip`, you can enable the `geoip-anycast` option. When enabled, IPs where the AnyCast option is set to `1` in `geoip_db` are bypassed in country matching and blocking.

You can only use CLI to configure this feature. See the following example.

To enable `geoip-anycast` setting in a policy:

```
config firewall policy
   edit 1
      set name "policyid-1"
      set uuid dfcaec9c-e925-51e8-cf3e-fed9a1d42a1c
      set srcintf "wan2"
      set dstintf "wan1"
      set srcaddr "all"
      set dstaddr "test-geoip-CA_1"
      set action accept
      set schedule "always"
      set service "ALL"
      set geoip-anycast enable
      set logtraffic all
      set nat enable
   next
end
```

To check the `geoip-anycast` option for an IP address:

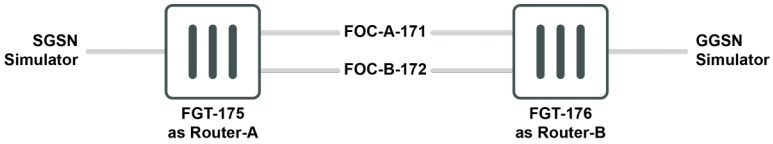
```
diag geoip ip2country 1.0.0.1
   1.0.0.1 - Australia, is anycast ip
```

`1.0.0.1` is the AnyCast IP.

GTP in Asymmetric Routing

FortiOS 6.2.0 improves communication for FortiGates acting as a GPRS Tunneling Protocol (GTP) firewall that is deployed in asymmetric routing environments. Previously in asymmetric routing environments, the `GTP-C` reply might be processed before the `GTP-C` request was fully synchronized by FortiGate Session Life Support Protocol (FGSP), which resulted in dropped sessions. With FortiOS 6.2.0, communication is improved by adding a new `set gtp-asym-fgsp` command in `system settings` that allows two members in FGSP to synchronize the `GTP-C` message.

Example



FOC-A-171 and FOC-B-172 are two FGSP members.

SGSN Simulator (10.1.100.60) generates a `GTP-C` request that is passed through FGT-175 to reach FGSP member FOC-A-171, but the response `GTP-C` from GGSN Simulator(172.16.200.61) is passed through FGT-176 to reach another FGSP member FOC-B-172. Previously in this asymmetric topology, FOC can't help establish the GTP tunnel between SGSN Simulator and GGSN Simulator.

However with the `set gtp-asym-fgsp` command, two members in FGSP can synchronize the `GTP-C` message. In both FOC-A-171 and FOC-B-172, when the `set gtp-asym-fgsp` command is enabled, the SGSN Simulator can obtain the correct tunnel private IP address(192.168.0.2) and establish the GTP tunnel with GGSN Simulator.

Check on the SGSN simulator:

```
root@mmsclient:~# sgsnemu -c /root/openggsn-0.84/examples/fgt_sgsnemu.conf &
[1] 5592
root@mmsclient:~# cmdline_parser_configfile
remote: 172.16.200.61
listen: 10.1.100.60
conf: /root/openggsn-0.84/examples/fgt_sgsnemu.conf
debug: 1
imsi: 310150123456789
qos: 0x0b921f
charging: 0x800
apn: internet
msisdn: 6044301297
uid: mig
pwd: hemmelig
pidfile: ./sgsnemu.pid
statedir: ./
contexts: 1
timelimit: 0
createif: 1
ipup: /etc/sgsnemu/ip-up
ipdown: /etc/sgsnemu/ip-down
defaultroute: 1
pingrate: 1
pingsize: 56
pingcount: 0
pingquiet: 0
Using default DNS server
Local IP address is:  10.1.100.60 (10.1.100.60)
Remote IP address is:  172.16.200.61 (172.16.200.61)
IMSI is:  310150123456789 (0xf987654321051013)
Using NSAPI:  0
Using GTP version:  1
Using APN:  internet
Using selection mode:  1
Using MSISDN:  6044301297
Initialising GTP library
openggsn[5592]: GTP: gtp_newgsn() started
```

```
Setting up interface
Done initialising GTP library
Sending off echo request
Setting up PDP context #0
Waiting for response from ggsn........
idletime.tv_sec 3, idleTime.tv_usec 0
Received echo response
idletime.tv_sec 3, idleTime.tv_usec 0
Received create PDP context response. IP address: 192.168.0.2 <--------NOTE
```

Check on FOC that the GTP tunnel was established successfully:

```
FOC-A-171(vdom1) # dia firewall gtp tunnel list
list gtp tunnels
-----------prof=gtpp ref=6 imsi=310150123456789 msisdn=6044301297 mei=unknown ms_
     addr=192.168.0.2 s11_s4 0-----------
-----------index=00000001 life=2082(sec) idle=41(sec) vd=3  ver=1-----------
c_pkt=4 c_bytes=506 u_pkt=0 u_bytes=0
downlink cfteid:
addr=10.1.100.60 teid=0x00000001 role=control vd=3 intf_type=gn-gp sgsn gtp-c
uplink cfteid:
addr=172.16.200.61 teid=0x00000001 role=control vd=3 intf_type=gn-gp ggsn gtp-c
1/1 bearers:
id=0 linked_id=0 type=regular dead=0 apn=internet selection=ms-provided-apn user_
     addr=192.168.0.2 u_pkt=0 u_bytes=0
2 fteids:
addr=10.1.100.60 teid=0x00000001 role=data vd=3 intf_type=gn-gp sgsn gtp-u
addr=172.16.200.61 teid=0x00000001 role=data vd=3 intf_type=gn-gp ggsn gtp-u
```

Firewall - Allow to Customize Default Service

This feature allows the default service port range to be customized using the following CLI command:

```
config system global
   set default-service-source-port <port range>
end
```

Where `<port range>` is the new default service port range, that can have a minimum value down to 0 and a maximum value up to 65535. The default value is 1-65535.

