FortiOS - Cookbook

Version 5.6

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/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

Octobber 30, 2019
FortiOS 5.6 Cookbook
01-560-000000-20230711

TABLE OF CONTENTS

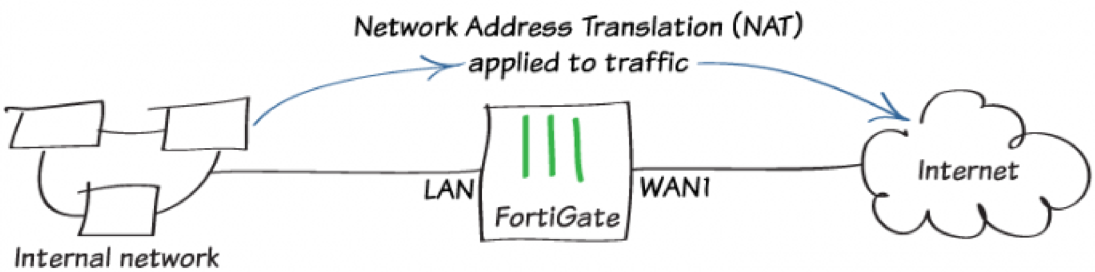
Change Log

Date	Change Description
2019-06-19	Initial release.
2019-09-12	Added the following topics: • Security Profiles > Transparent web filtering using a virtual wire pair. • VPNs > IPsec VPN to Azure.
2019-10-23	Added the following topics: • VPNs > Brainpool curves in IKEv2 IPsec VPN • VPNs > Client-Side SD-WAN with IPsec VPN Deployment Scenario (Expert)
2019-10-30	Added video links.

Getting started

This section contains information about installing and setting up a FortiGate, as well as common network configurations.

Installing a FortiGate in NAT mode



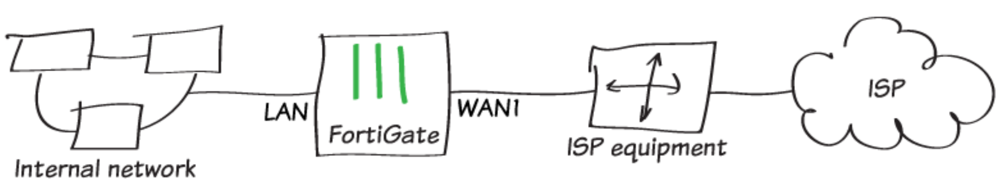
NAT mode is the most commonly used operating mode for a FortiGate.

This example shows how to connect and configure a new FortiGate in NAT mode to securely connect a private network to the Internet.

In NAT mode, you install a FortiGate as a gateway or router between two networks. Typically, you set up the FortiGate between a private network and the Internet, so that the FortiGate can hide the IP addresses of the private network using NAT.

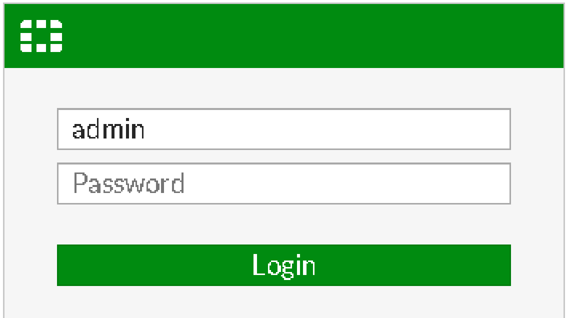
Connecting network devices

1. Connect the FortiGate to your ISP-supplied equipment using the Internet-facing interface. This is typically WAN or WAN1, depending on your model.
2. Connect a PC to the FortiGate using an internal port (in this example, port 3).



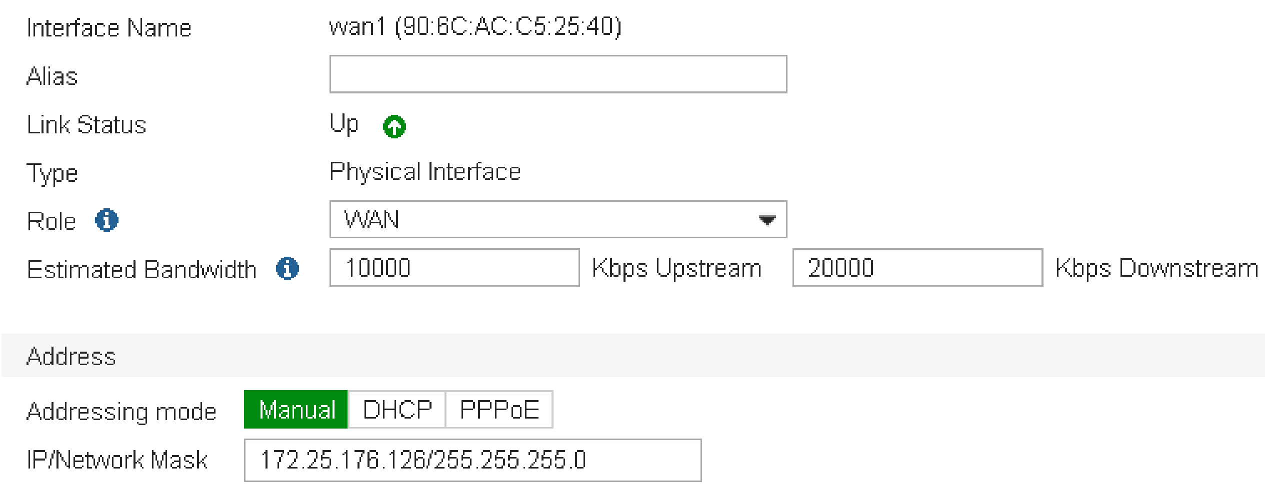
3. Power on the ISP equipment, the FortiGate, and the PC on the internal network.

4. Use the PC to connect to the FortiGate GUI using either FortiExplorer or an Internet browser. For more information about connecting to the GUI, see the QuickStart Guide for you FortiGate model.
5. Log in using an admin account. The default admin account has the username *admin* with no password.



Configuring interfaces

1. Go to *Network* > *Interfaces* and edit the Internet-facing interface (in this example, *wan1*).
2. Set the *Estimated Bandwidth* for the interface based on your Internet connection.
3. Set *Role* to *WAN*.

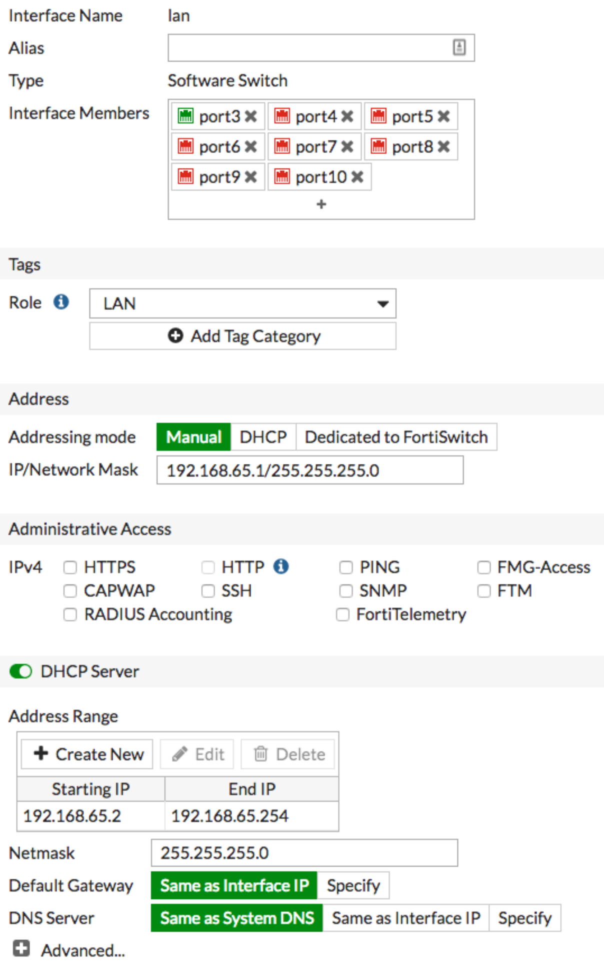


4. To determine which *Addressing mode* to use, check if your ISP provides an IP address for you to use or if the ISP equipment uses DHCP to assign IP addresses.
   - If your ISP provides an IP address, set *Addressing mode* to *Manual* and set the *IP/Network Mask* to that IP address.
   - If your ISP equipment uses DHCP, set *Addressing mode* to *DHCP* to allow the equipment to assign an IP address to WAN1.
5. Edit the *lan* interface, which is called *internal* on some FortiGate models.

> If your FortiGate doesn't have a default LAN interface, you can use either an individual interface or create a software switch to combine the separate interfaces into a single virtual interface.

6. Set *Role* to *LAN*.

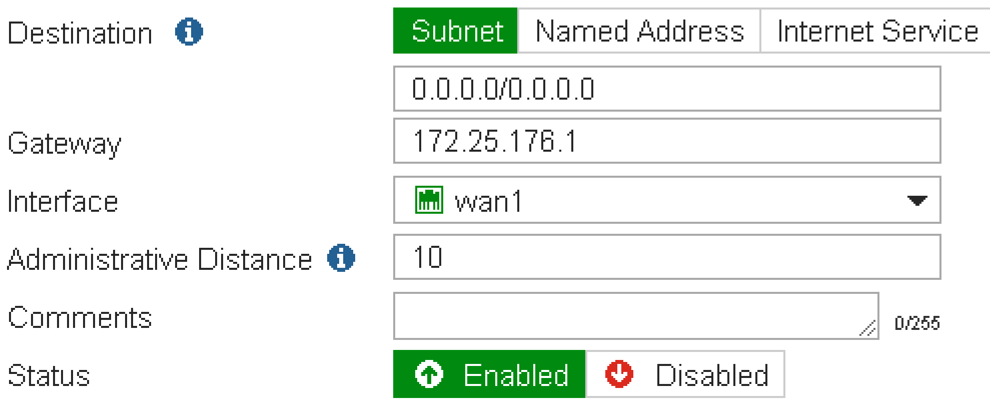
7. Set *Addressing mode* to *Manual* and set the *IP/Network Mask* to the private IP address you want to use for the FortiGate.
8. If you need to assign IP addresses to devices on your internal network, enable *DHCP Server*.



Adding a default route

1. To create a new default route, go to *Network > Static Routes*. Typically, you have only one default route. If the static route list already contains a default route, you can edit it, or delete the route and add a new one.
2. Set *Destination* to *Subnet* and leave the *Destination* IP address as *0.0.0.0/0.0.0.0*.

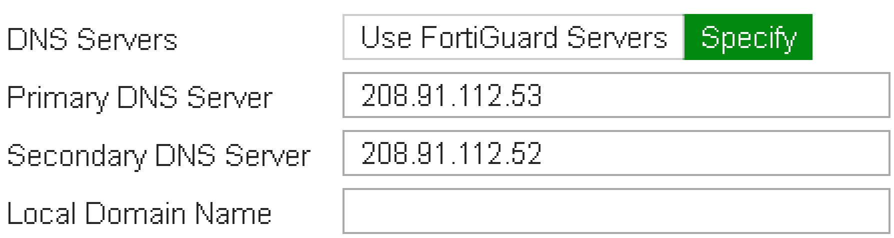
3. Set *Gateway* to the IP address provided by your ISP and *Interface* to the Internet-facing interface.



(Optional) Selecting DNS servers

The FortiGate DNS settings are configured to use FortiGuard DNS servers by default, which is sufficient for most networks.

If you need to change the DNS servers, go to *Network > DNS*, select *Specify*, and add primary and secondary DNS servers.

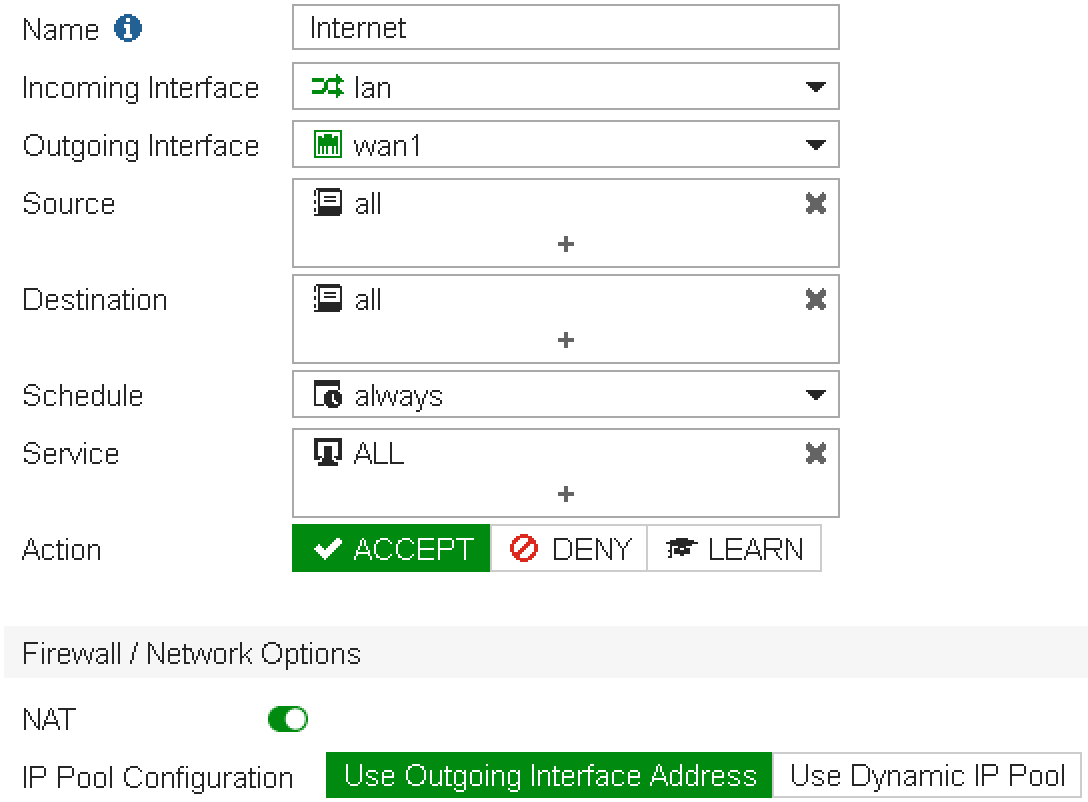


Creating a policy

Some FortiGate models include an IPv4 security policy in the default configuration. If you have one of these models, edit it to include the logging options shown below, then proceed to the results section.

1. To create a new policy, go to *Policy & Objects > IPv4 Policy*. Give the policy a *Name* that indicates that the policy will be for traffic to the Internet (in this example, *Internet*).
2. Set the *Incoming Interface* to *lan* and the *Outgoing Interface* to *wan1*. Set *Source*, *Destination*, *Schedule*, and *Service* as required.
3. Ensure *Action* is set to *ACCEPT*.

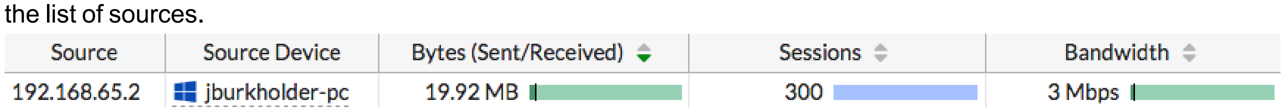
4. Turn on *NAT* and select *Use Outgoing Interface Address*.



5. Scroll down to the *Logging Options* section. To view the results later, enable *Log Allowed Traffic* and select *All Sessions*.

Results

1. Browse the Internet using the PC on the internal network.
   If you can't connect to the Internet, see FortiGate installation troubleshooting.
2. To view information about FortiGate traffic, go to *FortiView* > *Traffic From LAN/DMZ* > *Sources*. The PC appears on the list of sources.



3. To view more detailed information about the traffic from the PC, right-click the entry for the PC and select *Drill Down to Details*.

Summary of 192.168.65.2

Device	jburkholder-pc
Applications Detected	3
Bytes (Sent/Received)	27.10 MB
Bandwidth	1.94 Mbps
Sessions	287
Time Period	Realtime
FortiGate	FG800D3915800295

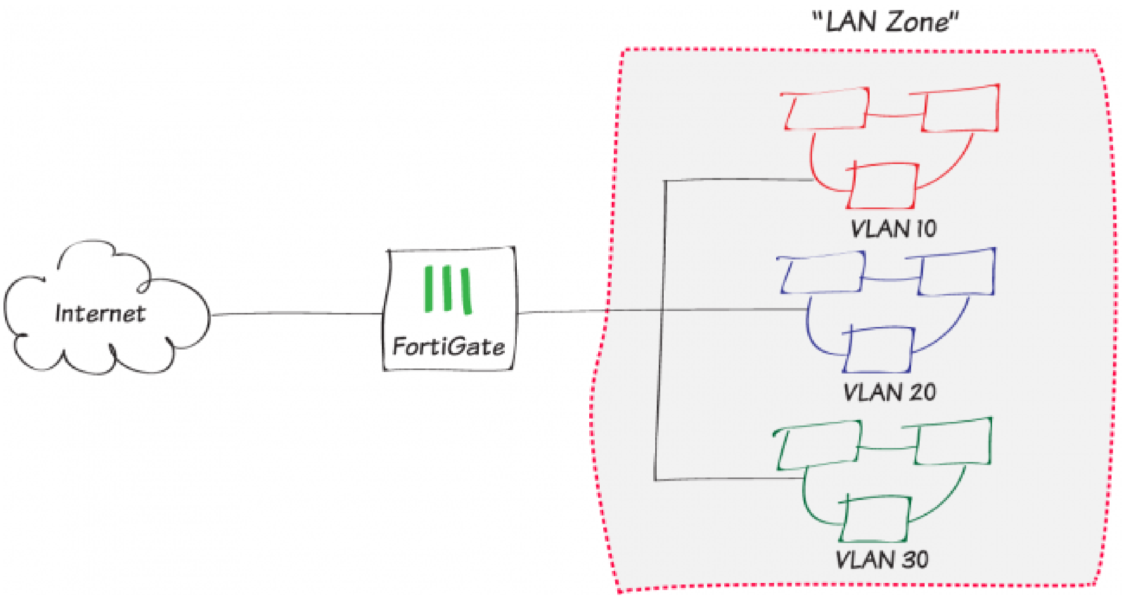
Destinations | Applications | Countries | Policies | Domains | Categories | Source Interfaces | Destination Interfaces | Sessions

Destination	Bytes (Sent/Received)	Sessions	Bandwidth
r1.sn-gvbxgn-tvve.googlevideo.com (209.148.198.204)	19.06 MB	1	2 Mbps
googleadapis.l.google.com (172.217.10.106)	3.93 MB	3	48 bps
ytimg.l.google.com (172.217.10.238)	1.65 MB	1	256 bps
fcmatch.youtube.com (172.217.9.238)	943.07 kB	2	40 bps
gstaticadssl.l.google.com (172.217.9.227)	339.81 kB	2	88 bps
www.google.ca (216.58.193.67)	317.69 kB	1	48 bps
pagead2.googlesyndication.com (172.217.11.2)	297.90 kB	1	48 bps
pagead-googlehosted.l.google.com (172.217.9.225)	152.98 kB	1	48 bps
208.91.112.53	86.07 kB	222	288 bps
partnerad.l.doubleclick.net (172.217.10.98)	83.45 kB	1	48 bps
redirector.gvt1.com (172.217.10.110)	65.40 kB	2	40 bps
yt3.ggpht.com (172.217.10.97)	63.22 kB	1	40 bps
www.google.com (172.217.3.164)	27.01 kB	1	48 bps
adservice.google.com (172.217.12.194)	21.46 kB	2	112 bps
cm.g.doubleclick.net (172.217.12.130)	16.69 kB	2	88 bps
pipeline-edge-prod-25-561439127.us-west-2.elb.amazonaws.com (54.68.157.14)	13.24 kB	1	3 kbps
208.91.112.52	12.10 kB	41	0 bps
cs9.wac.phicdn.net (72.21.91.29)	8.34 kB	1	56 bps
static-doubleclick-net.l.google.com (172.217.9.230)	6.43 kB	1	0 bps

If your FortiGate model has internal storage and disk logging enabled, a dropdown menu in the top corner allows you to view historical logging information for the previous *5 minutes*, *1 hour*, and *24 hours*.

If you’re not sure whether your model supports disk logging, check the FortiOS Feature/Platform Matrix.

Using zones to simplify firewall policies

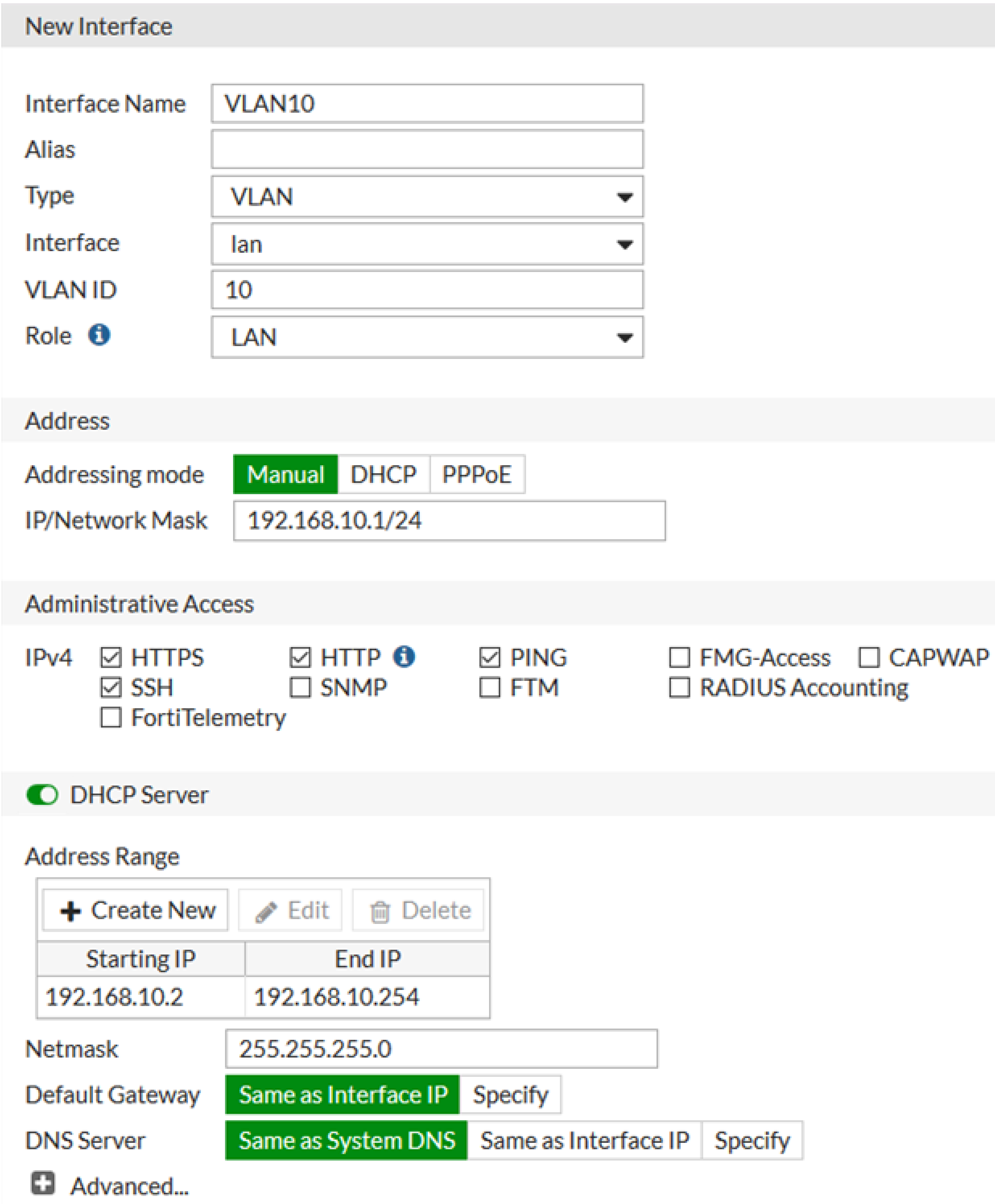


This example shows how grouping multiple interfaces into a zone can simplify firewall policies. In this example, we create *VLAN10*, *VLAN20*, and *VLAN30* and add them into a zone called *LAN Zone*. Instead of having to reference all three interfaces separately as a source interface in our firewall policy, we can just use the single zone object.

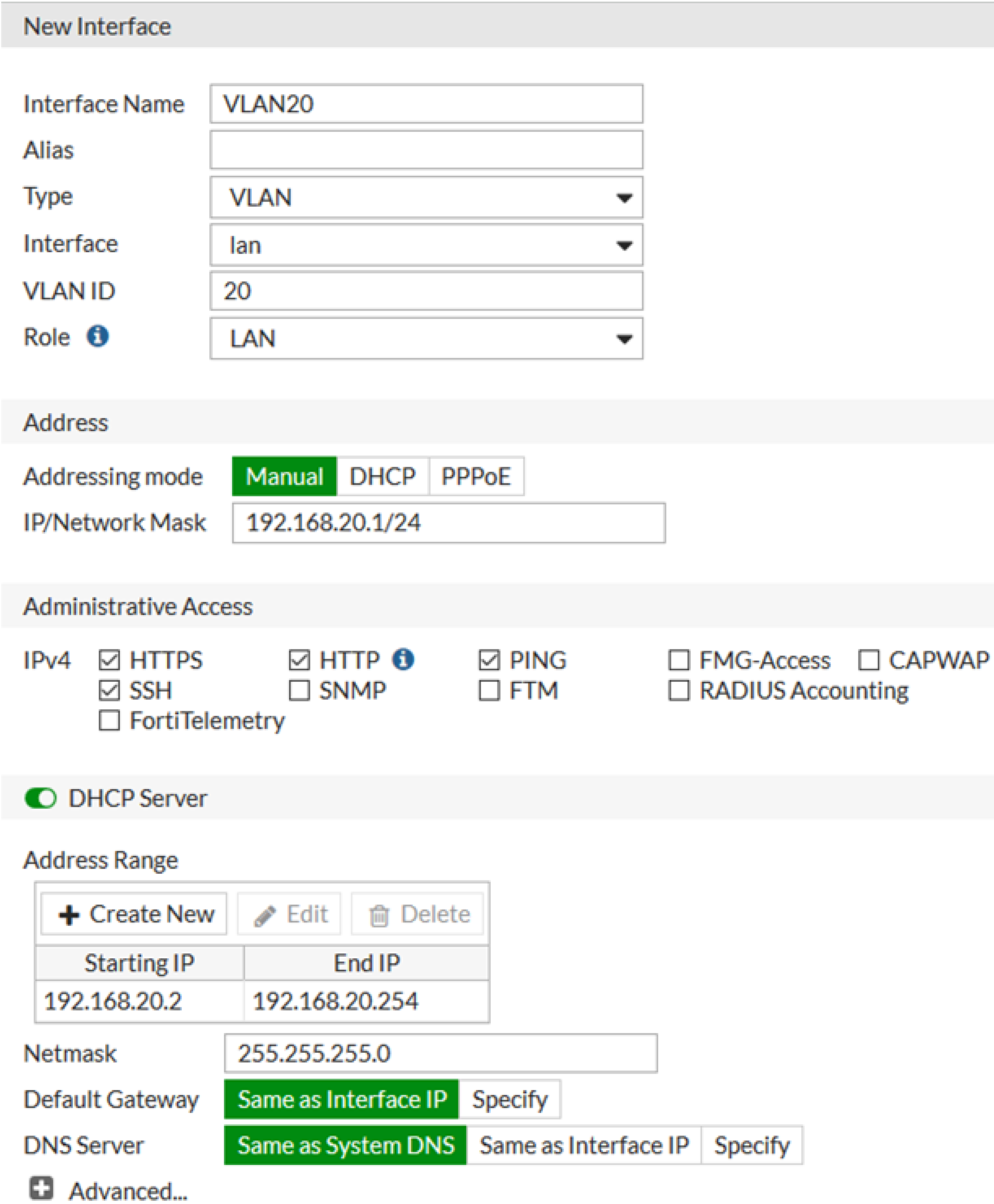
In addition to VLANs, zones can also group many other kinds of interfaces such as physical ports or IPsec tunnels.

