FortiOS - New Features Guide

Version 6.2.2

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 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: techdoc@fortinet.com

January 21, 2020
FortiOS 6.2.2 New Features Guide
01-622-538749-20200121

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-10-09	Initial release.
2019-10-25	Added IPsec VPN wizard hub-and-spoke ADVPN support on page 58. Added CPU only licensing for private clouds on page 37. Added VMware NSX-T managed by FortiManager on page 13.
2019-11-04	Added FortiGuard third Party SSL validation and Anycast support on page 67.
2019-11-06	Added Configuring single-sign-on in the Security Fabric on page 6.
2019-11-12	Added IPv6 FortiGuard connections on page 63.
2019-11-19	Updated FortiCare-generated license adoption for AWS PAYG variant on page 36.
2019-11-29	Added FortiClient EMS Cloud support on page 69.
2020-01-21	Added Virtual switch support for FortiGate 300E series on page 56.

Expanding fabric family

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

Configuring single-sign-on in the Security Fabric

In FortiOS 6.2.2, you can configure single-sign-on settings in the *Security Fabric* GUI menu. Prior to FortiOS 6.2.2, these settings were configured in the *User & Device* GUI menu.

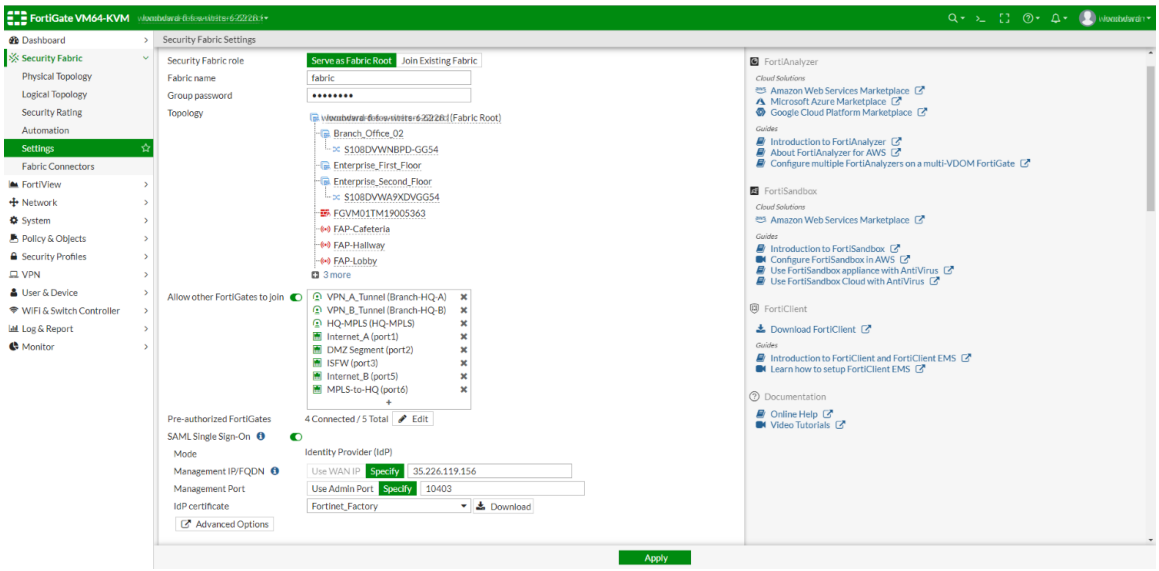
Only the root FortiGate can be the identity provider (IdP). The downstream FortiGates can be configured as service providers (SP).

Configuring the root FortiGate

To configure the root FortiGate as the IdP:

1. Log in to the root FortiGate.
2. Go to *Security Fabric* > *Settings*.
3. In the *FortiGate Telemetry* section, enable *SAML Single Sign-On*. The *Mode* field is automatically populated as *Identity Provider (IdP)*.
4. Enter an IP address in the *Management IP/FQDN* box.
5. Enter a management port in the *Management Port* box.
   The *Management IP/FQDN* will be used by the SPs to redirect the login request. The *Management IP/FQDN* and *Management Port* must be reachable from the user's device.
6. Select the *IdP certificate*.

7. Click *Apply*.

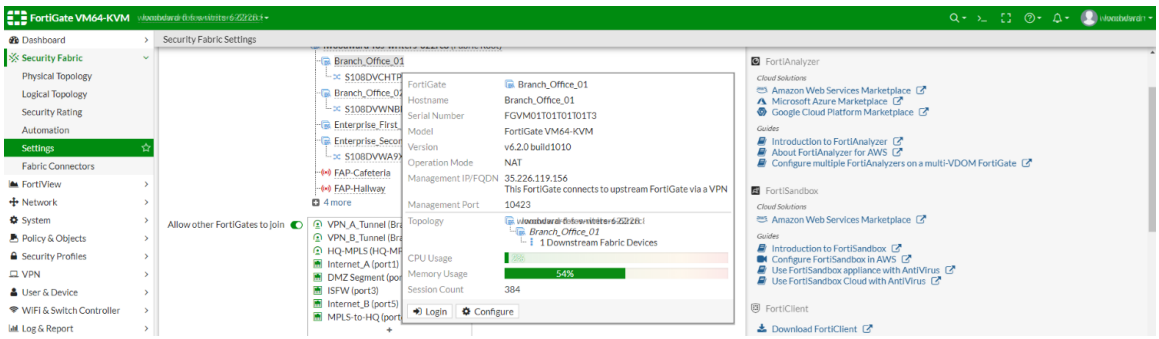


Configuring a downstream FortiGate as an SP

An SP must be a member of the Security Fabric before you configure it.

To configure the downstream FortiGate from the root FortiGate:

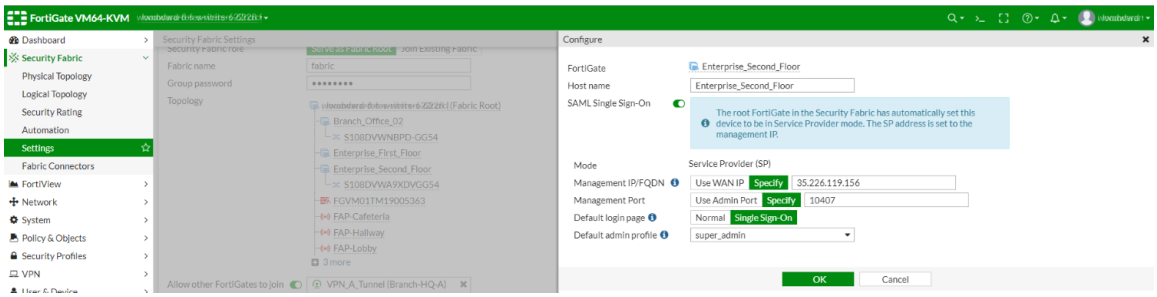
1. Log in to the root FortiGate.
2. Go to *Security Fabric* > *Settings* and locate the *Topology* section.
3. Hover over a FortiGate and click *Configure*.



The *Configure* pane opens.

4. Enable *SAML Single Sign-On*. The *Mode* field is automatically populated as *Service Provider (SP)*.
5. Enter an IP address in the *Management IP/FQDN* box.
6. Enter a management port in the *Management Port* box.
   The *Management IP/FQDN* will be used by the IdP and so other SPs can redirect to each other. The *Management Port* must be reachable from the user's device.

7. Select a *Default login page* option.
8. Select one of the following *Default admin profile* types: *prof_admin*, *super_admin*, or *super_admin_readonly*. The *no_access_admin profile* is set as the default.
9. Click *OK*.



To configure the downstream FortiGate within the device:

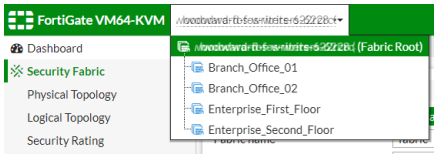
1. Log in to the downstream FortiGate.
2. Go to *Security Fabric* > *Settings*.
3. In the *FortiGate Telemetry* section, enable *SAML Single Sign-On*. The *Mode* field is automatically populated as *Service Provider (SP)*.
4. Enter an IP address in the *Management IP/FQDN* box.
5. Enter a management port in the *Management Port* box.
   The *Management IP/FQDN* will be used by the IdP and so other SPs can redirect to each other. The *Management Port* must be reachable from the user's device.
6. Select a *Default login page* option.
7. Select one of the following *Default admin profile* types: *prof_admin*, *super_admin*, or *super_admin_readonly*. The *no_access_admin profile* is set as the default.
8. Click *OK*.

Verifying the single-sign-on configuration

After you have logged in to a Security Fabric member using SSO, you can navigate between any Security Fabric member with SSO configured.

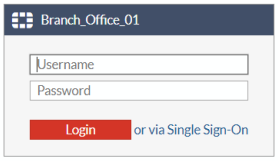
To navigate between Security Fabric members:

1. Log in to a Security Fabric member that is using SSO.
2. In the top banner, click the name of the device you are logged in to. A list of Security Fabric members displays.



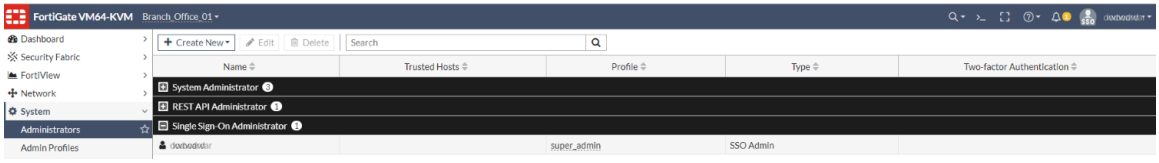
3. Click a Security Fabric member. The login page appears.

4. Select the option to log in *via Single-Sign-On*.



You are now logged in to the Security Fabric member with SSO. The letters "SSO" also display beside the user name in the top banner.

5. Go to *System* > *Administrators* > *Single-Sign-On Administrator* to view the list of SSO admins created.



FSSO dynamic address subtype

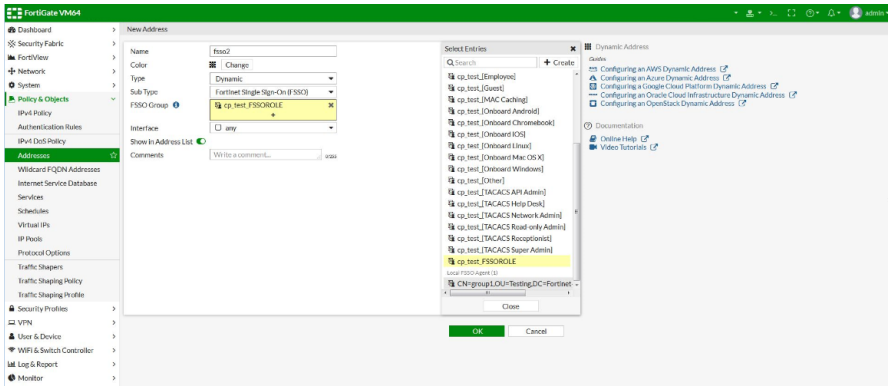
This new feature introduces a subtype for dynamic firewall address objects called *Fortinet Single Sign-On (FSSO)*. It can be used in all policies that support dynamic address types.

The FSSO dynamic address subtype can be used with FSSO group information being forwarded by ClearPass Policy Manager (CPPM) via FortiManager. The FortiGate will update dynamic address used in firewall policies based on source IP information for authenticated FSSO users.

It also can be used with other FSSO groups provided by the FSSO collector agent or FortiNAC.

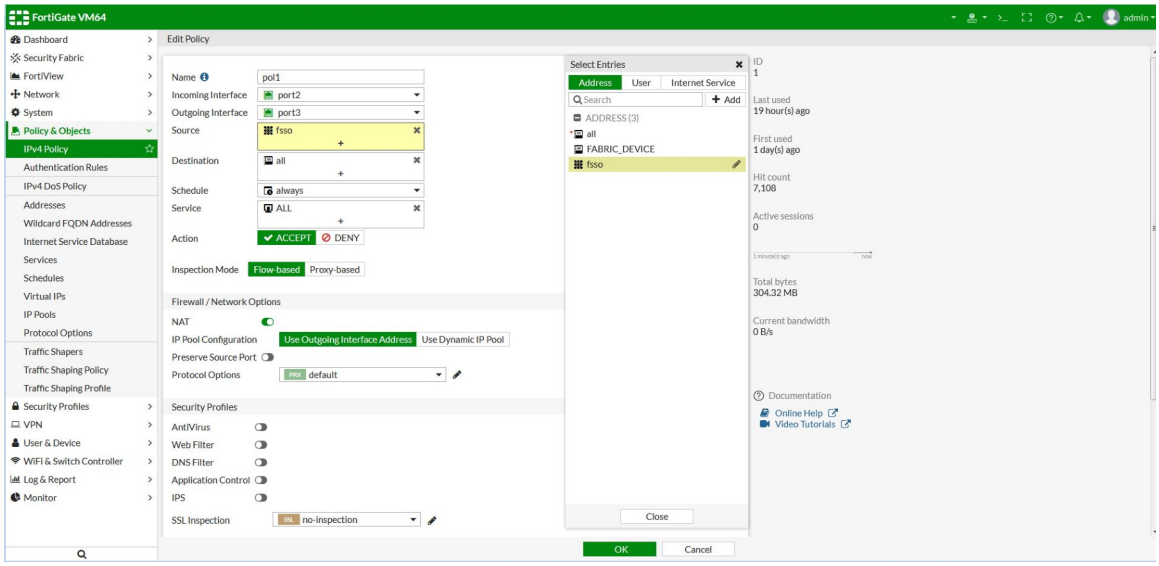
To configure FSSO dynamic addresses with CPPM and FortiManager in the GUI:

1. Create the dynamic address object:
   a. Go to *Policy & Objects* > *Addresses* > *Create New* > *Address*.
   b. For *Type*, select *Dynamic*.
   c. For *Sub Type*, select *Fortinet Single Sign-On (FSSO)*. The *Select Entries* pane opens and displays all available FSSO groups.
   d. Select one or more groups.
   e. Click *OK* to save the configuration.

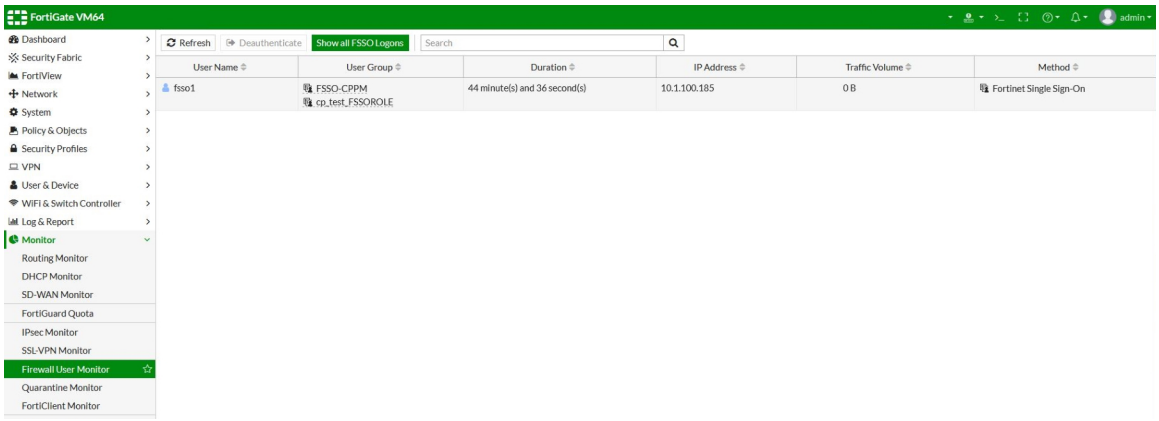


When the address table appears, there will be an error message for the address you just created (*Unresolved dynamic address: fsso*). This is expected because there are currently no authenticated FSSO users (based on source IP) in the local FSSO user list.

2. Add the dynamic address object to a firewall policy:
   a. Go to *Policy & Objects* > *IPv4 Policy*.
   b. Create a new policy or edit an existing policy.
   c. For *Source*, add the dynamic FSSO address object you just created.
   d. Configure the rest of the policy as needed
   e. Click *OK* to save your changes.

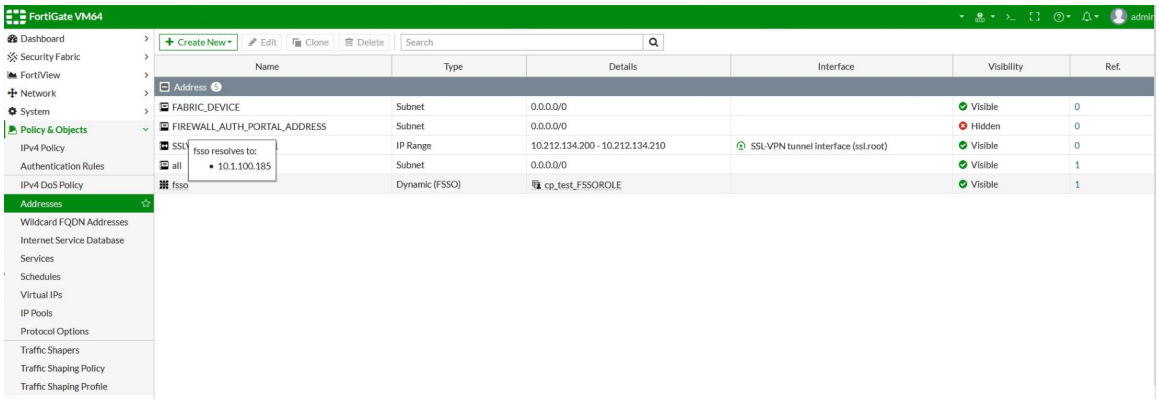


3. Test the authentication to add a source IP address to the FSSO user list:
   a. Log in as user and use CPPM for user authentication to connect to an external web server. After successful authentication, CPPM forwards the user name, source IP address, and group membership to the FortiGate via FortiManager.
   b. Go to *Monitor* > *Firewall User Monitor* to view the user name (*fsso1*) and IP address.



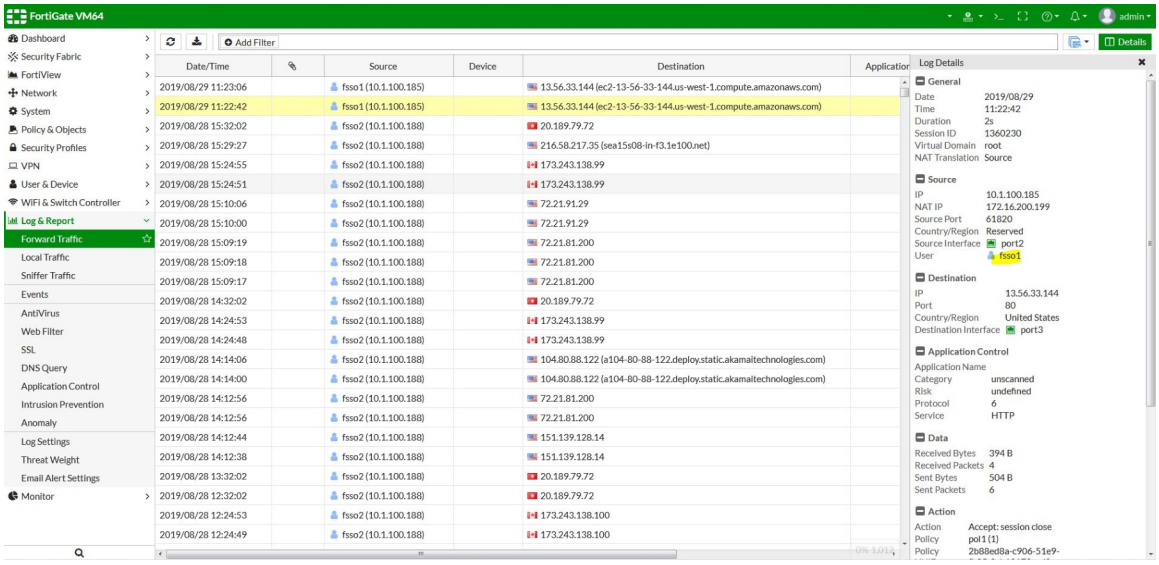
   c. Go to *Policy & Objects* > *Addresses* to view the updated address table. The error message no longer appears.

d. Hover over the dynamic FSSO address to view the IP address (*fsso resolves to: 10.1.100.185*).

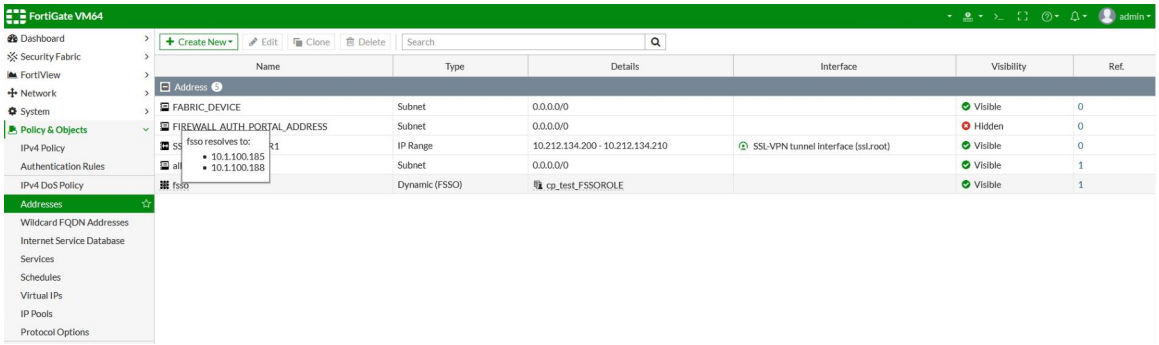


To verify user traffic in the GUI:

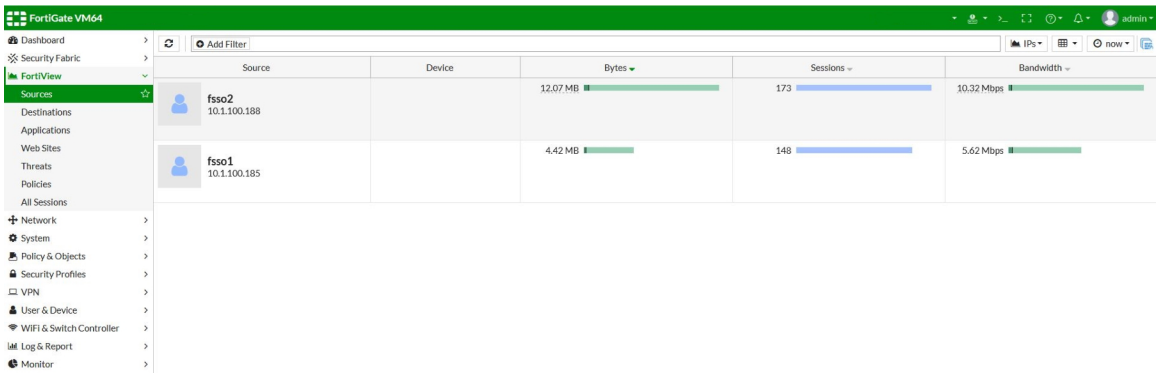
1. Go to *Log & Report* > *Forward Traffic*.
   Details for the user *fsso1* are visible in the traffic log:



- If another user is authenticated by CPPM, then the dynamic address *fsso* entry in the address table will be updated. The IP address for user *fsso2* (*10.1.100.188*) is now visible:



2. Go to *FortiView* > *Sources* to verify that the users were able to successfully pass the firewall policy.



If a user logs off and CPPM receives log off confirmation, then CPPS updates the FortiGate FSSO user list via FortiManager. The user IP address is deleted from the dynamic FSSO address, and the user is no longer be able to pass the firewall policy.