This change takes effect on the TCP/UDP protocol.

Firewall - Anti-Replay Option Per-Policy

When the global anti-replay option is disabled, the FortiGate does not check TCP flags in packets. This feature adds a per policy anti-replay option that overrides the global setting. This allows you to control whether or not TCP flags are checked per policy.

In this example, a policy is created with the anti-replay option enabled so that TCP flags are checked:

```
config firewall policy
   edit 1
      set name "policyid-1"
      set uuid dfcaec9c-e925-51e8-cf3e-fed9a1d42a1c
      set srcintf "wan2"
      set dstintf "wan1"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set anti-replay enable
      set logtraffic all
      set nat enable
   next
end
```

NTLM Extensions

FortiOS 6.2 extends agentless Windows NT LAN Manager (NTLM) authentication to include support for the following items:

- Multiple servers
- Individual users

Previously only one server and only group matching were supported.

You can now use multiple domain controller servers for the agentless NTLM for load balancing and high service stability.

You can also use user-based matching in groups for Kerberos and agentless NTLM. For Kerberos and agentless NTLM, FortiOS matches the user's group information from an LDAP server.

To support multiple domain controllers for agentless NTLM:

1. Configure an LDAP server:

```
config user ldap
   edit "ldap-kerberos"
      set server "172.18.62.177"
      set cnid "cn"
      set dn "dc=fortinetqa,dc=local"
      set type regular
      set username "CN=root,CN=Users,DC=fortinetqa,DC=local"
      set password ENC
           PD0++FaJxGwPta/dE4GFboqOJpk4WNHk12JAMBQrn6s3hkMWlhN+Hg36ULQOMl9/OvbJ7lJFgPnpFv8Z
           4QnZeBtzIcqenr2jmcYPTsbegmSjEPyO6/vl4rX5ZRfF2l3adKcCf56575TkRpIdlYELBpc44eNfoxA2
           KWqmANKkzOnv2w12eDEXanXkHaDgs8WBBnvZnQ==
   next
end
```

2. Configure multiple Domain Controllers:

```
config user domain-controller
   edit "dc1"
      set ip-address 172.18.62.177
      config extra-server
         edit 1
```

```
            set ip-address 172.18.62.220
         next
      end
      set ldap-server "ldap-kerberos"
   next
end
```

3. Create an authenticate scheme and rule:

```
config authentication scheme
   edit "au-ntlm"
      set method ntlm
      set domain-controller "dc1"
   next
end
config authentication rule
   edit "ru-ntlm"
      set srcaddr "all"
      set ip-based disable
      set active-auth-method "au-ntlm"
   next
end
```

4. In the proxy policy, append the user group for authorization:

```
config firewall proxy-policy
   edit 1
      set uuid 6cfe58e4-2ff1-51e9-6b4c-a7d4a8db0f30
      set proxy explicit-web
      set dstintf "port1"
      set srcaddr "all"
      set dstaddr "all"
      set service "web"
      set action accept
      set schedule "always"
      set groups "ldap-group"
      set utm-status enable
      set av-profile "av"
      set ssl-ssh-profile "deep-custom"
   next
end
```

This configuration uses a round-robin method. When the first user logs in, FortiGate sends the authentication request to the first domain controller. Later when another user logs in, FortiGate sends the authentication request to another domain controller. After the user successfully logs in, you can verify the behavior by using the following CLI:

```
FGT_A (vdom1) # diagnose wad user list
ID: 1825, IP: 10.1.100.71, VDOM: vdom1
   user name : test1
   duration : 497
   auth_type : Session
   auth_method : NTLM
   pol_id : 1 g_id : 5
   user_based : 0 e
   xpire : 103
   LAN:
      bytes_in=2167 bytes_out=7657
   WAN:
      bytes_in=3718 bytes_out=270
```

To support individual users for agentless NTLM:

1. Configure an LDAP server:
```
config user ldap
   edit "ldap-kerberos"
      set server "172.18.62.177"
      set cnid "cn"
      set dn "dc=fortinetqa,dc=local"
      set type regular
      set username "CN=root,CN=Users,DC=fortinetqa,DC=local"
      set password ENC
           PD0++FaJxGwPta/dE4GFboqOJpk4WNHk12JAMBQrn6s3hkMWlhN+Hg36ULQOMl9/OvbJ7lJFgPnpFv8Z
           4QnZeBtzIcqenr2jmcYPTsbegmSjEPyO6/vl4rX5ZRfF2l3adKcCf56575TkRpIdlYELBpc44eNfoxA2
           KWqmANKkzOnv2w12eDEXanXkHaDgs8WBBnvZnQ==
   next
end
```
2. Configure user group and allow user based matching in the group:
```
config user group
   edit "ldap-group"
      set member "ldap" "ldap-kerberos"
      config match
         edit 1
            set server-name "ldap-kerberos"
            set group-name "test1"
         next
      end
   next
end
```
3. Create an authentication scheme and rule:
```
config authentication scheme
   edit "au-ntlm"
      set method ntlm
      set domain-controller "dc1"
   next
end
config authentication rule
   edit "ru-ntlm"
      set srcaddr "all"
      set ip-based disable
      set active-auth-method "au-ntlm"
   next
end
```
4. In the proxy policy, append the user group for authorization:
```
config firewall proxy-policy
   edit 1
      set uuid 6cfe58e4-2ff1-51e9-6b4c-a7d4a8db0f30
      set proxy explicit-web
      set dstintf "port1"
      set srcaddr "all"
      set dstaddr "all"
      set service "web"
      set action accept
      set schedule "always"
      set groups "ldap-group"
      set utm-status enable
      set av-profile "av"
```

```
      set ssl-ssh-profile "deep-custom"
   next
end
```

This implementation lets you configure a single user instead of a whole group, and FortiGate will allow user named test1. You can verify the configuration by using the CLI:

```
diagnose wad user list
   ID: 1827, IP: 10.1.15.25, VDOM: vdom1
   user name : test1
   duration : 161
   auth_type : Session
   auth_method : NTLM
   pol_id : 1
   g_id : 5
   user_based : 0
   expire : 439
   LAN:
      bytes_in=1309 bytes_out=4410
   WAN:
      bytes_in=2145 bytes_out=544
```

Option to Disable Stateful SCTP Inspection

You now have the option to disable stateful SCTP inspection. This option is useful when FortiGates are deployed in a High Availability (HA) cluster that uses the FortiGate Clustering Protocol (FGCP) and virtual clustering in a multihoming topology. In this configuration, the primary Stream Control Transmission Protocol (SCTP) path traverses the master FortiGate node by using its active VDOM (for example, VDOM1), and the backup SCTP path traverses the other passive FortiGate node by using its active VDOM (for example VDOM2).

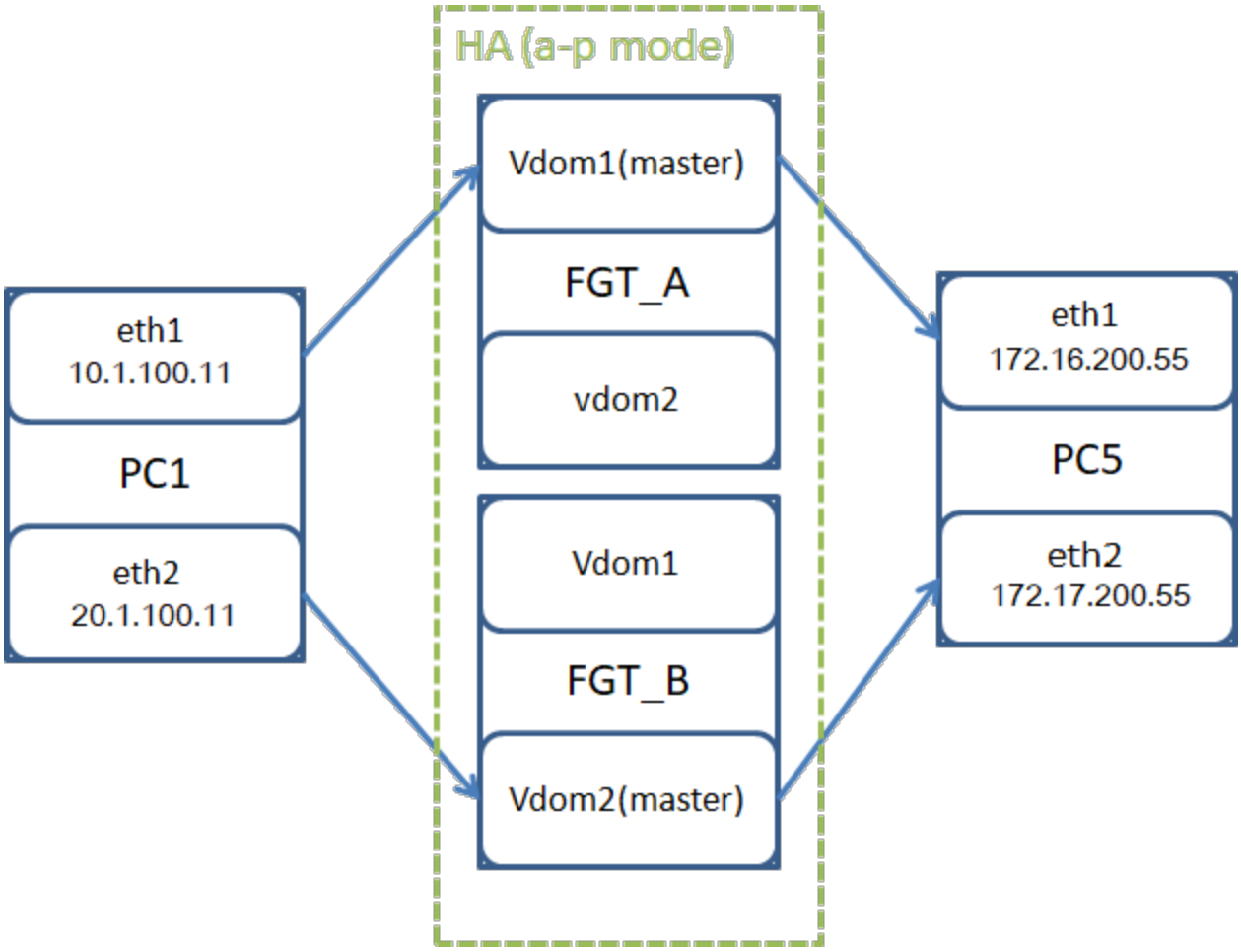
When stateful SCTP inspection is enabled, SCTP heartbeat traffic will fail via the backup path because the primary path goes through a different platform and VDOM. Since there is no state sharing between VDOMs, the passive FortiGate is not aware of the original SCTP session and drops the heartbeats because of no associated sessions.