Creating the VLAN interfaces

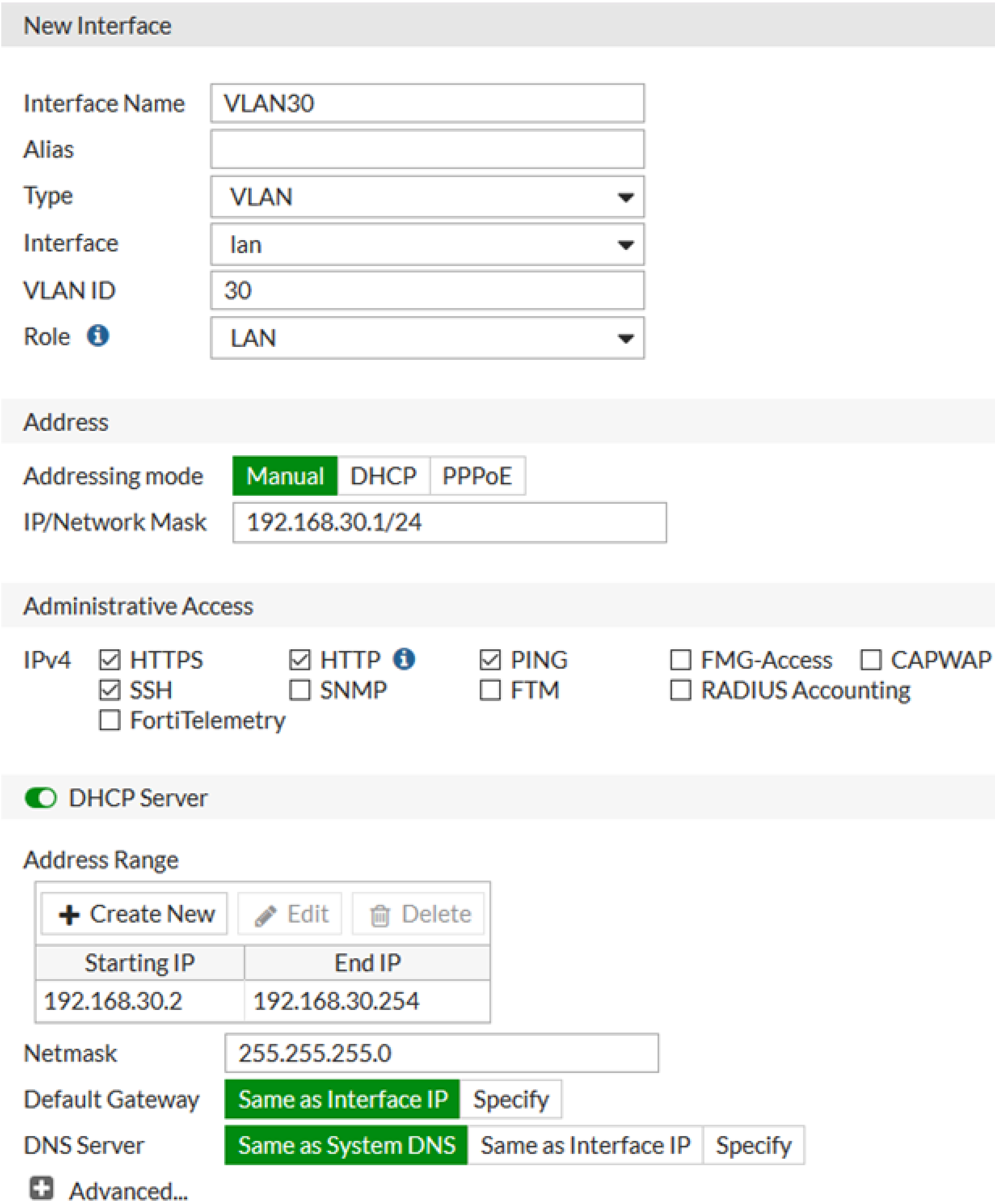
1. Go to *Network* > *Interfaces* and select *Create New* > *Interface*.
2. Create the VLAN interface for VLAN ID 10 and enable *DHCP Server*.



3. Create the VLAN interface for VLAN ID 20 and enable *DHCP Server*.

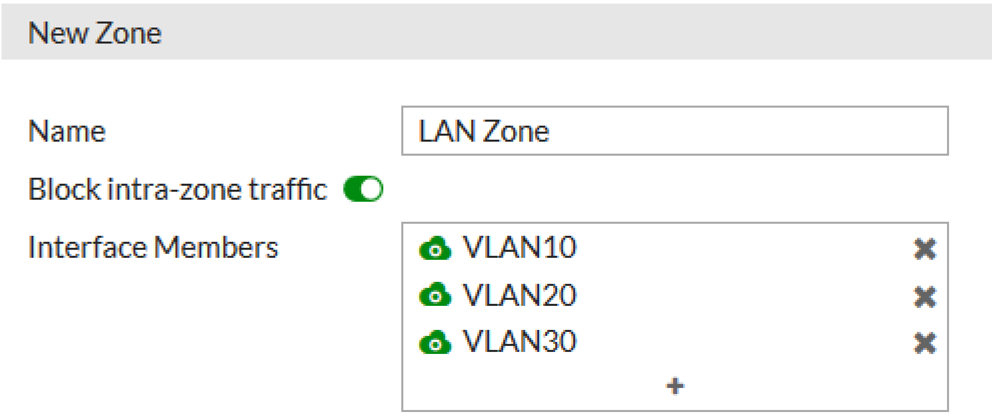


4. Create the VLAN interface for VLAN ID 30 and enable *DHCP Server*.



Creating the zone

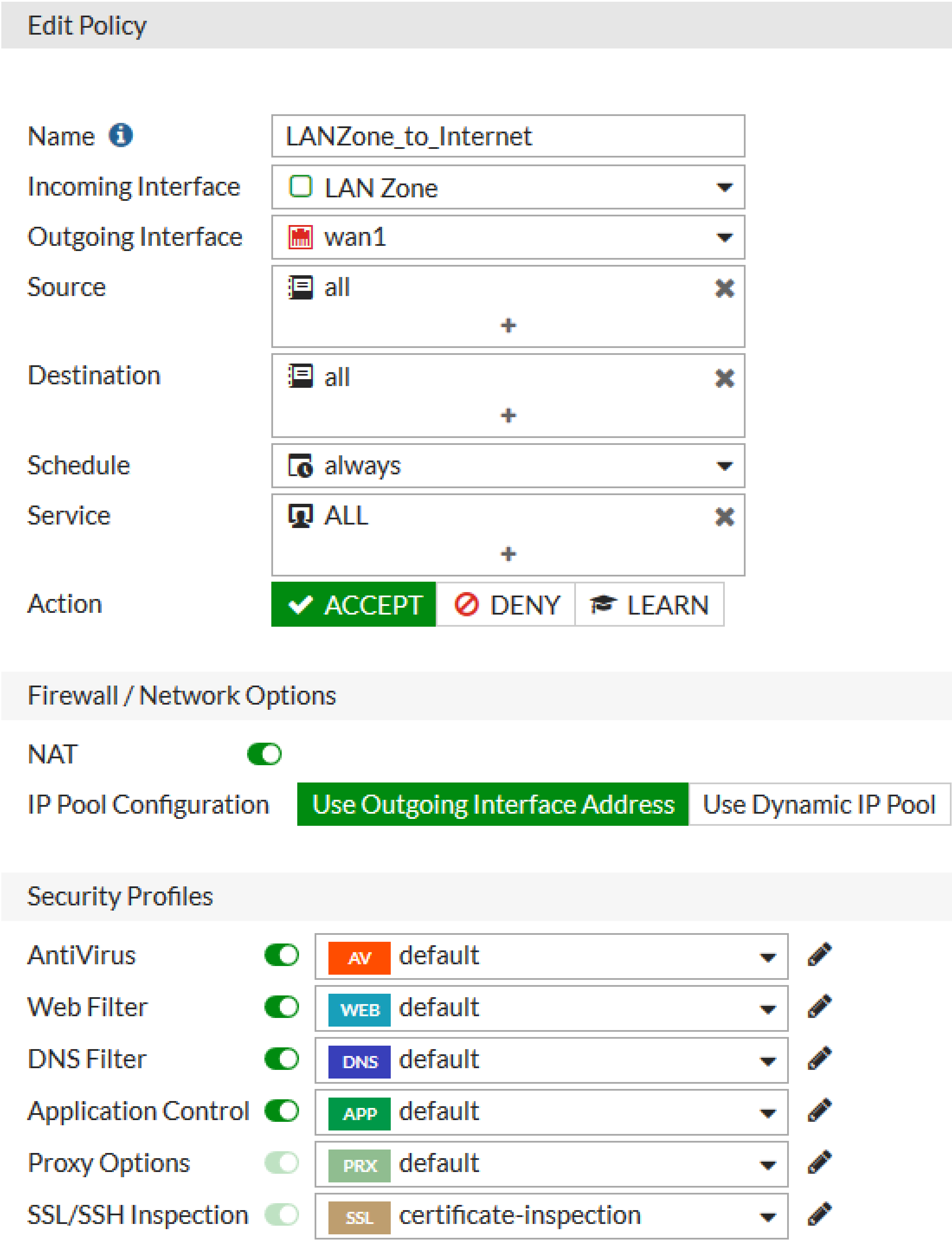
1. Go to *Network* > *Interfaces* and select *Create New* > *Zone*
2. Name the zone *LAN Zone*, and add the newly created VLANs to the zone.
   Ensure *Block intra-zone traffic* is enabled to prevent communication between the VLAN interfaces.



Creating a firewall policy for the zone

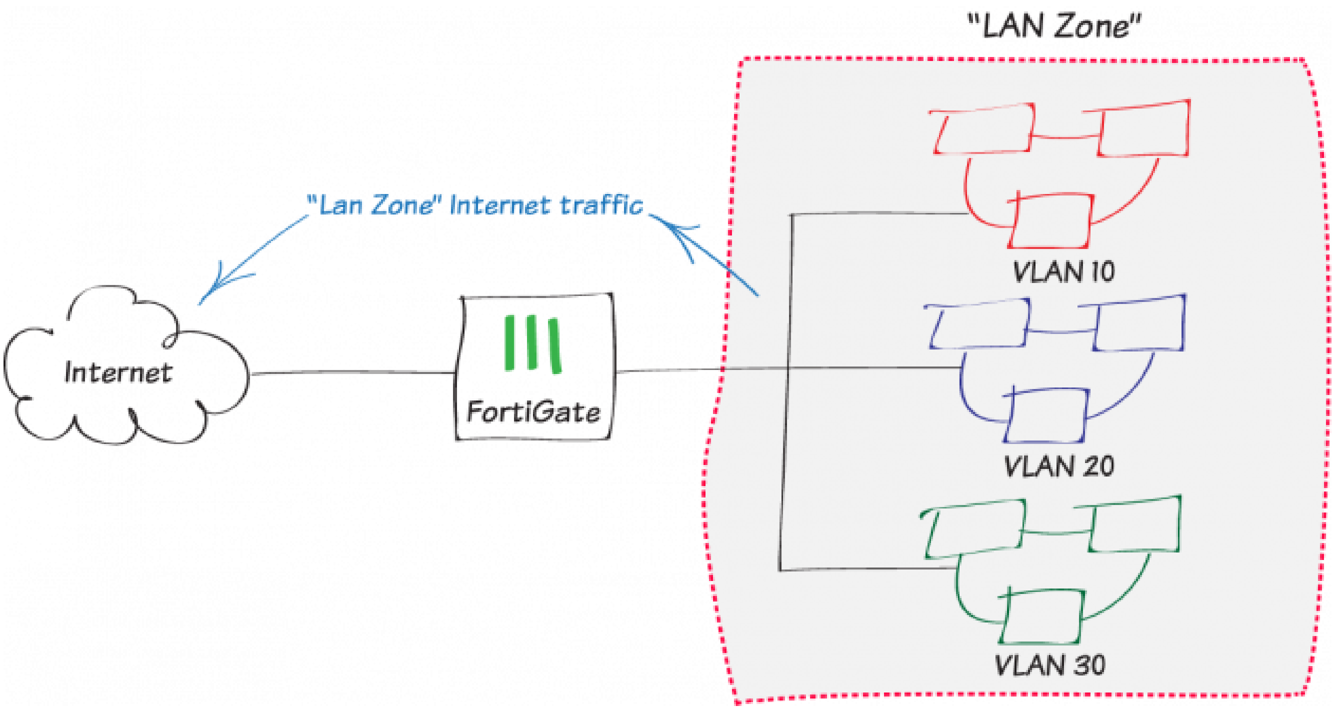
1. Go to *Policy & Objects* > *IPv4 Policy* and create a firewall policy giving any VLAN in the *LAN Zone* permission to access the Internet.

2. Set up *Security Profiles* according to your organization's requirements.

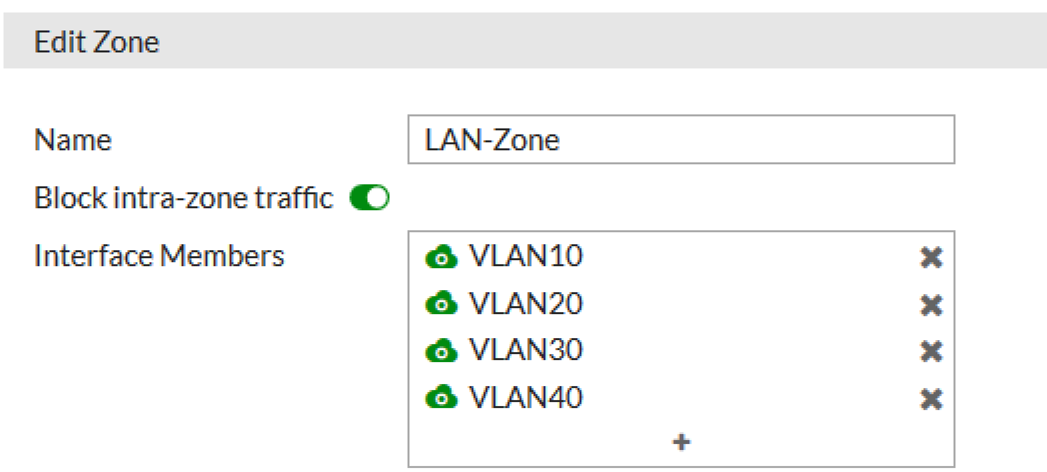


Results

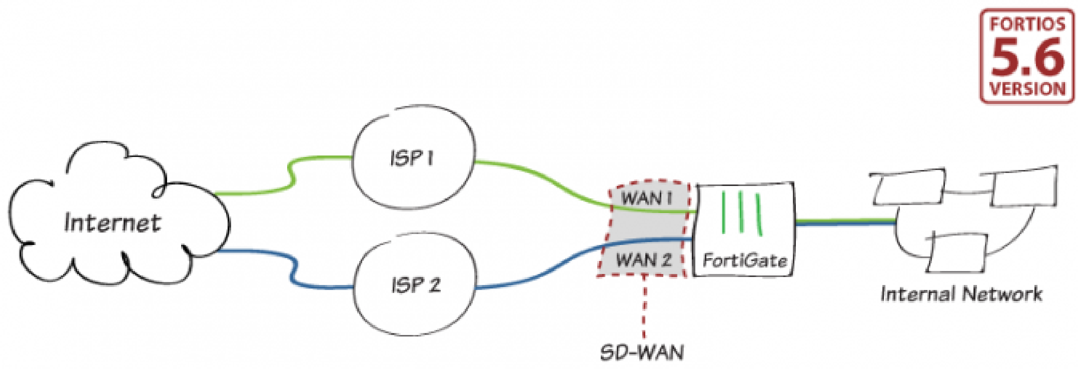
Users from VLAN10, VLAN20, or VLAN30 now have Internet access.



When you add new VLANs in the future, you can add them to *LAN Zone* without modifying the firewall policy created earlier.



Redundant Internet with SD-WAN



This example shows how to configure redundant Internet using SD-WAN.

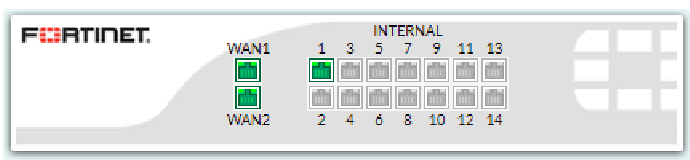
SD-WAN can seamlessly manage traffic at the Layer 2 level of the OSI model without the need to manage hardware-based switches or WAN controllers.

This example includes volume-based weighted load balancing so that 75% of your Internet traffic is handled by the ISP connected to WAN1 and the remaining 25% handled by the ISP connected to WAN2.

With this configuration, in the event of a failure connecting to one ISP, all traffic will divert or failover to the other WAN interface.

Connecting your ISPs to the FortiGate

1. Connect your ISP devices to your FortiGate so that the ISP you wish to use for most traffic is connected to WAN1 and the other connects to WAN2.



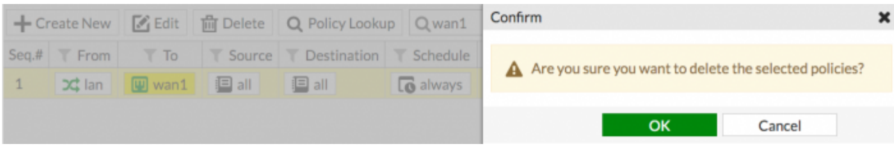
Modifying existing policies

If any interface is already used in the FortiGate configuration, you cannot add it to the SD-WAN interface. In this case, you must delete any security policies that use either WAN1 or WAN2, such as the default Internet access policy. Traffic cannot reach WAN1 or WAN2 through the FortiGate after you delete the existing policies.

Also check for any other references to WAN1 or WAN2 and make the necessary modifications.

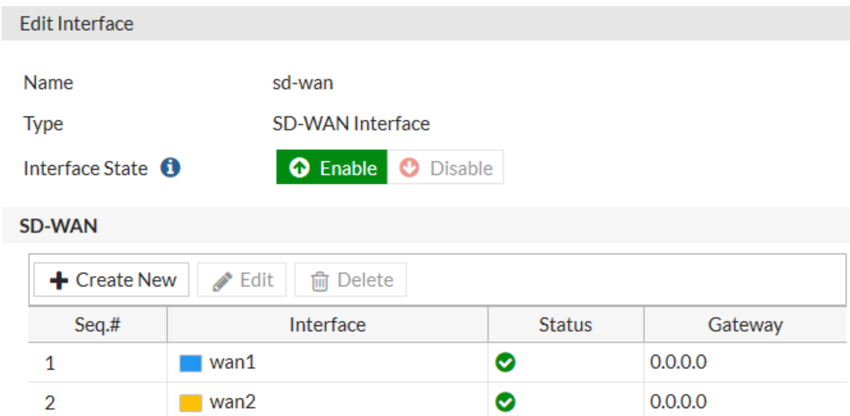
If you have many policies that reference WAN1 or WAN2, you can redirect those policies to unused ports rather than delete them, so that you don't have to recreate those policies again. You can redirect those policies back to the SD-WAN interface when it is created.

1. Go to *Policy & Objects* > *IPv4 Policy* and delete any policies that use WAN1 or WAN2.

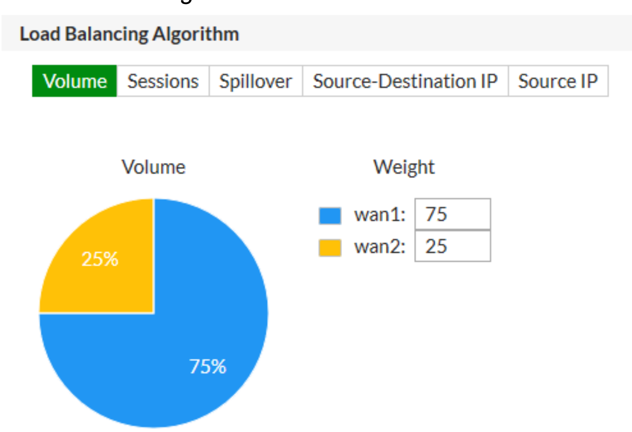


Creating the SD-WAN interface

1. Go to *Network* > *SD-WAN*.
2. Set the *Interface State* to *Enable*.
3. Under *SD-WAN*, add the two WAN interfaces.

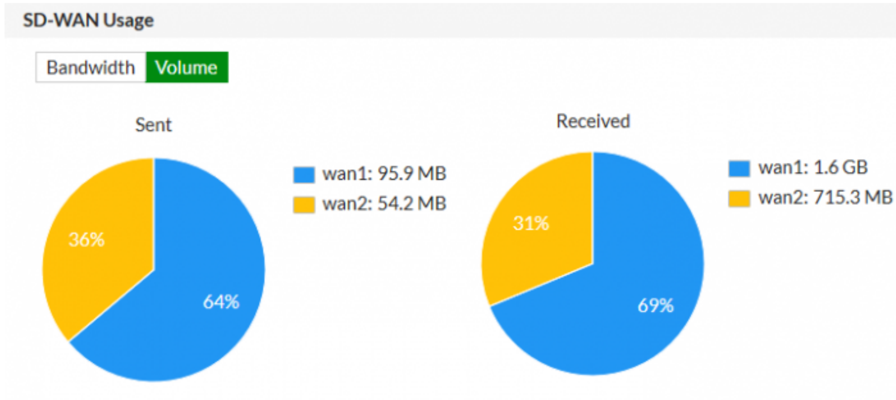


4. Under *Load Balancing Algorithm*, select *Volume* and set the WAN1 interface to serve more traffic.
   In this example, the ISP connected to WAN1 is a 40Mb link and the ISP connected to WAN2 is a 10Mb link, so we balance the *Weight 75%* to *25%* in favor of WAN1.



5. To help visualize the effectiveness of the algorithm, the *SD-WAN Usage* graph shows you the *Bandwidth* and

Volume usage.

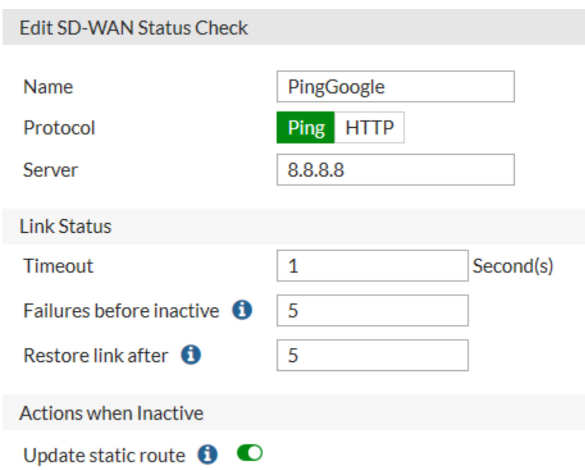


(Optional) Configuring SD-WAN Status Check

You can optionally configure *SD-WAN Status Check* to verify the health and status of the links that make up the virtual WAN link.

This configuration uses the Ping protocol to verify the status of the SD-WAN.

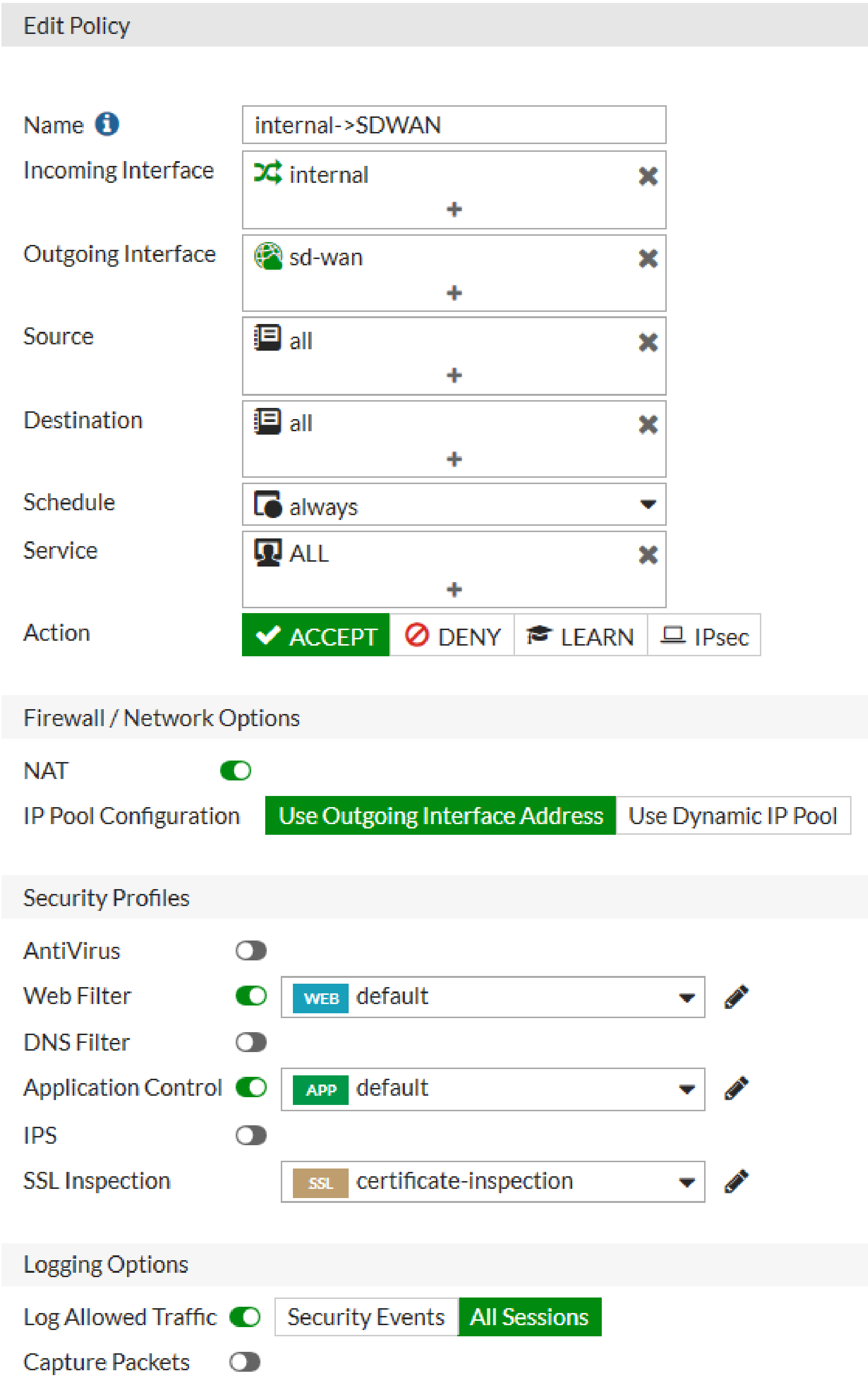
1. Go to *Network* > *SD-WAN Status Check* and select *Create New*. If you wish to use Google, enter the values shown here.