To configure FSSO dynamic addresses with CPPM and FortiManager in the CLI:

1. Create the dynamic address object:

```
config firewall address
    edit "fsso"
        set uuid 6f63c872-c90b-51e9-ebfd-16c18807c795
        set type dynamic
        set sub-type fsso
        set fsso-group "cp_test_FSSOROLE"
    next
end
```

2. Add the dynamic address object to a policy:

```
config firewall policy
    edit 1
        set name "pol1"
        set uuid 2b88ed8a-c906-51e9-fb25-8cb12172acd8
        set srcintf "port2"
        set dstintf "port3"
        set srcaddr "fsso"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set fsso disable
        set nat enable
    next
end
```

To verify user traffic in the CLI:

1. Check the FSSO user list:

```
diagnose debug authd fsso list
----FSSO logons----
IP: 10.1.100.185  User: fsso1  Groups: cp_test_FSSOROLE  Workstation:  MemberOf: FSSO-CPPM
cp_test_FSSOROLE
Total number of logons listed: 1, filtered: 0
----end of FSSO logons----
```

2. Check the authenticated firewall users list:

```
diagnose firewall auth list
10.1.100.185, fsso1
type: fsso, id: 0, duration: 2928, idled: 2928
server: FortiManager
packets: in 0 out 0, bytes: in 0 out 0
group_id: 2 33554433
group_name: FSSO-CPPM cp_test_FSSOROLE
----- 1 listed, 0 filtered ------
```

- After user traffic passes through the firewall, the number of packets in and out should increase:

```
diagnose firewall auth list
10.1.100.185, fsso1
type: fsso, id: 0, duration: 3802, idled: 143
server: FortiManager
packets: in 1629 out 1817, bytes: in 2203319 out 133312
group_id: 2 33554433
group_name: FSSO-CPPM cp_test_FSSOROLE
----- 1 listed, 0 filtered ------
```

VMware NSX-T managed by FortiManager

FortiGate-VM can receive dynamic FSSO addresses, along with address settings in firewall policies, pushed by the FortiManager.

The FortiManager retrieves groups from VMware NSX-T manager and stores them as dynamic firewall address objects. The FortiGate-VM that is deployed by the registered VMware NSX-T service then connects to the FortiManager to receive the dynamic objects.

For more information, see VMware NSX-T connector in the FortiManager New Features Guide.

To configure a VMware NSX-T connector on a FortiManager and send dynamic FSSO firewall addresses to a managed FortiGate:

1. Enable read-write JSON API access on the FortiManager
2. Create an NSX-T connector on the FortiManager
3. Create a dynamic FSSO address on the FortiManager
4. Create a firewall policy with the dynamic FSSO address on the FortiManager
5. Install the firewall policy to the FortiGate from the FortiManager

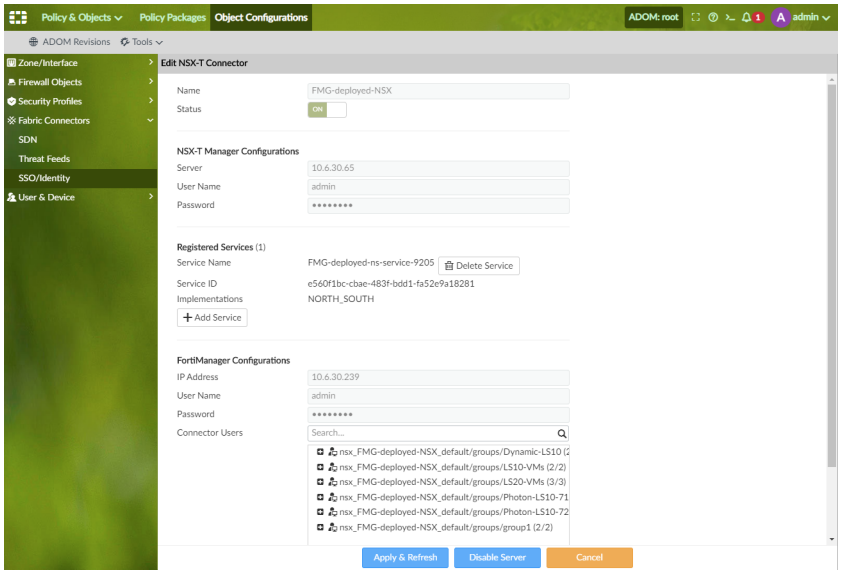
6. Confirm that the firewall policy with the address option was pushed to the FortiGate
7. Confirm that the FortiGate received the dynamic FSSO address

To enable read-write JSON API access:

1. Go to *System Settings* > *Admin* > *Administrators*.
2. Edit the administrator.
3. For *JSON API Access*, select *Read-Write*.
4. Click *OK*.

To create an NSX-T connector on the FortiManager:

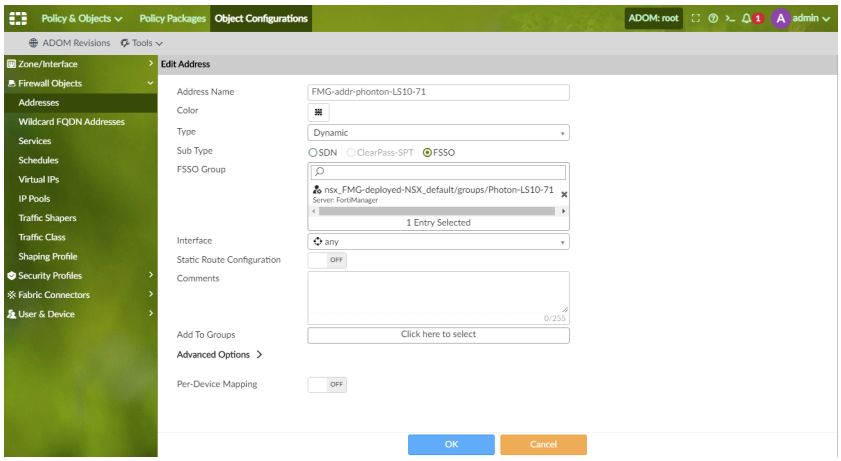
1. Go to *Policy & Objects* > *Object Configurations* > *Fabric Connectors* > *SSO/Identity*.
2. Click *Create New* > *NSX-T Connector*.
   Only one NSX-T connector can be created per ADOM.



3. Configure the *NSX-T Manager Configurations* settings.
4. Configure the *FortiManager Configurations* settings.
5. Click *Apply & Refresh*.
6. Ensure that there is a password for FortiManager.
7. Add a service:
   a. Click *Add Service*.
   b. Enter a *Service Name* and select the *Integration* to identify the flow of traffic
   c. Set the *Image Location* to the URL where the preconfigured FortiGate VM deployment image is located.
   d. Click *OK*.
8. Click *Apply & Refresh*.

To create a dynamic FSSO address on the FortiManager:

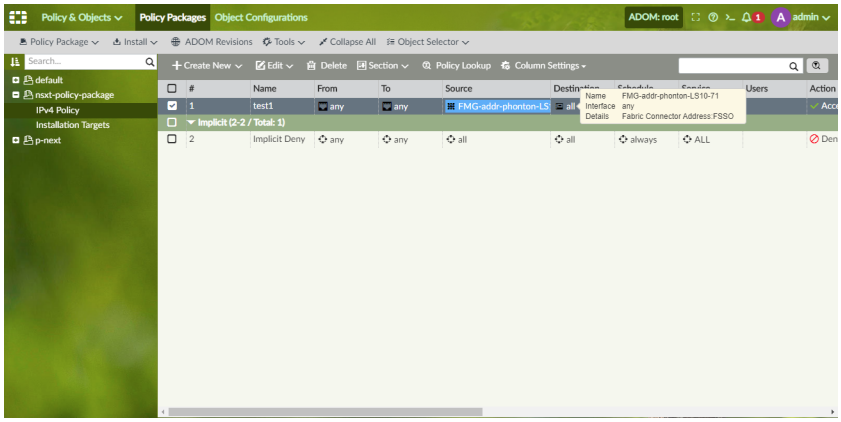
1. Go to *Policy & Objects* > *Object Configurations* > *Firewall Objects* > *Addresses*.
2. Click *Create New* > *Address*.



3. Set *Type* to *Dynamic*.
4. Set *Sub Type* to *FSSO*.
5. For the *FSSO Group*, select the group defined on the NSX-T manager.
6. Click *OK*.

To create a firewall policy with the dynamic FSSO address on the FortiManager:

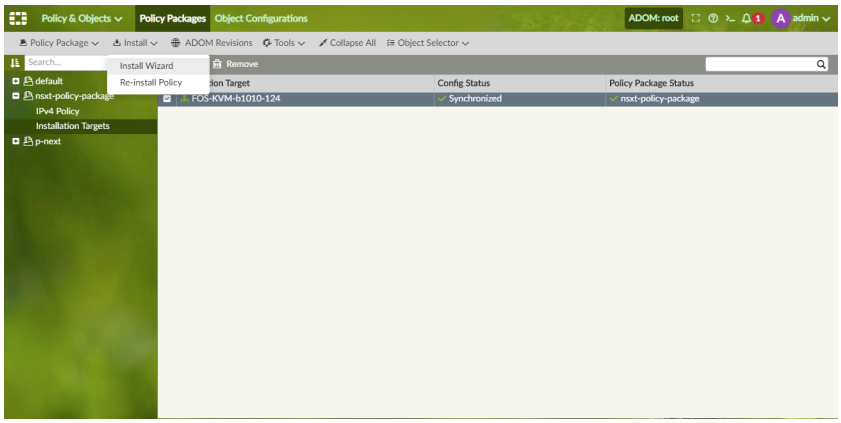
1. Go to *Policy & Objects* > *Policy Packages*.
2. Select the policy package and go to *IPv4 Policy*.
3. Click *Create New*.
4. Set the *Source Address* to the dynamic FSSO address.
5. Configure the remaining settings as needed, then click *OK*.



To install the firewall policy to the FortiGate from the FortiManager:

1. Go to *Policy & Objects* > *Policy Packages*.
2. Select the policy package and go to *Installation Targets*.
3. Click *Add* and add the FortiGate as a target if it is not already listed as a target.

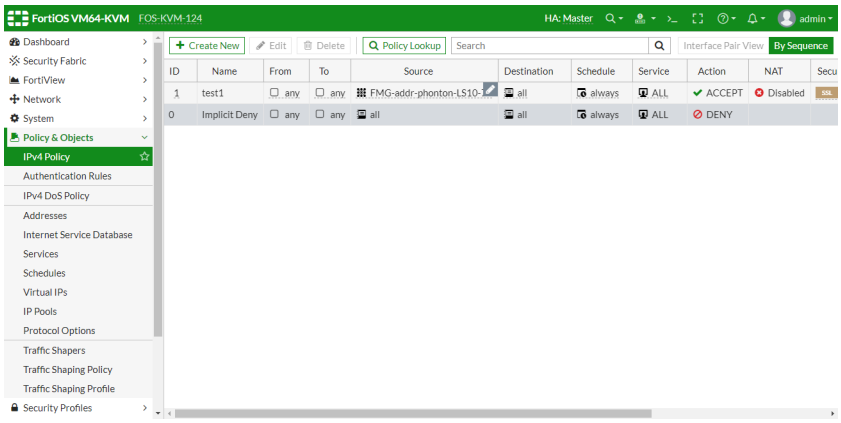
4. Select the FortiGate and , in the toolbar, click *Install* > *Install Wizard*.



5. Make sure that *Install Policy Package & Device Settings* is selected, and that the correct *Policy Package* is selected.
6. Follow the steps in the wizard to install the policy package to the FortiGate. For more information, see Using the Install Wizard to install policy packages and device settings in the FortiManager Administration Guide.

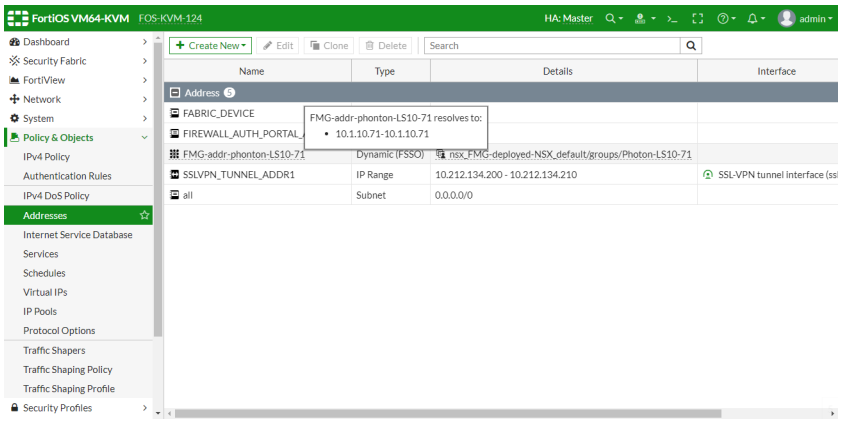
To confirm that the firewall policy with the address option was pushed to the FortiGate:

1. On the FortiGate, go to *Policy & Objects* > *IPv4 Policy* and confirm that the policy is on the list.



To confirm that the FortiGate received the dynamic FSSO address:

1. Go to *Policy & Objects* > *Addresses* and confirm that the dynamic FSSO address in on the list.



2. In the FortiGate CLI console, check the firewall addresses:

```
# show firewall address
config firewall address
    ...
    edit "FMG-addr-phonton-LS10-71"
        set uuid 2d5c5a46-e965-51e9-c3aa-c74bf993ce83
        set type dynamic
        set sub-type fsso
        set fsso-group "nsx_FMG-deployed-NSX_default/groups/Photon-LS10-71"
    next
    ...
end
```

The address name is inserted automatically by the FortiManager.

Diagnose commands

The following commands can be used on the FortiGate to help with diagnostics.

To view a list of current FSSO logons:

```
# diagnose debug authd fsso list
----FSSO logons----
IP: 1.1.1.1-1.1.1.1  User: nsx  Groups: nsx_FMG-deployed-NSX_default/groups/group1  Work-
station:
IP: 1.1.1.2-1.1.1.2  User: nsx  Groups: nsx_FMG-deployed-NSX_default/groups/group1
Workstation:
IP: 10.1.10.71-10.1.10.71  User: nsx  Groups: nsx_FMG-deployed-NSX_default/groups/Photon-LS10-
71  Workstation:  MemberOf: nsx_FMG-deployed-NSX_default/groups/Photon-LS10-71
IP: 10.1.10.72-10.1.10.72  User: nsx  Groups: nsx_FMG-deployed-NSX_default/groups/Photon-LS10-
72  Workstation:
IP: 10.1.10.73-10.1.10.73  User: nsx  Groups: nsx_FMG-deployed-NSX_default/groups/LS20-VMs
Workstation:
IP: 10.1.20.73-10.1.20.73  User: nsx  Groups: nsx_FMG-deployed-NSX_default/groups/LS20-VMs
Workstation:
IP: 10.1.20.74-10.1.20.74  User: nsx  Groups: nsx_FMG-deployed-NSX_default/groups/LS20-VMs
```

```
Workstation:
Total number of logons listed: 7, filtered: 0
----end of FSSO logons----
```

To turn on Auth daemon debug messages for 30 minutes:

```
# diagnose debug application authd -1
```

Fabric connectors

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

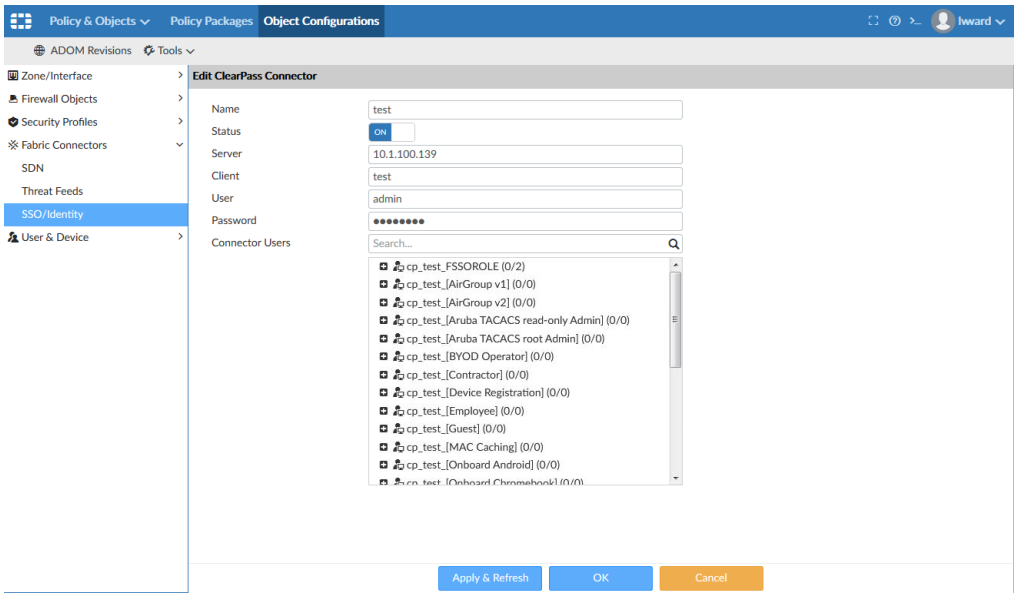
ClearPass endpoint connector via FortiManager

ClearPass Policy Manager (CCPM) is a network access system that can send information about authenticated users to third party systems, such as a FortiGate or FortiManager.

In this example, communications are established between CCPM and FortiManager, and then the FortiManager forwards information to a managed FortiGate. On the FortiGate, the user information can be used in firewall policies and added to FSSO dynamic addresses.

Configure the FortiManager

Establish communications between FortiManager and CPPM so that FortiManager can synchronize CPPM user groups. See Creating a ClearPass connector in the FortiManager Administration Guide.

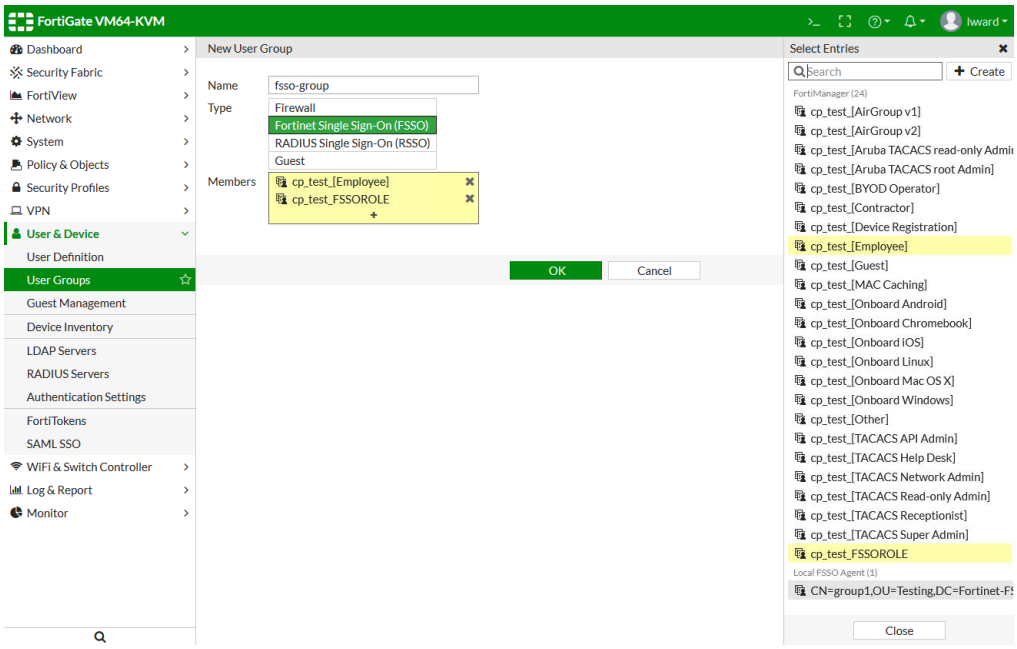


FortiManager forwards the group information to managed FortiGates.

Add CPPM FSSO user groups to a local user group

To add CPPM user groups to a local user group in the GUI:

1. On the FortiGate, go to *User & Device* > *User Groups*.
2. Click *Create New*.
3. Enter a name for the group and set *Type* to *Fortinet Single Sign-On (FSSO)*.
4. Click the *Members* field, and add one or more FSSO groups.
   FSSO groups can come from multiple sources; CPPM FSSO groups are prefixed with *cp_* and are listed under the *FortiManager* heading.



5. Click *OK*.

To add CPPM user groups to a local user group in the CLI:

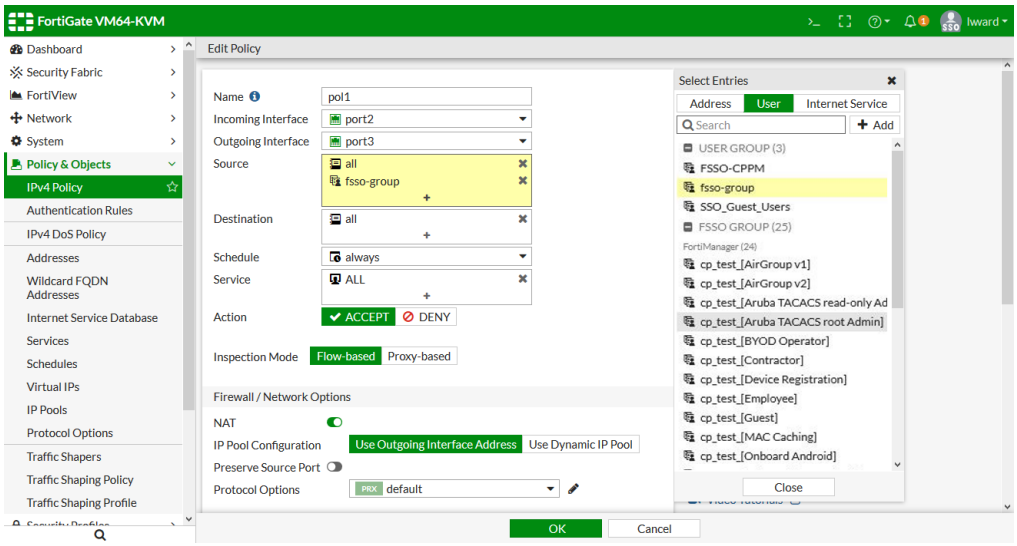
```
config user group
    edit fsso-group
        set group-type fsso-service
        set member "cp_test_[Employee]" "cp_test_FSSOROLE"
    next
end
```

Use the local FSSO user group in a firewall policy

To add the local FSSO user group to a firewall policy in the GUI:

1. Go to *Policy & Objects* > *IPv4 Policy*.
2. Create a new policy, or edit an existing one.

3. Click in the *Source* field and add the *fsso-group* user group.



CPPM user groups can also be added directly to the policy.

4. Click *OK*.

To add the local FSSO user group to a firewall policy in the CLI:

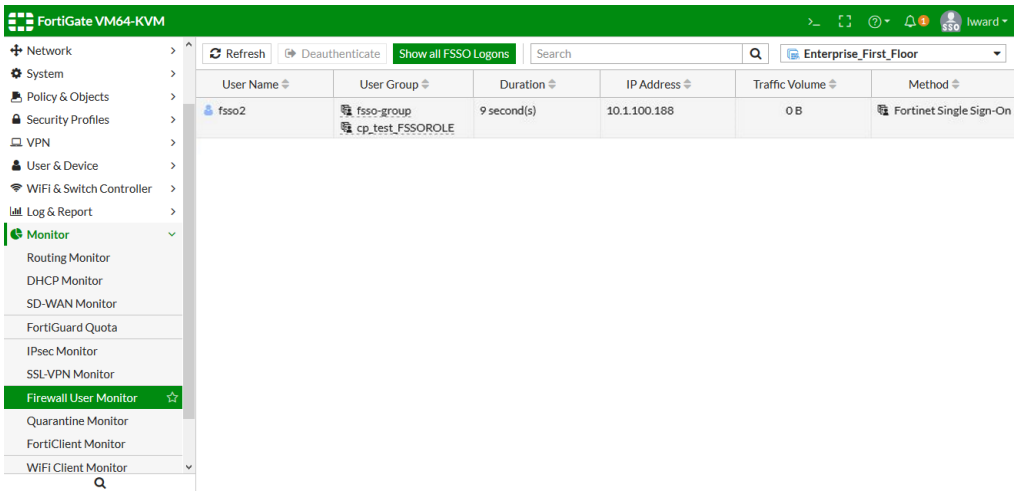
```
config firewall policy
    edit 1
        set name "pol1"
        set uuid 2b88ed8a-c906-51e9-fb25-8cb12172acd8
        set srcintf "port2"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
        set groups "fsso-group"
        set nat enable
    next
end
```

Verification

To verify that a user was added to the FSSO list on the FortiGate:

1. Log on to the client and authenticate with CPPM.
   After successful authentication, the user is added to the FSSO list on the FortiGate.