You can now use the following command to disable stateful inspection of SCTP, which allows the passive node to permit the SCTP heartbeats to pass:

```
config sys settings
   set sctp-session-without-init enable
end
```

When set to `enable`, SCTP session creation without SCTP INIT is enabled. When set to `disable`, SCTP session creation without SCTP INIT is disabled. The default setting is disabled.

Following is an example topology and scenario:



In this example, FGT_A and FGT_B are in HA a-p mode with two virtual clusters. Two masters exist on different FortiGate units. PC1 eth1 can access PC5 eth1 through Vdom1, and PC1 eth2 can access PC5 eth2 through Vdom2.

On PC5, listening for SCTP connection:

```
sctp_darn -H 172.16.200.55 -B 172.17.200.55 -P 2500 -l
```

On PC1, start SCTP connection:

```
sctp_darn -H 10.1.100.11 -B 20.1.100.11 -P 2600 -c 172.16.200.55 -c 172.17.200.55 -p 2500 -s
```

SCTP 4-way handshake is on one VDOM, and a session is created on that VDOM. With the default configuration, there is no session on any other VDOM, and the heartbeat on another path (another VDOM) is dropped. After enabling `sctp-session-without-init`, the other VDOM creates the session when it receives the heartbeat, and the heartbeat is forwarded.

Option to Fragment IP Packets Before IPSec Encapsulation

A new `ip-fragmentation` option has been added to control fragmentation of packets before IPsec encapsulation, which can benefit packet loss in some environments.

The following options are available for the `ip-fragmentation` variable:

Option	Description
pre-encapsulation	Fragment before IPsec encapsulation.
post-encapsulation (default value)	Fragment after IPsec encapsulation (RFC compliant).

You can only control this option using the CLI:

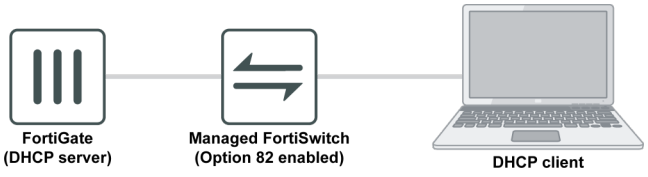
```
config vpn ipsec phase1-interface
   edit "demo"
      set interface "port1"
      set authmethod signature
      set peertype any
      set net-device enable
      set proposal aes128-sha256 aes256-sha256 aes128-sha1 aes256-sha1
      set ip-fragmentation pre-encapsulation
      set remote-gw 172.16.200.4
      set certificate "Fortinet_Factory"
   next
end
```

DHCP Relay Agent Information Option

This feature adds DHCP option 82 (DHCP relay information option). It can help protect the FortiGate against attacks such as spoofing (or forging) of IP and MAC addresses, and DHCP IP address starvation.

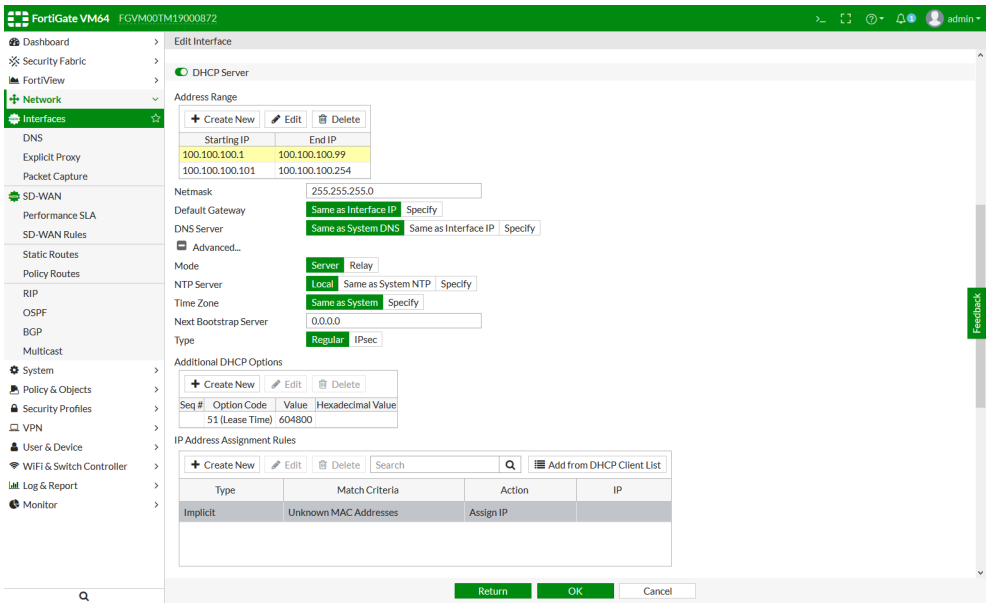
The following CLI variables are added to or modified in the `config system dhcp server` > `config reserved-address` command:

`circuit-id-type {hex | string}`	DHCP option type, hex or string (default).
`circuit-id <value>`	Option 82 circuit ID of the client that will get the reserved IP address. Format: *vlan-mod-port* • vlan: VLAN ID (2 bytes) • mod: 1 = snoop, 0 = relay (1 byte) • port: port number (1 byte)
`remote-id-type {hex | string}`	DHCP option type, hex or string (default).
`remote-id <value>`	Option 82 remote ID of the client that will get the reserved IP address. Format: the MAC address of the client.
`type {mac | option82}`	The DHCP reserved-address type, either mac (default) or option82 (newly added).

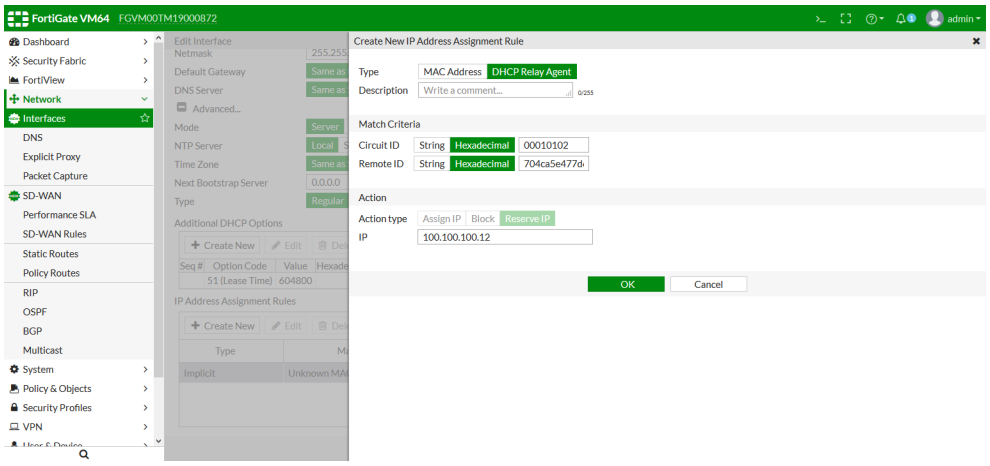


To create an IP address assignment rule using option 82 in the GUI:

1. On the FortiGate, go to *Network* > *Interfaces*.
2. Edit and existing port, or create a new one.
3. Ensure that the *Role* is either *LAN* or *Undefined*.
4. Enable *DHCP Server*.
5. Configure address ranges and other settings as needed.



6. In the *IP Address Assignment Rules* table, click *Create New*. The *Create New IP Address Assignment Rule* pane opens.
7. For the *Type*, select *DHCP Relay Agent*.



8. Enter the *Circuit ID*, *Remote ID*, and the *IP* address that will be reserved.
9. Click *OK* to create the rule.

To create an IP address assignment rule using option 82 with the CLI:

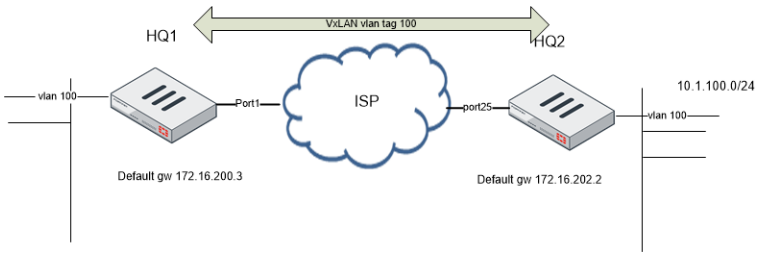
```
config system dhcp server
    edit 1
```

```
        set netmask 255.255.255.0
        set interface "port4"
        config ip-range
            edit 1
                set start-ip 100.100.100.1
                set end-ip 100.100.100.99
            next
            edit 2
                set start-ip 100.100.100.101
                set end-ip 100.100.100.254
            next
        end
        config reserved-address
            edit 1
                set type option82
                set ip 100.100.100.12
                set circuit-id-type hex
                set circuit-id "00010102"
                set remote-id-type hex
                set remote-id "704ca5e477d6"
            next
        end
    next
end
```

VLAN Inside VXLAN

In this version, VLANs can be assigned to VXLAN interfaces.