Allowing traffic from the internal network to the SD-WAN interface

1. Go to *Policy & Objects* > *IPv4 Policy* and create a new policy.
2. Set *Incoming Interface* to your internal network's interface and set *Outgoing Interface* to the SD-WAN interface.
3. Enable *NAT* and apply *Security Profiles* as required.

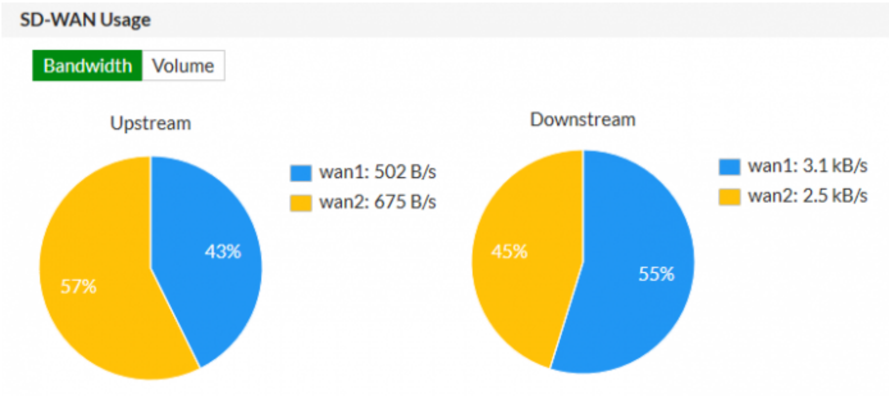
4. Enable *Log Allowed Traffic* for *All Sessions* to allow you to verify the results later.



If you had redirected or deleted any policies, you can redirect them to the SD-WAN interface or recreate those policies.

Results

1. Browse the Internet using a computer on the internal network and then go to *Network > SD-WAN > SD-WAN Usage*.
   Check the bandwidth and volume of traffic traversing the SD-WAN interfaces.



2. If configured earlier, check the status by viewing the table at *Network > SD-WAN Status Check*.

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold
PingGoogle	8.8.8.8	wan1: 23.33 % wan2: 13.33 %	wan1: 9.02 ms wan2: 8.93 ms	wan1: 14.75 ms wan2: 14.95 ms	5

3. Go to *Monitor > SD-WAN Monitor* to view the number of sessions for each interface, bit rate, and more.

+	Interface	Status	Sessions	Upload	Download
	sd-wan				
	wan1		68	255 B/s	4.03 kB/s
	wan2		30	174 B/s	715 B/s

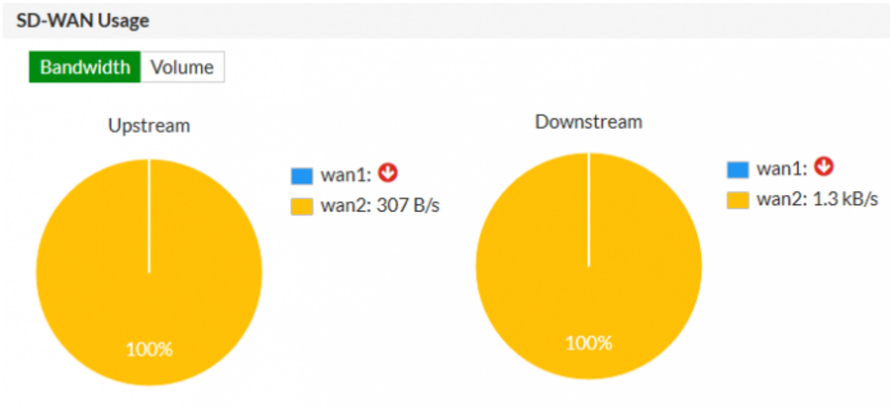
Testing failover

To test failover of the redundant Internet configuration, you must simulate a failed Internet connection to one of the ports. You can do this by physically disconnecting the Ethernet cable connected to WAN1.

1. Verify that users still have Internet access by going to *Monitor > SD-WAN Monitor* and checking the *Upload* and *Download* of each WAN interface.

+	Interface	Status	Sessions	Upload	Download
	sd-wan				
	wan1		16	0 B/s	0 B/s
	wan2		103	242 B/s	1.24 kB/s

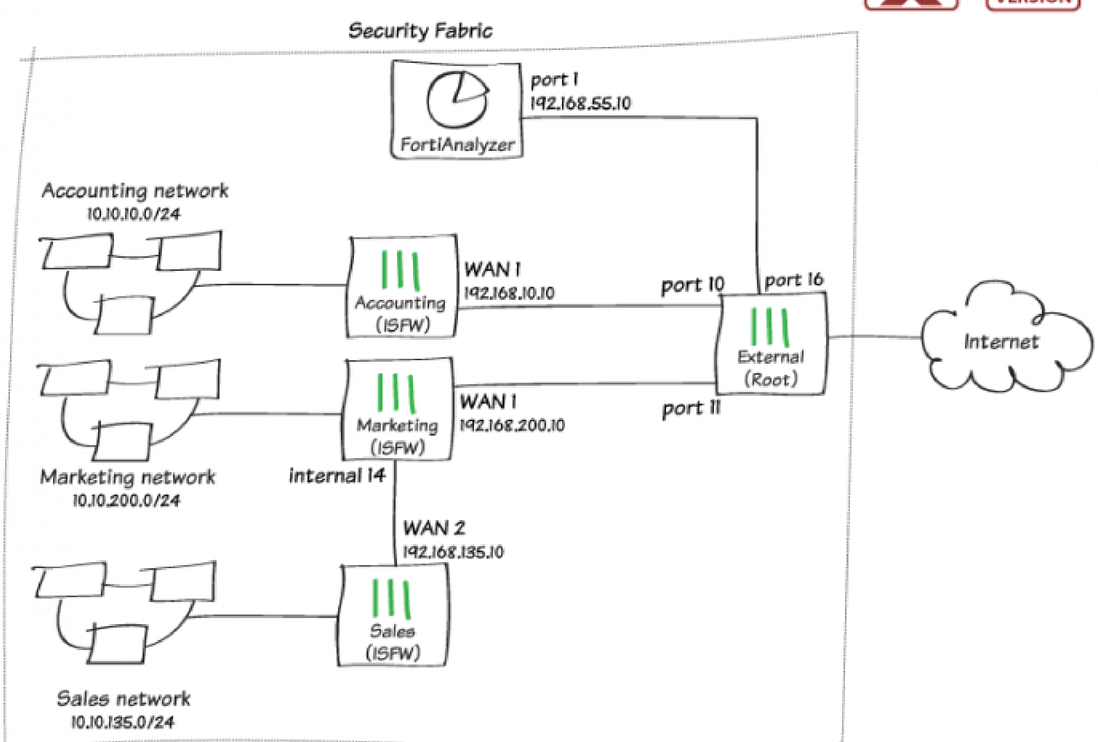
2. In *Network* > *SD-WAN* > *SD-WAN Usage*, check that bandwidth and volume have diverted entirely through WAN2.



Users on the internal network have no knowledge of the WAN1 failure. Likewise, if you are using the WAN1 gateway IP to connect to the admin dashboard, nothing changes from your perspective. It appears that you are still connecting through WAN1.

Reconnect the WAN1 Ethernet cable when you have verified successful failover.

Fortinet Security Fabric installation and audit



This example shows you how to configure a Fortinet Security Fabric that consists of four FortiGates and a FortiAnalyzer. One FortiGate acts as the network edge firewall and root FortiGate of the Security Fabric while the others function as Internal Segmentation Firewalls (ISFWs).

When the network is configured, a Security Fabric Audit is run to analyze the Security Fabric and recommend changes to help improve the configuration.

This sample network uses the following FortiGate aliases:

- **External**: the root FortiGate in the Security Fabric. This FortiGate is named *External* because it is the only FortiGate that directly connects to the Internet. This role is also known as the edge or gateway FortiGate.
- **Accounting**: an ISFW FortiGate that connects to External.
- **Marketing**: an ISFW FortiGate that connects to External.
- **Sales**: an ISFW FortiGate that connects to Marketing.

Security Fabric Installation

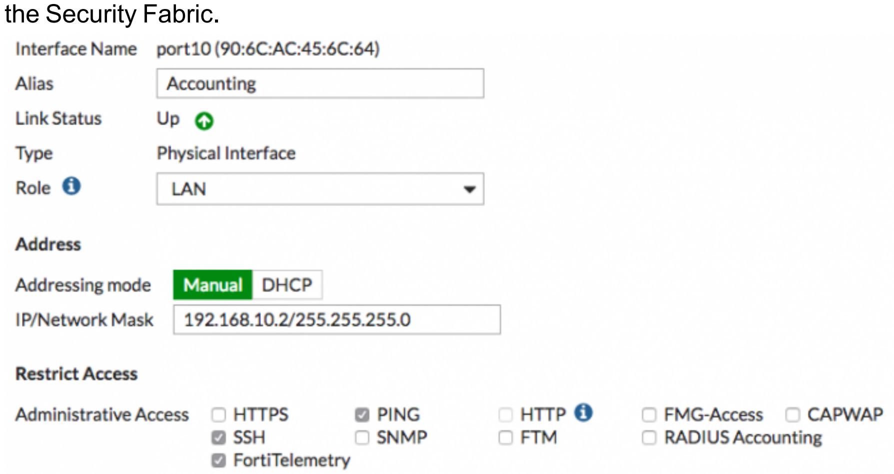
Configuring External

In the Security Fabric, External is the root FortiGate. This FortiGate receives information from the other FortiGates in the Security Fabric and is used to run the Security Fabric Audit.

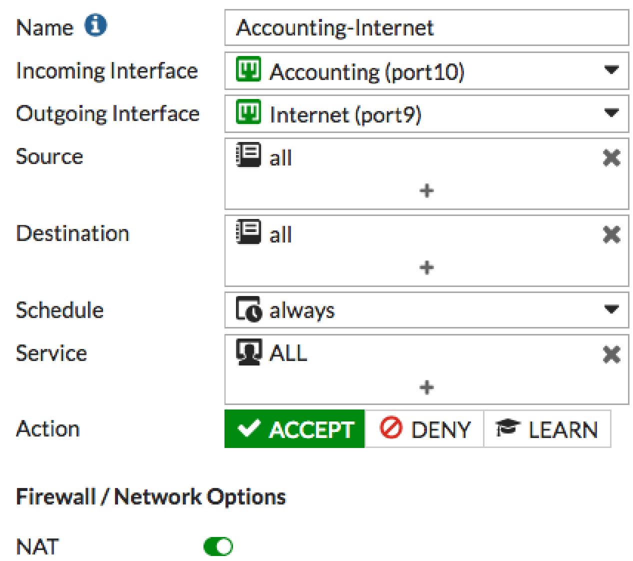
In this example, the following interfaces on External connect to other network devices:

- Port 9 connects to the Internet (this interface was configured when External was initially installed).
- Port 10 connects to Accounting (IP address: 192.168.10.2).
- Port 11 connects to Marketing (IP address: 192.168.200.2).
- Port 16 connects to the FortiAnalyzer (IP address: 192.168.55.2).

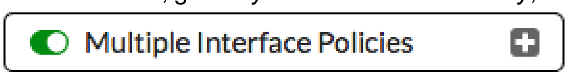
1. On External, go to *Network* > *Interfaces* and edit port 10.
2. Set an *IP/Network Mask* for the interface. In this example, *192.168.10.2/255.255.255.0*.
3. Under *Administrative Access*, enable *FortiTelemetry*, which is required for communication between FortiGates in the Security Fabric.



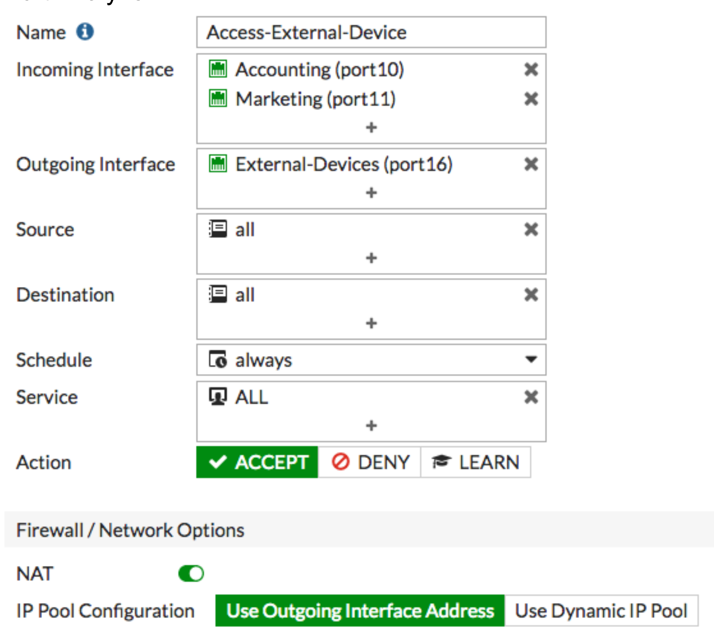
4. Repeat these steps to configure the other interfaces with the appropriate IP addresses.
5. Go to *Policy & Objects* > *IPv4 Policy* and create a policy for traffic from Accounting to the Internet. Ensure *NAT* is enabled.



6. Repeat this step to create a similar policy for Marketing.
7. Still on External, go to *System > Feature Visibility*, and under *Additional Features*, enable *Multiple Interface Policies*.

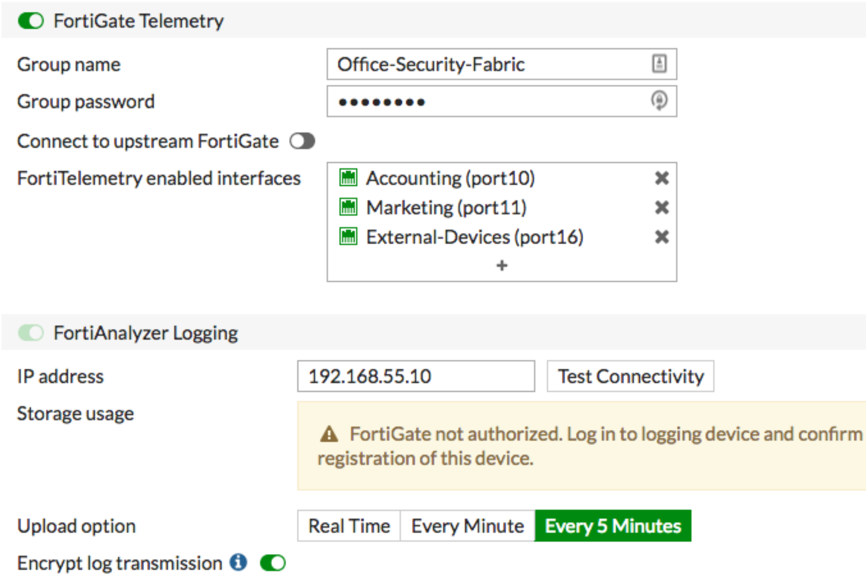


8. Go to *Policy & Objects > IPv4 Policy* and create a policy allowing Accounting and Marketing to access the FortiAnalyzer.



9. To enable communication between the FortiGates in the Security Fabric, go to *Security Fabric > Settings* and enable *FortiGate Telemetry*.
   Set a *Group name* and *Group password*.
   FortiAnalyzer Logging is enabled by default.

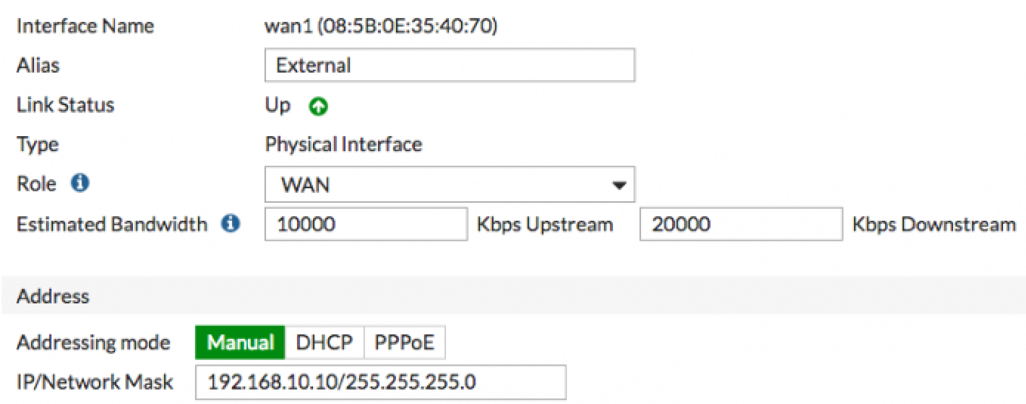
Set *IP address* to an internal address that will later be assigned to port 1 on the FortiAnalyzer (in this example, *192.168.55.10*).



10. Click *Test Connectivity*.
An error appears because the FortiGate is not yet authorized on the FortiAnalyzer. This authorization will be configured in a later step.

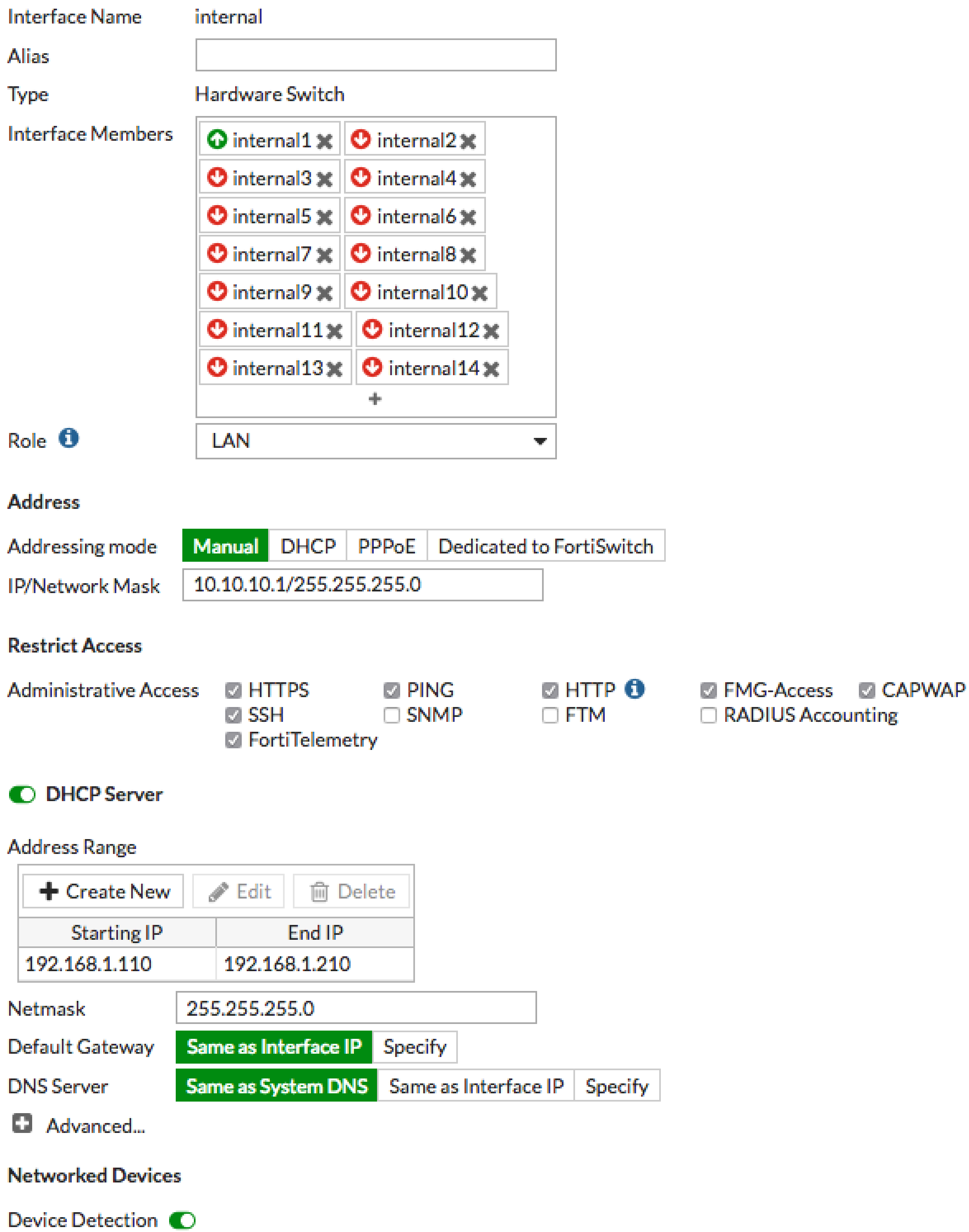
Installing Accounting and Marketing

1. On Accounting, go to *Network > Interfaces* and edit WAN1.
Set an *IP/Network Mask* for the interface that is on the same subnet as port 10 on External (in this example, *192.168.10.10/255.255.255.0*).

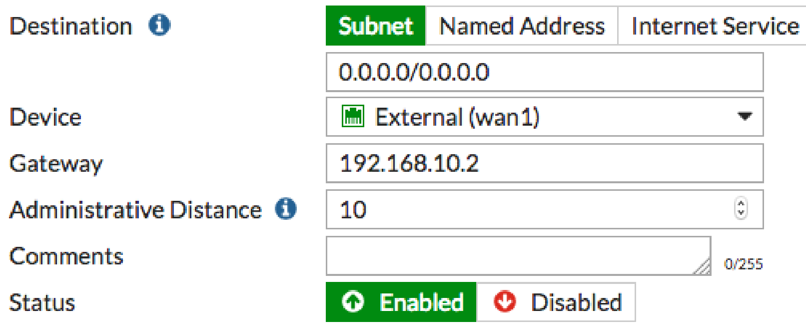


2. Edit the internal interface.
Set *Addressing mode* to *Manual* and set the *IP/Network Mask* to a private IP address (in the example, *10.10.10.1/255.255.255.0*).
Under *Administrative Access*, enable *FortiTelemetry*.
If you require the FortiGate to provide IP addresses using DHCP to devices that connect to this interface, enable *DHCP Server*.

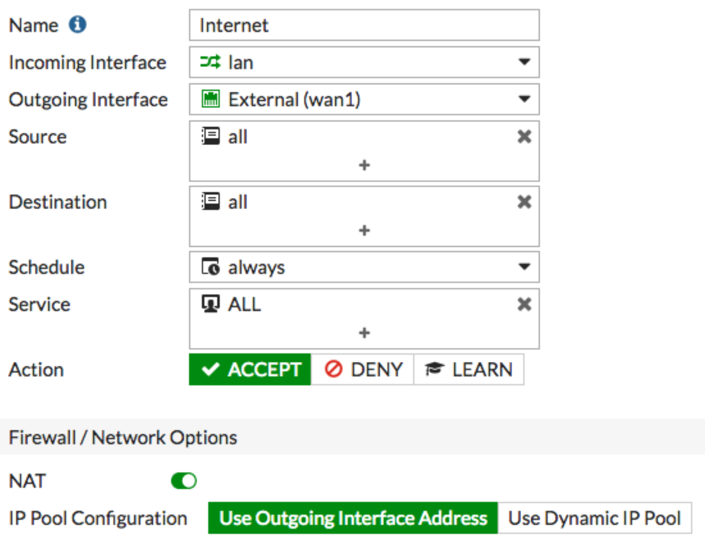
Under *Networked Devices*, enable *Device Detection*.



3. Go to *Network* > *Static Routes* and add a static route.
   Set *Gateway* to the IP address of port 10 on External.

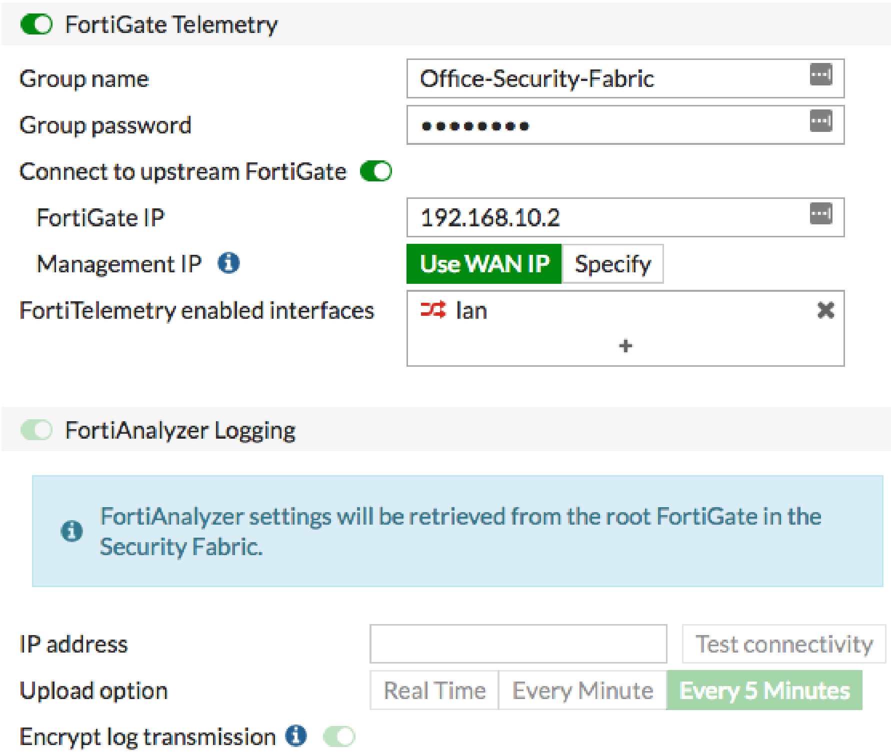


4. Go to *Policy & Objects* > *IPv4 Policy* and create a policy to allow users on the Accounting network to access External.



5. Go to *Security Fabric* > *Settings* to add Accounting to the Security Fabric.
   Enable *FortiGate Telemetry*, then enter the same *Group name* and *Group password* that you set previously on External.
   Enable *Connect to upstream FortiGate* and enter the IP address of port 10 on External.

FortiAnalyzer Logging is enabled by default. Settings for the FortiAnalyzer will be retrieved when Accounting connects to External.