2. On the FortiGate, go to *Monitor* > *Firewall User Monitor* to verify that the user was added.



The user group *cp_test_FSSOROLE* is listed separately because the user is a member of that group on the CPPM.

To verify that traffic can pass the firewall:

1. Log on to the client and browse to an external website.
2. On the FortiGate, go to *FortiView* > *Sources*.
3. Double-click on the user and select the *Destinations* tab to verify that traffic is being passed by the firewall.

To verify the user address groups:

```
show user adgrp
    config user adgrp
        edit "cp_test_FSSOROLE"
            set server-name "FortiManager"
        next
        edit "cp_test_[AirGroup v1]"
            set server-name "FortiManager"
        next
        edit "cp_test_[AirGroup v2]"
            set server-name "FortiManager"
        next
        edit "cp_test_[Aruba TACACS read-only Admin]"
            set server-name "FortiManager"
        next
        edit "cp_test_[Aruba TACACS root Admin]"
            set server-name "FortiManager"
        next
        edit "cp_test_[BYOD Operator]"
            set server-name "FortiManager"
        next
        edit "cp_test_[Contractor]"
            set server-name "FortiManager"
        next
        edit "cp_test_[Device Registration]"
            set server-name "FortiManager"
        next
```

```
        ...
        edit "CN=group1,OU=Testing,DC=Fortinet-FSSO,DC=COM"
            set server-name "Local FSSO Agent"   <----- !!!
        next
    end
```

ClearPass integration for dynamic address objects

ClearPass Policy Manager (CPPM) can gather information about the statuses of network hosts, for example, the latest patches or virus infections. Based on this information, CPPM send the IP addresses and current states, such as Healthy or Infected, to the FortiGate.

On the FortiGate, the IP addresses received from CPPM are added to a dynamic firewall address with the *clearpass-spt* subtype. This address can be used in any policy that supports dynamic addresses, such as Firewall or SSL-VPN policies.

In this example, you create two dynamic IP addresses that are used in two firewall policies (deny and allow). One policy allows traffic (host state = Healthy), and the other denies traffic (host state = Infected). When CPPM sends the information, the IP addresses are assigned according to their host state: Healthy or Infected.

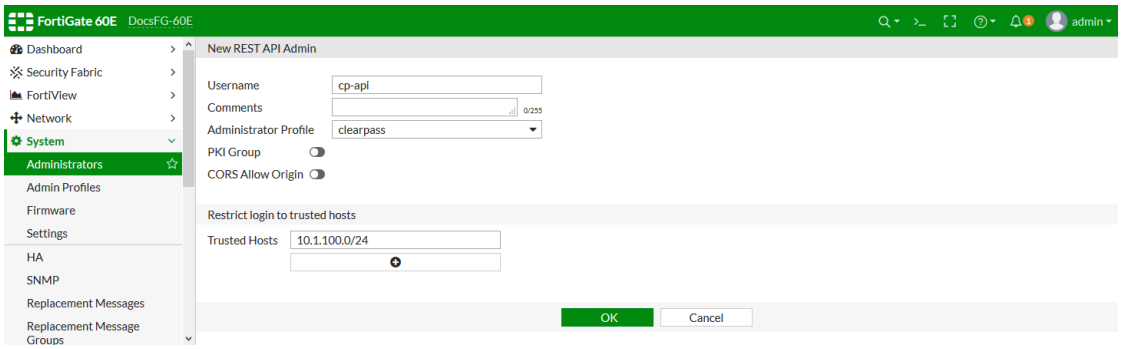
You can then verify that traffic from the Infected host is denied access by the deny policy, and traffic from the Healthy host is allowed access by the allow policy.

Create a REST API administrator

A RESET API administrator is required to generate an authorization token for REST API messages, and to limit hosts that can send REST API messages to the FortiGate.

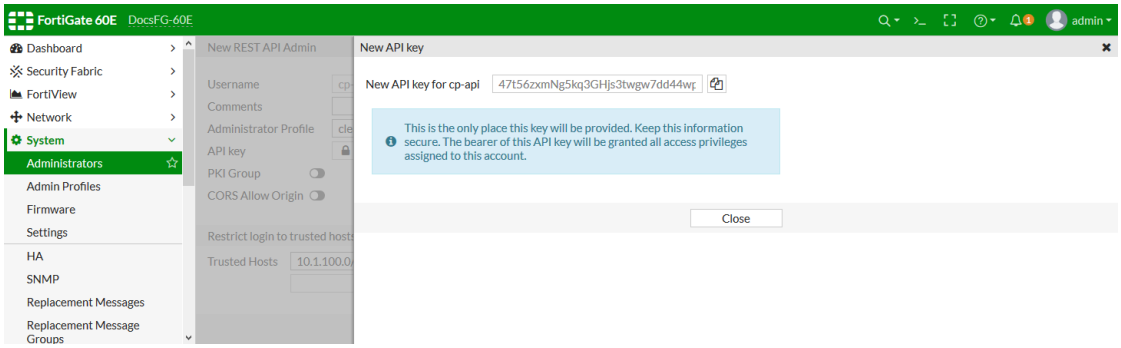
To create a REST API administrator in the GUI:

1. Go to *System* > *Administrators*.
2. Click *Create New* > *REST API Admin*.
3. Configure the *Username* and other information as needed.
4. Disable *PKI Group*.
5. In the *Trusted Hosts* field, enter *10.1.100.0/24*.



For this example, an administrator profile called *clearpass* was created with full read/write access. See Administrator profiles for details.

6. Click *OK*.
   The *New API key* pane opens.



   The API key is the REST API authorization token that is used in REST API messages sent by CPPM to the FortiGate.
7. Copy the API key to a secure location. A new key can be generated if this one is lost or compromised.
8. Click *Close*.

To create a REST API administrator in the CLI:

```
config system api-user
    edit "cpi-back"
        set accprofile "clearpass"
        config trusthost
            edit 1
                set ipv4-trusthost 10.1.100.0 255.255.255.0
            next
        end
    next
end
```

```
execute api-user generate-key cp-api
    New API key: 0f1HxGHh9r9p74k7qgfHNH40p51bjs
    NOTE: The bearer of this API key will be granted all access privileges assigned to the
api-user cp-api.
```

Create dynamic IP addresses with the clearpass subtype

Two dynamic IP addresses are required, one for the allow policy, and the other for the deny policy.

To create the dynamic IP addresses:

```
config firewall address
    edit "cppm"
        set uuid 62a180c0-cb36-51e9-6e70-4a2034d82179
        set type dynamic
        set sub-type clearpass-spt
        set clearpass-spt healthy
        set comment ''
        set visibility enable
        set associated-interface ''
        set color 0
```

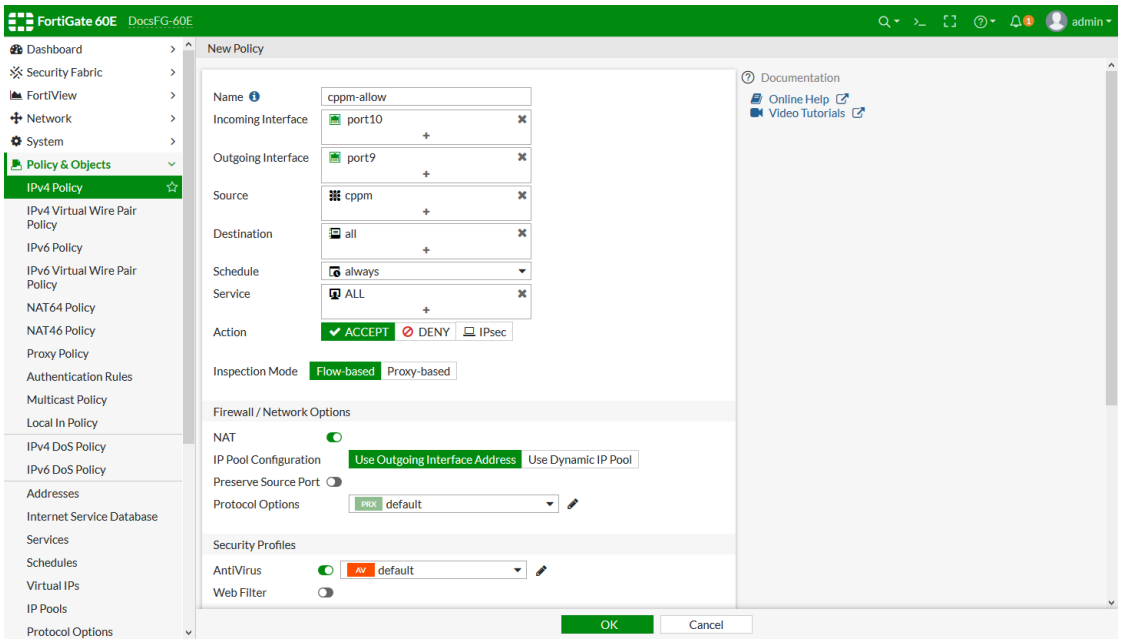
```
    next
    edit "cppm-deny"
        set uuid b318e962-cb36-51e9-7a34-74a34cf3bf0b
        set type dynamic
        set sub-type clearpass-spt
        set clearpass-spt infected
        set comment ''
        set visibility enable
        set associated-interface ''
        set color 0
    next
end
```

Create firewall policies

Two firewall policies are required, one to accept traffic (*cppm-allow*), and the other to deny traffic (*cppm-deny*).

To create the firewall policies in the GUI:

1. Go to *Policy & Objects* > *IPv4 Policy*.
2. Configure the allow policy:
   a. Click *Create New*.
   b. Enter a name for the policy.
   c. Set *Source* set to *cppm*.
   d. Set *Action* to *ACCEPT*.
   e. Configure the remaining settings as needed.

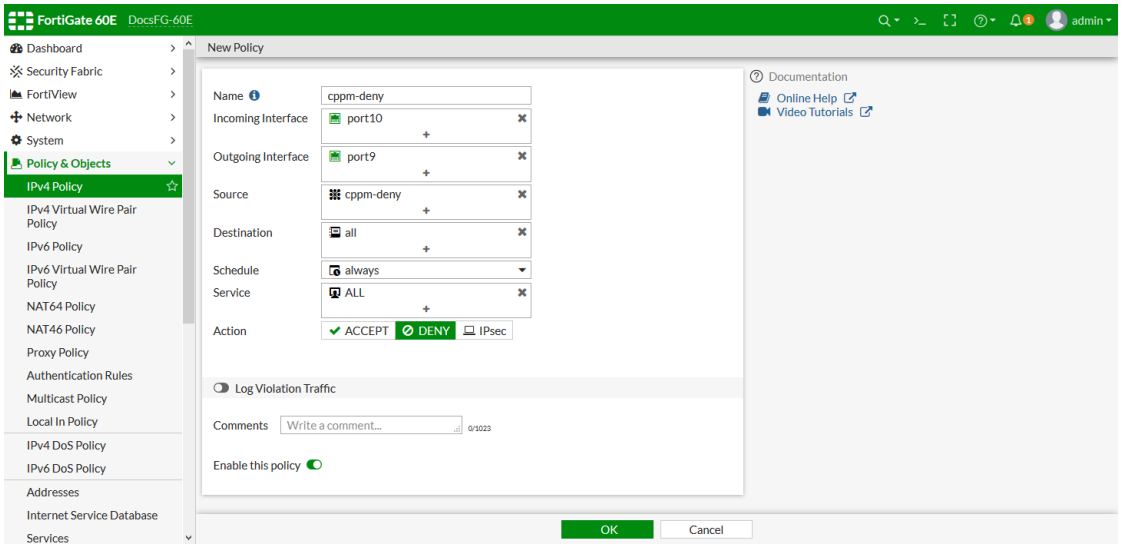


   f. Click *OK*.
3. Configure the deny policy:
   a. Click *Create New*.
   b. Enter a name for the policy.

c. Set *Source* set to *cppm-deny*.

d. Set *Action* to *DENY*.

e. Configure the remaining settings as needed.



f. Click *OK*.

To create the firewall policies in the CLI:

```
config firewall address
    edit "cppm"
        set uuid 62a180c0-cb36-51e9-6e70-4a2034d82179
        set type dynamic
        set sub-type clearpass-spt
        set clearpass-spt healthy
        set comment ''
        set visibility enable
        set associated-interface ''
        set color 0
    next
    edit "cppm-deny"
        set uuid b318e962-cb36-51e9-7a34-74a34cf3bf0b
        set type dynamic
        set sub-type clearpass-spt
        set clearpass-spt infected
        set comment ''
        set visibility enable
        set associated-interface ''
        set color 0
    next
end
```

Verification

Go to *Log & Report* > *Forward Traffic* to review traffic logs and ensure that traffic is allowed or denied as expected.

To verify that FortiGate addresses are assigned correctly, enter the following CLI command:

```
diagnose firewall dynamic list
List all dynamic addresses:
cppm-deny: ID(141)
        ADDR(10.1.100.188)

cppm: ID(176)
        ADDR(10.1.100.185)
        ADDR(10.1.100.186)
```

Symantec endpoint connector

With the Fabric connector for Symantec Endpoint Protection Manager (SEPM), you can use the client IP information from SEPM to assign to dynamic IP addresses on FortiOS.

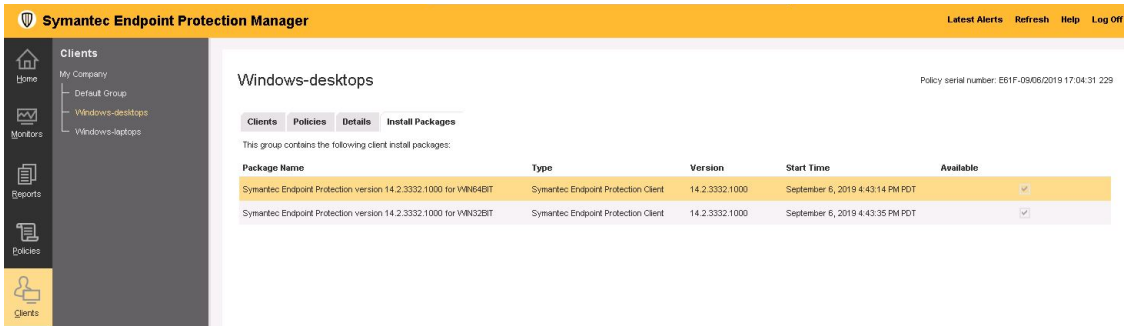
When communication between FortiGate and SEPM is established, FortiGate polls every minute for updates via TLS over port 8446. You can use the CLI to change the default one minute polling interval.

For example, you can create a dynamic Fabric Connector IP address subtype and use it in firewall policies as the source address. The dynamic IP address contains all IP addresses sent by SEPM.

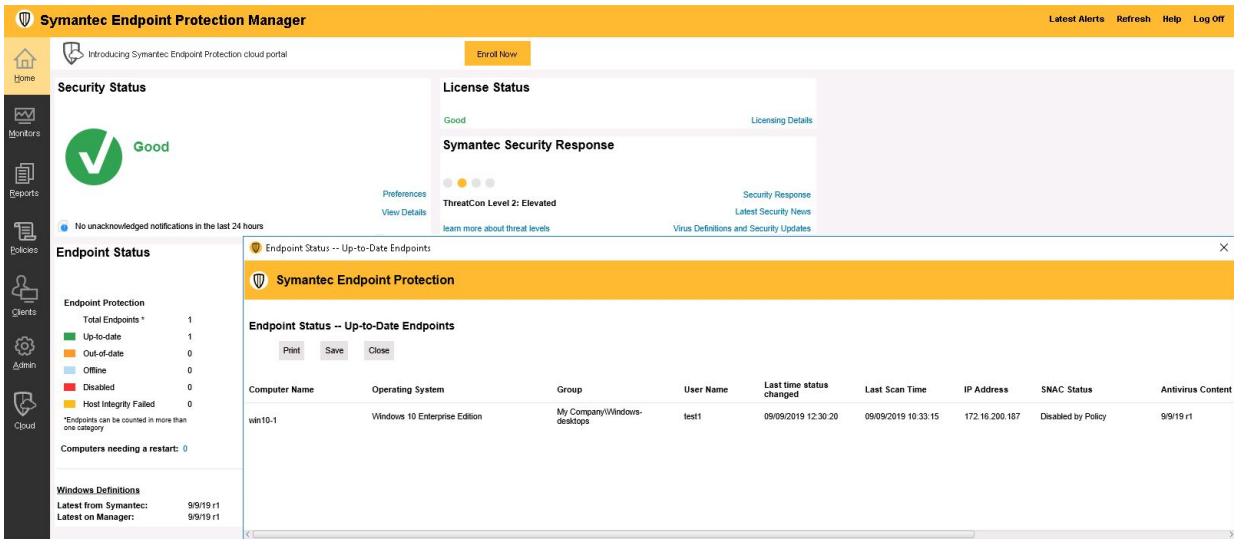
This example shows a dynamic IP address with SEPM and one client PC managed by SEPM using FortiGate as the default gateway.

To configure SEPM on a managed client PC:

1. In SEPM, create client packages for client hosts and group them into SEPM groups.
   You can install packages locally on clients or download them directly from SEPM.

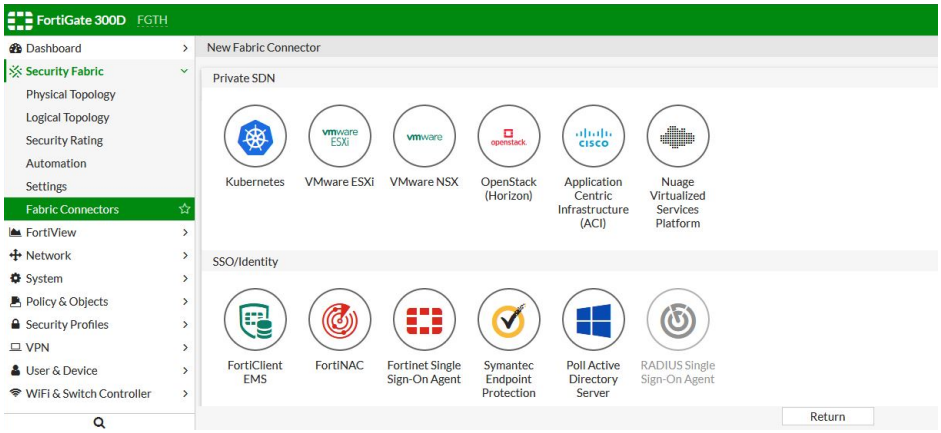


2. When a package is installed on the client host, the host is considered managed by SEPM. Even if the host has multiple interfaces, only one IP per host is displayed.

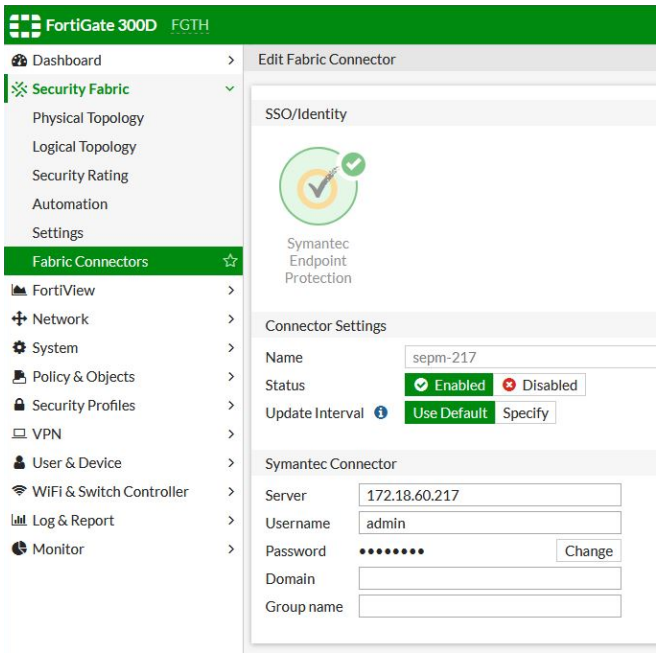


To configure Symantec endpoint connector on FortiGate:

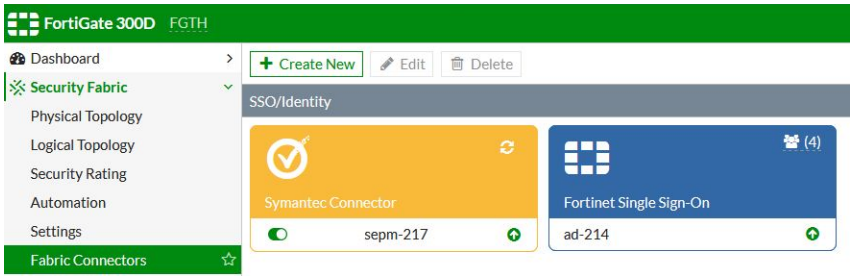
1. Go to *Security Fabric > Fabric Connectors*.
2. Click *Create New*.



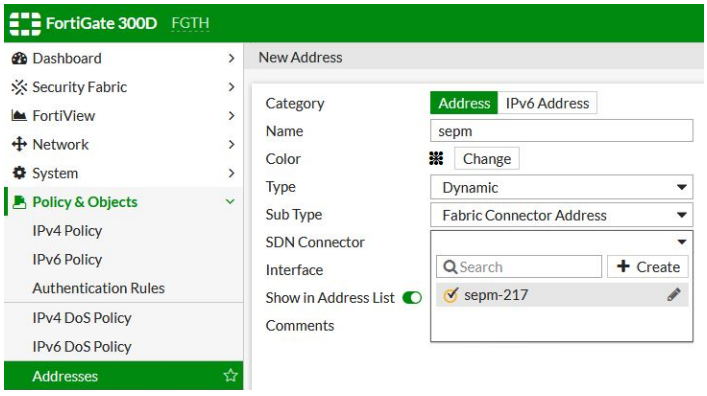
3. Click *Symantec Endpoint Protection*.
   - In the *Connector Settings* section, if options are left empty, then all SEPM domains and groups are monitored.
   - In the *Symantec Connector* section:
     - In the *Server* field, enter the SEPM IP address.
     - Enter the *Username* and *Password*.
     - If you want to limit the domains or groups that are monitored, enter the information in *Domain* and *Group name*.



4. Click OK.
   When the connection is established, you can see a green up arrow in the bottom right of the tile. You might need to refresh your browser to see the established connection.