In a data center network where VxLAB is used to create a L2 overlay network and for multi-tenant environment, a customer VLAN tag needs to be kept on VXLAN tunnel. This version introduces a solution where the VLAN tag can be assigned to VXLAN interface.



You can only use CLI to configure this feature. See the following example.

To configure VLAN inside VXLAN:

1. Configure VXLAN.

```
config system vxlan
   edit vxlan1
      set interface port1
      set vni 1000
      set remote-ip 172.16.200.3
```

```
    next
end
```

2. Configure system interface.

```
config system interface
   edit vlan100
     set vdom root
     set vlanid 100
     set interface dmz
   next
   edit vxlan100
     set type vlan
     set vlanid 100
     set vdom root
     set interface vxlan1
   next
end
```

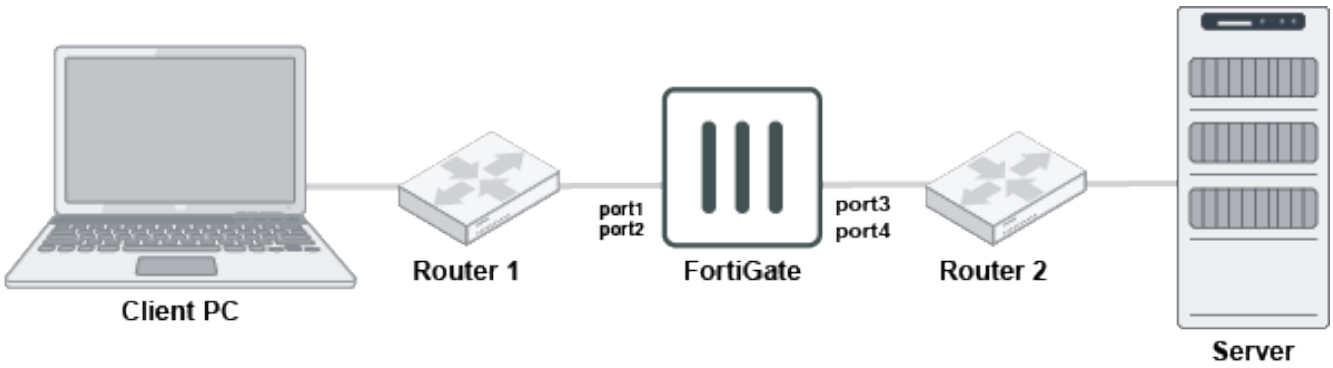
3. Configure software-switch.

```
config system switch-interface
  edit sw1
    set vdom root
    set member vlan100 vxlan100
  next
end
```

ECMP Acceleration in NAT Mode

In 6.0, Equal-Cost Multi-Path (ECMP) traffic is not offloaded to the NP6 processor in NAT mode. This is now supported in 6.2.

Topology



Set up ECMP for both client and server on FortiGate. FortiGate uses ECMP through port1 (p1) and port2 (p2) to the client and ECMP through port 3 (p3) and port 4 (p4) to the server.

Example

This example demonstrates how the feature works.

Session one

This session demonstrates symmetric traffic with symmetric routing. No auxiliary session for the initial session.

Set the priority in the static route to prefer p1 to p3 and reply p3 to p1. Verify that the session can be established and offloaded to the NP6 processor and that session counters are correctly reflecting the status of the session.

```
session info: proto=17 proto_state=00 duration=27 expire=473 timeout=500 flags=00000000
      sockflag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu route_preserve
statistic(bytes/packets/allow_err): org=60/2/1 reply=0/0/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=37->38/38->37 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.1.100.22:35101->172.16.204.44:5001(0.0.0.0:0)
hook=post dir=reply act=noop 172.16.204.44:5001->10.1.100.22:35101(0.0.0.0:0)
src_mac=90:6c:ac:19:19:58
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=2
serial=00001c8e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000400
npu info: flag=0x91/0x00, offload=8/0, ips_offload=0/0, epid=129/0, ipid=142/0,
      vlan=0x0017/0x0000
vlifid=142/0, vtag_in=0x0017/0x0000 in_npu=1/0, out_npu=1/0, fwd_en=0/0, qid=7/0
no_ofld_reason:
total session 1
```

Session two

Keep session one alive in the session table. Change the UDP session from client to server through p2, p3, unidirectional. Verify that a new auxiliary session can be established and offloaded to the NP6 processor and that session counters are correctly reflecting the status of session.

```
session info: proto=17 proto_state=00 duration=241 expire=495 timeout=500 flags=00000000
      sockflag=00000000 sockport=0 av_idx=0 use=5
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu route_preserve
statistic(bytes/packets/allow_err): org=126/4/1 reply=0/0/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=37->38/38->37 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.1.100.22:35101->172.16.204.44:5001(0.0.0.0:0)
hook=post dir=reply act=noop 172.16.204.44:5001->10.1.100.22:35101(0.0.0.0:0)
src_mac=90:6c:ac:19:19:58
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=2
serial=00001c8e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
```

```
dd_type=0 dd_mode=0
npu_state=0x000400
npu info: flag=0x91/0x00, offload=8/0, ips_offload=0/0, epid=129/0, ipid=142/0,
     vlan=0x0017/0x0000
vlifid=142/0, vtag_in=0x0017/0x0000 in_npu=1/0, out_npu=1/0, fwd_en=0/0, qid=7/0
no_ofld_reason:
reflect info 0:
dev=36->38/38->36
npu_state=0x000400
npu info: flag=0x91/0x00, offload=8/0, ips_offload=0/0, epid=129/0, ipid=142/0,
     vlan=0x0016/0x0000
vlifid=142/0, vtag_in=0x0016/0x0000 in_npu=1/0, out_npu=1/0, fwd_en=0/0, qid=7/0
total reflect session num: 1
total session 1
```