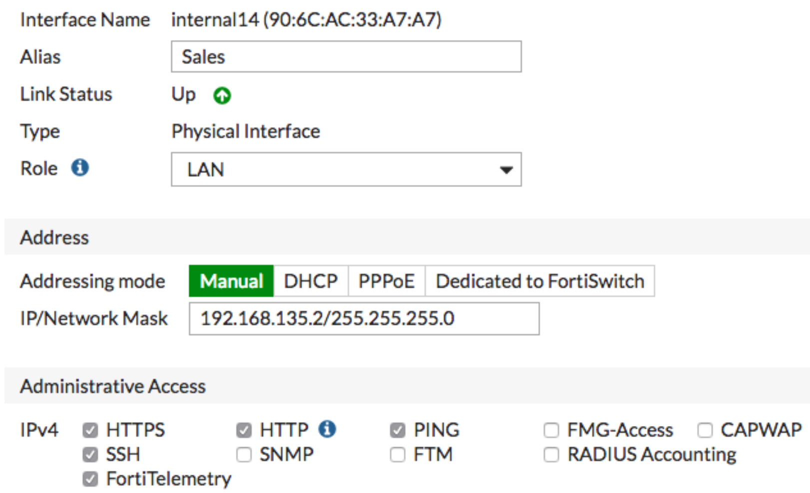


6. If you have not already done so, connect WAN1 on Accounting to port 10 on External.
7. Connect and configure Marketing, using the same method you used to configure Accounting. Make sure to complete the following steps:
   - Configure WAN1 to connect to External (IP address: *192.168.200.10/255.255.255.0*).
   - Configure the LAN interface for the Marketing network (IP address: *10.10.200.2/255.255.255.0*).
   - Create a static route pointing traffic to port 11 on External.
   - Create a policy to allow users on the Marketing network to access External.
   - Add Marketing to the Security Fabric.

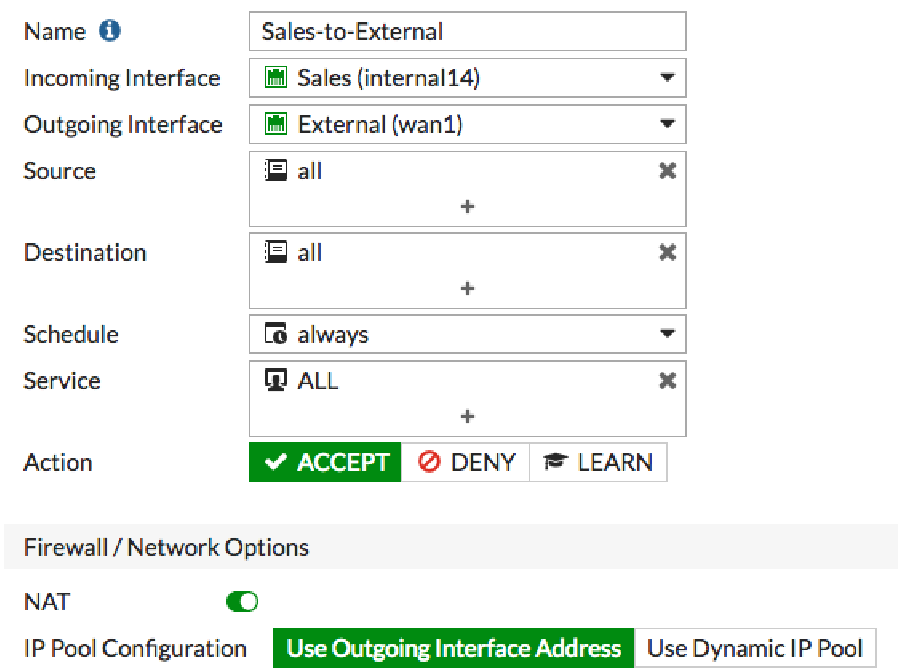
Installing Sales

1. On Marketing, go to *Network* > *Interfaces* and edit the interface that Sales will connect to (in this example, *internal14*).
   Set an *IP/Network Mask* for the interface (in this example, *192.168.135.2/255.255.255.0*).

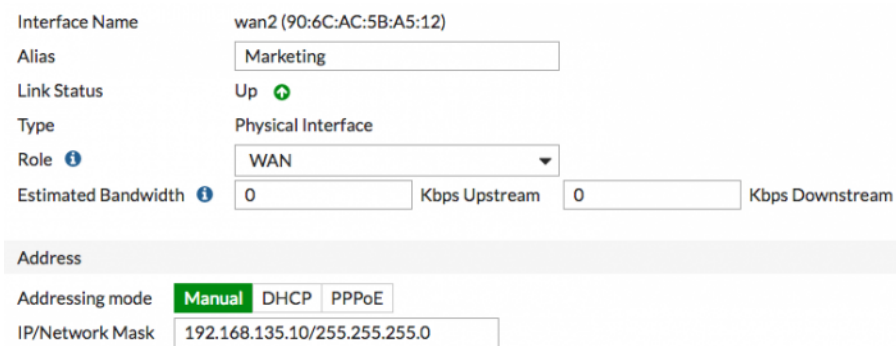
Under *Administrative Access*, enable *FortiTelemetry*.



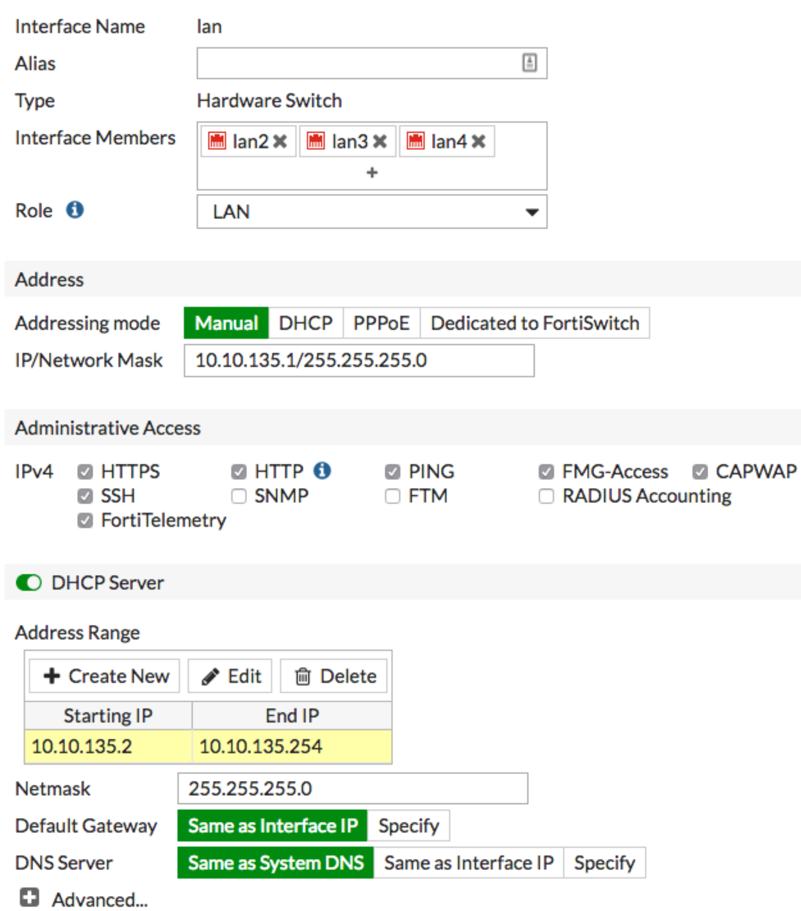
2. Go to *Policy & Objects > IPv4 Policy* and create a policy for traffic from Sales to External. Enable *NAT*.



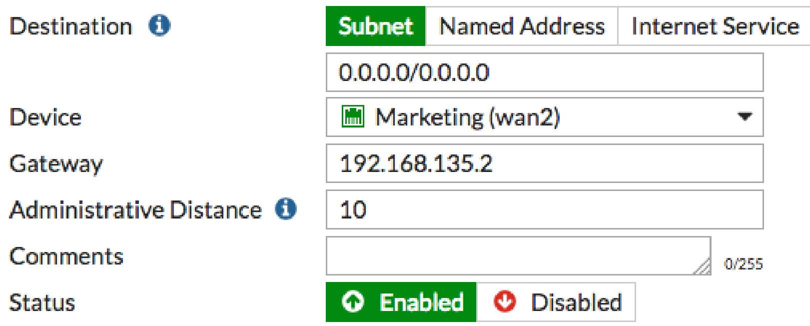
3. On Sales, go to *Network* > *Interfaces* and edit WAN2.
Set an *IP/Network Mask* for the interface that is on the same subnet as the internal 14 interface on Marketing (in this example, *192.168.135.10/255.255.255.0*).



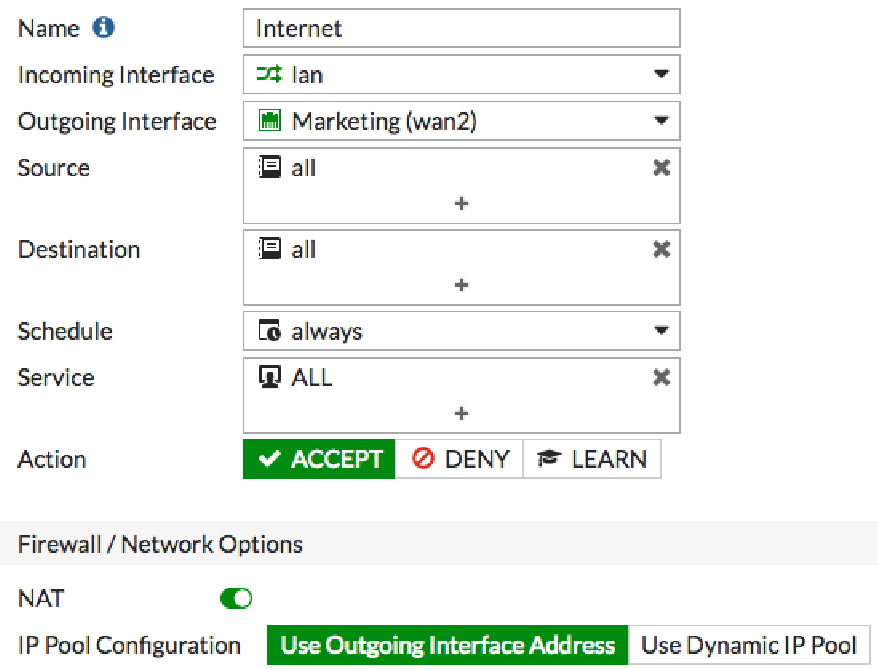
4. Edit the LAN interface.
Set *Addressing Mode* to *Manual*, and set the *IP/Network Mask* to a private IP address (in this example, *10.10.135.1/255.255.255.0*).
Under *Administrative Access*, enable *FortiTelemetry*.
If you require the FortiGate to provide IP addresses, using DHCP to devices that connect to this interface, enable *DHCP Server*.
Under *Networked Devices*, enable *Device Detection*.



5. Go to *Network* > *Static Routes* and add a route.
   Set *Gateway* to the IP address of the internal 14 interface on Marketing.

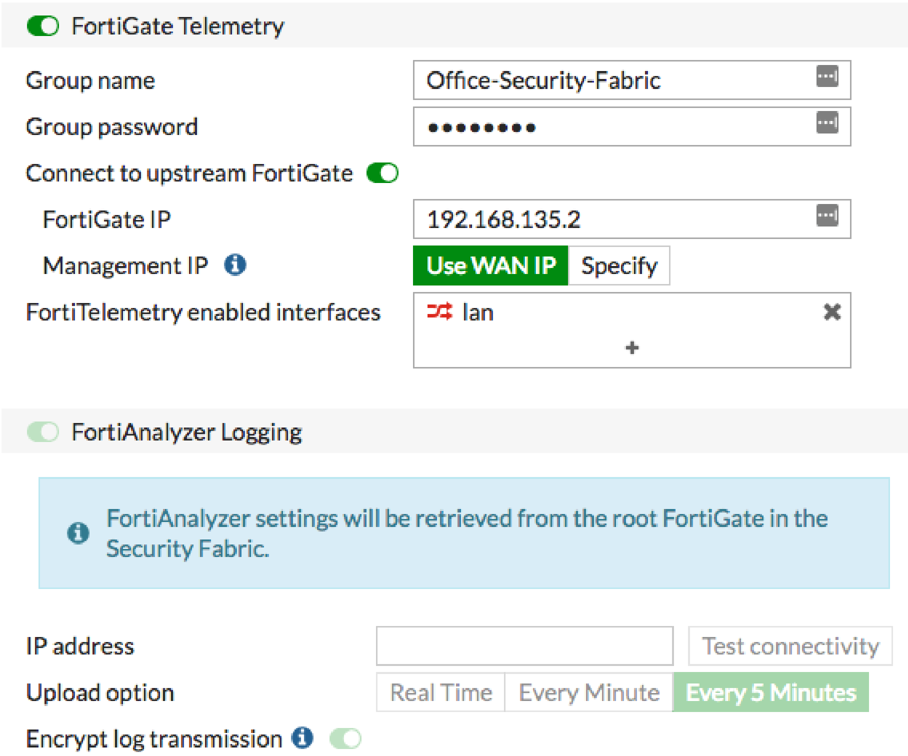


6. Go to *Policy & Objects* > *IPv4 Policy* and create a policy to allow users on the Sales network to access Marketing.



7. Go to *Security Fabric* > *Settings* to add Sales to the Security Fabric.
   Enable *FortiGate Telemetry*, then enter the same *Group name* and *Group password* that you set previously.
   Enable *Connect to upstream FortiGate* and enter the IP address of the internal 14 interface on Marketing.

FortiAnalyzer Logging is enabled by default. Settings for the FortiAnalyzer will be retrieved when Accounting connects to External.

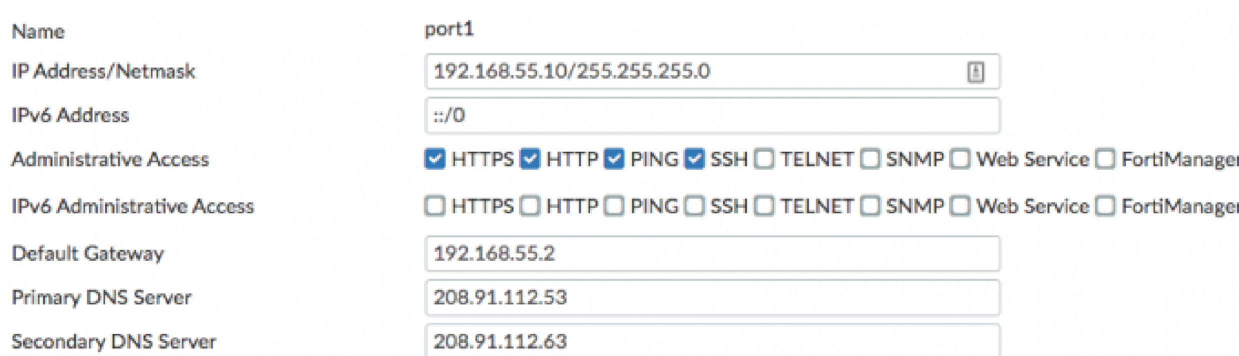


8. If you have not already done so, connect WAN2 on Sales to the internal 14 interface on Marketing.

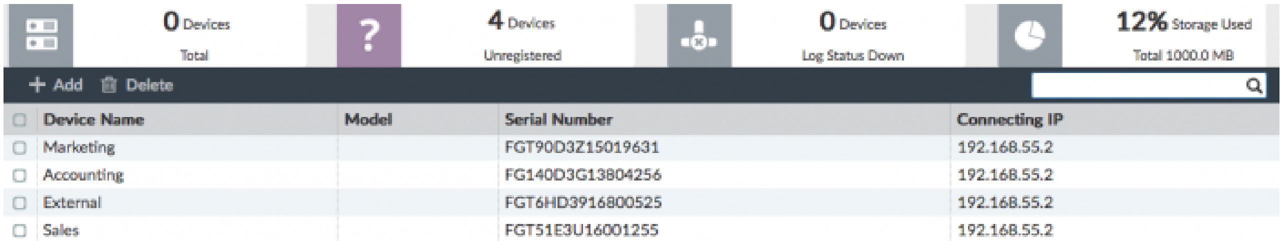
Configuring the FortiAnalyzer

To use the FortiAnalyzer in the Security Fabric, make sure that the firmware is compatible with the version of FortiOS on the FortiGates. To check for compatibility, see the FortiAnalyzer Release Notes.

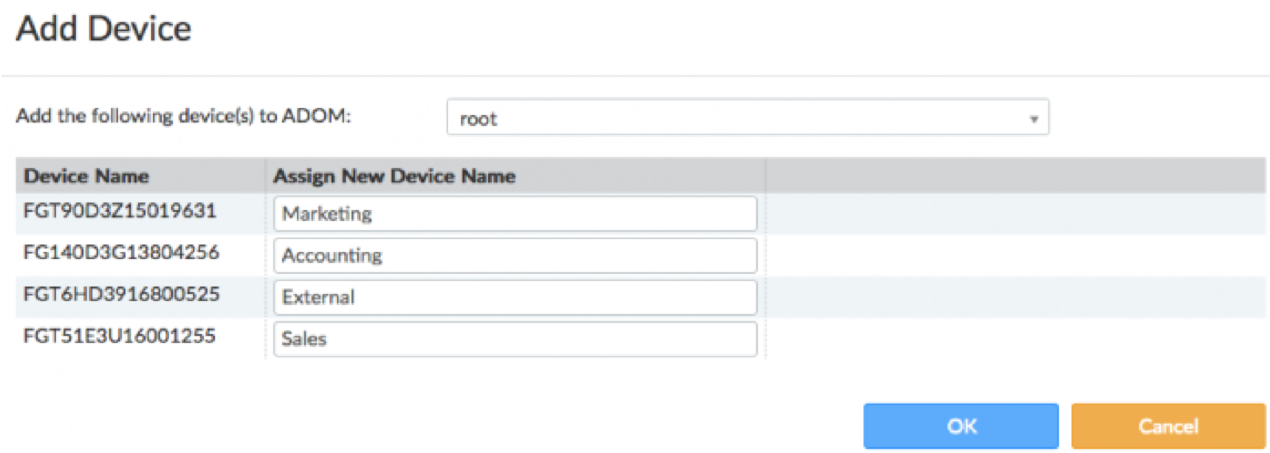
1. On the FortiAnalyzer, go to *System Settings > Network*.
   Select *All Interfaces* and edit port 1.
   Set *IP Address/Netmask* to the IP address used for the Security Fabric configuration on External (*192.168.55.10/255.255.255.0*).
   Add a *Default Gateway*, using the IP address of port 16 on External.



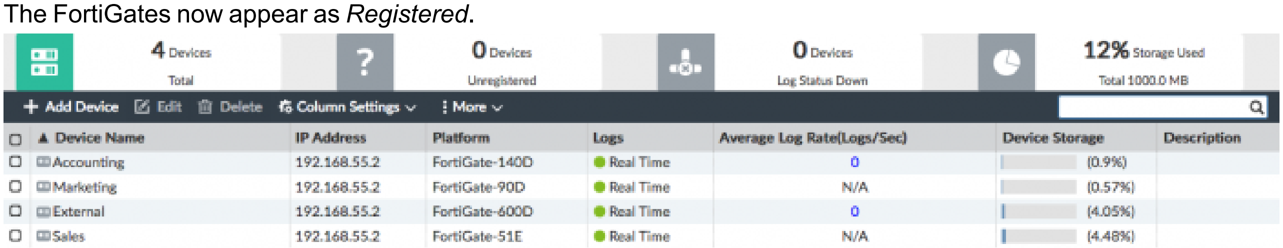
2. Go to *Device Manager*. The FortiGates are listed as *Unregistered*.



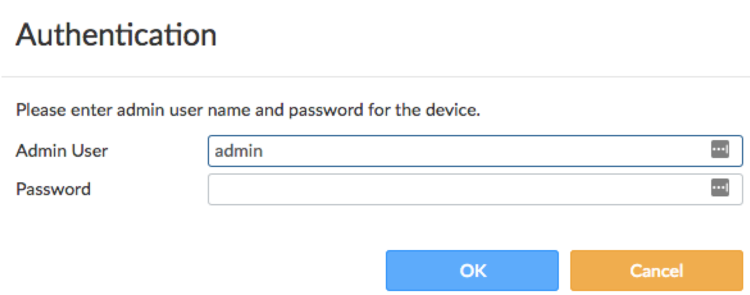
3. Select the FortiGates, then select *Add*.



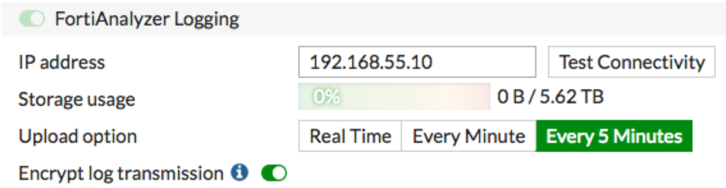
4. The FortiGates now appear as *Registered*.



5. After a moment, a warning icon appears beside External because the FortiAnalyzer needs administrative access to the root FortiGate in the Security Fabric.
   Select the FortiGate and enter the administrative authentication information.



6. On External, go to *Security Fabric* > *Settings*.
   FortiAnalyzer Logging now shows *Storage usage* information.



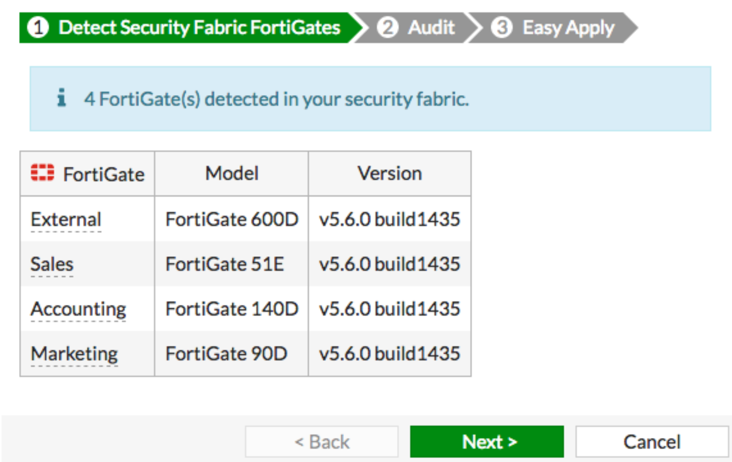
Running a Security Fabric Audit

You can use the *Security Fabric Audit* to analyze your Security Fabric deployment, identify potential vulnerabilities, and highlight best practices. Using the Security Audit helps you improve your network configuration, deploy new hardware and software, and gain more visibility and control over your network.

The *Security Score* is determined by how many checks your network passes or fails during the Security Audit. It also makes recommended improvements. By checking the *Security Score* and applying its recommendations, you can have confidence that your network is getting more secure over time.

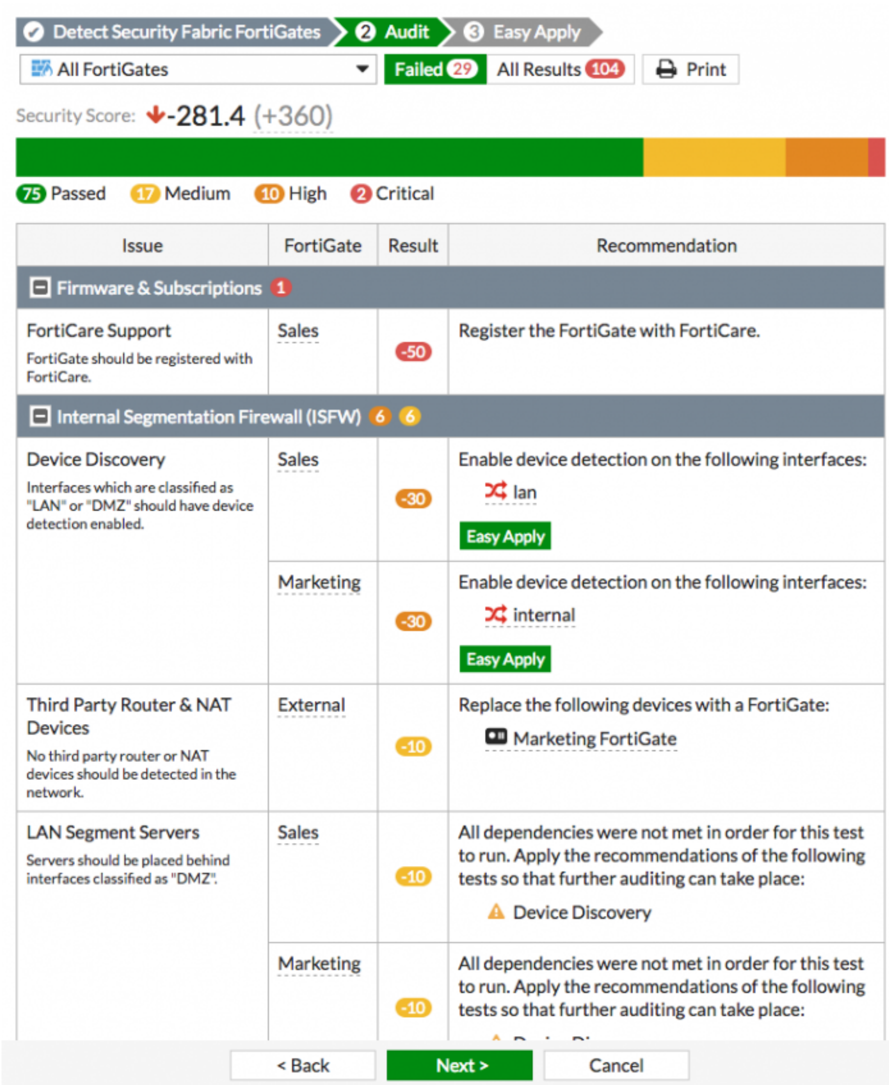
You must run the Security Fabric Audit on the root FortiGate in the Security Fabric.