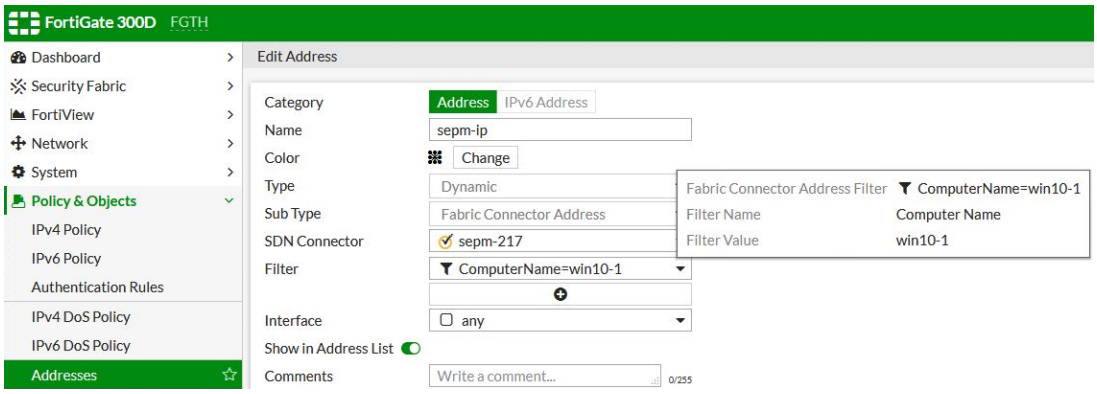


5. Go to *Policy & Objects* > *Addresses*.
6. Click *Create New* > *Address*.
   - Set *Type* to *Dynamic*.
   - Set *Sub Type* to *Fabric Connector Address*.
   - Set *SDN Connector* to the Fabric Connector that you just created.



7. Click *OK*.

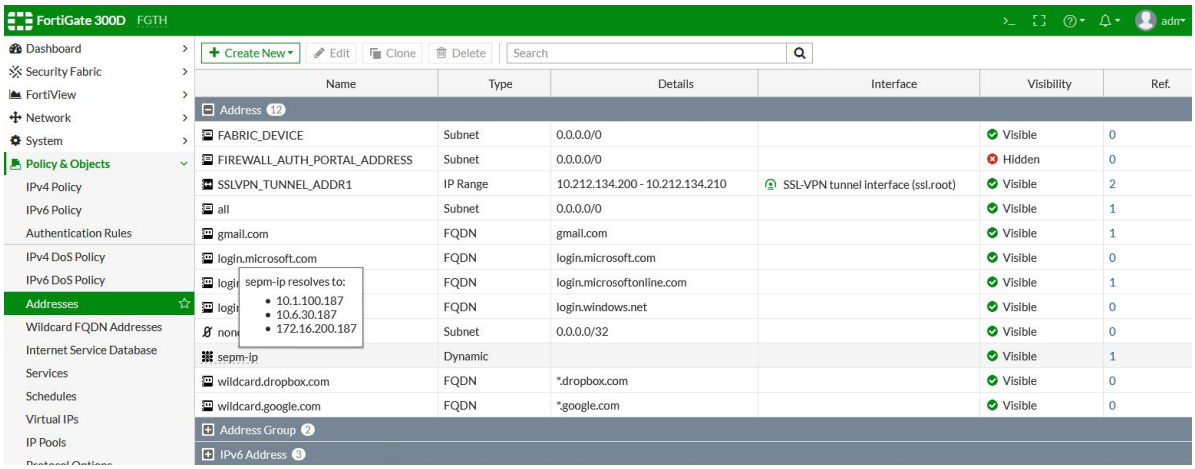
8. Edit the address to see the configuration.
   - *Filter* shows the hostnames of the client PCs managed by SEPM. The GUI shows the ComputerName by default. You can change this using the CLI; see Specify filters for details.



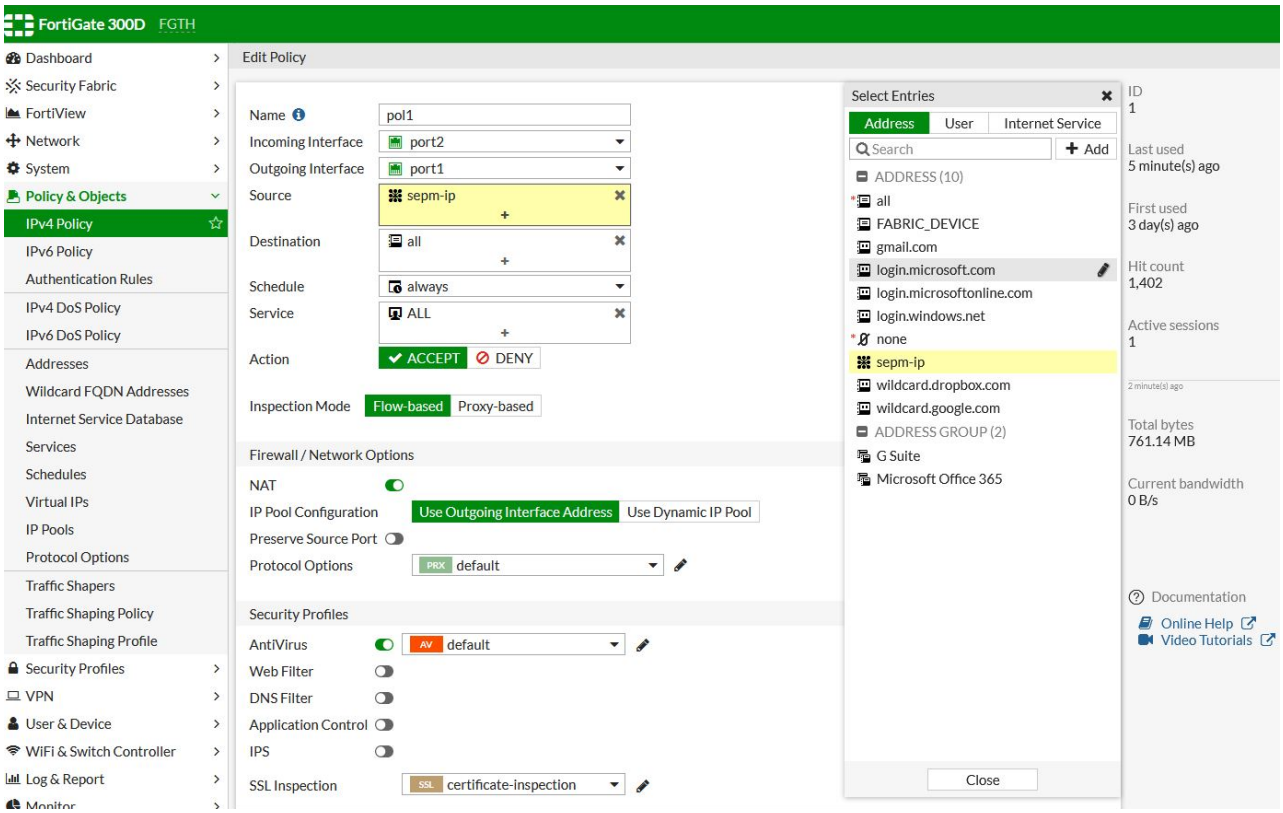
Filter options are only available for active computers that are configured and registered in SEPM. Free-form filters can be created manually by clicking *Create* and entering the filter, in the format: `filter_type=value`.

Possible manual filter types are: `GroupName`, `GroupID`, `ComputerName`, `ComputerUUID`, and `OSName`. For example: `GroupName=MyGroup`.

9. In *Policy & Objects* > *Addresses*, you can see all the IP addresses of the host.

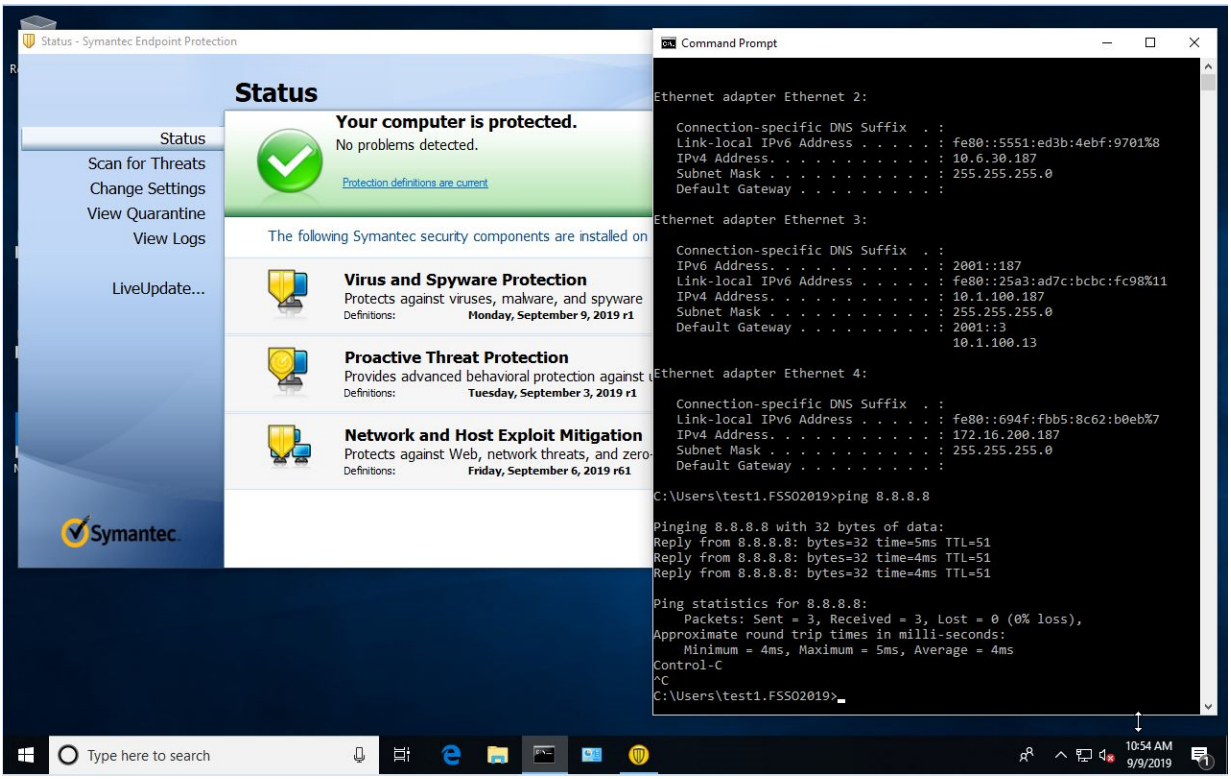


10. Go to *Policy & Objects* > *IPv4 Policy*, click *Create New*, and add the dynamic IP address to the firewall policy.

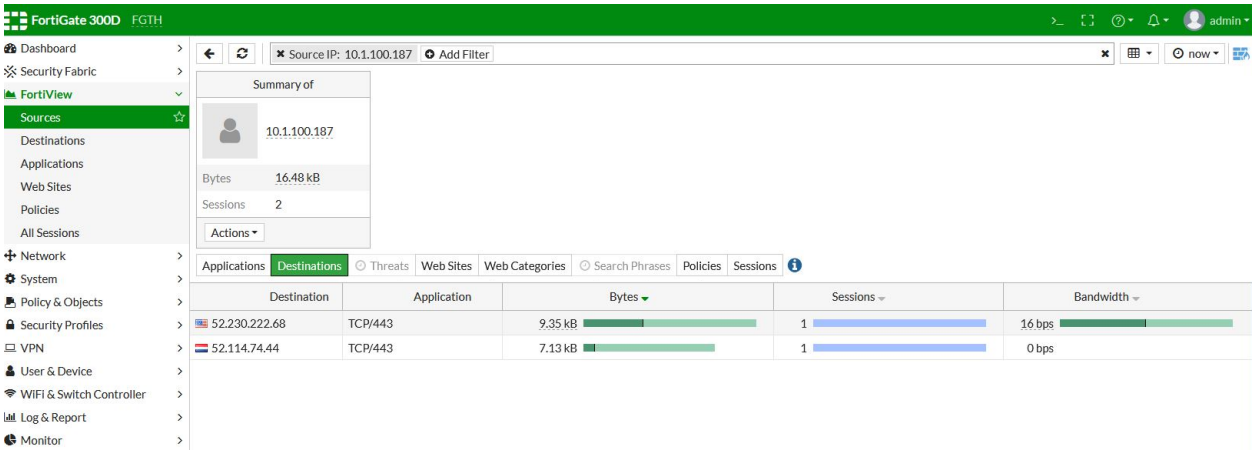


To verify the configuration:

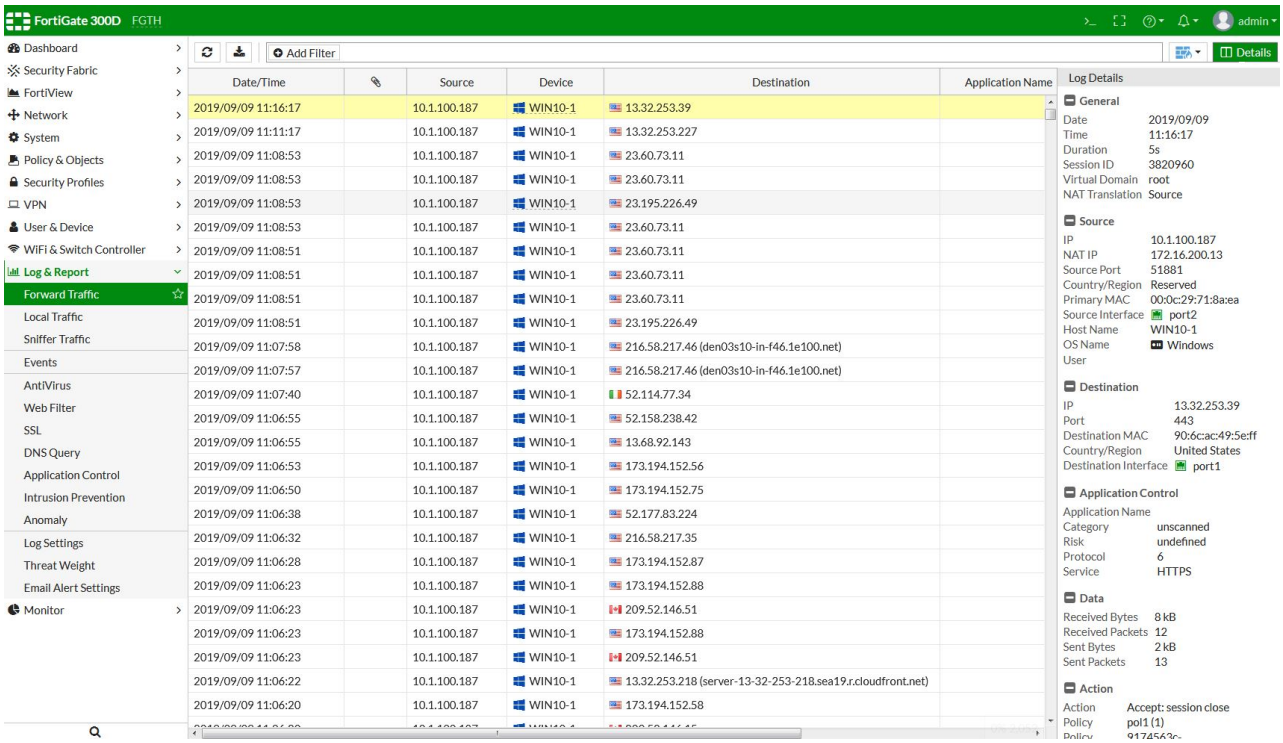
1. On the client PC, check that it is managed by SEPM to access the Internet.



2. In FortiGate, you can check in *FortiView* > *Sources*.



3. In FortiGate, you can also check in *Log & Report* > *Forward Traffic*.



Since this traffic is not authenticated traffic but is based on source IP address only, this traffic is not shown in the GUI firewall monitor or in the CLI `diagnose firewall auth list` command.

To configure Symantec endpoint connector on FortiGate in the CLI:

1. Create the fabric connector:

```
config system sdn-connector
    edit "sepm-217"
        set type sepm
        set server "172.18.60.217"
        set username "admin"
        set password ENC -1v3UoTmp1RV+gIQNklbzxp4HdoNg=
        set status enable
    next
end
```

2. Create the dynamic IP address:

```
config firewall address
    edit "sepm-ip"
        set uuid 645552a0-d0c9-51e9-282d-c7ed6d7ee7de
        set type dynamic
        set sdn "sepm-217"
        set filter "ComputerName=win10-1"
        config list
            edit "10.1.100.187"
```

```
            next
            edit "10.6.30.187"
            next
            edit "172.16.200.187"
            next
        end
    next
end
```

You can specify other filters and combine them with | and &, for example:

```
FGTH (sepm-ip) # set filter
<key1=value1>    [& <key2=value2>] [| <key3=value3>]
Available filter keys are:
        <ComputerName><ComputerUuid><GroupId><GroupName> <DomainId><DomainName><OsName>
```

3. Add the dynamic IP address to the firewall policy:

```
config firewall policy
    edit 1
        set name "pol1"
        set uuid 9174563c-d0c9-51e9-1a32-4e14385239e9
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "sepm-ip"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
        set logtraffic all
        set fsso disable
        set nat enable
    next
end
```

To troubleshoot Symantec SD connector in the CLI:

```
# diagnose debug application sepmd -1

Output is sent every minute (default). All IPv4 learned from SEPM. IPv6 also sent but not yet
supported.

2019-09-09 12:01:09 sepmd sdn connector sepm-217 start updating IP addresses
2019-09-09 12:01:09 sepmd checking firewall address object sepm-ip, vd 0
2019-09-09 12:01:09 sepmd sdn connector sepm-217 finish updating IP addresses
2019-09-09 12:01:09 sepmd reap child pid: 18079
2019-09-09 12:02:09 sepmd sdn connector sepm-217 prepare to update
2019-09-09 12:02:09 sepmd sdn connector sepm-217 start updating
2019-09-09 12:02:09 sepm-217 sdn connector will retrieve token after 9526 secs
2019-09-09 12:02:09 sym_new_ip_addr ComputerName win10-1
    ComputerUuid AC894D56-BD86-A786-7DDB-7FD98B718AE0, OsName Windows 10
    IP 172.16.200.187
    GroupName My Company\Windows-desktops, GroupId E61FDEA2AC10C80E46D0B31BB58D7CB3
    DomainName Default, DomainId 6C507580AC10C80E5F3CAED5B1711A8E
2019-09-09 12:02:09 sym_new_ip_addr ComputerName win10-1
```

```
    ComputerUuid AC894D56-BD86-A786-7DDB-7FD98B718AE0, OsName Windows 10
    IP 10.6.30.187
    GroupName My Company\Windows-desktops, GroupId E61FDEA2AC10C80E46D0B31BB58D7CB3
    DomainName Default, DomainId 6C507580AC10C80E5F3CAED5B1711A8E
2019-09-09 12:02:09 sym_new_ip_addr ComputerName win10-1
    ComputerUuid AC894D56-BD86-A786-7DDB-7FD98B718AE0, OsName Windows 10
    IP 10.1.100.187
    GroupName My Company\Windows-desktops, GroupId E61FDEA2AC10C80E46D0B31BB58D7CB3
    DomainName Default, DomainId 6C507580AC10C80E5F3CAED5B1711A8E
2019-09-09 12:02:09 2001:0000:0000:0000:0000:0000:0000:0187 is not in IPv4 presentation format


2019-09-09 12:02:09 sepmd sdn connector sepm-217 start updating IP addresses
2019-09-09 12:02:09 sepmd checking firewall address object sepm-ip, vd 0
2019-09-09 12:02:09 sepmd sdn connector sepm-217 finish updating IP addresses
2019-09-09 12:02:09 sepmd reap child pid: 18089
2019-09-09 12:03:09 sepmd sdn connector sepm-217 prepare to update
2019-09-09 12:03:09 sepmd sdn connector sepm-217 start updating
2019-09-09 12:03:09 sepm-217 sdn connector will retrieve token after 9466 secs
2019-09-09 12:03:09 sym_new_ip_addr ComputerName win10-1
    ComputerUuid AC894D56-BD86-A786-7DDB-7FD98B718AE0, OsName Windows 10
    IP 172.16.200.187
    GroupName My Company\Windows-desktops, GroupId E61FDEA2AC10C80E46D0B31BB58D7CB3
    DomainName Default, DomainId 6C507580AC10C80E5F3CAED5B1711A8E
2019-09-09 12:03:09 sym_new_ip_addr ComputerName win10-1
    ComputerUuid AC894D56-BD86-A786-7DDB-7FD98B718AE0, OsName Windows 10
    IP 10.6.30.187
    GroupName My Company\Windows-desktops, GroupId E61FDEA2AC10C80E46D0B31BB58D7CB3
    DomainName Default, DomainId 6C507580AC10C80E5F3CAED5B1711A8E
2019-09-09 12:03:09 sym_new_ip_addr ComputerName win10-1
    ComputerUuid AC894D56-BD86-A786-7DDB-7FD98B718AE0, OsName Windows 10
    IP 10.1.100.187
    GroupName My Company\Windows-desktops, GroupId E61FDEA2AC10C80E46D0B31BB58D7CB3
    DomainName Default, DomainId 6C507580AC10C80E5F3CAED5B1711A8E
2019-09-09 12:03:09 2001:0000:0000:0000:0000:0000:0000:0187 is not in IPv4 presentation format
```

To list the SEPM daemon SDN connectors:

```
diagnose test application sepmd 1
sepm SDN connector list:
  name: sepm-217, status: enabled, updater_interval: 60
```

To list the SEPM daemon SDN filters:

```
diagnose test application sepmd 2
sepm SDN connector sepm-217 filter list:
  name: sepm-ip, vd 0, filter 'ComputerName=win10-1'
```

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.

FortiCare-generated license adoption for AWS PAYG variant

FortiGate pay as you go (PAYG) instances were using locally self-generated licenses, which posed limitations with installing other licenses, such as FortiToken. The new implementation uses FortiCare-generated licenses to resolve these problems.

FortiGate-VM AWS PAYG instances can now obtain FortiCare-generated licenses and register to FortiCare.

The valid license allows you to register to FortiCare to use features including FortiToken with the FortiGate-VM instance.

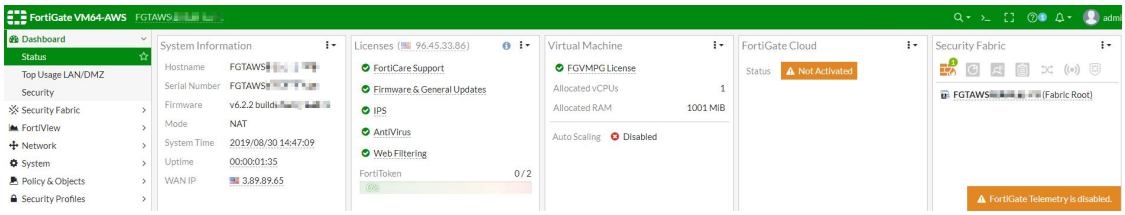
The FortiGate-VM must be able to reach FortiCare to receive a valid PAYG license. Ensure connectivity to FortiCare (https://directregistration.fortinet.com/) by checking all related setup on security groups, access control lists, Internet gateways, route tables, public IP addresses, and so on.

If the FortiGate-VM instance is created in a closed environment or unable to reach FortiCare, the FortiGate-VM self-generates a local license as in previous versions of FortiOS. You can obtain a FortiCare license, ensure that the FortiGate-VM is able to connect to FortiCare, then run the `execute vm-license` command to obtain the license from FortiCare.