Reply traffic through p4

Keep sessions one and two alive. Send reply traffic from server to client in the sessions one and two through p4 to p1/p2. Verify that new auxiliary sessions can be established and offloaded to the NP6 processor and that session counters correctly reflect the status of session.

```
session info: proto=17 proto_state=01 duration=356 expire=497 timeout=500 flags=00000000
     sockflag=00000000 sockport=0 av_idx=0 use=6
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty npu route_preserve
statistic(bytes/packets/allow_err): org=126/4/1 reply=66/2/1 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=37->38/38->37 gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 10.1.100.22:35101->172.16.204.44:5001(0.0.0.0:0)
hook=post dir=reply act=noop 172.16.204.44:5001->10.1.100.22:35101(0.0.0.0:0)
src_mac=90:6c:ac:19:19:58
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=2
serial=00001c8e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000400
npu info: flag=0x91/0x00, offload=8/0, ips_offload=0/0, epid=129/0, ipid=142/0,
     vlan=0x0017/0x0000
vlifid=142/0, vtag_in=0x0017/0x0000 in_npu=1/0, out_npu=1/0, fwd_en=0/0, qid=7/0
no_ofld_reason:
ofld_fail_reason(kernel, drv): none/not-established, none(0)/none(0)
npu_state_err=00/04
reflect info 0:
dev=36->39/39->36
npu_state=00000000
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag_in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
reflect info 1:
dev=36->38/38->36
npu_state=0x000400
npu info: flag=0x91/0x00, offload=8/0, ips_offload=0/0, epid=129/0, ipid=142/0,
     vlan=0x0016/0x0000
vlifid=142/0, vtag_in=0x0016/0x0000 in_npu=1/0, out_npu=1/0, fwd_en=0/0, qid=7/0
total reflect session num: 2
```

```
total session 1
```

Reply traffic through p3

Send reply traffic from the server to the client in the same sessions through p3 to p1/p2. Verify that no auxiliary sessions are created, sessions can be offloaded to the NP6 processor, and session counters correctly reflect the status of session.

Offloading

The main session and the auxiliary session can be offloaded to the NP6 processor, if the policy allows offloading.

Custom SIP RTP Port Range Support

A new `nat-port-range` attribute can be used to specify a port range in the Voice Over Internet Protocol (VoIP) profile to restrict the Network Address Translation (NAT) port range for Real-Time Transport Protocol/Real-Time Transport Control Protocol (RTP/RTCP) packets in a Session Initiation Protocol (SIP) call session that is handled by the SIP ALG (Application Layer Gateway) in a FortiGate device.

When NAT is enabled or VIP is used in a firewall policy for SIP ALG to handle a SIP call session established through a FortiGate device, the SIP ALG can perform NAT to translate the ports used for the RTP/RTCP packets when they are flowing through the device between the external and internal networks.

Previously, you could not configure the translated port range, and the fixed port range was [5117-65533]. Now you can control the translated port range for RTP/RTCP packets by using the CLI:

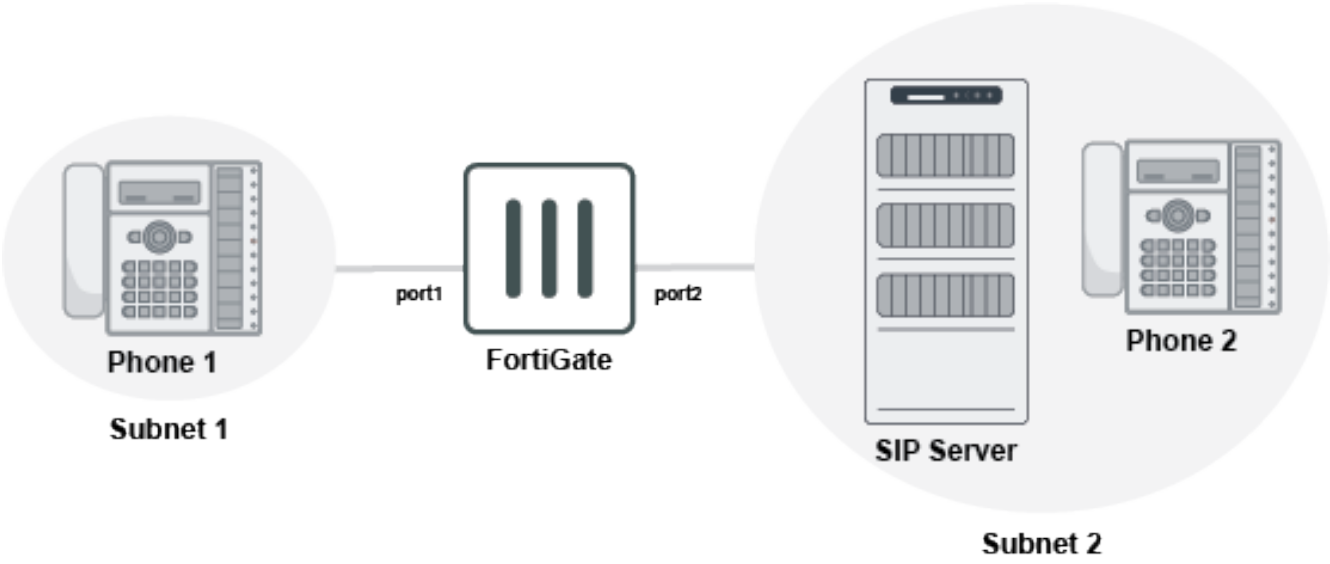
```
config voip profile
   edit <profile-name>
      config sip
         set nat-port-range <start_port_number>-<end_port_number>
      end
   next
end
FGT(sip) # set nat-port-range ?
<start>-<end>    NAT port range (default 5117-65533)
A valid port range must be configured within [5117-65533]. For example: set nat-port-range
      30000-30099 .
```