1. On External, go to *Security Fabric* > *Audit* to see all the FortiGates in the Security Fabric.
   Click *Next*.



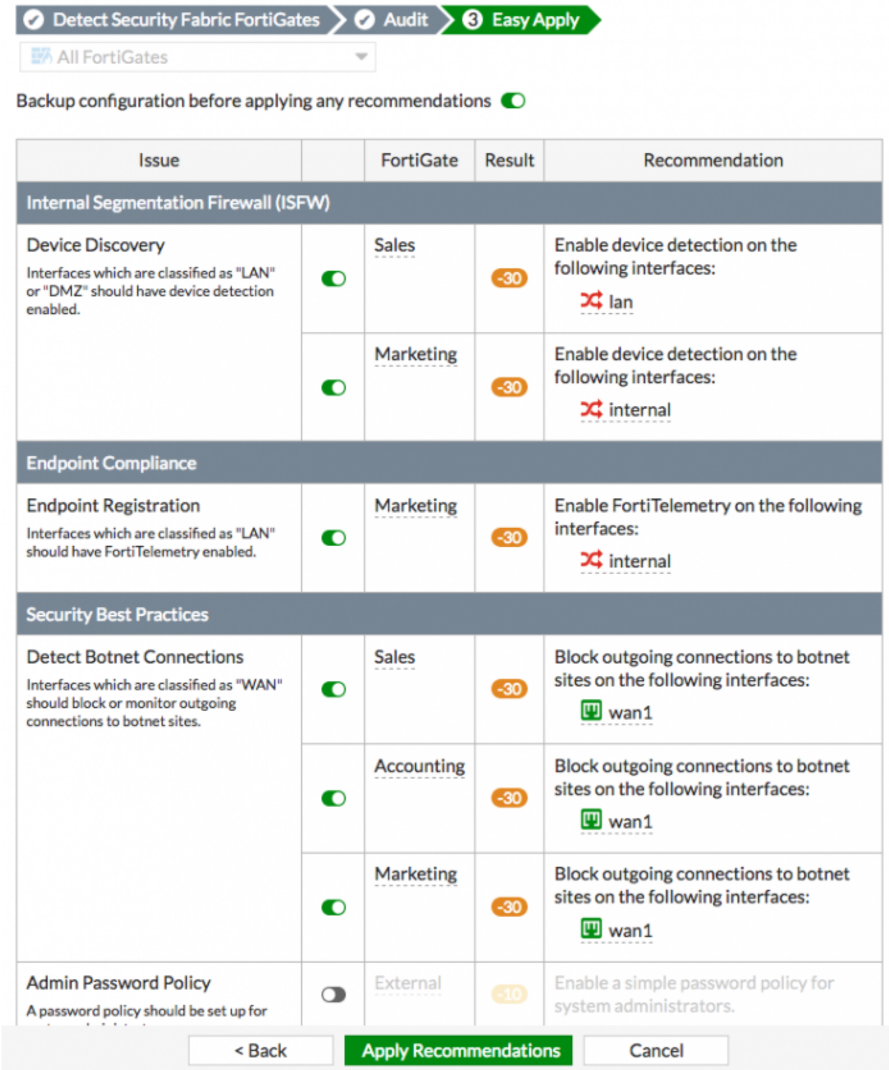
At the top of the page, you can see your network *Security Score* and the number of checks that passed or failed. The failed checks show the severity.

Further down, you can see information about each failed check, including which FortiGate failed the check, the effect on your network's score, and the recommendation for fixing the issue.



2. You can use *Easy Apply* to apply recommendations. *Easy Apply* can change the configuration of any FortiGate in the Security Fabric, not just the root FortiGate.

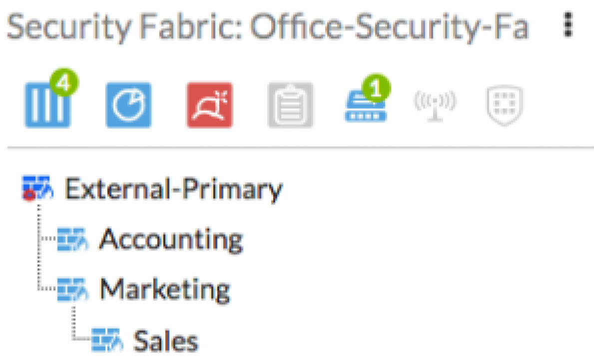
Select all the changes you want to make and click *Apply Recommendations*.



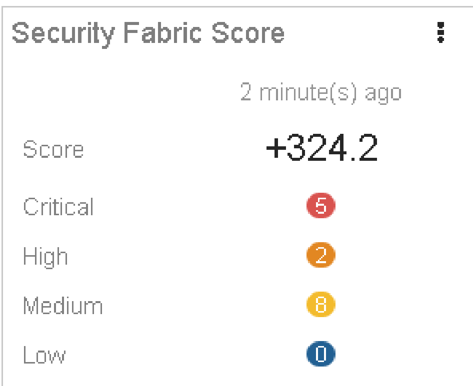
Results

1. On External, go to *Dashboard* > *Main*.
   The *Security Fabric* widget displays the names of the FortiGates in the Security Fabric.

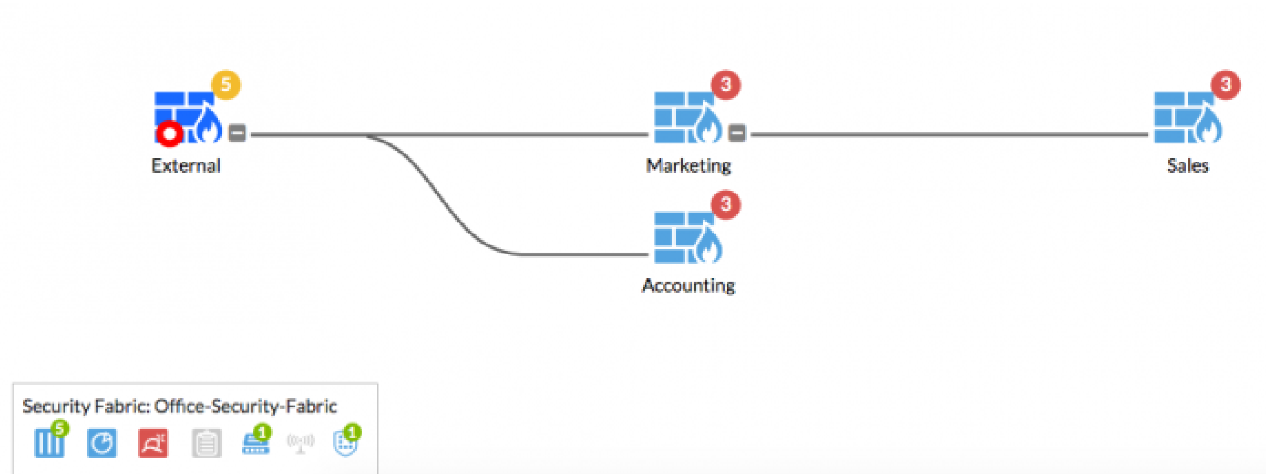
The icons on the top indicate which other Fortinet devices can be used in a Security Fabric. Devices in blue are detected in your network, devices in gray are not detected in your network, and devices in red are also not detected in your network but are recommended for a Security Fabric.



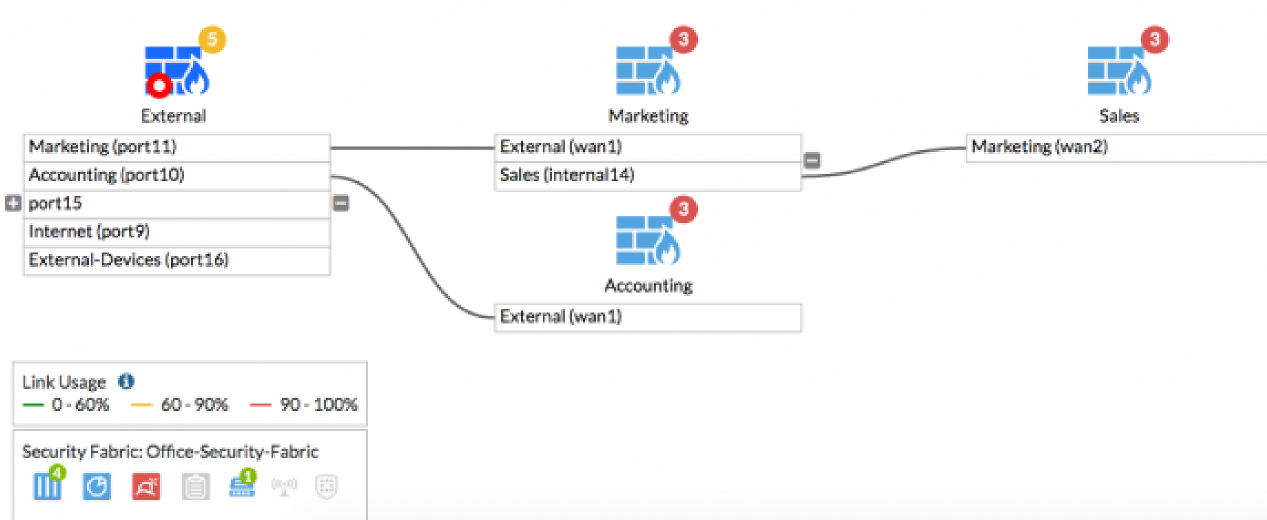
2. On the *Dashboard*, view the *Security Fabric Score* widget, which displays your network's current score.
   If any widget does not appear on your dashboard, you can add widgets using the *Settings* button in the bottom right.



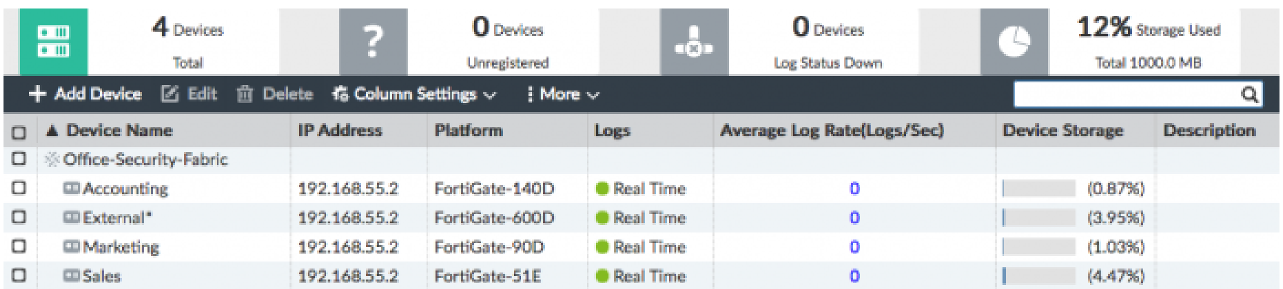
3. Go to *Security Fabric* > *Physical Topology*.
   This page shows a visualization of access layer devices in the Security Fabric.
   Security Fabric Audit recommendations are shown in the topology next to the device icon.



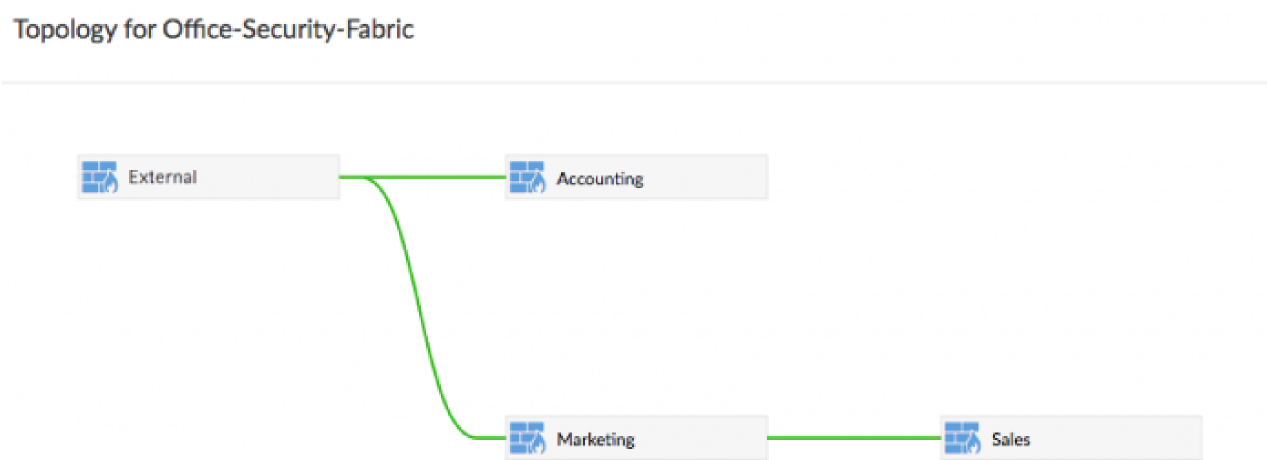
4. Go to *Security Fabric > Logical Topology*.
This page displays information about the interface (logical or physical) that each device in the Security Fabric is connected to.



5. On the FortiAnalyzer, go to *Device Manager*.
FortiGates are now shown as part of the *Office-Security-Fabric* group. The * beside External indicates that it is the root FortiGate in the Security Fabric.



6. Right-click the Security Fabric group and select *Fabric Topology* to display the topology of the Security Fabric.



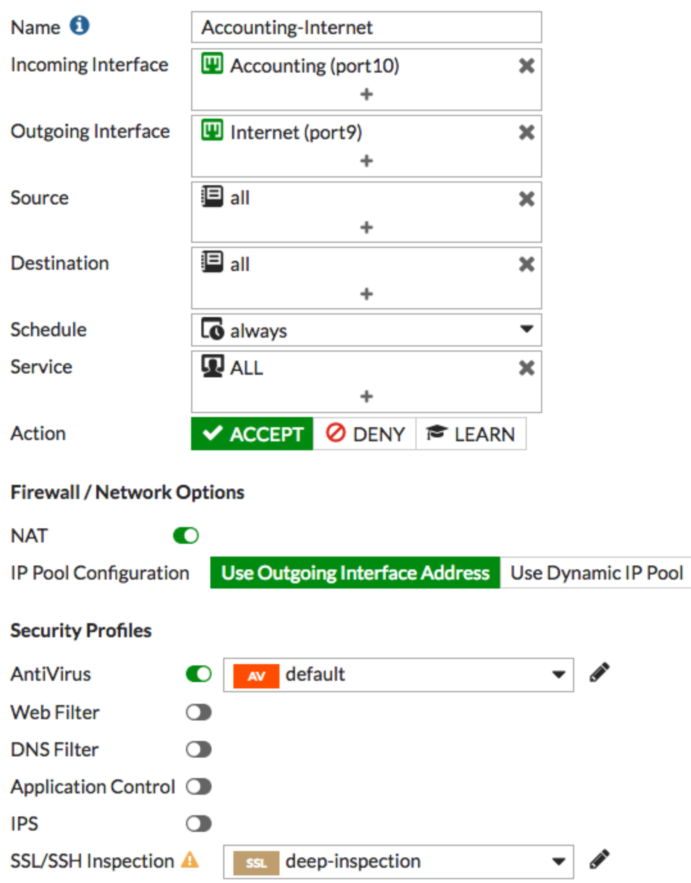
(Optional) Adding security profiles to the Security Fabric

Security Fabric allows you to distribute security profiles to different FortiGates in your network, which can lessen the workload of each device and avoid creating bottlenecks. For example, you can implement antivirus scanning on External while the ISFW FortiGates apply application control and web filtering.

This results in distributed processing between the FortiGates in the Security Fabric, which reduces the load on each one. It also allows you to customize the web filtering and application control for the specific needs of the Accounting network as other internal networks may have different application control and web filtering requirements.

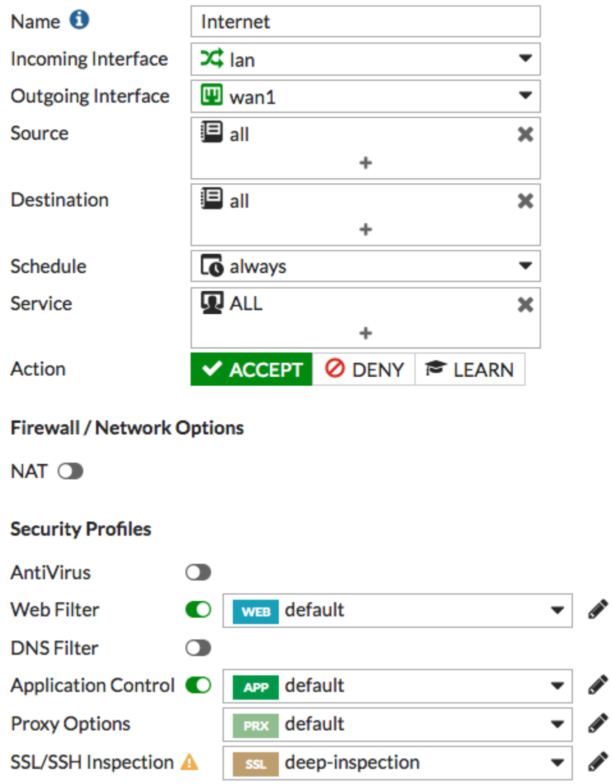
This configuration might result in threats getting through External so you should very closely limit access to the network connections between the FortiGates in the network.

1. On External, go to *Policy & Objects* > *IPv4 Policy* and edit the policy allowing traffic from Accounting to the Internet. Under *Security Profiles*, enable *AntiVirus* and select the *default* profile.
   Do the same for the policy allowing traffic from Marketing to the Internet.

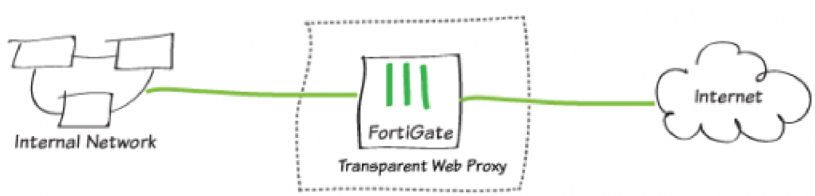


2. On Accounting, go to *Policy & Objects* > *IPv4 Policy* and edit the policy allowing traffic from the Accounting network to the Internet.
   Under *Security Profiles*, enable *Web Filter* and *Application Control*, and select the *default* profiles for both.

Repeat this step for both Marketing and Sales.



Transparent web proxy

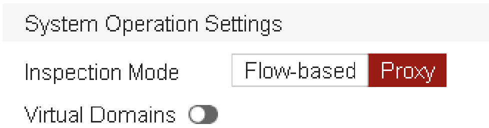


This example shows how to set up a basic transparent web proxy. You can use the transparent web proxy to apply web authentication to HTTP traffic accepted by a firewall policy.

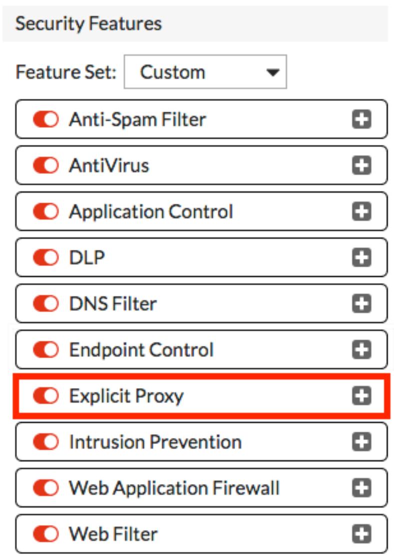
In previous versions of FortiOS, web authentication required using explicit web proxy. Now, FortiOS also supports a transparent web proxy. With transparent web proxy, you can forward your user's web traffic to the proxy without requiring your users to reconfigure their browsers or publish a proxy auto-configuration (PAC) file.

Configuring system and network settings

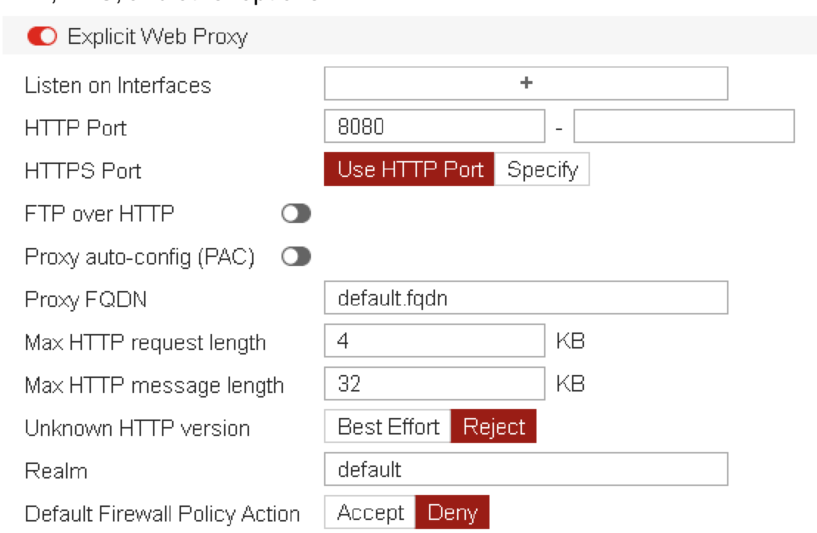
1. Go to *System* > *Settings*. Under *System Operation Settings*, set the *Inspection Mode* to *Proxy*.



2. Go to *System* > *Feature Visibility*. Under *Security Features*, enable *Explicit Proxy*.

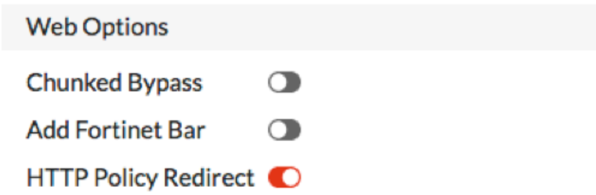


3. Go to *Network* > *Explicit Proxy* and enable *Explicit Web Proxy*.
   You can also change the *HTTP Port* that the proxy listens on (default is 8080) or specify different ports for HTTPS, FTP, PAC, and other options.



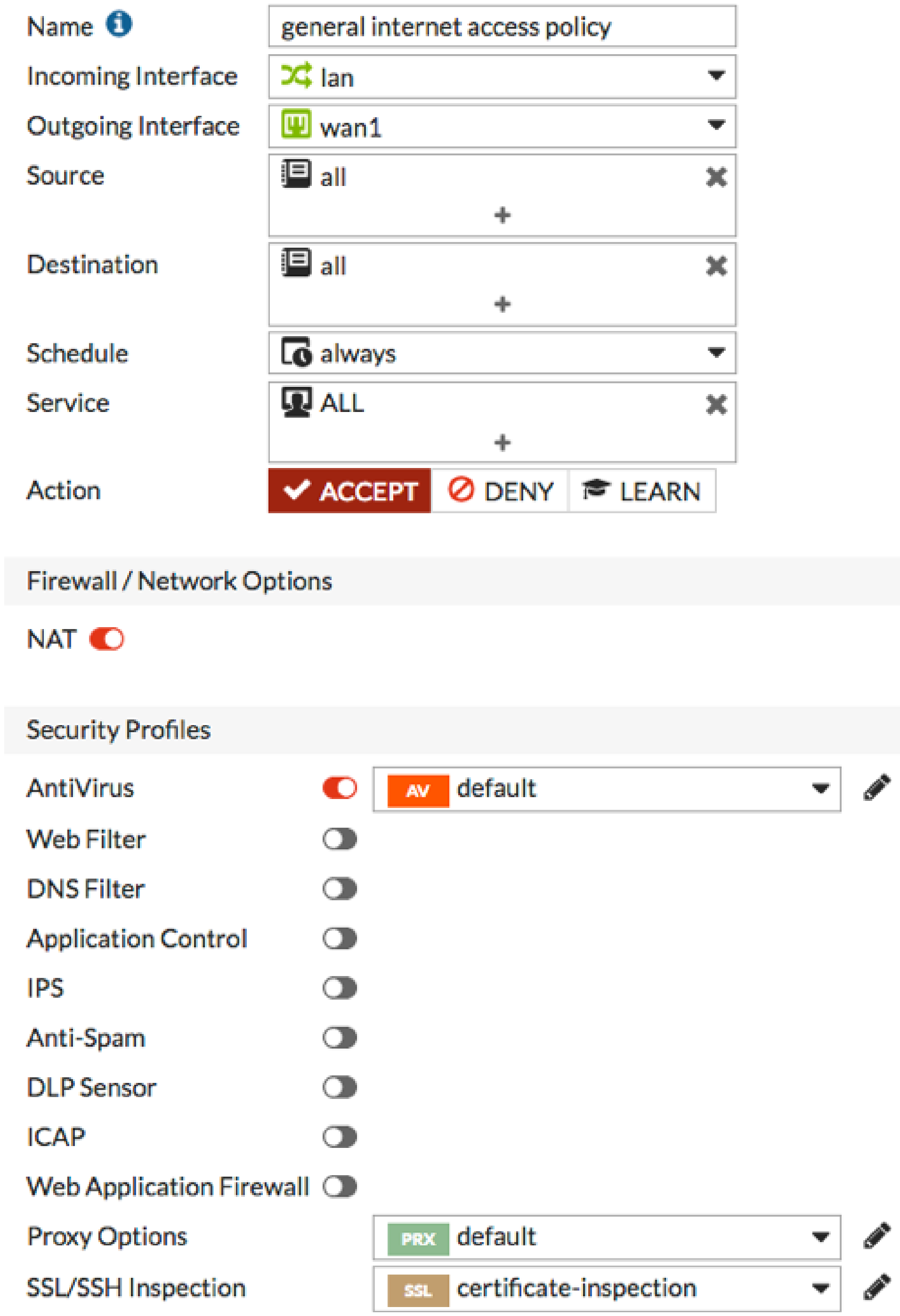
Adding proxy options to your policy

1. Go to *Security Profiles* > *Proxy Options*. Create or edit a proxy options profile. Under *Web Options*, enable *HTTP Policy Redirect*.



2. Go to *Policy & Objects* > *IPv4 Policy* and create or edit a policy controlling the traffic that you want to apply authentication to. Select a security profile (in this example, *AntiVirus*) and then enable the *Proxy Options* edited in

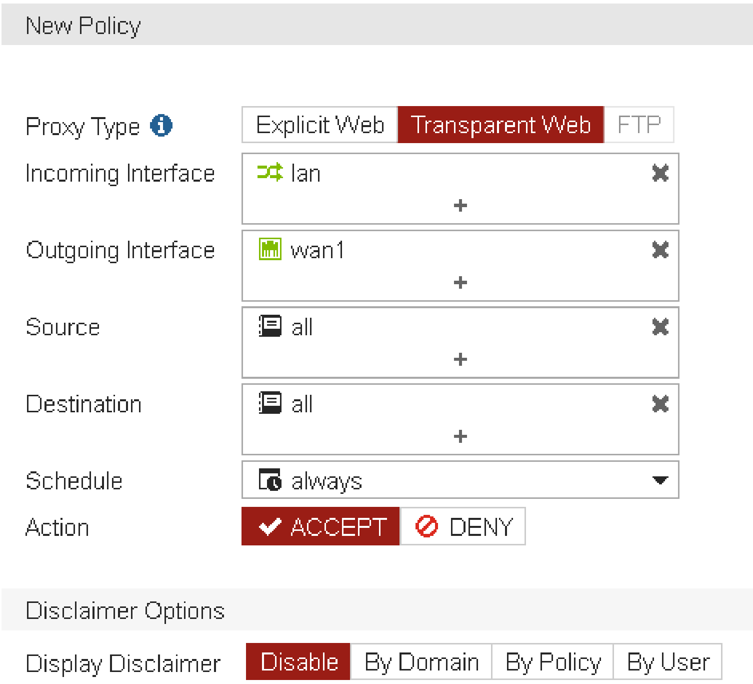
the previous step. *SSL/SSH inspection* becomes enabled by default.