To deploy a FortiGate-VM 6.2.2 AWS PAYG instance:

When deploying a FortiGate-VM PAYG instance for AWS, you will use the FGT_VM64_AWS-v6-buildXXXX-FORTINET.out image. After deployment with this image, running `get system status` results in output that includes the following lines:

```
Version: FortiGate-VM64-AWS v6.2.2,buildXXXX,XXXXXX (GA)
Virus-DB: 71.00242(2019-08-30 08:19)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 0.00000(2001-01-01 00:00)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
Serial-Number: FGTAWS12345678
```

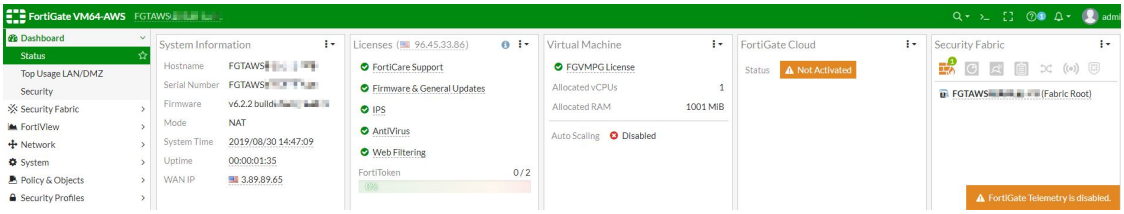


To upgrade a FortiGate-VM AWS PAYG instance from FortiOS 6.2.1 and earlier to 6.2.2:

Earlier versions used the FGT_VM64_AWSONDEMAND-v6-buildXXXX-FORTINET.out image to deploy a FortiGate-VM AWS PAYG instance. In 6.2.2, the FGT_VM64_AWS-v6-buildXXXX-FORTINET.out image is used to deploy a FortiGate-VM AWS PAYG instance.

When upgrading from an earlier FortiOS version, you must first upgrade using the FGT_VM64_AWSONDEMAND image, then use the FGT_VM64_AWS image.

1. In FortiOS, perform an upgrade using the FGT_VM64_AWSONDEMAND-v6-buildXXXX-FORTINET.out image.
2. Perform another upgrade, this time using the FGT_VM64_AWS-v6-buildXXXX-FORTINET.out image. This process is irreversible.



3. Run `get system status` results in output that includes the following lines:

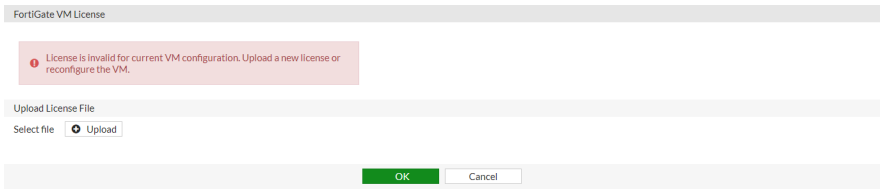
```
Version: FortiGate-VM64-AWS v6.2.2,buildXXXX,XXXXXX (GA)
Virus-DB: 71.00246(2019-08-30 12:19)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
IPS-DB: 14.00680(2019-08-30 02:29)
IPS-ETDB: 0.00000(2001-01-01 00:00)
APP-DB: 14.00680(2019-08-30 02:29)
INDUSTRIAL-DB: 14.00680(2019-08-30 02:29)
Serial-Number: FGTAWS1234567890
```

4. For future upgrades, use the FGT_VM64_AWS-v6-buildXXXX-FORTINET.out image to retain PAYG status. You cannot directly upgrade a FortiGate-VM AWS PAYG instance from 6.2.1 or earlier to 6.2.3 and later versions. You must first follow the procedure detailed above.

CPU only licensing for private clouds

In FortiOS 6.2.2 and later, there is no maximum memory limitation for each type of FortiGate VM license on private clouds.

In FortiOS 6.2.1, a FG-VM01 license is invalid on a FortiGate VM with more that 2GB of memory:

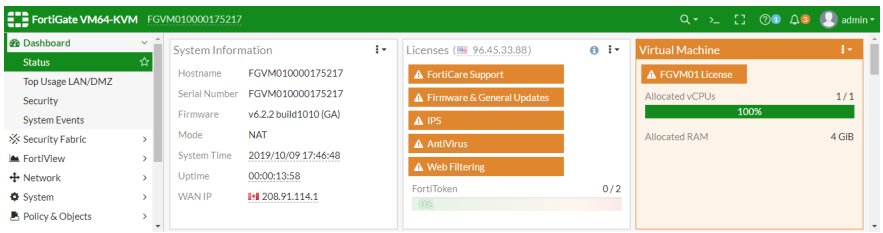



```
FGVM01 login: admin
Password:

License invalid due to exceeding allowed 1 CPUs and 2048 MB RAM.
Welcome !

FGVM01 # get system status
Version: FortiGate-VM64-KVM v6.2.1,build0932,190716 (GA)
Virus-DB: 1.00000(2018-04-09 18:07)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 0.00000(2001-01-01 00:00)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
Serial-Number: FGVM00UNLICENSED
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
Botnet DB: 1.00000(2012-05-28 22:51)
License Status: Invalid
License invalid due to exceeding allowed resources: 1 CPU, 2048 MB RAM
License Expires: 2019-10-18
Log hard disk: Not available
Hostname: FGVM010000175216
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 0932
Release Version Information: GA
FortiOS x86-64: Yes
System time: Wed Oct  9 17:25:37 2029
```

In FortiOS 6.2.2, a FG-VM01 license is valid on a FortiGate VM with more that 2GB of memory:




```
FGVM01 login: admin
Password:

FGVM01 # get system status
Version: FortiGate-VM64-KVM v6.2.2,build1010,191008 (GA)
```

```
Virus-DB: 72.00345(2019-10-15 07:19)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 0.00000(2001-01-01 00:00)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
Serial-Number: FGVM01XX11111111
IPS Malicious URL Database: 2.00439(2019-10-14 12:38)
Botnet DB: 1.00000(2012-05-28 22:51)
License Status: Valid
License Expires: 2020-10-12
VM Resources: 1 CPU/1 allowed, 3967 MB RAM
Log hard disk: Available
Hostname: FGVM01TM19007449
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: standalone
Branch point: 1010
Release Version Information: GA
FortiOS x86-64: Yes
System time: Tue Oct 15 09:58:31 2029
```

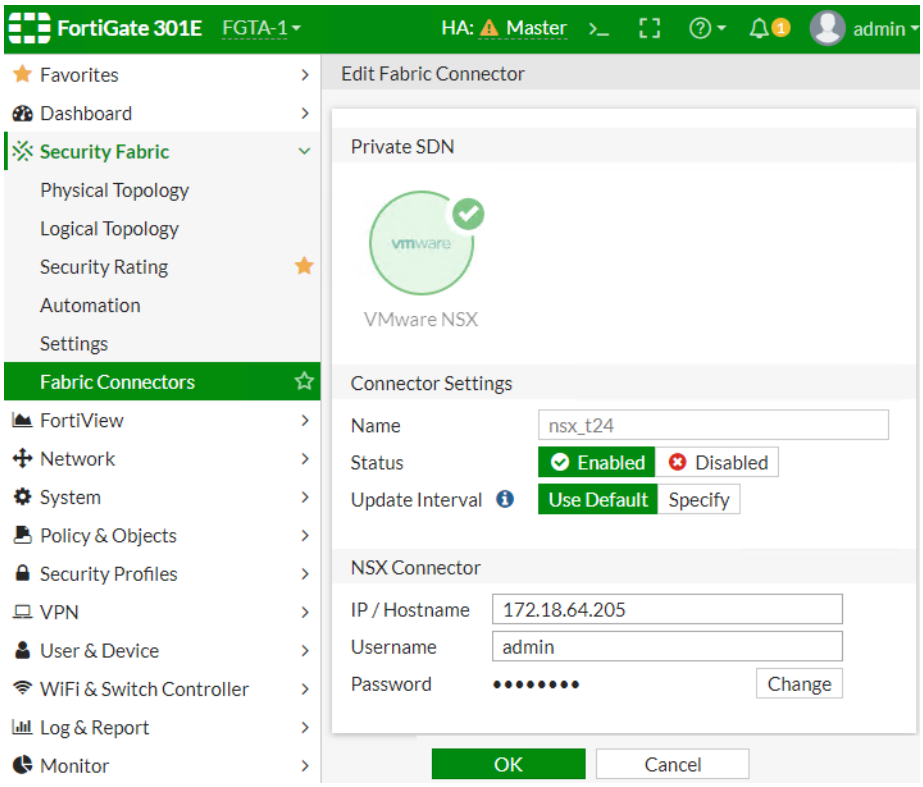
SDN connector for NSX-T manager

This feature provides SDN connector configuration for NSX-T manager. You can import specific groups or all groups from NSX-T manager.

To configure SDN connector for NSX-T manager using the GUI:

1. Go to *Security Fabric* > *Fabric Connectors* and click *Create New*.
2. In the *Private SDN* section, click *VMware NSX*.

3. Enter the settings and click *OK*.



To configure SDN connector for NSX-T manager using the CLI:

```
config system sdn-connector
    edit "nsx_t24"
        set type nsx
        set server "172.18.64.205"
        set username "admin"
        set password xxxxxx
    next
end
```

To import a specific group from the NSX-T manager using the CLI:

You must use the CLI for this function.

```
Root-F-1 # execute nsx group import nsx_t24 root csf_ns_group
[1] 336914ba-0660-4840-b0f1-9320f5c5ca5e csf_ns_group:
  Name:csf_ns_group
  Address:1.1.1.0
  Address:1.1.1.1
  Address:172.16.10.104
  Address:172.16.20.104
  Address:172.16.30.104
  Address:2.2.2.0
  Address:2.2.2.2
  Address:4.4.4.0
  Address:5.5.5.0
```

```
  Address:6.6.6.6
  Address:7.7.7.7
```

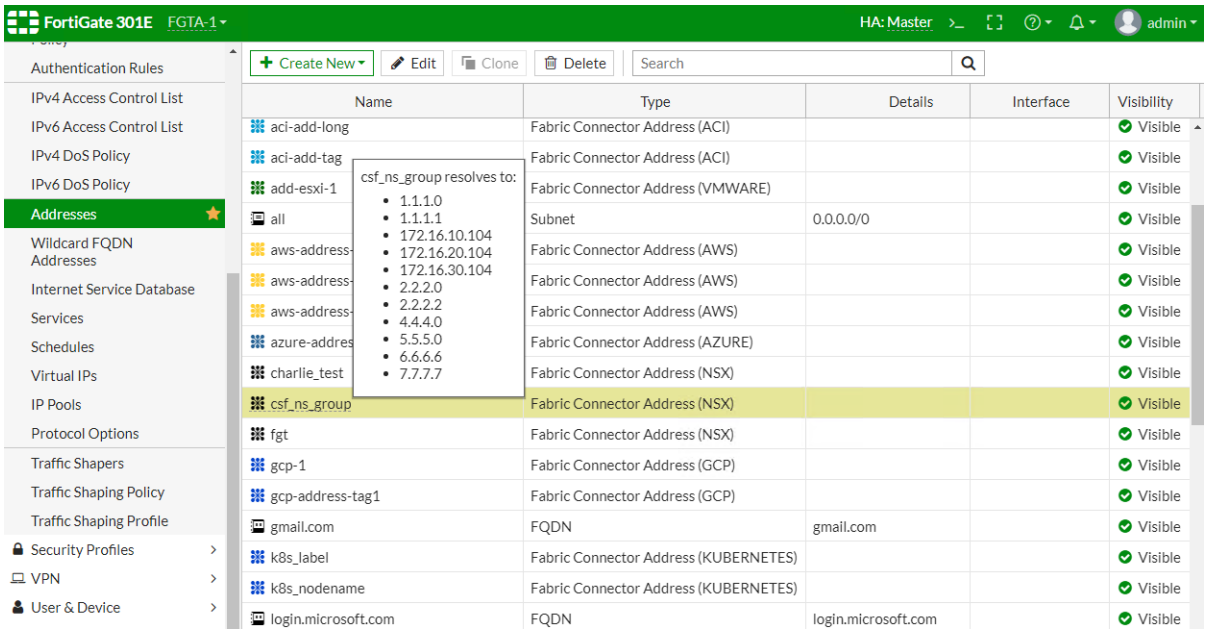
To import all groups from NSX-T manager using the CLI:

You must use the CLI for this function.

```
Root-F-1 # execute nsx group import nsx_t24 root
[1] 663a7686-b9a3-4659-b06f-b45c908349a0 ServiceInsertion_NSGroup:
  Name:ServiceInsertion_NSGroup
  Address:10.0.0.2
[2] 336914ba-0660-4840-b0f1-9320f5c5ca5e csf_ns_group:
  Name:csf_ns_group
  Address:1.1.1.0
  Address:1.1.1.1
  Address:172.16.10.104
  Address:172.16.20.104
  Address:172.16.30.104
  Address:2.2.2.0
  Address:2.2.2.2
  Address:4.4.4.0
  Address:5.5.5.0
  Address:6.6.6.6
  Address:7.7.7.7
[3] c462ec4d-d526-4ceb-aeb5-3f168cecd89d charlie_test:
  Name:charlie_test
  Address:1.1.1.1
  Address:2.2.2.2
  Address:6.6.6.6
  Address:7.7.7.7
[4] ff4dcb08-53cf-46bd-bef4-f7aeda9c0ad9 fgt:
  Name:fgt
  Address:172.16.10.101
  Address:172.16.10.102
  Address:172.16.20.102
  Address:172.16.30.103
[5] 3dd7df0d-2baa-44e0-b88f-bd21a92eb2e5 yongyu_test:
  Name:yongyu_test
  Address:1.1.1.0
  Address:2.2.2.0
  Address:4.4.4.0
  Address:5.5.5.0
```

To view the dynamic firewall IP addresses that are resolved by the SDN connector using the GUI:

1. Go to *Policy & Objects* > *Addresses* to view the IP addresses resolved by an SDN connector.



To view the dynamic firewall IP addresses that are resolved by the SDN connector using the CLI:

```
Root-F-1 # show firewall address csf_ns_group
config firewall address
    edit "csf_ns_group"
        set uuid ee4a2696-bacd-51e9-f828-59457565b880
        set type dynamic
        set sdn "nsx_t24"
        set obj-id "336914ba-0660-4840-b0f1-9320f5c5ca5e"
        config list
            edit "1.1.1.0"
            next
            edit "1.1.1.1"
            next
            edit "172.16.10.104"
            next
            edit "172.16.20.104"
            next
            edit "172.16.30.104"
            next
            edit "2.2.2.0"
            next
            edit "2.2.2.2"
            next
            edit "4.4.4.0"
            next
            edit "5.5.5.0"
            next
            edit "6.6.6.6"
            next
            edit "7.7.7.7"
```

```
            next
        end
    next
end
```

UX / Usability

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

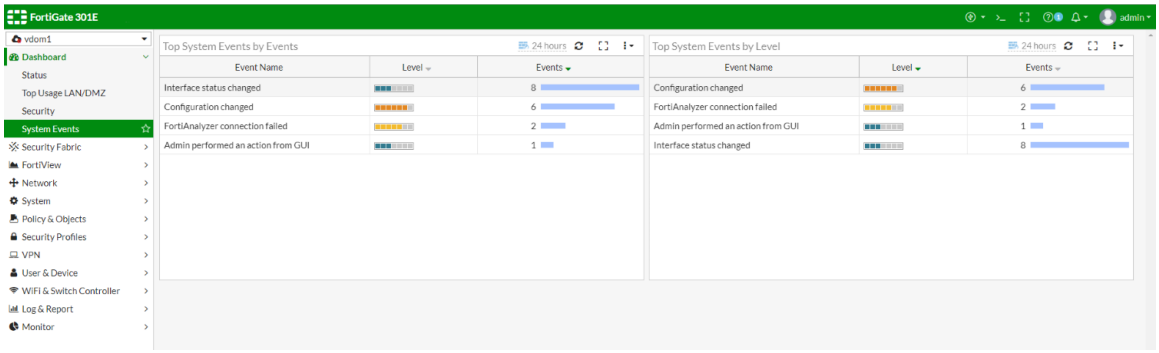
System Events default dashboard

The newly added *System Events* dashboard contains two widgets by default:

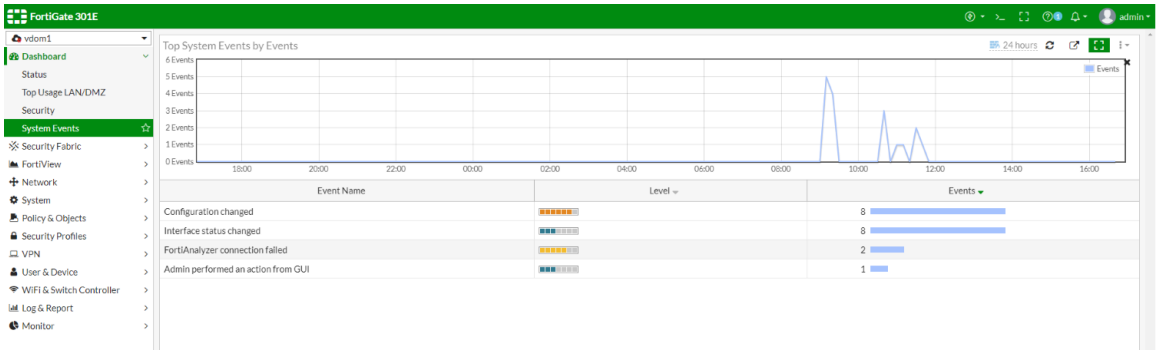
- *Top System Events by Events* (sorted by event count)
- *Top System Events by Level* (sorted by event severity)

To view the *System Events* dashboard in the GUI:

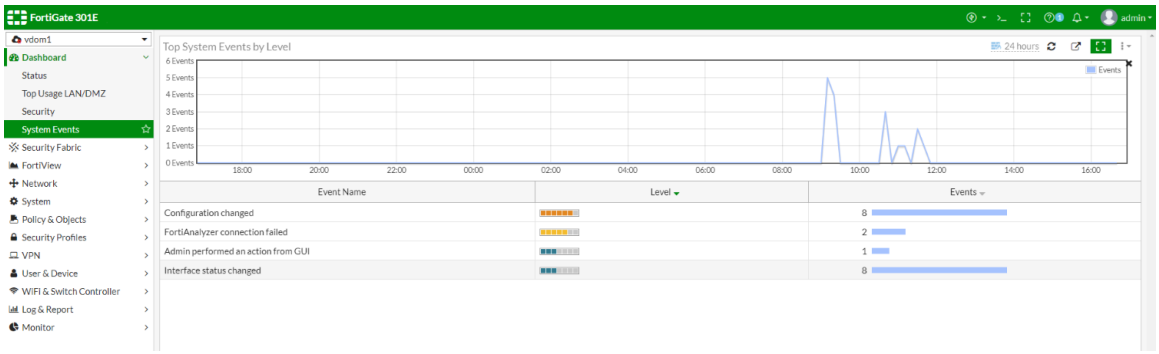
1. Go to *Dashboard* > *System Events*. The default dashboard appears.



2. Click the *Expand to full screen* icon within a widget to view additional details, such as historical trending charts.
   - Full screen view of *Top System Events by Events* widget:



- Full screen view of *Top System Events by Level* widget:



3. Double-click an event entry to view the specific event log.

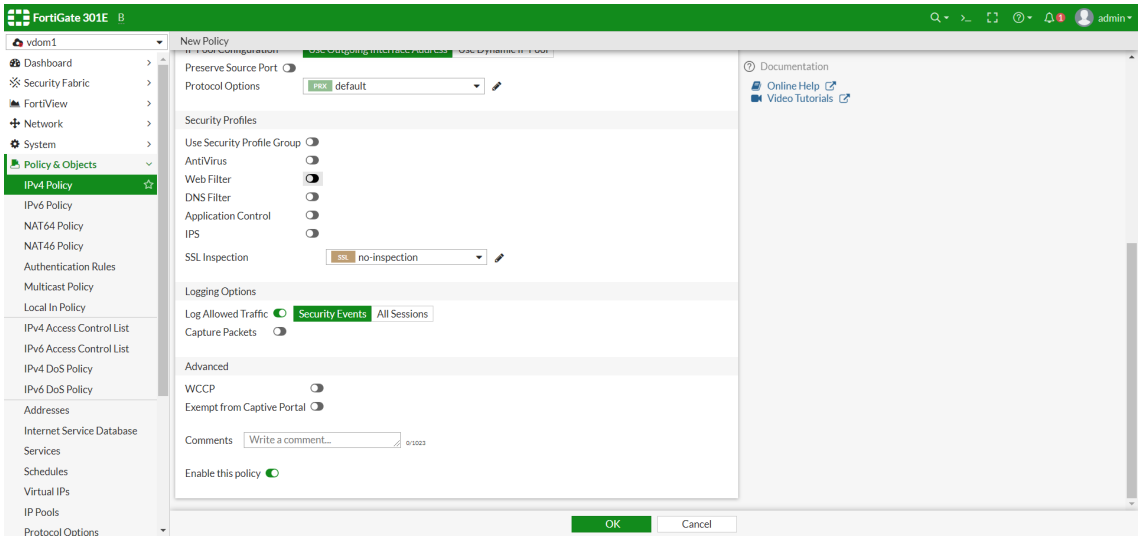
Advanced policy options in the GUI

Advanced policy options can be enabled so that they can be configured in the GUI.

To enable advanced policy options:

```
config system settings
    set gui-advanced-policy enable
end
```

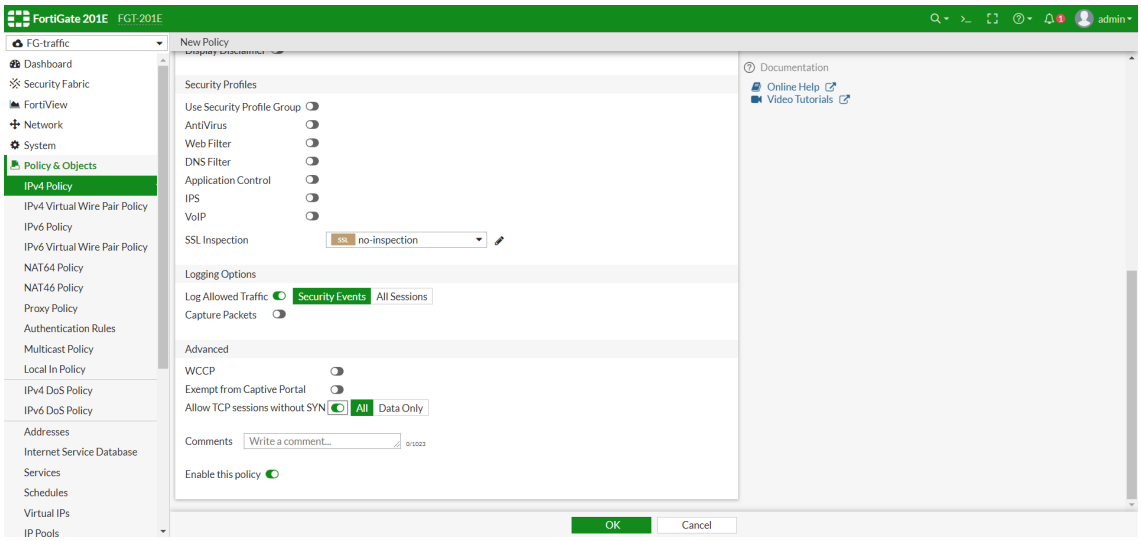
Advanced policy options are now available when creating or editing a policy in the GUI:



To enable configuring TCP sessions without SYN:

```
config system settings
    set tcp-session-without-syn enable
end
```

TCP sessions without SYN can now be configured when creating or editing a policy in the GUI:



Support for wildcard FQDN addresses in firewall policy

You can use wildcard FQDN addresses in firewall policies.