Example

This section provides an example for NAT where Phone1 is in subnet_1, and the SIP server and phone are in subnet_2. All SIP signaling messages and RTP/RTCP packets will go through the SIP Server. In this example, the RTP/RTCP ports on Phone1 are configured as 17078/17079.

The FortiGate administrator wants to use NAT for the port 17078/17079 to 30000/30001. As a result, all RTP/RTCP packets going out of port2 have source ports of 30000/30001, and all RTP/RTCP packets going into port2 have destination ports of 30000/30001 too, which can be specified in the nat-port-range.

The topology is shown as follows:



The configuration is as follows:

```
config voip profile
   edit "natPortRange"
         config sip
            set nat-port-range 30000-30001  <---------------------------------
         end
   next
end
configure firewall policy
   edit 1
         set srcintf port1
         set  dstintf port2
         set srcaddr all
         set dstaddr all
         set service SIP
         set action accept
         set schedule always
         set voip-profile natPortRange  <---------------------
         set nat enable  <---------------------
end
```

Now if phone1 and phone2 are registered to the SIP server, and they establish a call session between them through the FortiGate and the SIP server, then the RTP/RTCP ports 17078/17079 of phone1 will be NATed to 30000/30001 at the FortiGate unit based on the setting of nat-port-range. That is, the RTP/RTCP packets egressing port2 of the Fortigate will have the source port as 30000/30001, and the RTP/RTCP packets ingressing port2 will have the destination port as 30000/30001.

Custom Service Max Value Increase

In FortiOS 6.2.0, the number of custom services is increased on all FortiGate 100-series platforms and above. The following table identifies that maximum number of custom services supported for the different types of FortiGate model series:

FortiGate Model	Maximum Number of Custom Services
FortiGate 100 series and lower	1024 (no change)
FortiGate 100 to 400 series	2048
FortiGate 500 - 1200 series	4096
Two rack units	10240
Three rack units and chassis	16348

FortiCarrier License Activation

In FortiOS 6.0.x, when applying the FortiCarrier license, the FortiCarrier configuration is reset to the factory default settings. With FortiOS 6.2.0 and later, the basic system, interface, and routing settings are retained to avoid a full factory reset.

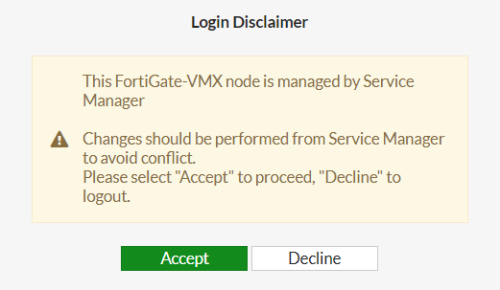
When you load a FortiCarrier license to FortiOS, the following message is displayed, informing you what settings are retained and not returned to factory default settings:

```
FortiGate-3000D (global) # execute forticarrier-license DD4K-PVIQ-TEXX-OHAM-XO5T-CHJG-ZQ
This operation will reset the system to factory default except system.global.vdom-
     mode/system.global.long-vdom-
     name/VDOMs/system.interface/system.settings/router.static/router.static6!
Do you want to continue? (y/n)
```

GUI Alert on Login to VMX Security Nodes

This version displays a warning on VMware NSX-V security nodes that VMX nodes are managed by SVM and to make all configuration changes on SVM. Changing configurations on each node might cause inconsistencies so you must use SVM as a single point of configuration changes.

This is a sample of the alert:



To view or configure this alert using CLI:

```
FortiGate-VMX # config global

FortiGate-VMX (global) # config sys replacemsg admin pre_admin-disclaimer-text
```

```
FortiGate-VMX (pre_admin-discla~ext) # unset buffer

FortiGate-VMX (pre_admin-discla~ext) # get
msg-type            : pre_admin-disclaimer-text
buffer              : This FortiGate-VMX node is managed by Service Manager

Changes should be performed from Service Manager to avoid conflict.
Please select Accept to proceed, Decline to logout.

header              : none
format              : text
```