Creating a proxy policy

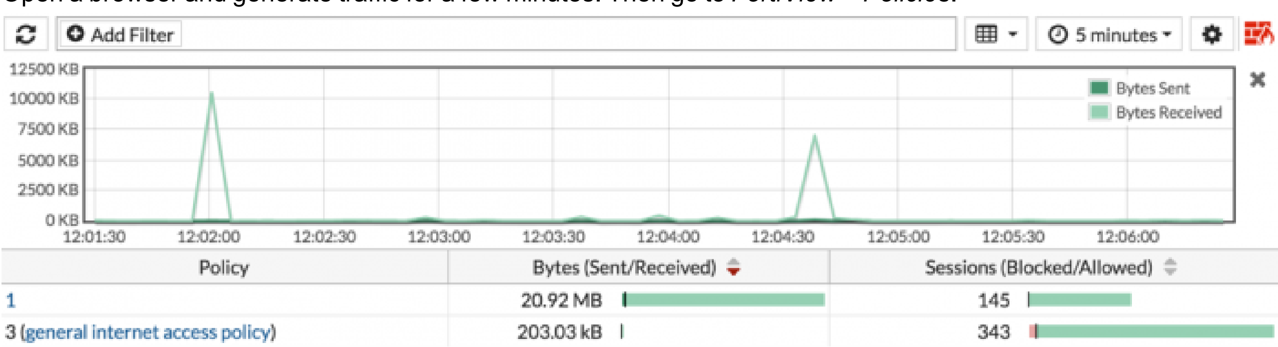
1. Go to *Policy & Objects* > *Proxy Policy* and create a transparent policy to accept the traffic that you want to apply authentication to. Set the *Proxy Type* to *Transparent Web*.

The *Incoming Interface*, *Outgoing Interface*, *Destination*, and *Schedule* must either match or be a subset of the source addresses in the IPv4 policy. Addresses added to the *Source* must match or be a subset of the source addresses added to the IPv4 policy. You can also add the users to be authenticated by the transparent policy to the *Source* field.

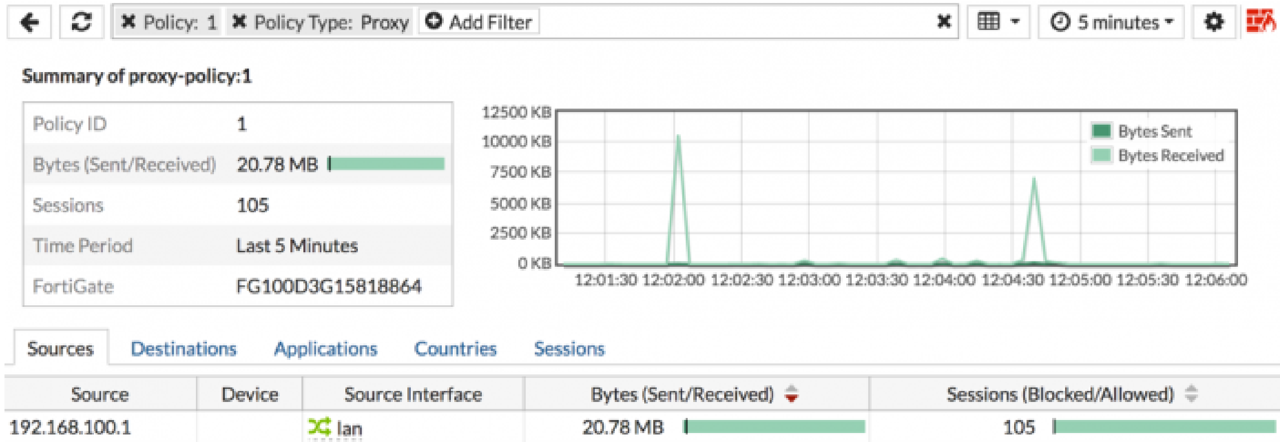


Results

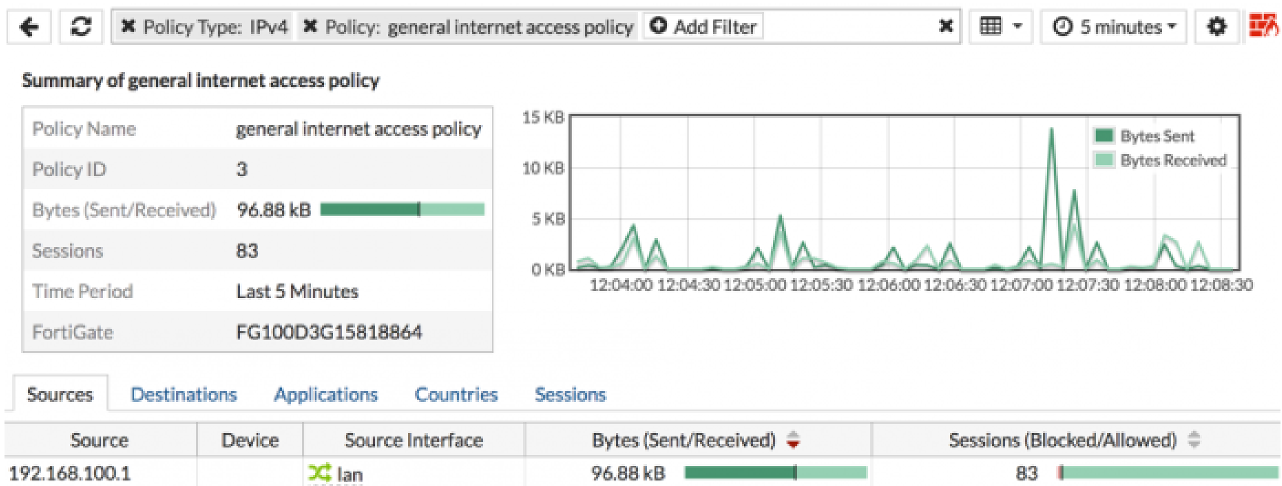
1. Open a browser and generate traffic for a few minutes. Then go to *FortiView* > *Policies*.



2. Right-click a row in the table to drill down for details. You can see that traffic is flowing through the proxy policy.

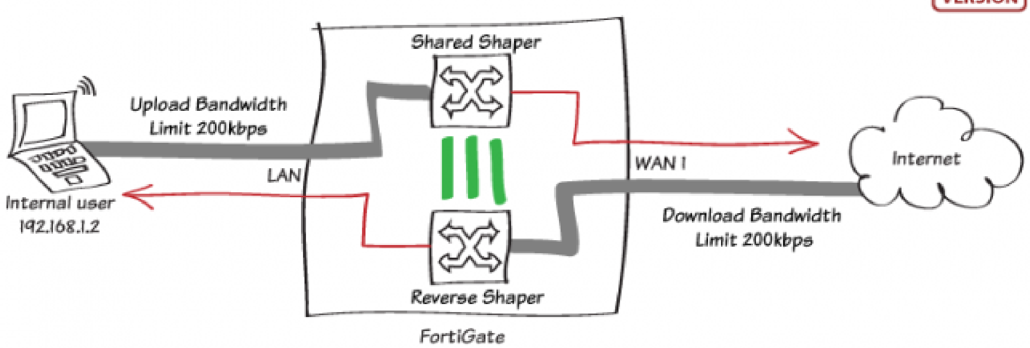


3. Traffic is flowing through the IPv4 policy configured with the proxy security profile.



Limiting bandwidth with traffic shaping

FORTIOS 5.6 VERSION

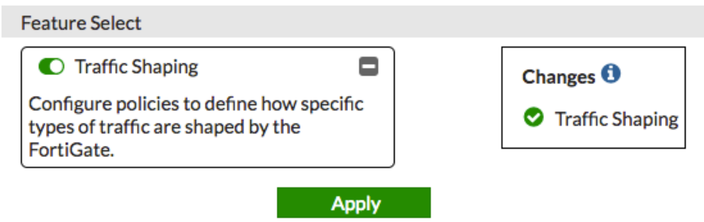


When one IP address uses too many resources, you can prevent the device with that IP address from consuming too much bandwidth. This example shows you how to use traffic shaping on your FortiGate to limit the bandwidth for a specific IP address.

This example also explains how to configure traffic shaping to set a maximum bandwidth limit for uploads and/or downloads to 200 kilobits per second (Kbps).

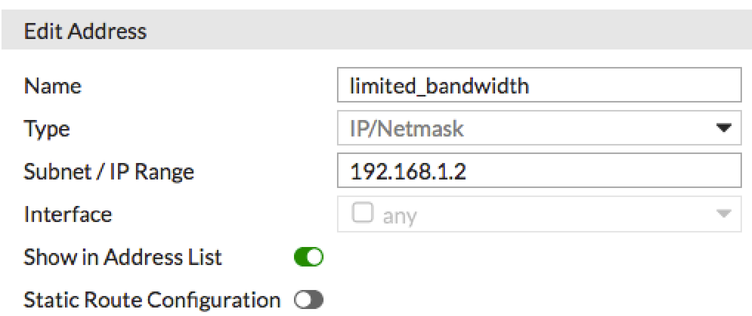
Enable Traffic Shaping

1. Go to *System > Feature Visibility* and under *Additional Features* enable *Traffic Shaping*.



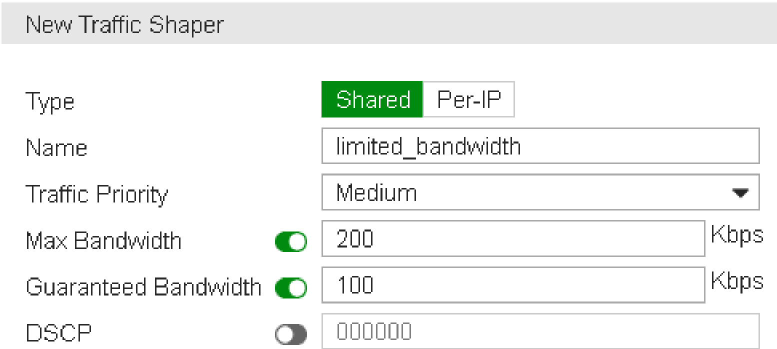
Creating a firewall address to limit

1. Go to *Policy & Objects > Addresses* to define the address you want to limit. Select *Create New > Address* from the dropdown menu.
   Enter a *Name* (in this example, *limited_bandwidth*). Set *Type* to *IP/Netmask*. Set the *Subnet / IP Range* to the internal IP address you want to limit. Set *Interface* to *any*.



Configuring a traffic shaper to limit bandwidth

1. Go to *Policy & Objects > Traffic Shapers* and select *Create New* to define a new shared Traffic Shaper profile.
   Set *Type* to *Shared*.
   Enter a *Name* (in this example, *limited_bandwidth*) and set the *Traffic Priority* to *Medium*.
   Set *Max Bandwidth* to `200` Kbps.
   If you want to set a *Guaranteed Bandwidth*, make sure the rate is lower than the *Max Bandwidth*.



Apply your changes.

2. By default, shared shapers apply shaping by evenly distributing the bandwidth to all policies using it. You can enable per policy shaping to apply shaping individually to each policy. Right-click your *limited_bandwidth* shaper and select *Edit in CLI* from the drop down menu.
Enter the following CLI command:

```
     set per-policy enable
end
```

3. With per policy shaping enabled, edit your *limited_bandwidth* shaper and verify that *Apply shaper* is set to *Per policy*.

Verifying your Internet access security policy

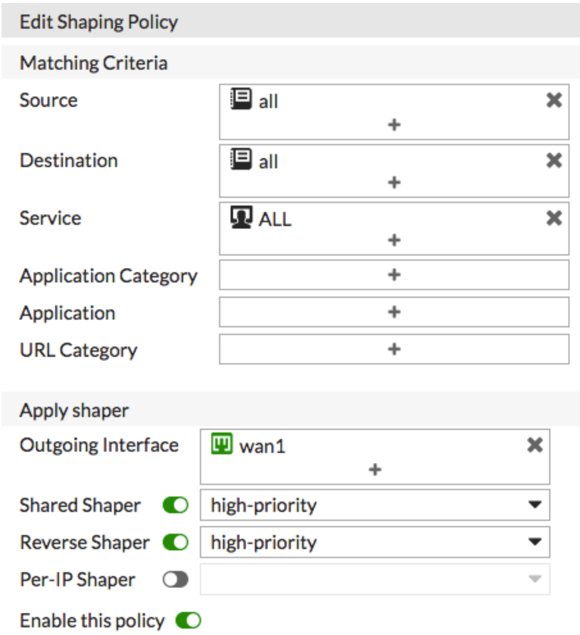
1. Go to *Policy & Objects* > *IPv4 Policy* and check the general Internet access policy. Check the *Incoming Interface*, *Outgoing Interface*, *Source*, and *Destination*.
2. If necessary, edit the policy and ensure that *Logging Options* is set to *All Sessions* for testing purposes.

Seq.#	Name	Source	Destination
lan - wan1 (1 - 1)			
1	Internet-access	all	all
Implicit (2 - 2)			

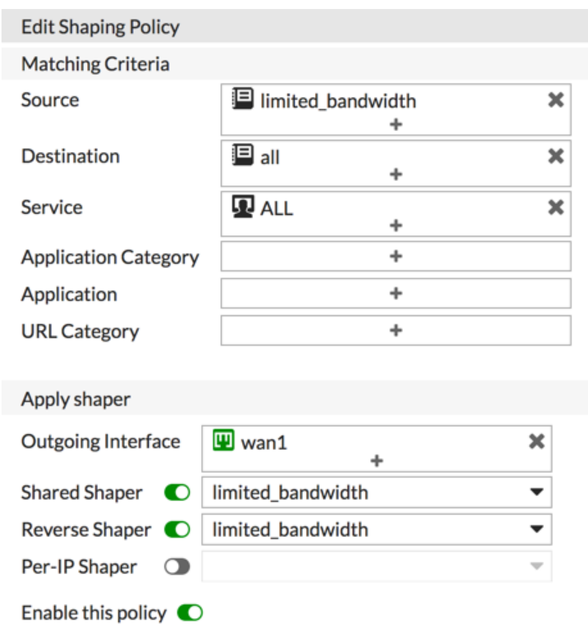
Creating two traffic shaping policies

1. Go to *Policy & Objects* > *Traffic Shaping Policy* and click *Create New* to create a shaping policy to set regular traffic to high priority.
Under *Matching Criteria*, set *Source*, *Destination*, and *Service* to match your Internet access policy.

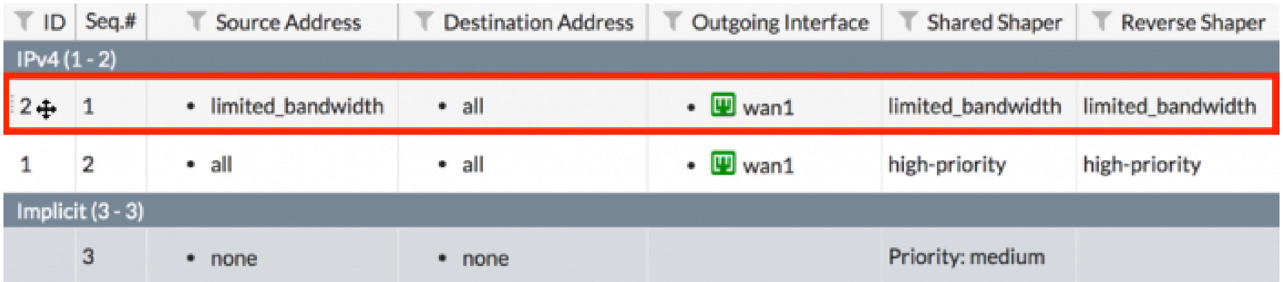
Under *Apply shaper*, set the *Outgoing Interface* to match your Internet access policy and enable *Shared Shaper* and *Reverse Shaper*. Shared shapers affect upload speeds and reverse shapers affect download speeds. Set both shapers to *high-priority*.



2. Click *Create New* to create a second traffic shaping policy to control the IP address you want to limit.
   Under *Matching Criteria*, set *Source* to *limited_bandwidth*. Set *Destination* and *Service* to *ALL*. Apply the shaper to the same *Outgoing Interface*. Enable *Shared Shaper* and *Reverse Shaper* and set both shapers to *limited_ bandwidth*.



3. Order your traffic shaping policies so that your more granular *limited_bandwidth* policy is above your general *high-priority* Internet access policy.

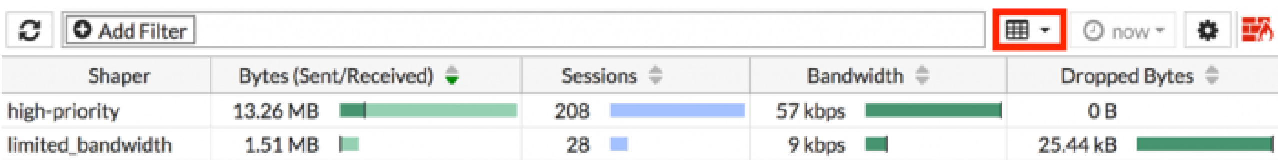


ID	Seq.#	Source Address	Destination Address	Outgoing Interface	Shared Shaper	Reverse Shaper
IPv4 (1 - 2)						
2	1	• limited_bandwidth	• all	• wan1	limited_bandwidth	limited_bandwidth
1	2	• all	• all	• wan1	high-priority	high-priority
Implicit (3 - 3)						
	3	• none	• none		Priority: medium	

Results

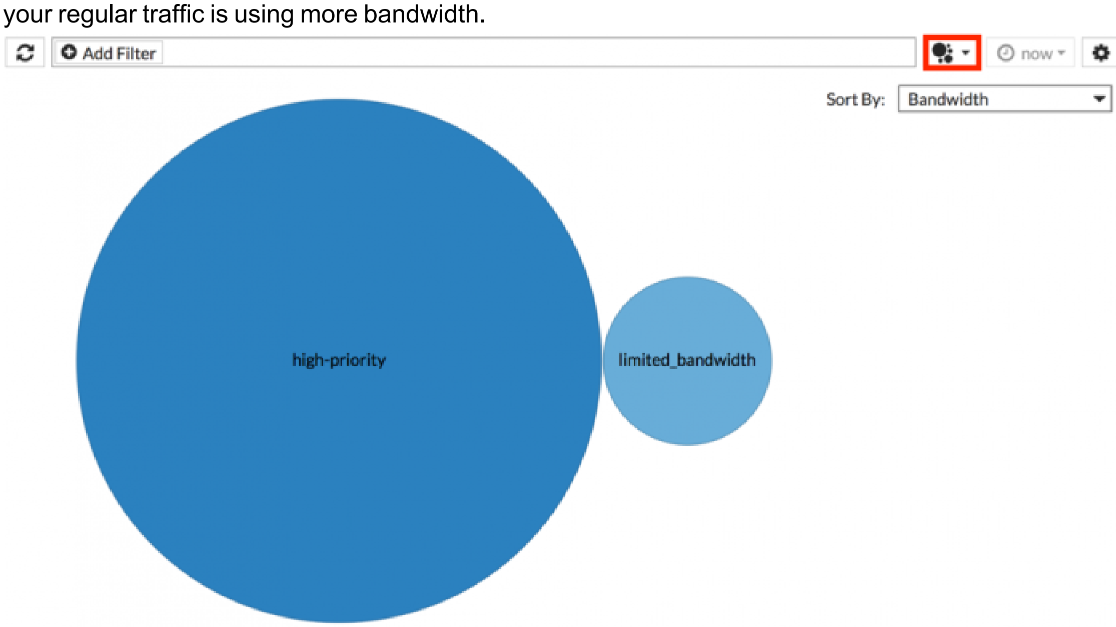
When a computer with the IP you have specified (192.168.1.2) browses the Internet from your internal network, its bandwidth is restricted to what you set in your shaper.

1. Go to *FortiView > Traffic Shaping* to view the current bandwidth usage for active shapers. Users on the local network have *high-priority* traffic.
   The IP address you specified receive *limited_bandwidth* treatment and may experience dropped bytes. Your *limited_bandwidth* shaper should not exceed 200 Kbps.
   Results show the *Bytes (Sent/Received)* in megabytes (MB) and the *Bandwidth* in Kbps.



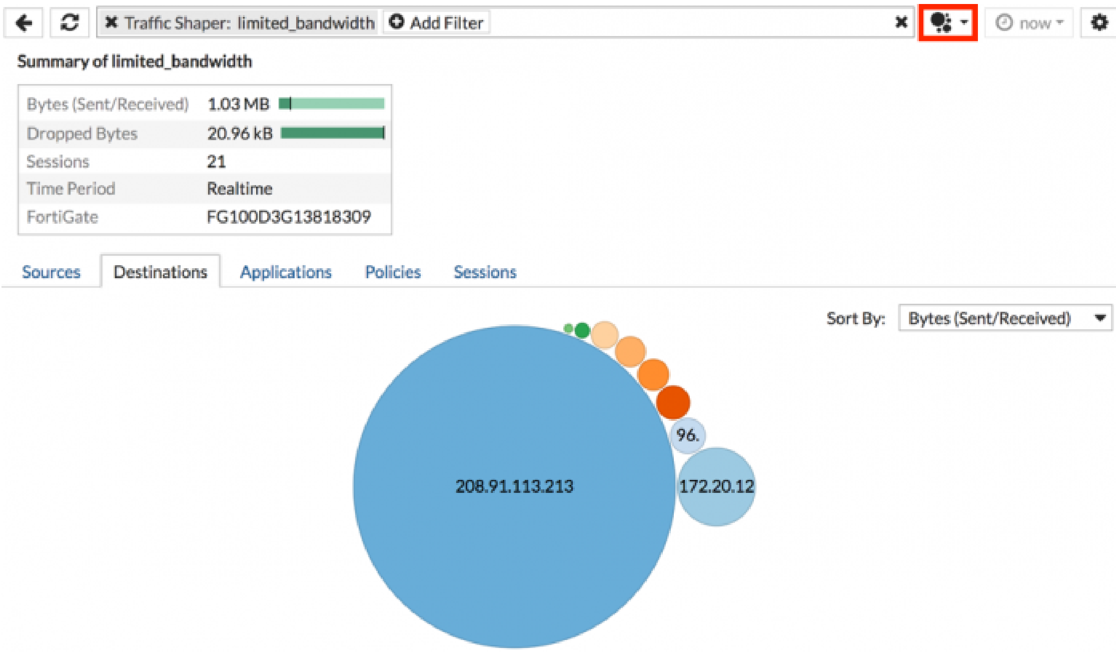
Shaper	Bytes (Sent/Received)	Sessions	Bandwidth	Dropped Bytes
high-priority	13.26 MB	208	57 kbps	0 B
limited_bandwidth	1.51 MB	28	9 kbps	25.44 kB

2. To view results in a bubble graph, change the graph type in the dropdown menu. Sort by *Bandwidth* to verify that your regular traffic is using more bandwidth.

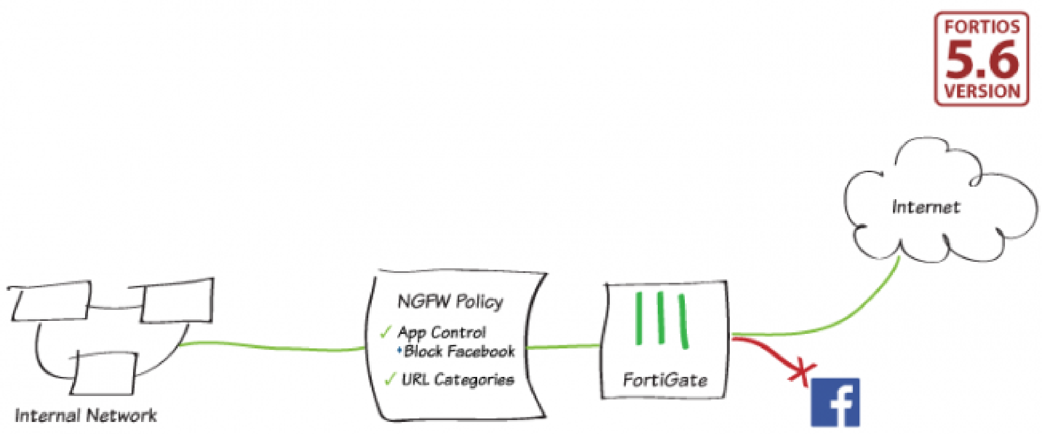


3. You can also double-click a shaper to see more granular information. Select the *Destinations* tab to see which

websites use the most bandwidth.



NGFW policy-based mode



You can operate your FortiGate or individual VDOMs on your FortiGate in Next Generation Firewall (NGFW) policy-based mode when you select flow-based inspection. In NGFW policy-based mode, you can add applications and web filtering categories directly to a policy without having to first create and configure Application Control or Web Filtering profiles. If a URL category is set, the applications that are added to the policy must be within the browser-based technology category.

Switching NGFW mode from profile-based to policy-based converts your profile-based security policies to policy-based security policies. If you don't want this to happen or you just want to experiment with policy-based NGFW mode, consider creating a new VDOM for policy-based NGFW mode. You can also back up your configuration before switching modes.

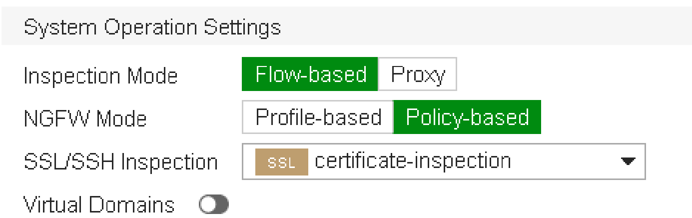
NGFW policy-based firewall policies may have unintended consequences to the passing or blocking of traffic. For example, if you add new firewall policies that are designed to DENY social media traffic based on applications or URLs, having a traditional “catch all” firewall policy to DENY all other traffic at the bottom of the firewall policy list may have the unintended consequence of blocking legitimate traffic.

NGFW policy-based mode applies the NAT settings from matching Central SNAT policies. If you don’t already have a Central SNAT policy in place, you will have to create one.

This recipe demonstrates a basic configuration of blocking Facebook using the new NGFW policy-based mode.

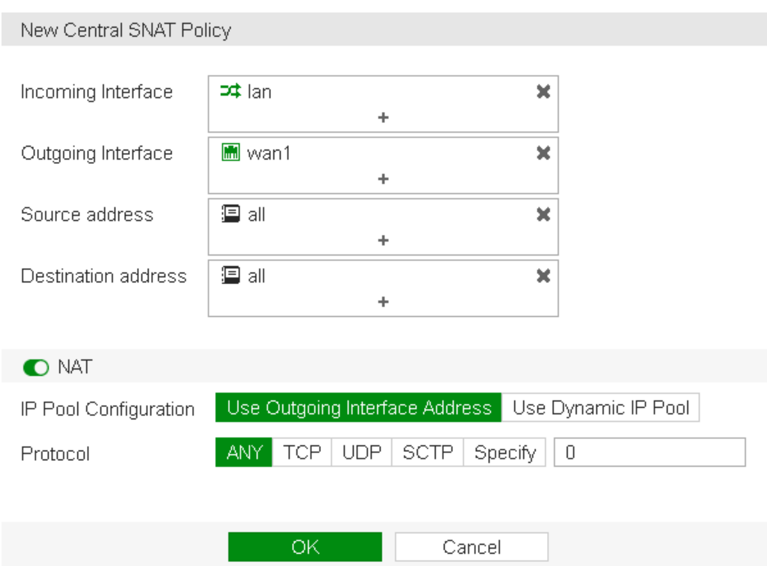
Configuring your FortiGate for NGFW policy-based mode

1. Go to *System > Settings* and scroll down to *System Operation Settings*.
   For *Inspection Mode*, select *Flow-based*.
   For *NGFW Mode*, select *Policy-based*.
   Select an *SSL/SSH Inspection* profile.