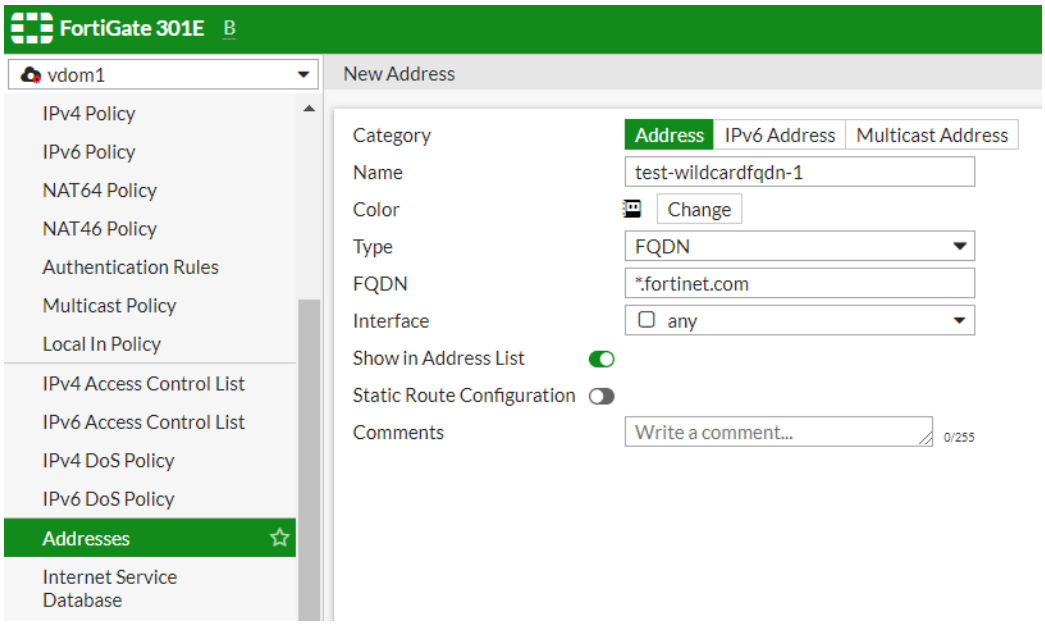
Firewall policies that support wildcard FQDN addresses include IPv4, IPv6, ACL, local, shaping, NAT64, NAT46, and NGFW.

When the wildcard FQDN gets the resolved IP addresses, FortiOS loads the addresses into the firewall policy for traffic matching.

To create a wildcard FQDN using the GUI:

1. Go to *Policy & Objects* > *Addresses* and click *Create New* > *Address*.
2. Specify a *Name*.
3. For *Type*, select *FQDN*.

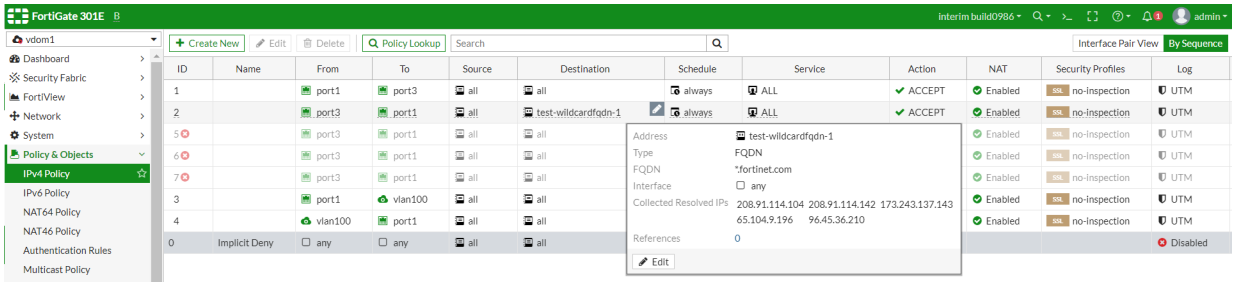
4. For *FQDN*, enter a wildcard FQDN address, for example, **.fortinet.com*.



5. Click *OK*.

To use wildcard FQDN in a firewall policy using the GUI:

1. Go to *Policy & Objects* > *IPv4 Policy* to view the policy you created with the wildcard FQDN. In this example, policy ID 2 uses the wildcard FQDN.



To create a wildcard FQDN using the CLI:

```
config firewall address
    edit "test-wildcardfqdn-1"
        set uuid 7288ba26-ce92-51e9-04c0-39c707eb4519
        set type fqdn
        set fqdn "*.fortinet.com"
    next
end
```

To use wildcard FQDN in a firewall policy using the CLI:

```
config firewall policy
    edit 2
        set uuid 2f5ffcc0-cddc-51e9-0642-ab9966b202dd
        set srcintf "port3"
```

```
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "test-wildcardfqdn-1"
        set action accept
        set schedule "always"
        set service "ALL"
        set auto-asic-offload disable
        set nat enable
    next
end
```

To use the diagnose command to list resolved IP addresses of wildcard FQDN objects:

```
B (vdom1) # diag firewall fqdn list
List all FQDN:
*.fortinet.com: ID(48) ADDR(208.91.114.104) ADDR(208.91.114.142) ADDR(173.243.137.143) ADDR
(65.104.9.196) ADDR(96.45.36.210)
*.google.com: ID(66) ADDR(172.217.14.238)
login.microsoftonline.com: ID(15) ADDR(40.126.7.64) ADDR(40.126.7.65) ADDR(40.126.7.66) ADDR
(40.126.7.97) ADDR(40.126.7.99) ADDR(40.126.7.100) ADDR(40.126.7.101) ADDR(40.126.7.103)
```

To use the diagnose command for firewall policies which use wildcard FQDN:

```
B (vdom1) # diag firewall iprope list 100004
policy index=2 uuid_idx=46 action=accept
flag (8050108): redir nat master use_src pol_stats
flag2 (4200): no_asic resolve_sso
flag3 (20):
schedule(always)
cos_fwd=255  cos_rev=255
group=00100004 av=00004e20 au=00000000 split=00000000
host=3 chk_client_info=0x0 app_list=0 ips_view=0
misc=0 dd_type=0 dd_mode=0
zone(1): 11 -> zone(1): 9
source(1): 0.0.0.0-255.255.255.255, uuid_idx=0,
destination fqdn or dynamic address (1):
        *.fortinet.com ID(48) uuid_idx=57 ADDR(208.91.114.104) ADDR(208.91.114.142) ADDR
(173.243.137.143) ADDR(65.104.9.196) ADDR(96.45.36.210)
service(1):
        [0:0x0:0/(0,0)->(0,0)] helper:auto
```

Traffic class ID configuration updates

These updates make the shaping feature more user-friendly, which can be configured per VDOM. You can configure each traffic class ID with a descriptive name in three locations within the GUI or with the new `firewall traffic-class` CLI command. This will help you correlate traffic shaping policy and profile entries.

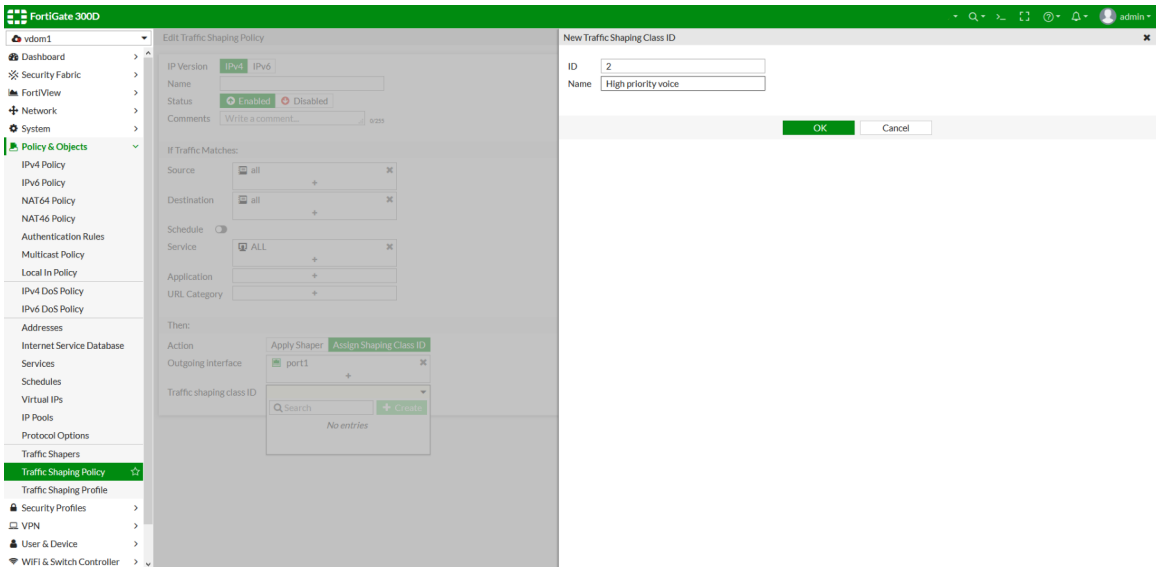
GUI updates

Within the GUI, there are three locations to configure the traffic class ID:

- Traffic shaping policy
- Traffic shaping profile
- Interface

To configure the traffic class ID in a traffic shaping policy:

1. Go to *Policy & Objects* > *Traffic Shaping Policy*.
2. Edit an existing policy, or create a new one.
3. In the *Then: Action* section, click *Assign Shaping Class ID*.
4. In *Traffic shaping class ID*, click *Create*.
5. Enter a value for the *ID* (integer) and a description for the *Name*.
6. Click *OK* to save the class ID.

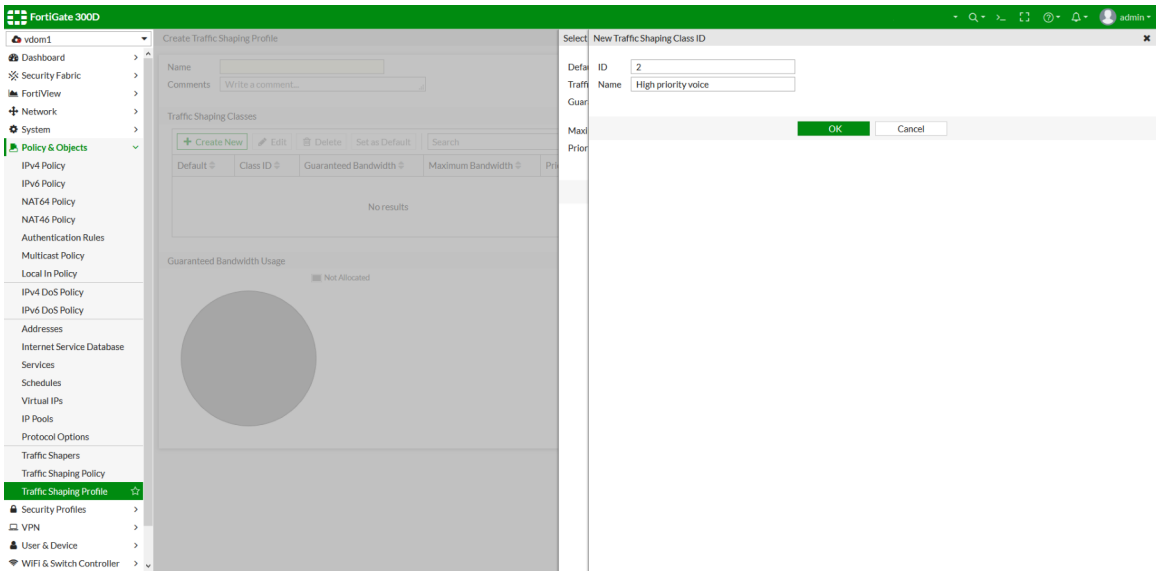


7. Configure the rest of the policy as needed.
8. Click *OK* to save the policy.

To configure the traffic class ID in a traffic shaping profile:

1. Go to *Policy & Objects* > *Traffic Shaping Profile*.
2. Edit an existing profile, or create a new one.
3. In the *Traffic Shaping Classes* section, click *Create New*. The *Select Traffic Shaping Class ID* window opens.
4. Click *Create*. The *New Traffic Shaping Class ID* window opens.
5. Enter a value for the *ID* (integer) and a description for the *Name*.

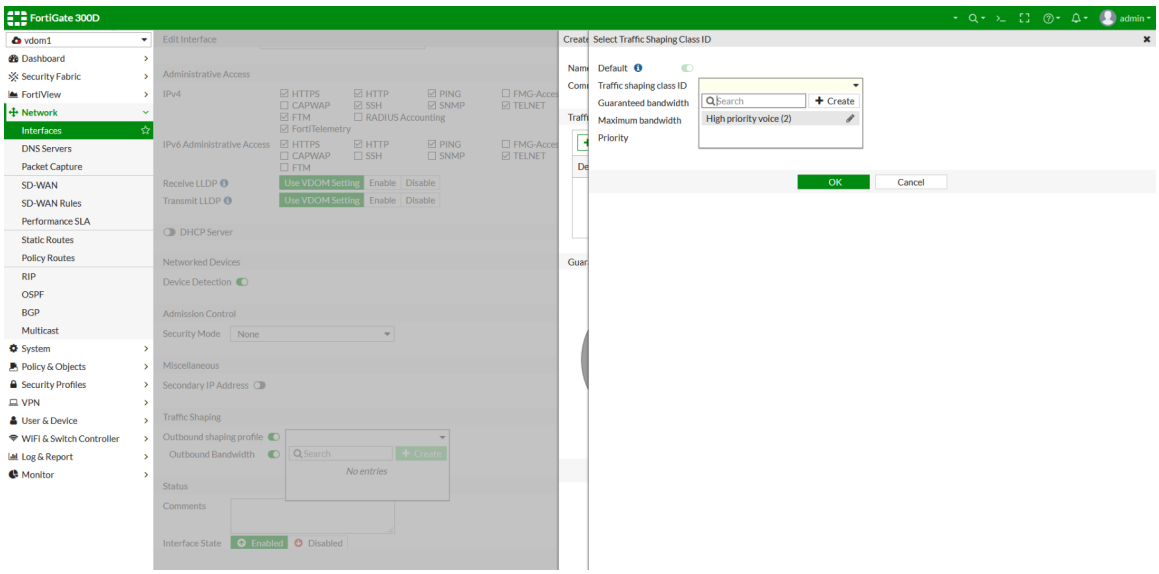
6. Click *OK* to save the class ID.



7. Click *OK* to add the class ID.
8. Configure the rest of the profile as needed.
9. Click *OK* to save the profile.

To configure the traffic class ID in an interface:

1. Go to *Network* > *Interfaces*.
2. Edit an existing interface, or create a new one.
3. In the *Traffic Shaping* section, enable *Outbound shaping profile* and *Outbound Bandwidth*.
4. Click *Create*. The *Create Traffic Shaping Profile* window opens.
5. Click *Create New*. The *Select Traffic Shaping Class ID* window opens.
6. Select an existing class ID, or create a new one.
7. Click *OK* to save the class ID.



8. Click *OK* to add the class ID .
9. Configure the rest of the interface as needed.
10. Click *OK* to save the interface.

CLI update

To configure the traffic class ID in the CLI:

```
config firewall traffic-class
    edit 2
        set class-name "High priority voice."
    next
    ...
end
```

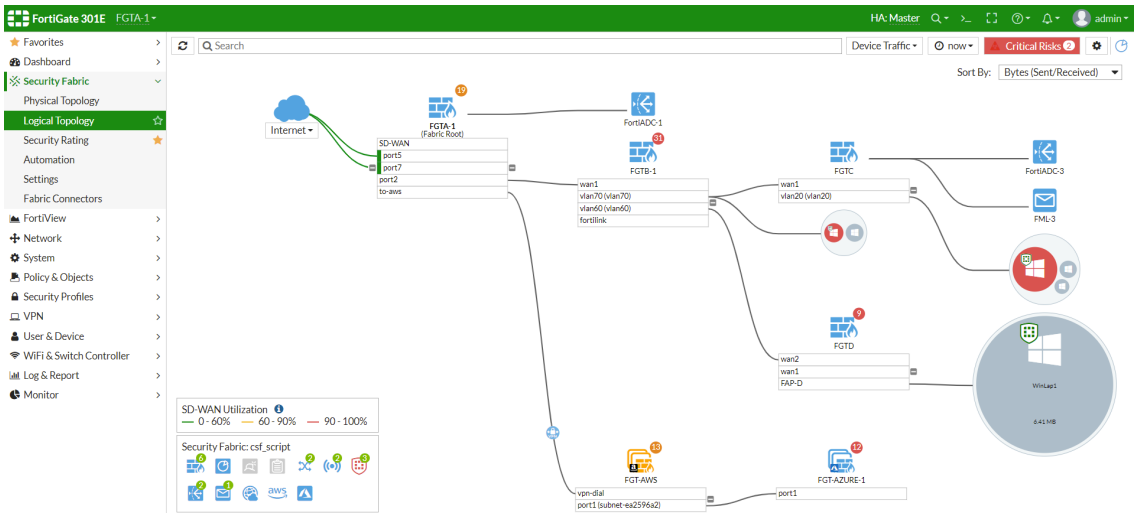
Security Fabric topology improvements

The topology views have been enhanced to include:

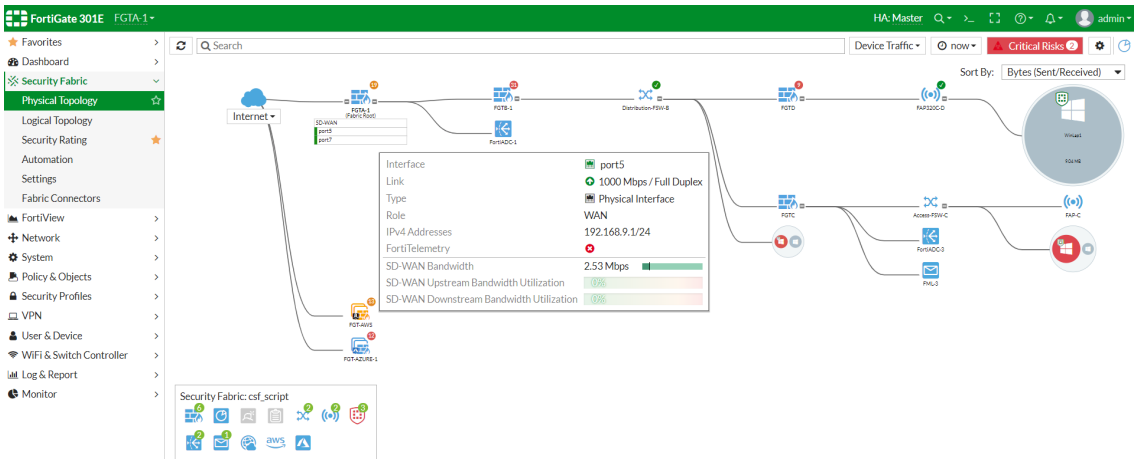
- Broader visibility into SD-WAN link utilization
- Simplified filtering for AWS, Azure, SD-WAN, and Security Fabric devices

SD-WAN visibility

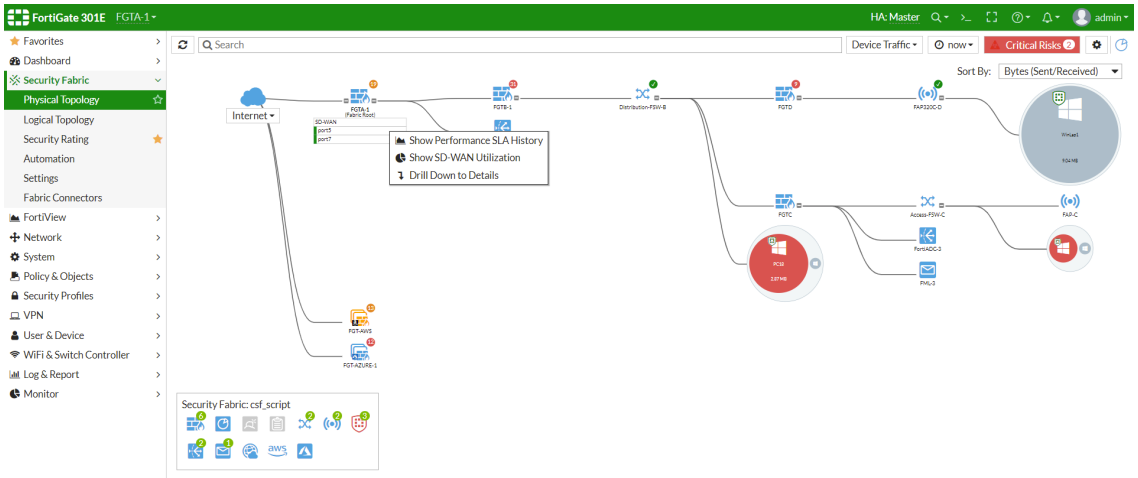
SD-WAN links are shown in the physical and logical topology views:

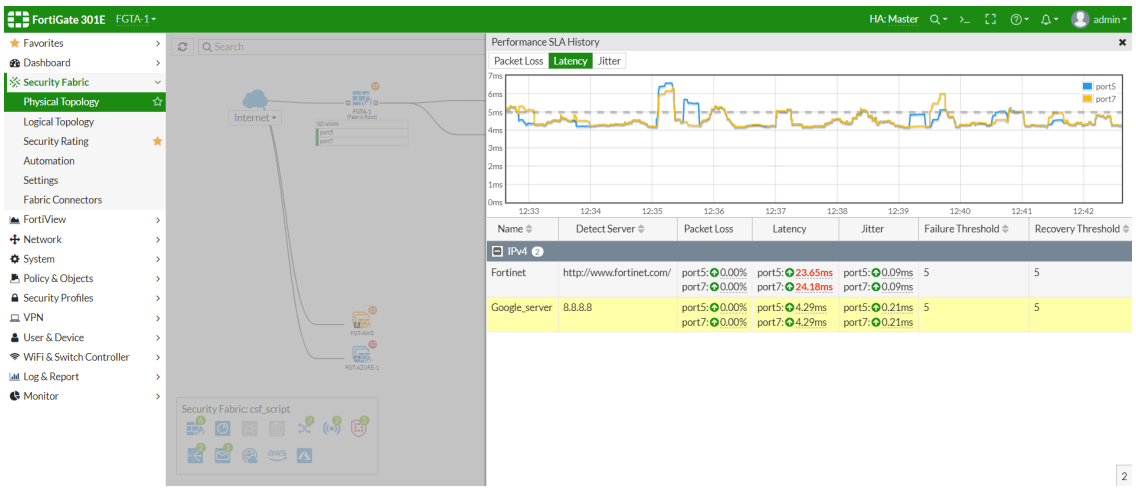


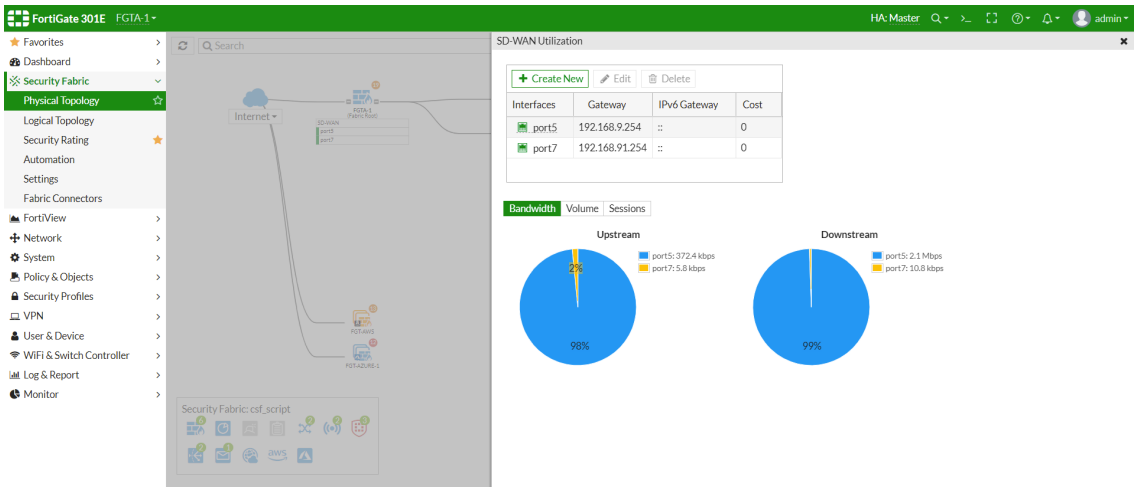
The SD-WAN utilization is shown in the tooltips:



You can drill down to view performance SLA history and SD-WAN utilization:

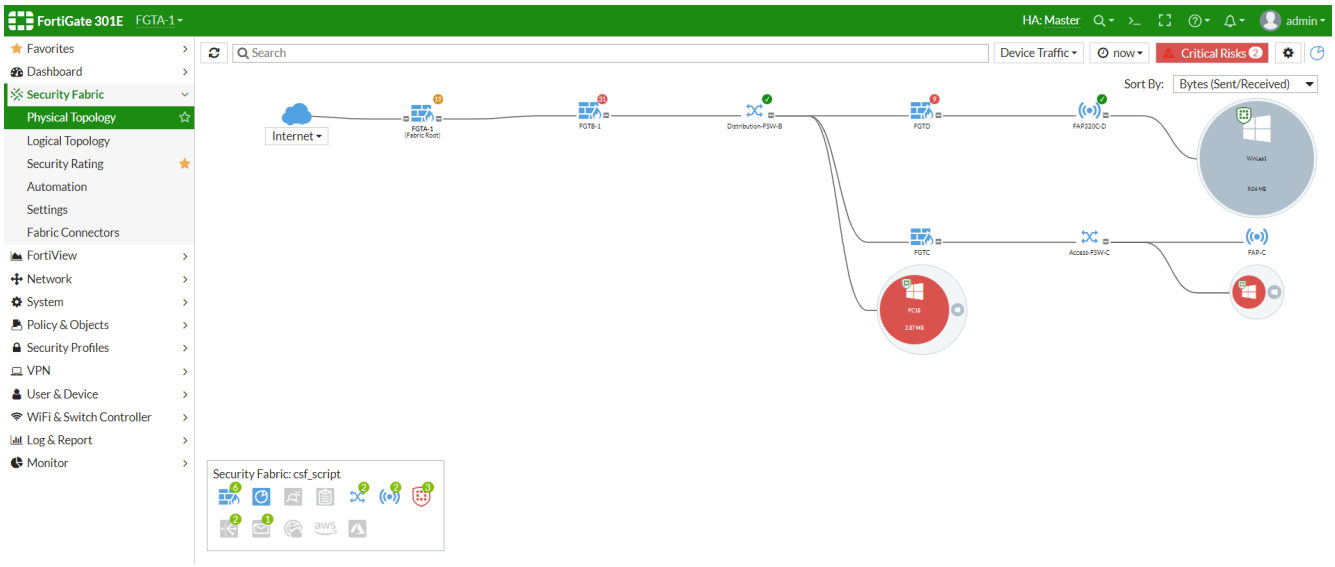






Fabric device filtering

SD-WAN, AWS, Azure, and fabric devices can be shown or hidden in the topology view by toggling their icons in the box at the bottom of the topology view.