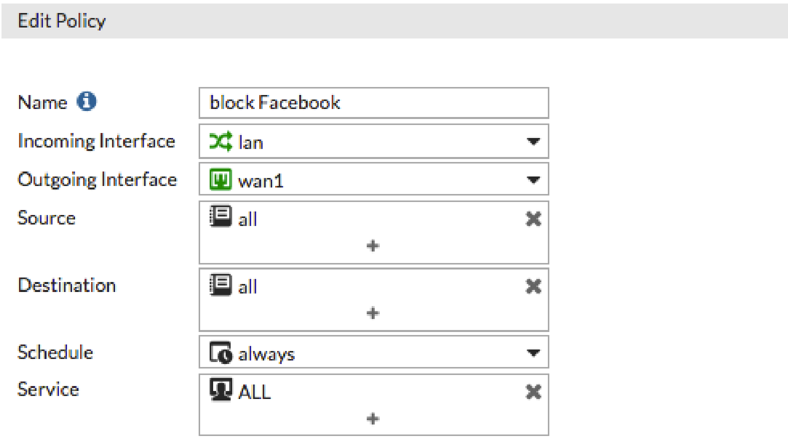
Creating a Central SNAT Policy

1. Go to *Policy & Objects > Central SNAT* and click *Create New*.
   Set *Incoming Interface* to the local network interface.
   Set *Outgoing Interface* to your Internet-facing interface.
   Set *IP Pool Configuration* to *Use Outgoing Interface Address*.
   Set *Protocol* to *ANY*.

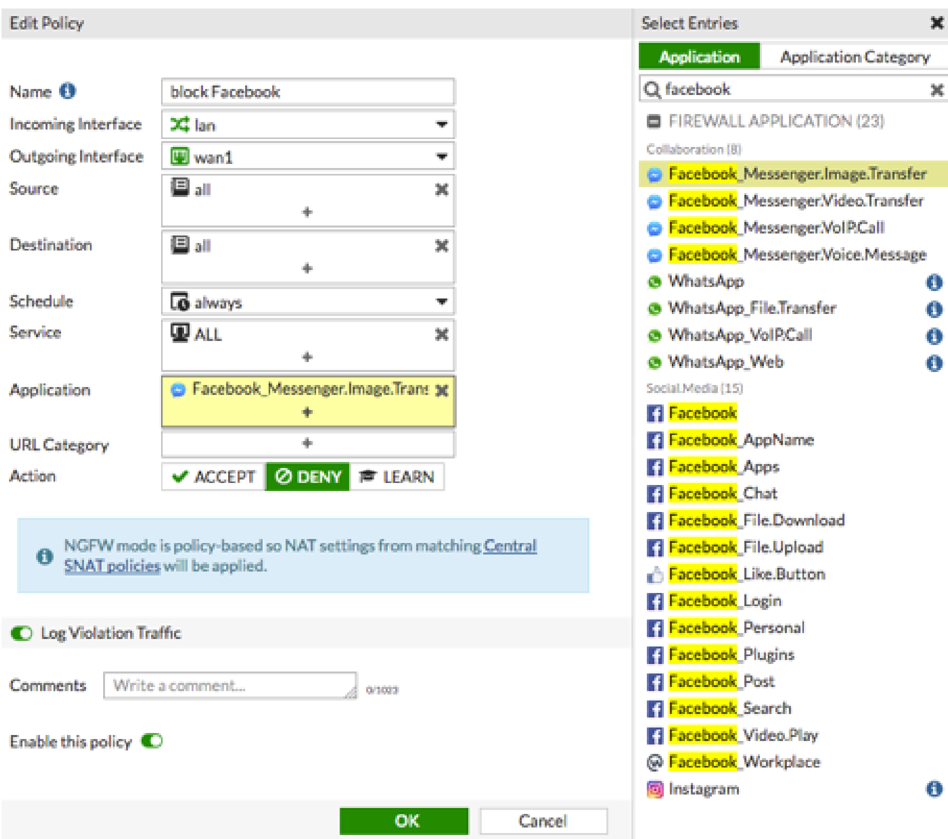


Creating an IPv4 policy to block Facebook

1. Go to *Policy & Objects* > *IPv4 Policy* and create a new policy.
   Set *Incoming Interface* to the local network interface.
   Set *Outgoing Interface* to your Internet-facing interface.

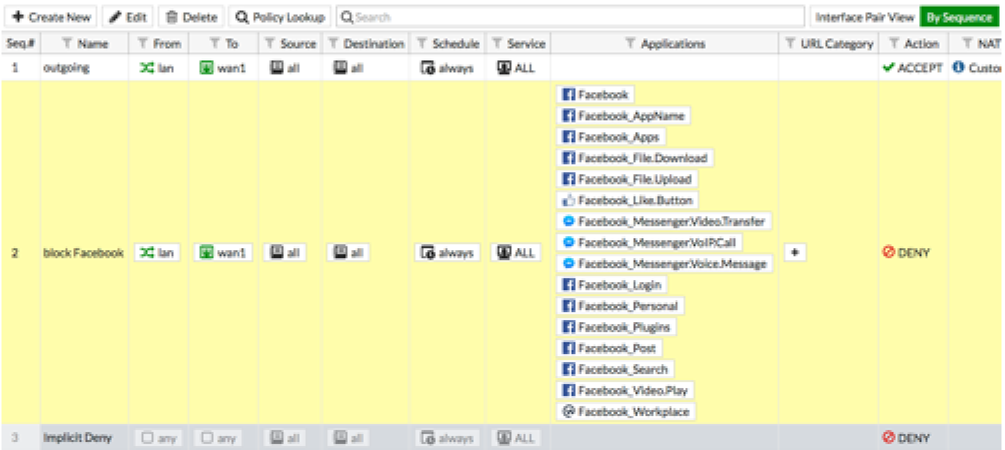


2. Under *Application*, click the plus sign. Type *Facebook* in the search field.
   Add all the Facebook applications to the policy. Set the *Action* to *DENY*.
   Enable *Log Violation Traffic* to see results later. You can disable this feature later to conserve network resources.

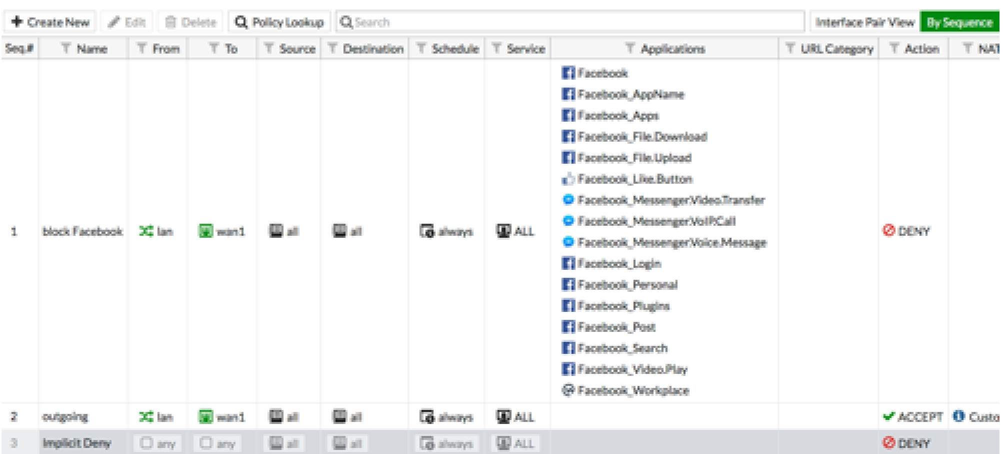


Ordering the policy table

1. Go to *Policy & Objects* > *IPv4 Policy* to view the policy table.
   To have the correct traffic flowing through each policy, they must be arranged so that the more specific policies are located at the top.

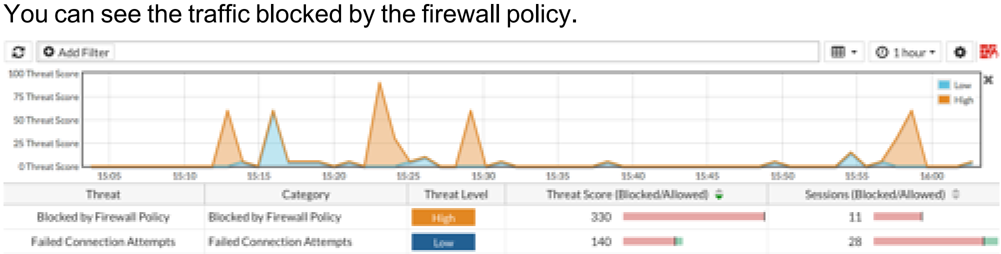


2. To rearrange the policies, select the column on the far left (in this example, *Seq.#*) and drag the policy to the desired position.

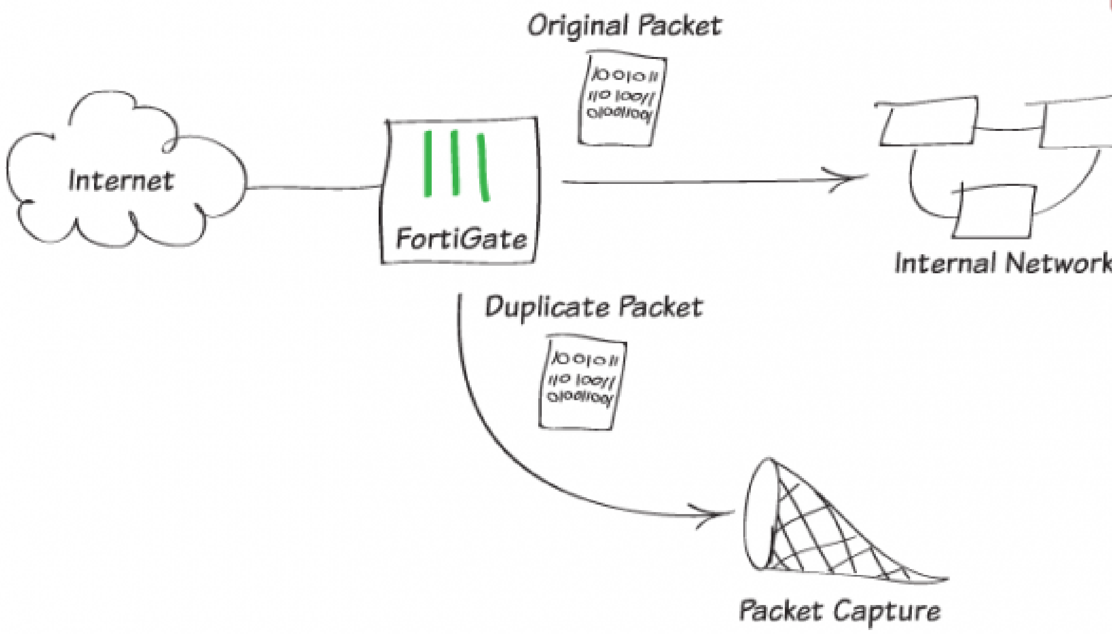


Results

1. Browse to www.facebook.com. Your connection will time out.
2. Go to *FortiView* > *Threats*.
   You can see the traffic blocked by the firewall policy.



Packet capture



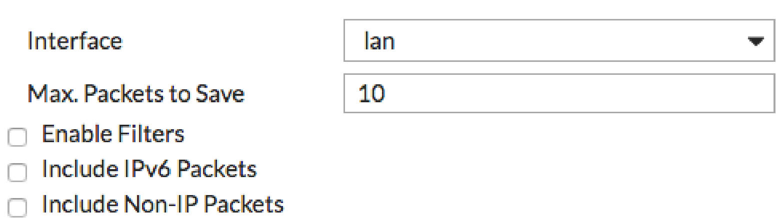
In this example you look inside the headers of the HTTP and HTTPS packets on your network.

Packet capture is also called network tapping, packet sniffing, or logic analyzing.

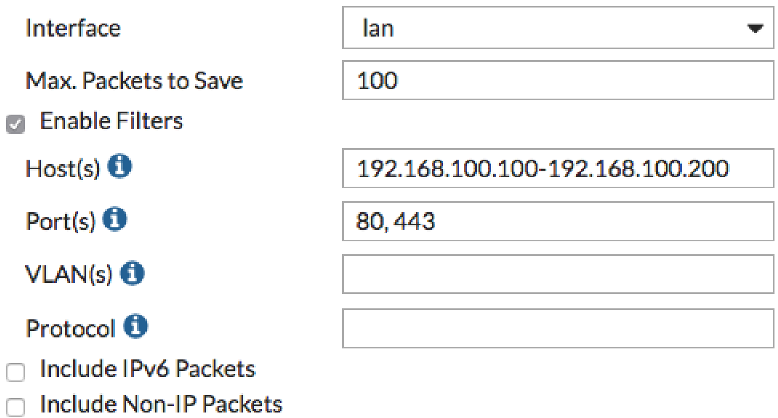
To use packet capture through the GUI, your FortiGate model must have internal storage and disk logging must be enabled. If you are not sure whether your model supports disk logging, check the FortiGate Feature/Platform Matrix.

Creating packet capture filters

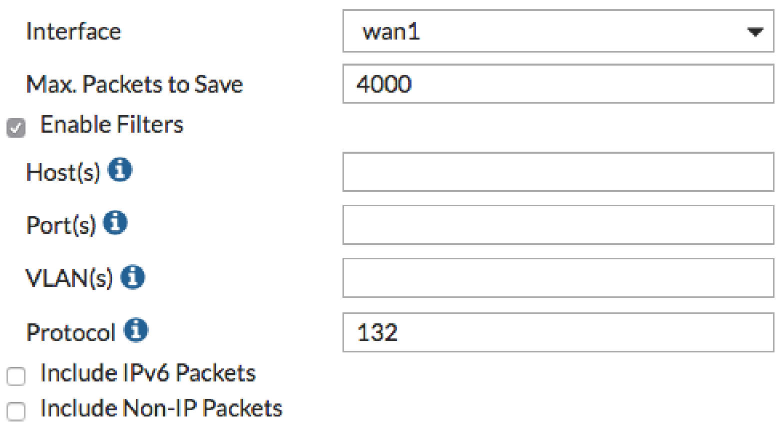
1. Go to *Network > Packet Capture* and create a new filter.
   If the *Packet Capture* option does not appear in the main GUI, you can also access this menu using the URL `https://[management-IP]/ng/page/p/firewall/sniffer/`.
2. The simplest filter just captures all of the packets received by an interface. This filter captures ten packets received by the LAN interface.



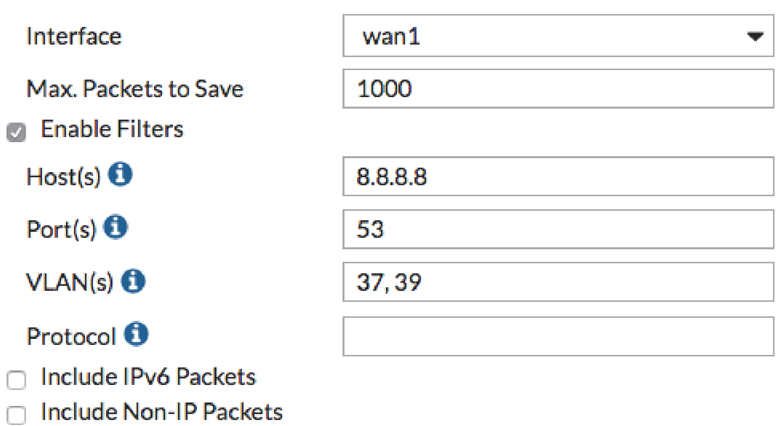
3. To be more specific about the packets to capture, select *Enable Filters*.
This filter captures 100 HTTP and HTTPS packets (port 80 and 443) received by the lan interface that has a source or destination address in the range 192.168.100.100-192.168.100.200.



4. This filter captures the first 4000 Stream Control Transmission Protocol (SCTP) packets received by the wan1 interface.



5. This filter captures the first 1000 DNS packets (port 53) querying the Google DNS server (IP address 8.8.8.8) with VLAN IDs 37 or 39.



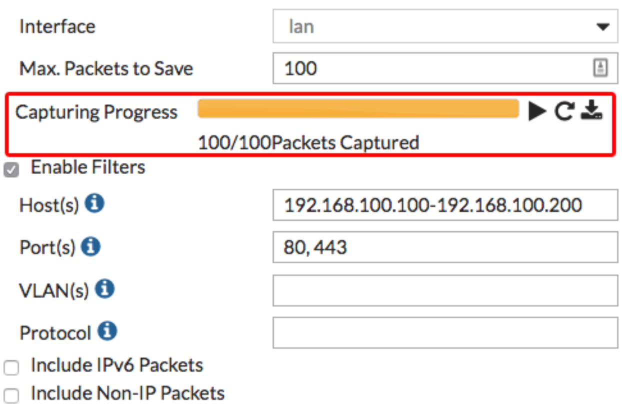
Results

Running packet capture filters may affect FortiGate performance.

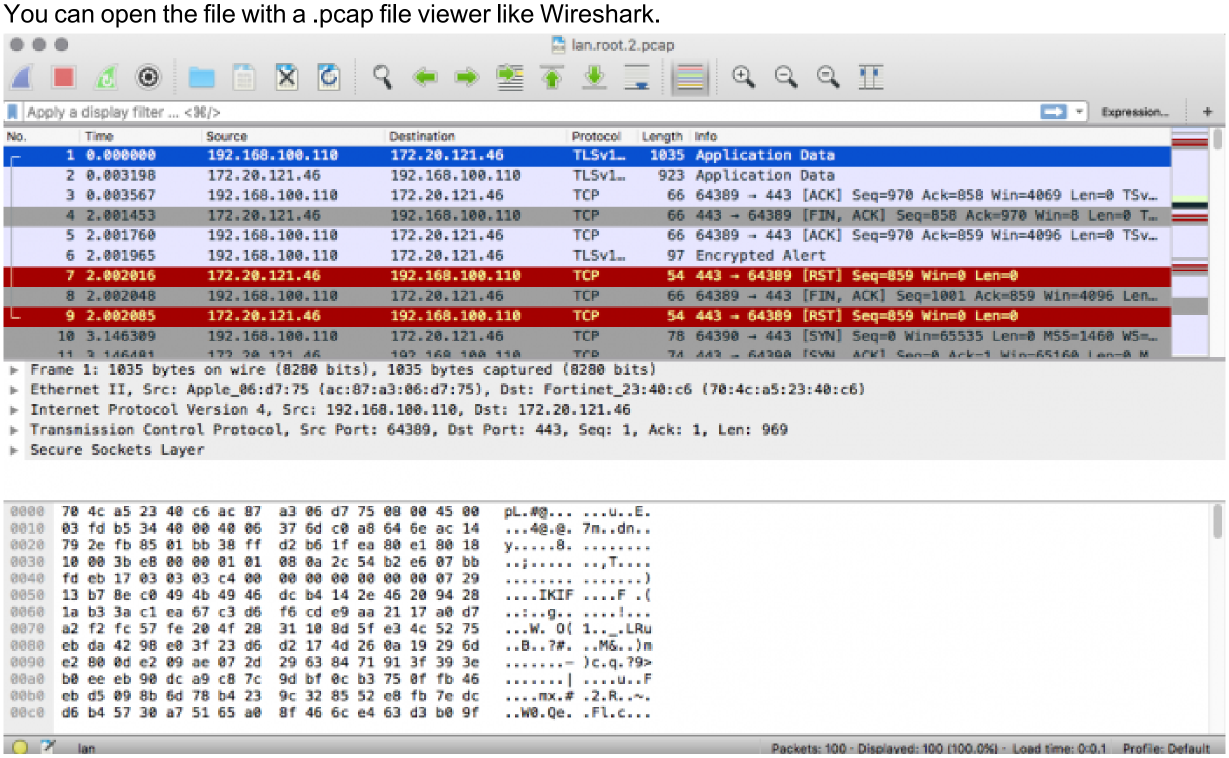
1. Go to *Network > Packet Capture*, choose a filter, and select the *Play* icon.
   You can watch the filter capture packets. When the number of packets specified in the filter are captured, the filter stops.
   You can stop and restart any filter at any time.

Interface	Filter Criteria	# Packets	Max Packet Count	Progress
lan		10	10	
lan	host=192.168.100.100-192.168.100.200 port=80, 443	42	100	
wan1	proto=132	0	4000	Not Running
wan1	host=8.8.8.8 port=53 vlan=37, 39	0	1000	

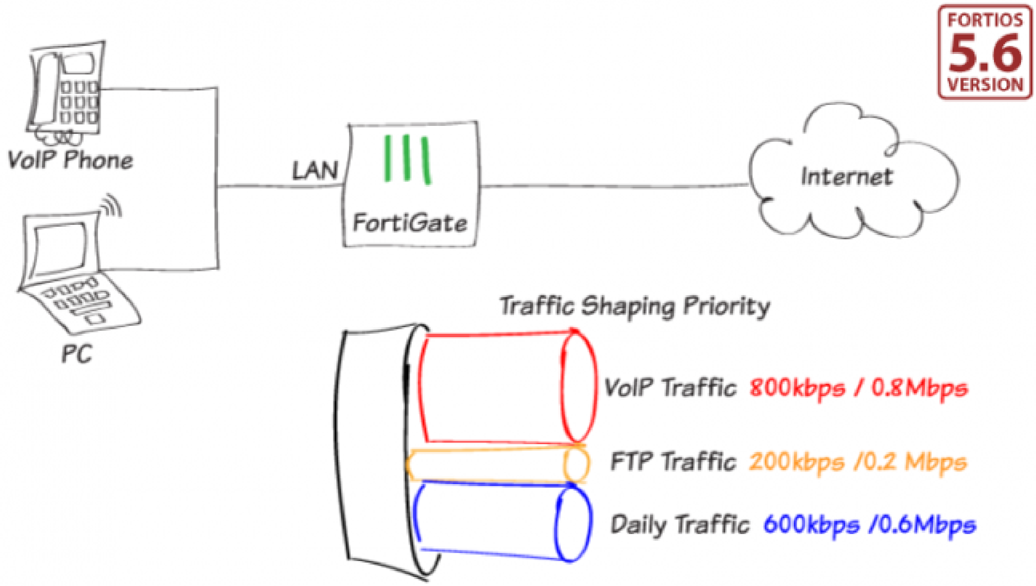
2. After a filter runs, select and edit it. You can download the capture packets.



3. You can open the file with a .pcap file viewer like Wireshark.



Traffic shaping for VoIP

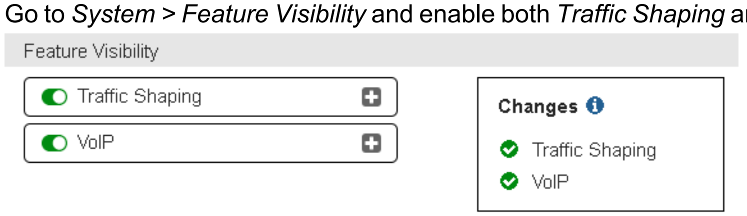


The quality of VoIP phone calls through a firewall often suffers when the firewall is busy and the bandwidth available for VoIP traffic fluctuates. This can be lead to unpredictable results and caller frustration. This example describes how to add traffic shaping to your FortiGate to ensure enough bandwidth for VoIP traffic regardless of other activities on the network.

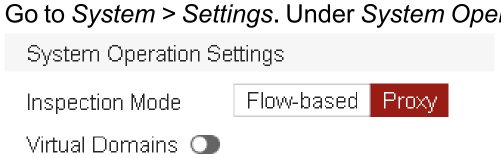
To achieve high-quality real-time voice transmissions, VoIP traffic requires priority over other types of traffic, minimal packet loss, and jitter buffers. You can limit bandwidth consuming services, like FTP, while providing a consistent bandwidth for day-to-day email and web-based traffic. First, you customize three existing traffic shaper profiles—high priority, medium priority, and low priority—and then create a separate traffic shaping policy for each service type.

Enable Traffic Shaping and VoIP features

1. Go to *System* > *Feature Visibility* and enable both *Traffic Shaping* and *VoIP*.



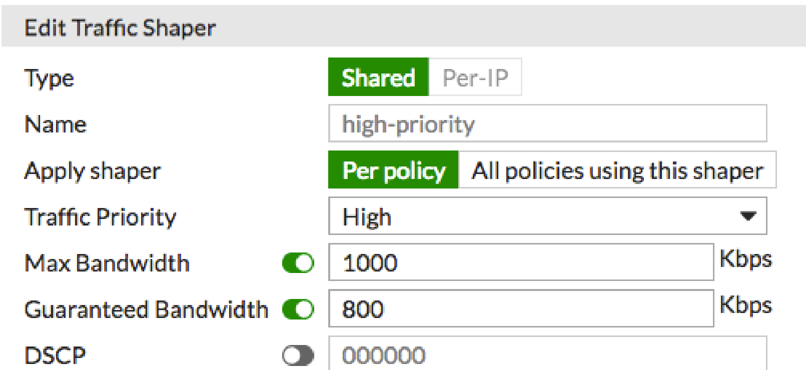
2. Click *Apply*.
3. Go to *System* > *Settings*. Under *System Operation Settings*, set the *Inspection Mode* to *Proxy*.



This allows you to apply VoIP profiles.

Creating a high priority VoIP traffic shaper

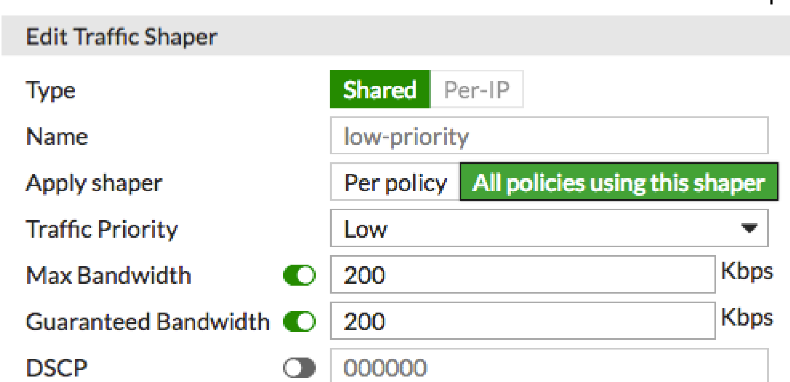
1. Go to *Policy & Objects* > *Traffic Shapers* and edit the default *high-priority* traffic shaper.
   Set *Type* to *Shared*.
   Set *Apply shaper* to *Per Policy*.
   Set *Traffic Priority* to *High*.
   Enable *Max Bandwidth* and enter `1000` Kbps.
   Enable *Guaranteed Bandwidth* and enter `800` Kbps.