Other

This section lists other new features added to FortiOS.

Protocols

This section lists other new features added to FortiOS related to protocols.

LACP support on entry-level devices

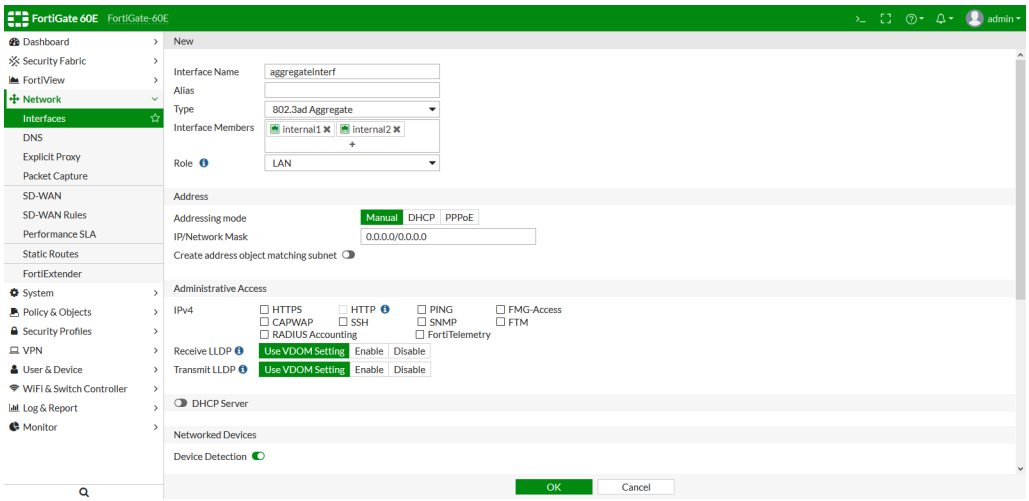
Link Aggregation Control Protocol (LACP) is now supported on the following devices in FortiOS 6.2.2:

- FortiGate Rugged 30D and 35D
- FortiGate 30E-MI, 30E-MN, 51E, 52E, 60E-POE, 61E, 80D, 80E-POE, 81E, 81E-POE, 91E, and 92D
- FortiWiFi 30E-MI, 30E-MN, 50E-2R, 51E, and 61E

To create a link aggregation interface in the GUI:

1. Go to *Network* > *Interfaces*.
2. Click *Create New* > *Interface*.
3. Set *Type* to *802.3ad Aggregate*.

4. Configure the other settings as required.



5. Click *OK*.

To create a link aggregation interface in the CLI:

```
configure system interface
    edit "aggregateinterf"
        set vdom "root"
        set type aggregate
        set member "internal1" "internal2"
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 13
    next
end
```

To check the aggregate interface status:

```
diagnose netlink aggregate name <name of aggregate interface>
```

Ignore AUTH TLS command for DLP

If the FortiGate receives an AUTH TLS (PBSZ and PROT) command before receiving plain text traffic from a decrypted device, by default, it will expect encrypted traffic, determine that the traffic belongs to an abnormal protocol, and by-pass the traffic.

When the `ssl-offloaded` command is enabled, the AUTH TLS command is ignored, and the traffic is treated as plain text rather than encrypted data.

To ignore received AUTH TLS commands:

```
config firewall profile-protocol-options
    edit "test"
        config ftp
            set ssl-offloaded yes
```

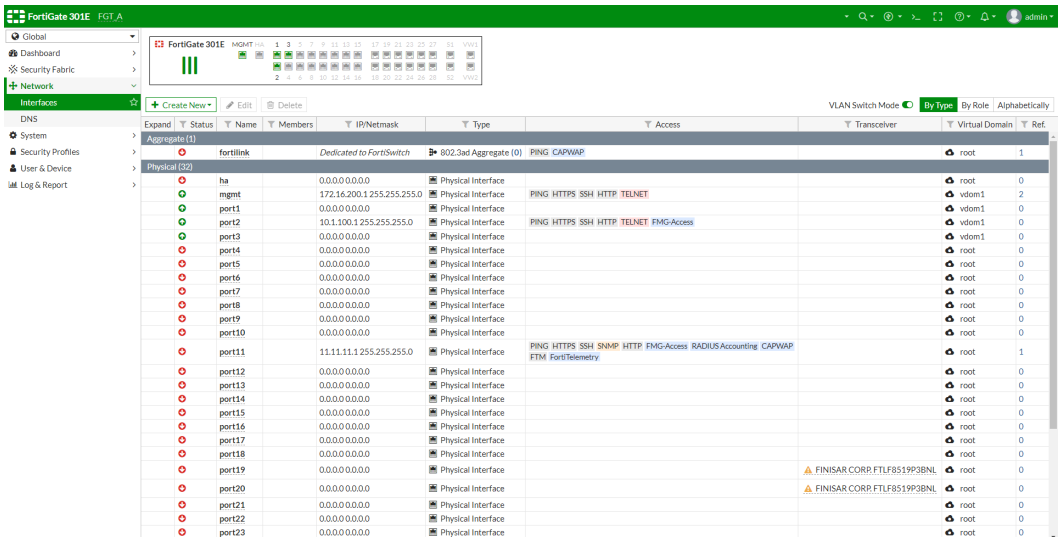
```
        end
        config imap
            set ssl-offloaded yes
        end
        config pop3
            set ssl-offloaded yes
        end
        config smtp
            set ssl-offloaded yes
        end
    next
end
```

Virtual switch support for FortiGate 300E series

Support has been added for virtual switches in the FortiGate 300E series. This allows switch ports to be assigned to different VLANs.

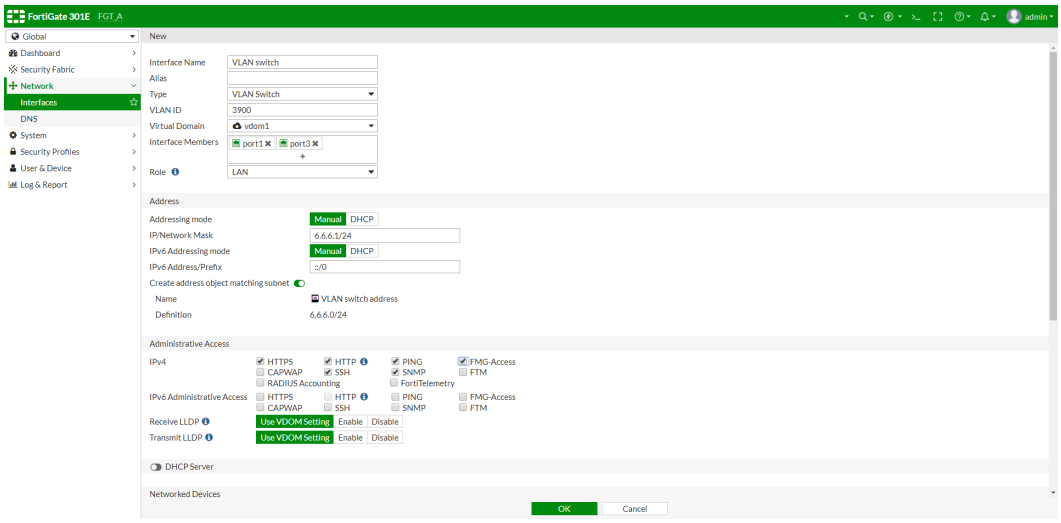
To create a VLAN switch in the GUI:

1. Go to *Network* > *Interfaces* and enable *VLAN Switch Mode*.

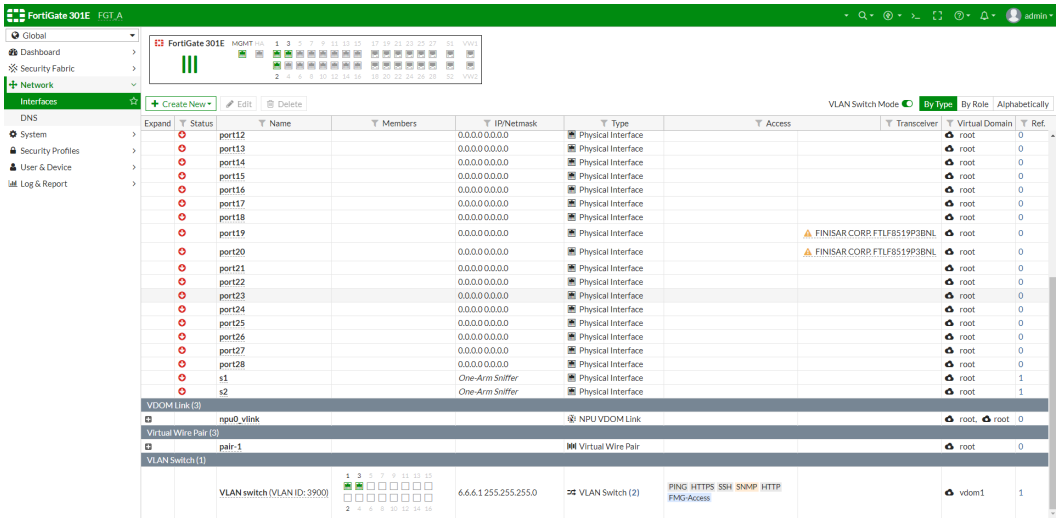


2. Click *Create New* > *Interface*.
3. Enter an interface name and configure the following:
   a. For *Type*, select *VLAN Switch*.
   b. (Optional) Enter a *VLAN ID* (range is 3900–3999).
   c. If applicable, select a *Virtual Domain*.
   d. Add the *Interface Members*.
   e. Configure the *Address* and *Administrative Access* settings as needed.

4. Click *OK*.



The new VLAN switch is visible in the interface table:



To create a VLAN switch in the CLI:

1. Enable VLAN switch mode:

```
config system global
    set virtual-switch-vlan enable
end
```

2. Create the VLAN switch. Optionally, you can assign an ID to the VLAN:
The default ID is `0`. You can use the default ID, or you can assign an ID to the VLAN (3900–3999).

```
config system virtual-switch
    edit "VLAN switch"
        set physical-switch "sw0"
        set vlan 3900
        config port
            edit "port1"
            next
```

```
            edit "port3"
            next
        end
    next
end
```

3. Configure the VLAN switch interface:

```
config system interface
    edit "VLAN switch"
        set vdom "vdom1"
        set ip 6.6.6.1 255.255.255.0
        set allowaccess ping https ssh snmp http fgfm
        set type hard-switch
        set snmp-index 15
    next
end
```

4. (Optional) Create a trunk interface:

```
config system interface
    edit port2
        set trunk enable
    next
end
```

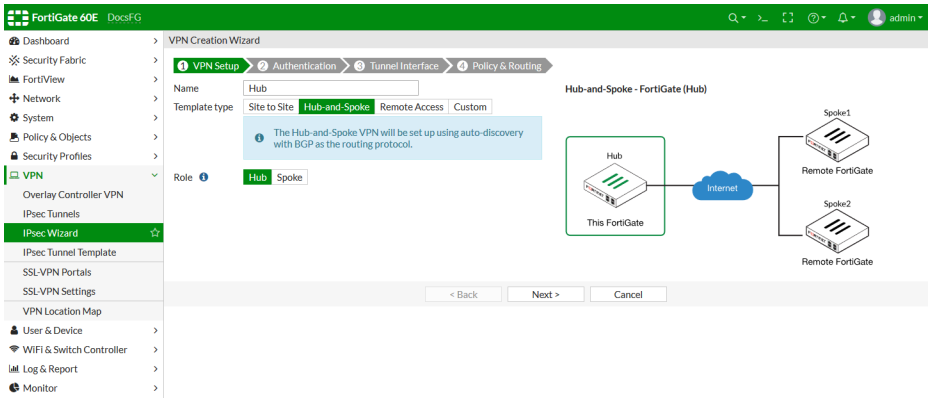
IPsec VPN wizard hub-and-spoke ADVPN support

The IPsec Wizard can be used to create hub-and-spoke VPNs, with ADVPN enabled to establish tunnels between spokes.

The following example shows the steps in the wizard for configuring a hub and a spoke.

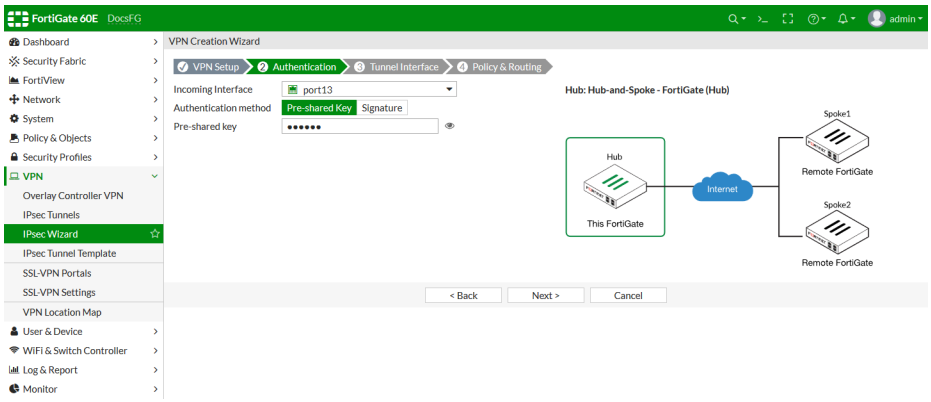
To configure the hub:

1. On the hub FortiGate, go to *VPN* > *IPsec Wizard*.

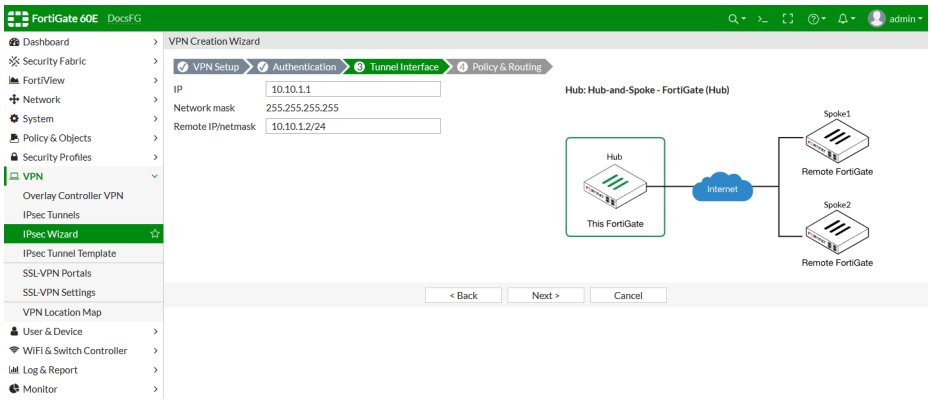


2. Enter a name, set the *Template Type* to *Hub-and-Spoke*, and set the *Role* to *Hub*.

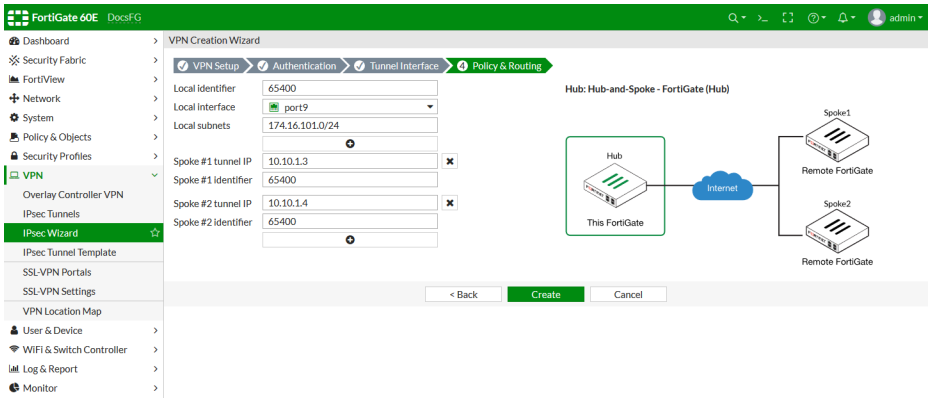
3. Click *Next*.



4. Select the *Incoming Interface* and configure the *Authentication method*.
5. Click *Next*.

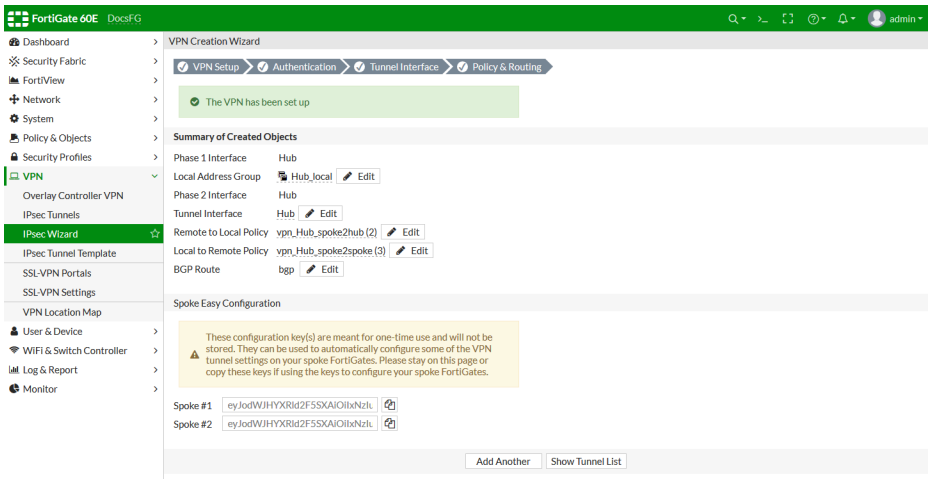


6. Set the *IP* address and *Remote IP/netmask*.
7. Click *Next*.



8. Configure the *Local identifier*, *Local interface*, and *Local subnets*, then configure the tunnel IP addresses and identifiers for the spokes.

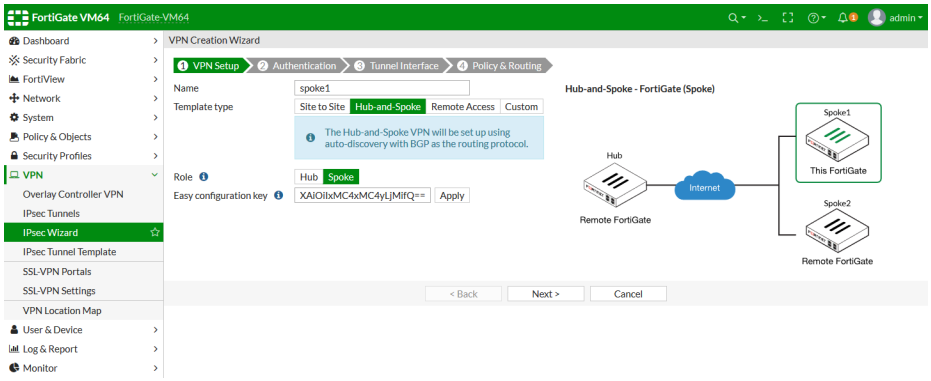
9. Click *Create*.



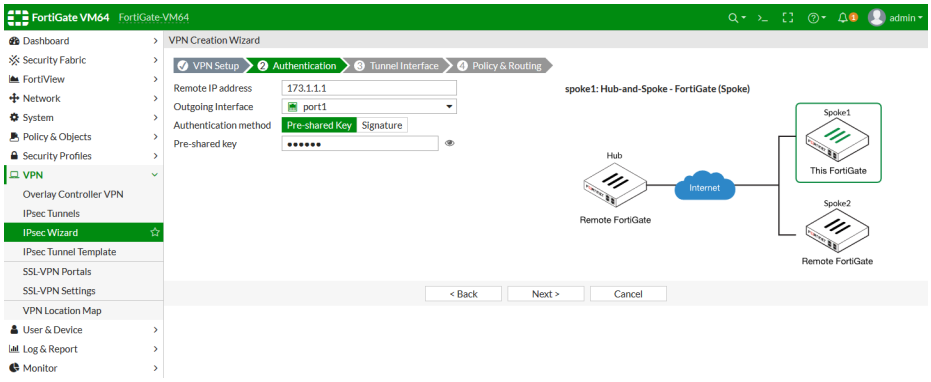
10. Review the summary to ensure that everything looks as expected.
11. Copy the spokes' easy configuration keys to a temporary location for use when configuring the spokes.

To configure a spoke:

1. On the spoke FortiGate, go to *VPN > IPsec Wizard*.

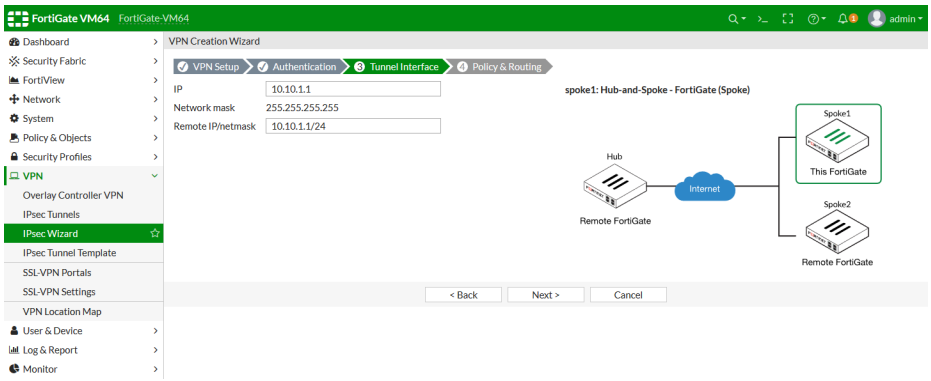


2. Enter a name, set the *Template Type* to *Hub-and-Spoke*, set the *Role* to *Spoke*, and paste in the requisite *Easy configuration key* that you saved when configuring the hub.
3. Click *Next*.

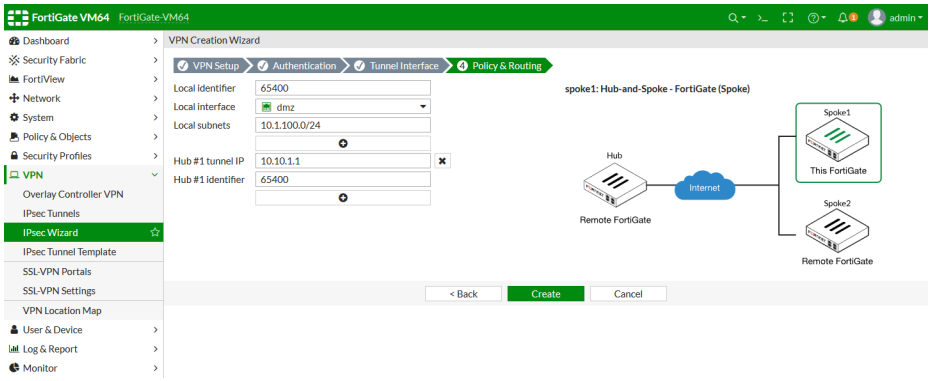


4. Set the *Remote IP address*, select the *Incoming Interface*, and configure the *Authentication method*.

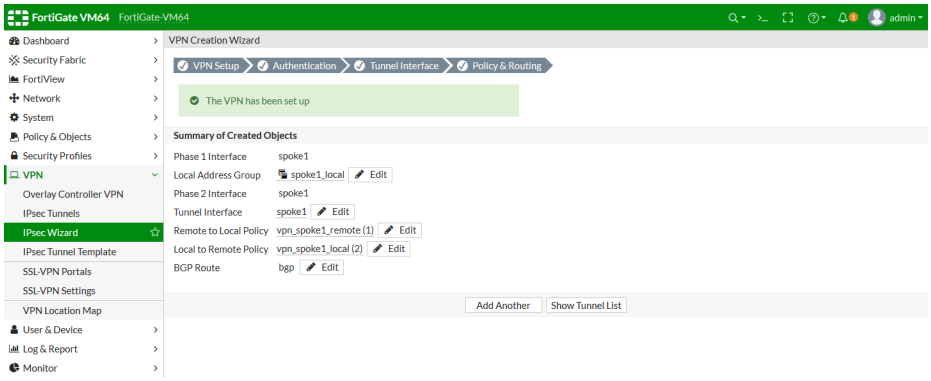
5. Click *Next*.



6. Set the *IP* address and *Remote IP/netmask*.
7. Click *Next*.



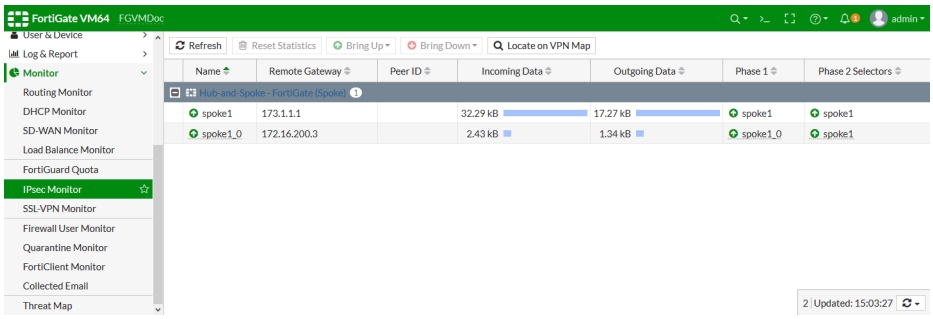
8. Configure the *Local identifier*, *Local interface*, and *Local subnets*, then configure the IP address and identifier of the hub FortiGate.
9. Click *Create*.



10. Review the summary to ensure that everything looks as expected.

To check the ADVPN shortcut with the IPsec monitor:

1. On either the hub or spoke FortiGate, go to *Monitor* > *IPsec Monitor*.



FortiGuard communication over port 443 with HTTPS

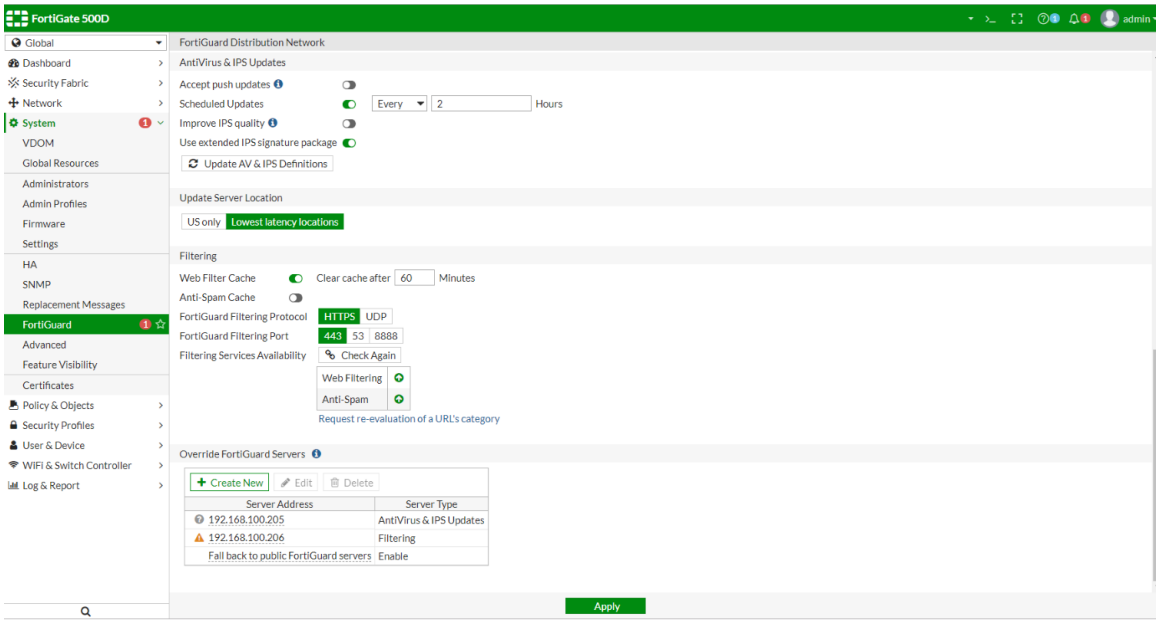
In FortiOS 6.2.2, the FortiGuard server now supports HTTPS on port 443, which allows for FortiManager support.

FortiGuard filtering now supports the following protocol and port configurations:

- HTTPS: ports 443, 53, and 8888 (default port)
- UDP: ports 53 and 8888
- HTTP: port 80

To configure the FortiGuard filtering protocol for HTTPS in the GUI:

1. Go to *System* > *FortiGuard* and navigate to the *Filtering* section.
2. For *FortiGuard Filtering Protocol*, select *HTTPS*.
3. For *FortiGuard Filtering Port*, select a port (either *443*, *53*, or *8888*).
4. Click *Apply* to save your changes.



To configure the FortiGuard filtering protocol for HTTPS in the CLI:

```
config system fortiguard
    set protocol https
    set port {8888 | 53 | 443}
    ...
end
```

IPv6 FortiGuard connections

The Fortinet DNS can resolve FortiGuard related servers to both IPv4 and IPv6 addresses. FortiOS daemons (update, forticldd, url) connect using either IPv4 or IPv6 addresses. The first available connection will be used for updates or the rating service.

To configure an interface and route for IPv6:

```
config system interface
    edit "wan1"
        set vdom "root"
        config ipv6
            set ip6-address 2000:172:16:200::1/64
        end
    next
end
```

```
config router static6
    edit 1
        set gateway 2000:172:16:200::254
        set device "wan1"
    next
end
```

To configure push updates:

```
config system autoupdate push-update
    set status enable
    set override enable
    set address "2620:101:9005:3860::94"
end
```

SSH file scan

File scanning over SSH traffic (SCP and SFTP) is part of firewall profile-protocol-options, ssh-filter profile, AV profile, and DLP sensor. FortiGate devices can buffer, scan, log, or block files sent over SCP and SFTP depending on its file-size, file-type, or file-contents (such as virus or sensitive contents).

This feature includes the following SSH settings in CLI:

- SSH protocol options in firewall `protocol-profile` options.
- SCP block/log options in `ssh-filter-profile`.

- `file-filter` feature added in `ssh-filter-profile`.
- SCP/SFTP options in DLP sensor.
- SSH scan options in AV profile.
- SSH AV quarantine options.
- Logs for SCP and SFTP traffic.
- Replacement message for SCP and SFTP traffic.

To configure SSH protocol options in firewall protocol-profile options:

```
config firewall profile-protocol-options
  edit "protocol"
    config ssh
      set options [oversize | clientcomfort | servercomfort]    <-- Block oversized file | pre-
vent client/server timeout.
      set comfort-interval [1 - 900]                            <-- Frequency in seconds that
FGT periodically sends packet to client/server to prevent timeout.
      set comfort-amount [1 - 65535]                            <-- Number of bytes to send in
each transmission to prevent timeout.
      set oversize-limit [1 - 798]                              <-- Maximum in-memory file
size that can be scanned (MB).
      set uncompressed-oversize-limit [0 - 798]                 <-- Maximum in-memory uncom-
pressed file size that can be scanned.
      set uncompressed-nest-limit [2 - 100]                     <-- Maximum nested levels of
compression that can be uncompressed and scanned.
      set scan-bzip2 [enable | disable]                         <-- Enable/disable scanning of
BZip2 compressed files.
    end
```

To configure SCP block/log options in ssh-filter-profile:

```
config ssh-filter profile
  edit "ssh-test"
      set block scp             <-- Block scp traffic.
      set log scp               <-- Log scp traffic.
  next
end
```

To configure file-filter feature added in ssh-filter-profile:

```
config ssh-filter profile
  edit "ssh-test"
    config file-filter
      set status [enable | disable]                   <-- Enable/disable disable file-filter.
      set log [enable | disable]                      <-- Enable/disable file-filter log.
      set scan-archive-contents [enable | disable]    <-- Allow FGT to scan contents of
archive file.
      config entries
        edit "1"
          set comment ''
          set action [block | log]                    <-- Block/only log the file transfer.
          set direction [incoming | outgoing | any]   <-- Allow file-filter to take effect on
incoming/outgoing/any traffic.
          set password-protected [yes | any]          <-- If 'yes', file-filter only matches
password-protected archive files (encrypted zip).
```

```
          set file-type "msoffice"                    <-- Choose file-types for file-filter to
match.
        next
      end
    end
  next
end
```

To configure SCP/SFTP options in DLP sensor:

```
config dlp sensor
  edit "test"
    set full-archive-proto ssh      <-- Allow dlp sensor to archive scp and sftp traffic.
    set summary-proto ssh           <-- Allow dlp sensor to summarize archive records inform-
ation for scp and sftp traffic.
    config filter
      edit 1
        set proto ssh               <-- Allow dlp sensor to check files sent over scp and
sftp.
      next
    end
  next
end
```

To configure SSH scan options in AV profile:

```
config antivirus profile
  edit "av"
    config ssh                                                  <-- Allow FGT to scan scp and
sftp traffic.
      set options [scan | avmonitor | quarantine]
      set archive-block [encrypted | corrupted | partiallycorrupted | multipart | nested |
mailbomb | fileslimit | timeout | unhandled]  <-- Choose archive file types to block.
      set archive-log [encrypted | corrupted | partiallycorrupted | multipart | nested | mail-
bomb | fileslimit | timeout | unhandled]    <-- Choose archive file types to log.
      set emulator [enable | disable]                           <-- Enable/disable virus emu-
lator.
      set outbreak-prevention [disabled | files | full-archive]  <-- Analyze (or not analyze)
contents of archives for outbreak prevention.
    end
  next
end
```

To configure SSH AV quarantine options:

```
config antivirus quarantine
  set drop-infected ssh      <-- Drop and delete infected files sent over scp and sftp.
  set store-infected ssh     <-- Quarantine infected files sent over scp and sftp.
  set drop-blocked ssh       <-- Drop and delete blocked files sent over scp and sftp.
  set store-blocked ssh      <-- Quarantine blocked files sent over scp and sftp.
  set drop-heuristic ssh     <-- Drop and delete files detected by heuristics sent over scp
and sftp.
  set store-heuristic ssh    <-- Quarantine files detected by heuristics sent over scp and
sftp.
end
```

To configure logs for SCP and SFTP traffic:

```
scp traffic blocked by ssh-filter profile:
    1: date=2019-07-24 time=10:34:42 logid="1601061010" type="utm" subtype="ssh" event-
type="ssh-channel" level="warning" vd="vdom1" eventtime=1563989682560488314 tz="-0700" poli-
cyid=1 sessionid=2693 profile="ssh-test" srcip=10.1.100.11 srcport=33044 dstip=172.16.200.44
dstport=22 srcintf="port1" srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" pro-
to=6 action="blocked" direction="outgoing" login="root" channeltype="scp"

scp traffic blocked by file-filter:
    1: date=2019-07-24 time=10:36:44 logid="1900064000" type="utm" subtype="file-filter" event-
type="file-filter" level="warning" vd="vdom1" eventtime=1563989804387444023 tz="-0700" poli-
cyid=1 sessionid=2732 srcip=10.1.100.11 srcport=33048 srcintf="port1" srcintfrole="undefined"
dstip=172.16.200.44 dstport=22 dstintf="port3" dstintfrole="undefined" proto=6 service="SSH"
subservice="SCP" profile="ssh-test" direction="incoming" action="blocked" filtername="1" file-
name="test.xls" filesize=13824 filetype="msoffice" msg="File was blocked by file filter."

sftp traffic blocked by file-filter:
    1: date=2019-07-24 time=10:43:58 logid="1900064000" type="utm" subtype="file-filter" event-
type="file-filter" level="warning" vd="vdom1" eventtime=1563990238339440605 tz="-0700" poli-
cyid=1 sessionid=2849 srcip=10.1.100.11 srcport=33056 srcintf="port1" srcintfrole="undefined"
dstip=172.16.200.44 dstport=22 dstintf="port3" dstintfrole="undefined" proto=6 service="SSH"
subservice="SFTP" profile="ssh-test" direction="incoming" action="blocked" filtername="1" file-
name="test.xls" filesize=13824 filetype="msoffice" msg="File was blocked by file filter."

scp traffic blocked by dlp sensor:
    1: date=2019-07-24 time=10:41:23 logid="0954024576" type="utm" subtype="dlp" event-
type="dlp" level="warning" vd="vdom1" eventtime=1563990083875731367 tz="-0700" filteridx=1 fil-
tername="test" dlpextra="builtin-patterns" filtertype="file-type" filtercat="file"
severity="medium" policyid=1 sessionid=2809 epoch=1425775842 eventid=0 srcip=10.1.100.11 src-
port=33052 srcintf="port1" srcintfrole="undefined" dstip=172.16.200.44 dstport=22 dstint-
f="port3" dstintfrole="undefined" proto=6 service="SSH" subservice="SCP" filetype="msoffice"
direction="incoming" action="block" filename="test.xls" filesize=13824 profile="test"

sftp traffic blocked by dlp sensor:
    1: date=2019-07-24 time=10:42:42 logid="0954024576" type="utm" subtype="dlp" event-
type="dlp" level="warning" vd="vdom1" eventtime=1563990162266253784 tz="-0700" filteridx=1 fil-
tername="test" dlpextra="builtin-patterns" filtertype="file-type" filtercat="file"
severity="medium" policyid=1 sessionid=2838 epoch=1425775843 eventid=0 srcip=10.1.100.11 src-
port=33054 srcintf="port1" srcintfrole="undefined" dstip=172.16.200.44 dstport=22 dstint-
f="port3" dstintfrole="undefined" proto=6 service="SSH" subservice="SFTP" filetype="msoffice"
direction="incoming" action="block" filename="test.xls" filesize=13824 profile="test"

scp traffic blocked by av profile:
    1: date=2019-07-24 time=10:45:57 logid="0211008192" type="utm" subtype="virus" event-
type="infected" level="warning" vd="vdom1" eventtime=1563990357330463670 tz="-0700" msg="File
is infected." action="blocked" service="SSH" subservice="SCP" sessionid=2875 srcip=10.1.100.11
dstip=172.16.200.44 srcport=33064 dstport=22 srcintf="port1" srcintfrole="undefined" dstint-
f="port3" dstintfrole="undefined" policyid=1 proto=6 direction="incoming" filename="eicar.exe"
checksum="53badd68" quarskip="No-skip" virus="EICAR_TEST_FILE" dtype="Virus" ref-
f="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE" virusid=2172 profile="av" ana-
lyticscksum="7fc2dfc5a2247d743556ef59abe3e03569a6241e2b1e44b9614fc764847fb637"
analyticssubmit="false" crscore=50 craction=2 crlevel="critical"

sftp traffic blocked by av profile:
    2: date=2019-07-24 time=10:45:46 logid="0211008192" type="utm" subtype="virus"
```

```
eventtype="infected" level="warning" vd="vdom1" eventtime=1563990346334781409 tz="-0700" msg-
g="File is infected." action="blocked" service="SSH" subservice="SFTP" sessionid=2874 srcip-
p=10.1.100.11 dstip=172.16.200.44 srcport=33062 dstport=22 srcintf="port1"
srcintfrole="undefined" dstintf="port3" dstintfrole="undefined" policyid=1 proto=6 dir-
ection="incoming" filename="eicar.exe" checksum="53badd68" quarskip="No-skip" virus="EICAR_
TEST_FILE" dtype="Virus" ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE" virusid=2172 pro-
file="av" analyticscksum="7fc2dfc5a2247d743556ef59abe3e03569a6241e2b1e44b9614fc764847fb637"
analyticssubmit="false" crscore=50 craction=2 crlevel="critical"

    antivirus quarantine list that triggered by infected file sent over scp/sftp:
    CHECKSUM SIZE     FIRST-TIMESTAMP  LAST-TIMESTAMP   SERVICE STATUS     DC       TTL
   FILENAME DESCRIPTION
    53badd68 12939    2019-07-24 10:45          2019-07-24 10:45         SSH     Infected
 1   FOREVER    'eicar.exe' 'EICAR_TEST_FILE'
```

Replacement messages for SCP and SFTP traffic

SFTP download/upload does not display replacement message due to client behavior.
SCP download does not currently display replacement message.

Replacement message for scp upload blocked by av:

```
The file "eicar.exe" has been blocked because it contains the virus "EICAR_TEST_FILE".
```

Replacement message for scp upload blocked by file-filter:

```
The file "test.xls" has been blocked due to its file type or properties.
```

Replacement message for scp upload blocked by dlp:

```
The file "eicar.exe" has been blocked due to a detected data leak.
```

FortiGuard third Party SSL validation and Anycast support

You can enable Anycast to optimize the routing performance to FortiGuard servers. Relying on Fortinet DNS servers, the FortiGate will get a single IP address for the domain name of each FortiGuard service. BGP routing optimization is transparent to the FortiGate. The domain name of each FortiGuard service is the common name in that service's certificate. The certificate is signed by a third party intermediate CA. The FortiGuard server uses the Online Certificate Status Protocol (OCSP) stapling technique, so that the FortiGate can always validate the FortiGuard server certificate efficiently.

To enable Anycast in the FortiGuard settings:

```
config system fortiguard
    set protocol https
    set port 443
    set fortiguard-anycast enable
```

```
    set fortiguard-anycast-source fortinet
end
```

After Anycast is enabled, the FortiGuard settings will enforce a connection using HTTPS and port 443.

Connection to FortiGuard

The FortiGate will only complete the TLS handshake with a FortiGuard that provides a *good* OCSP status for its certificate. Any other status will result in a failed SSL connection. OCSP stapling is reflected on the signature interval (currently, 24 hours) so that *good* means that the certificate is not revoked at that timestamp. The FortiGuard servers query the CA's OCSP responder every four hours and update its OCSP status. If the FortiGuard is unable to reach the OCSP responder, it will keep the last known OCSP status for seven days. This cached OCSP status will be sent out immediately when a client connection request is made, thus optimizing the response time.

The following steps are taken to connect to FortiGuard:

1. The FortiGate embeds the CA_bundle certificate, that includes the root CA with CRL list and third party intermediate CA, in the root CA level.
2. The FortiGate finds the FortiGuard IP address from its domain name from DNS:

   ```
   fds=qaupdate.fortinet.net-192.168.100.242
   ```

3. The FortiGate starts a TLS handshake with the FortiGuard IP address. The client Hello includes an extension of the *status request*.
4. The FortiGuard servers provide a certificate with its OCSP status: *good*, *revoked*, or *unknown*.
5. The FortiGate verifies the CA chain against the root CA in CA_bundle.
6. The FortiGate verifies the intermediate CA's revoke status against the root CA's CRL.
7. The FortiGate verifies the FortiGuard certificate's OCSP status:

   ```
   OCSP Response Data:
       OCSP Response Status: successful (0x0)
       Response Type: Basic OCSP Response
       Version: 1 (0x0)
       Responder Id: 3DD350A5D6A0ADEEF34A600A65D321D4F8F8D60F
       Produced At: Aug 20 07:50:58 2019 GMT
       Responses:
       Certificate ID:
         Hash Algorithm: sha1
         Issuer Name Hash: 49F4BD8A18BF760698C5DE402D683B716AE4E686
         Issuer Key Hash: 3DD350A5D6A0ADEEF34A600A65D321D4F8F8D60F
         Serial Number: 02555C9F3901B799DF1873402FA9392D
       Cert Status: good
       This Update: Aug 20 07:50:58 2019 GMT
       Next Update: Aug 27 07:05:58 2019 GMT
   ```

Override FortiGuard servers

FortiManager can provide a local FortiGuard server with port 443 access.

Anycast FortiGuard settings force the rating process to use port 443, even with an override server. Using a unique address in the same subnet as the FortiManager access IP address, the FortiManager can provide local FortiGuard updates and rating access with a dedicated IP address and port 443.

To use a FortiManager as a local FortiGuard server:

```
config system central-management
    set type fortimanager
    set fmg "172.18.37.148"
    config server-list
        edit 1
            set server-type update
            set server-address 172.18.37.150
        next
        edit 2
            set server-type rating
            set server-address 172.18.37.149
        next
    end
    set fmg-update-port 443
    set include-default-servers enable
end
```

When `fmg-update-port` is set to `443`, the update process will use port 443 to connect to the override update server, which is the local FortiGuard server in the FortiManager. If this is not set, the update process will use port 8890, and the server address setting has to be the FortiManager access IP address. Override FortiGuard services come from the server list that is the local FortiGuard server in the FortiManager, and use the traditional, non-OCSP TLS handshake. If override servers in the FortiManager are not available, the default FortiGuard servers are connected, and the Anycast OCSP TLS handshake is used.

FortiClient EMS Cloud support

Both cloud-based and on-premise EMS servers are supported.

To enable cloud-based EMS services, FortiGate must be registered to FortinetOne with an appropriate user account. Only one FortiClient EMS Cloud server can be configured.

To enable authentication of FortiClient EMS Cloud through a FortinetOne account:

```
config endpoint-control fctems
    edit <name>
        set fortinetone-cloud-authentication enable
    next
end
```

To configure a FortiClient EMS Cloud server connection:

```
config user fsso
    edit "cloud_ems_fsso_connector"
        set type fortiems-cloud
        set password ******
        set source-ip <class_ip>
    next
end
```