2. Click *OK*.

Creating a low priority FTP traffic shaper

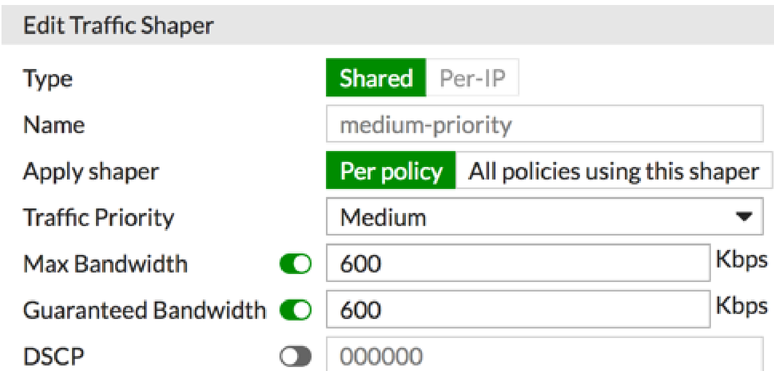
1. Go to *Policy & Objects* > *Traffic Shapers* and edit the default *low-priority* traffic shaper.
   Set *Type* to *Shared*.
   Set *Apply shaper* to *All policies using this shaper*.
   Set *Traffic Priority* to *Low*.
   Enable *Max Bandwidth* and *Guaranteed Bandwidth* and enter `200` Kbps for both.



2. Click *OK*.

Creating a medium priority daily traffic shaper

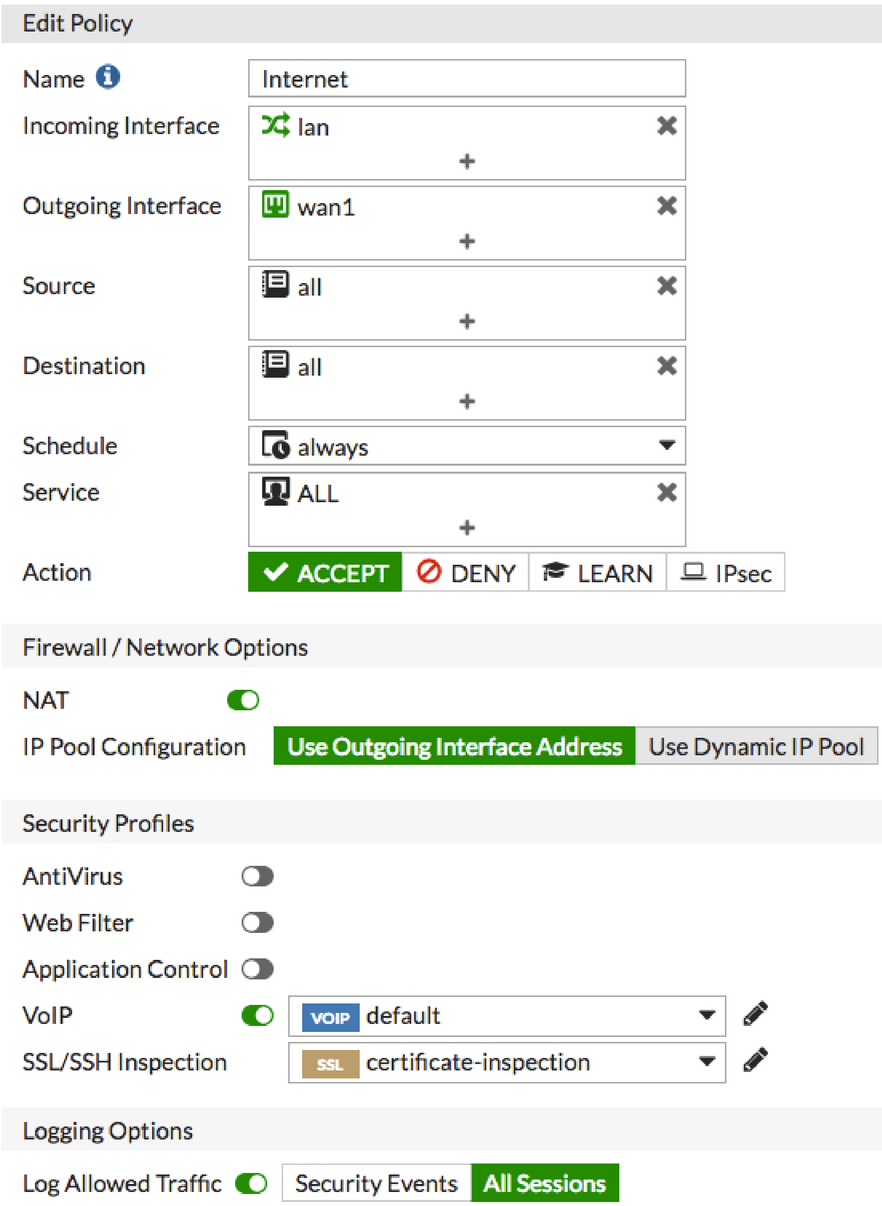
1. Go to *Policy & Objects* > *Traffic Shapers* and edit the default *medium-priority* traffic shaper.
   Set *Type* to *Shared*.
   Set *Apply shaper* to *Per Policy*.
   Set *Traffic Priority* to *Medium*.
   Enable *Max Bandwidth* and enter `600` Kbps.
   Enable *Guaranteed Bandwidth* and enter `600` Kbps.



2. Click *OK*.

Adding a VoIP security profile to your Internet access policy

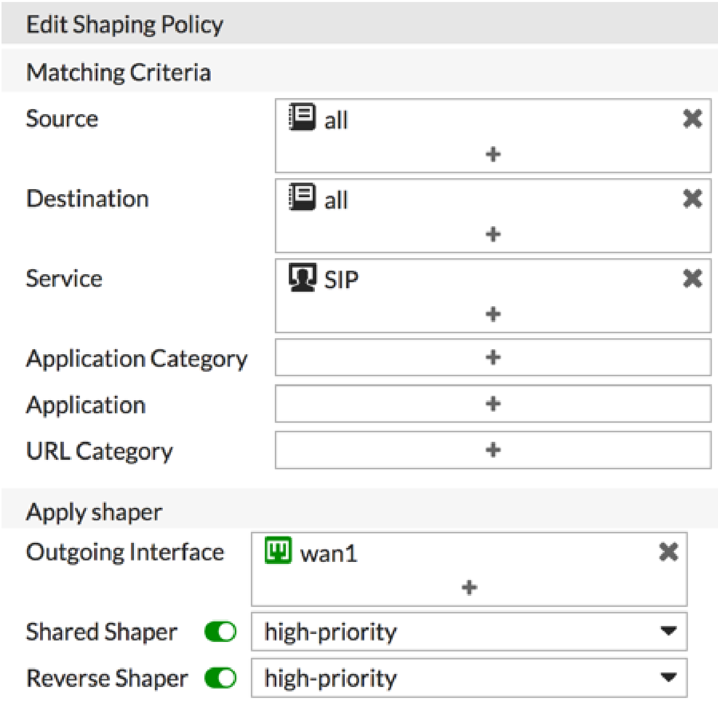
1. Go to *Policy & Objects* > *IPv4 Policy* and edit your Internet access policy.
   Under *Security Profiles*, enable *VoIP*.
   Under *Logging Options*, set *Log Allowed Traffic* to *All Sessions* so that you can test the results later.
   Note your *Source*, *Destination*, and *Outgoing Interface* for the next step.



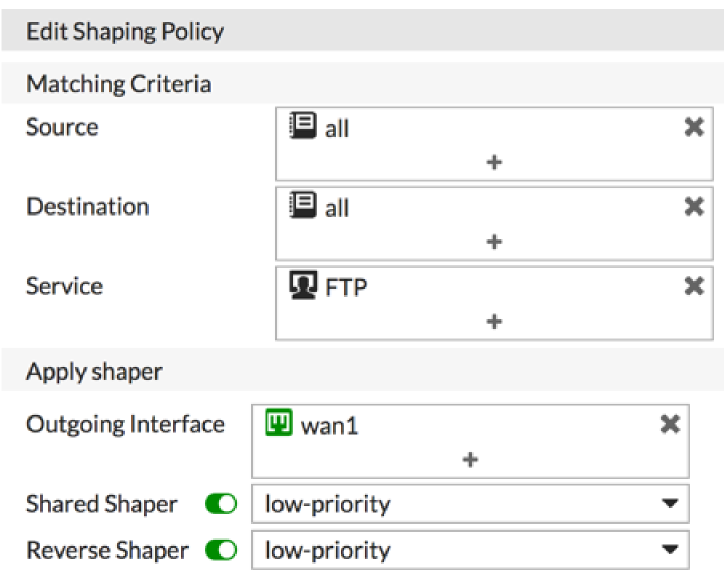
Creating three traffic shaping policies

1. Go to *Policy & Objects* > *Traffic Shaping Policy* and create a high-priority traffic shaping policy for SIP traffic.
   Set the *Matching Criteria* to the same settings as the Internet access policy you would like to apply traffic shaping to.

Enable *Shared Shaper* and *Reverse Shaper* and set both to *high-priority*.

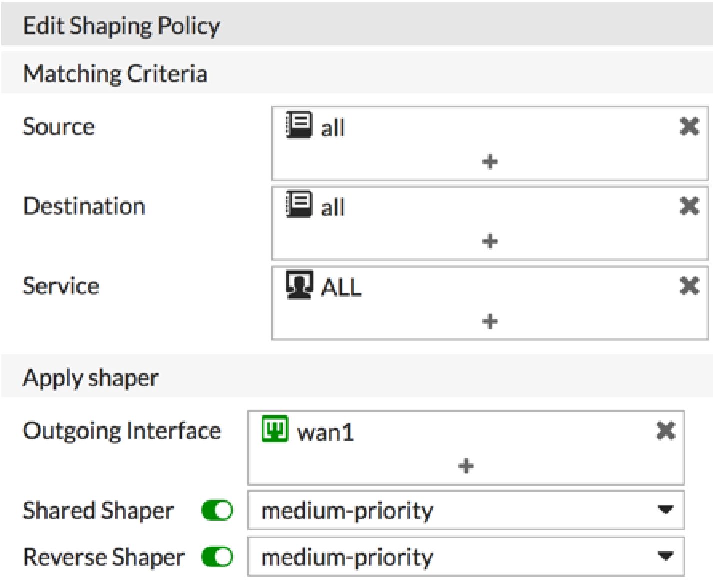


2. Create a low-priority traffic shaping policy for FTP traffic.
   Set *Service* to *FTP*.
   Enable *Shared Shaper* and *Reverse Shaper* and set both to *low-priority*.



3. Create a medium-priority traffic shaping policy for daily traffic.
   Set *Service* to *ALL*.

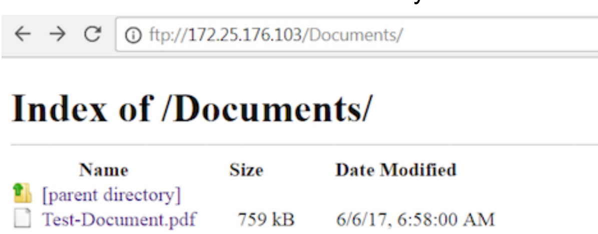
Enable *Shared Shaper* and *Reverse Shaper* and set both to *medium-priority*.



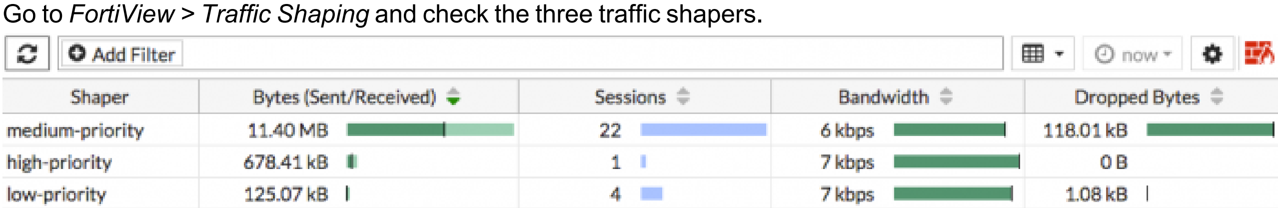
4. Arrange the policies in the following order:
   a. High-priority (SIP/VoIP traffic).
   b. Low-priority (FTP traffic).
   c. Medium-priority (day-to-day traffic).

Results

1. Browse the Internet using a PC on your internal network to generate daily web traffic and also generate FTP traffic. The FTP sessions should occur slowly.



2. Generate SIP traffic.
3. Go to *FortiView* > *Traffic Shaping* and check the three traffic shapers.

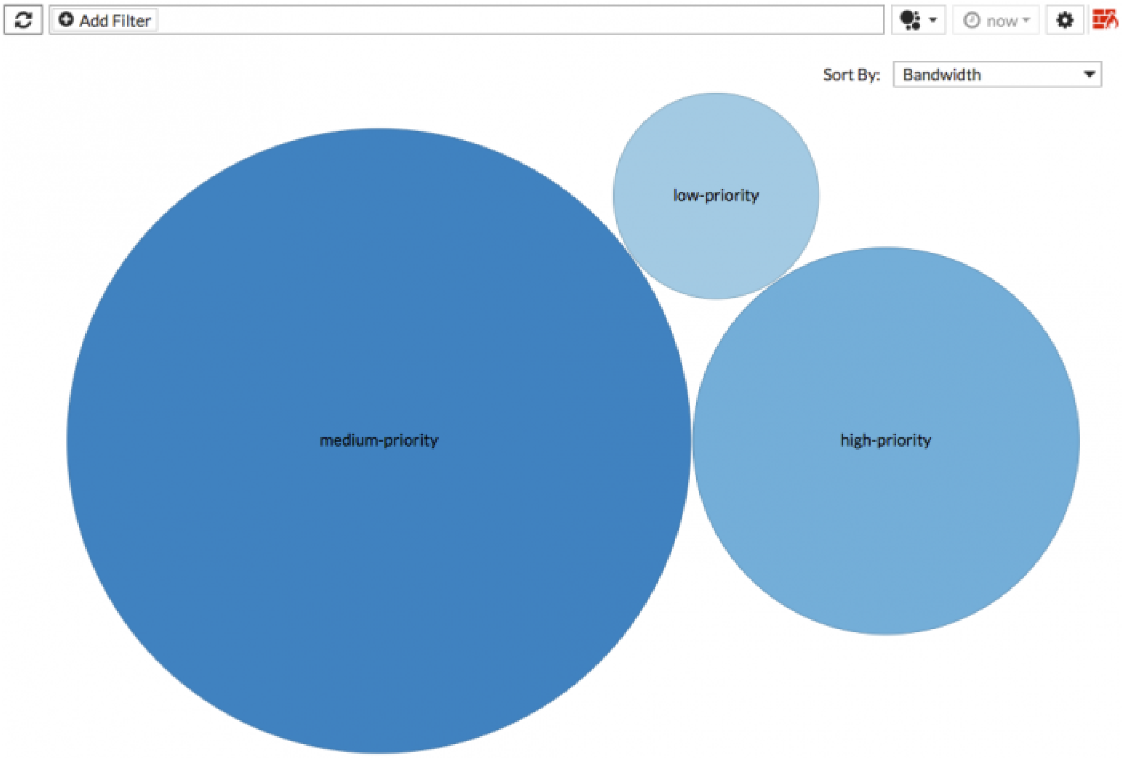


If the standard traffic volume is high enough, it will top out at the maximum bandwidth defined by each shaper.

The high-priority VoIP (SIP) policy should show no dropped bytes. Either of the other two policies might show dropped bytes if the set bandwidth is maxed out.

This allows normal voice quality on VoIP calls even with daily traffic and FTP downloads.

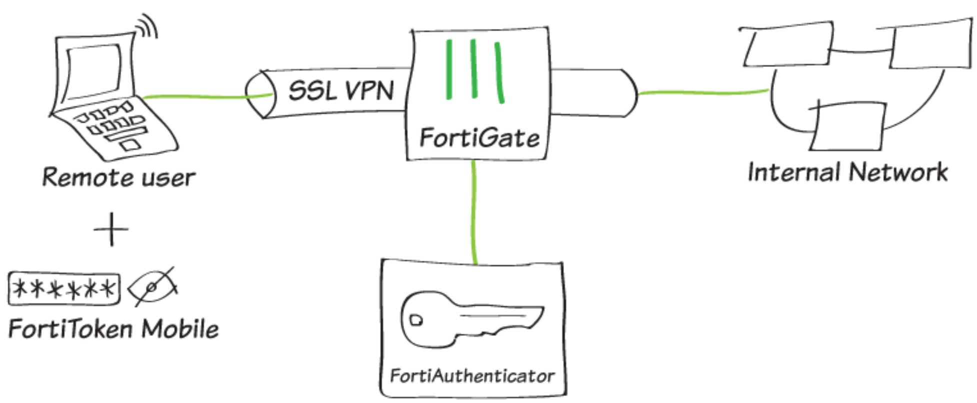
4. Select the graph icon to switch to bubble graph view.
   Sort by *Bandwidth* and hover over a shaper to view details.
   Double-click to drill down for more details.



Authentication

This section contains information about authenticating users and devices.

FortiToken Mobile Push for SSL VPN



This example shows how to set up FortiAuthenticator to function as a RADIUS server to authenticate SSL VPN users using FortiToken Mobile Push two-factor authentication. With push notifications, you can easily accept or deny the authentication request.

This example includes the following activities:

- Creating a user account on the FortiAuthenticator.
- Assigning a FortiToken Mobile license to the user.
- Creating the RADIUS client (FortiGate) on the FortiAuthenticator.
- Enabling FortiToken Mobile Push notifications.
- Connect the FortiGate to the RADIUS server (FortiAuthenticator).
- Creating an SSL VPN on the FortiGate to allow internal access for remote users.

This example uses the following names and IP addresses:

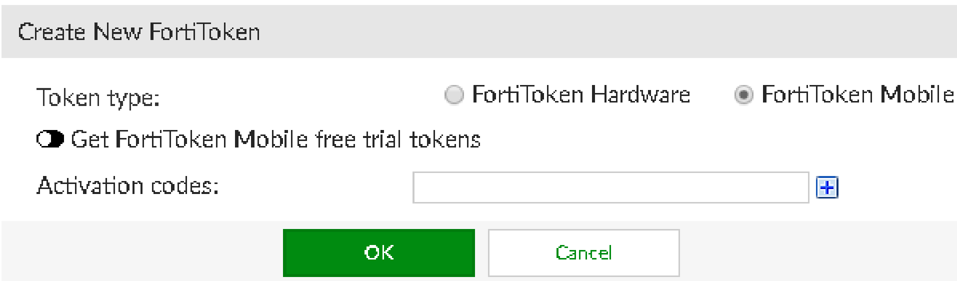
- Username: *gthreepwood*
- User group: *RemoteFTMGroup*
- RADIUS server: *OfficeRADIUS*
- RADIUS client: *OfficeServer*
- SSL VPN user group: *SSLVPNGroup*
- FortiAuthenticator: *172.25.176.141*
- FortiGate: *172.25.176.92*

For this example, you must have already installed the FortiToken Mobile application on your smartphone. For details, see:

- FortiToken Mobile for Android
- FortiToken Mobile for iOS

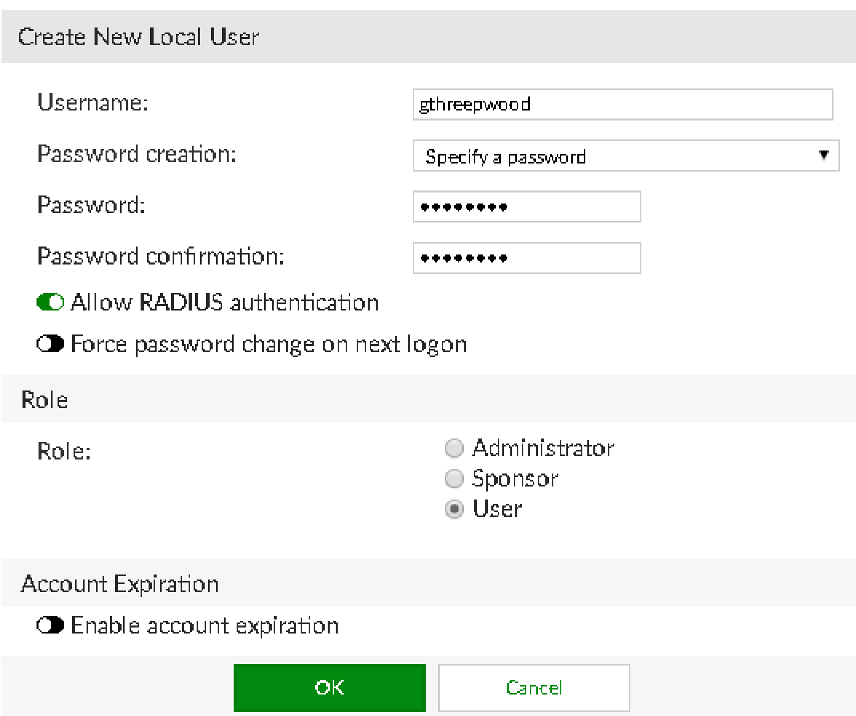
Adding a FortiToken to the FortiAuthenticator

1. On the FortiAuthenticator, go to *Authentication* > *User Management* > *FortiTokens*, and select *Create New*.
2. Set *Token type* to *FortiToken Mobile* and enter the FortiToken *Activation codes*.

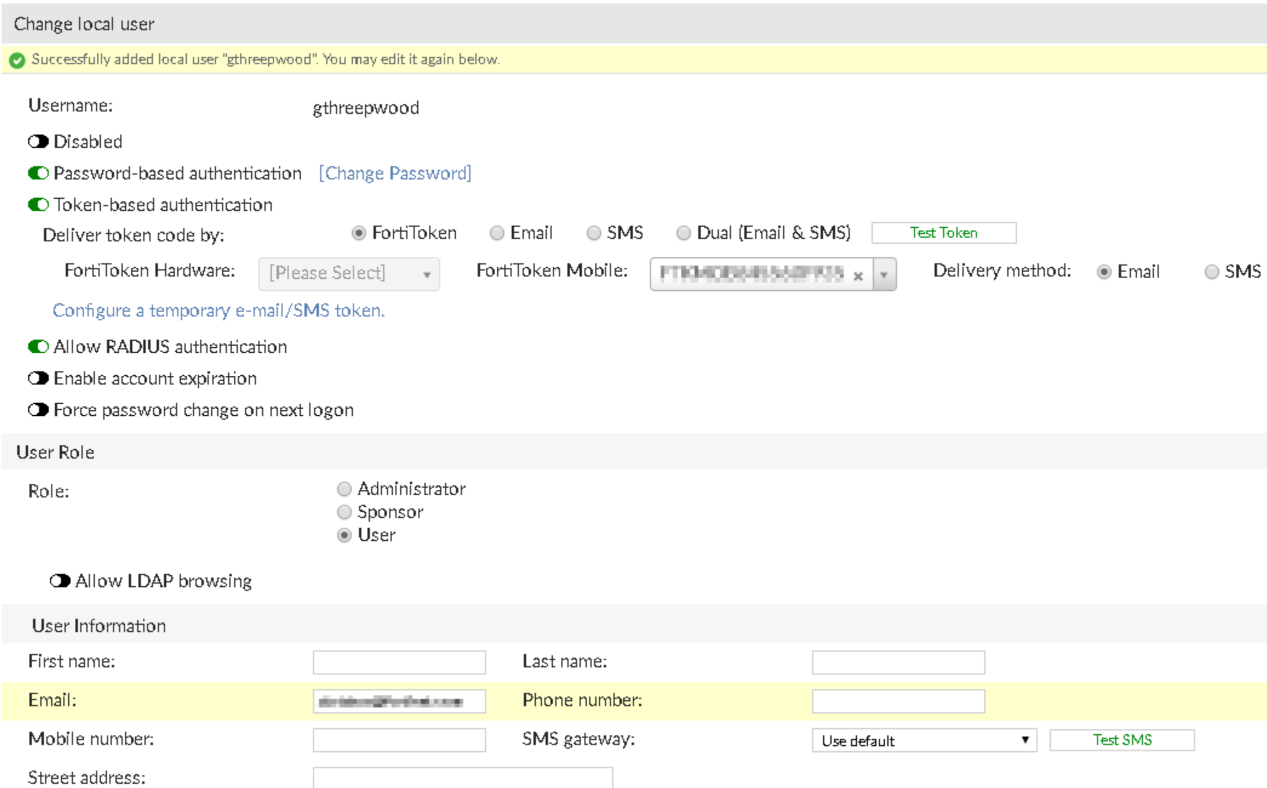


Adding the user to the FortiAuthenticator

1. On the FortiAuthenticator, go to *Authentication* > *User Management* > *Local Users* and select *Create New*.
Enter the *Username* (*gthreepwood*) and password.
Enable *Allow RADIUS authentication*, and click *OK* to access additional settings.

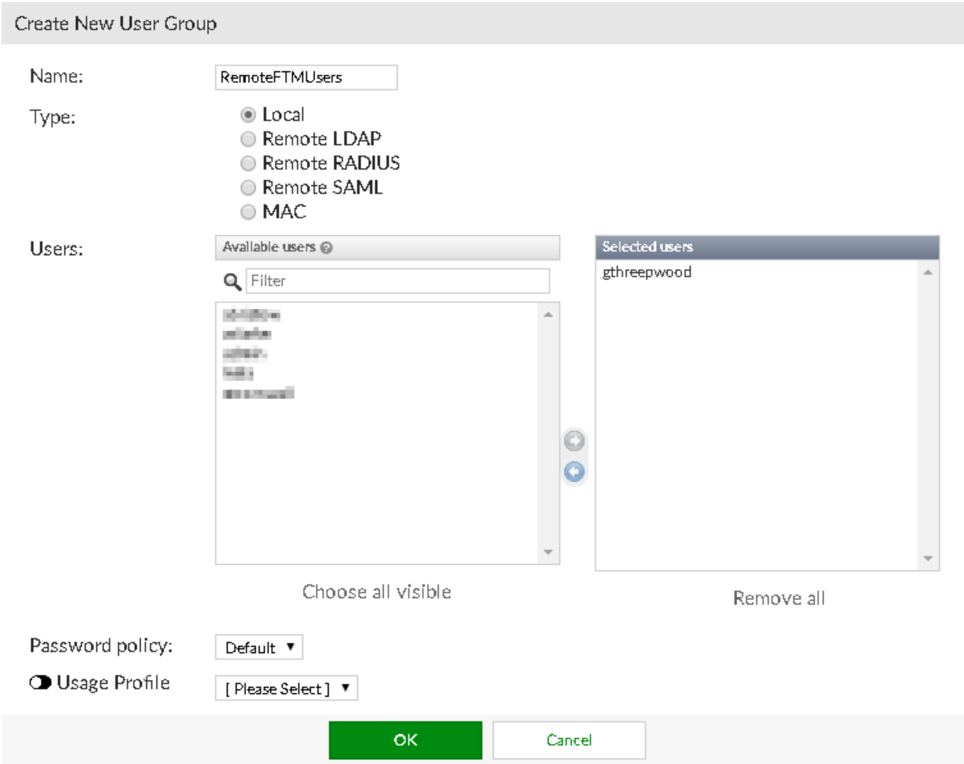


2. Enable *Token-based authentication* and select *Deliver token code by FortiToken*.
   For *FortiToken Mobile*, select the FortiToken you added.
   Set *Delivery method* to *Email* and, in the *User Information* section, enter the email address.

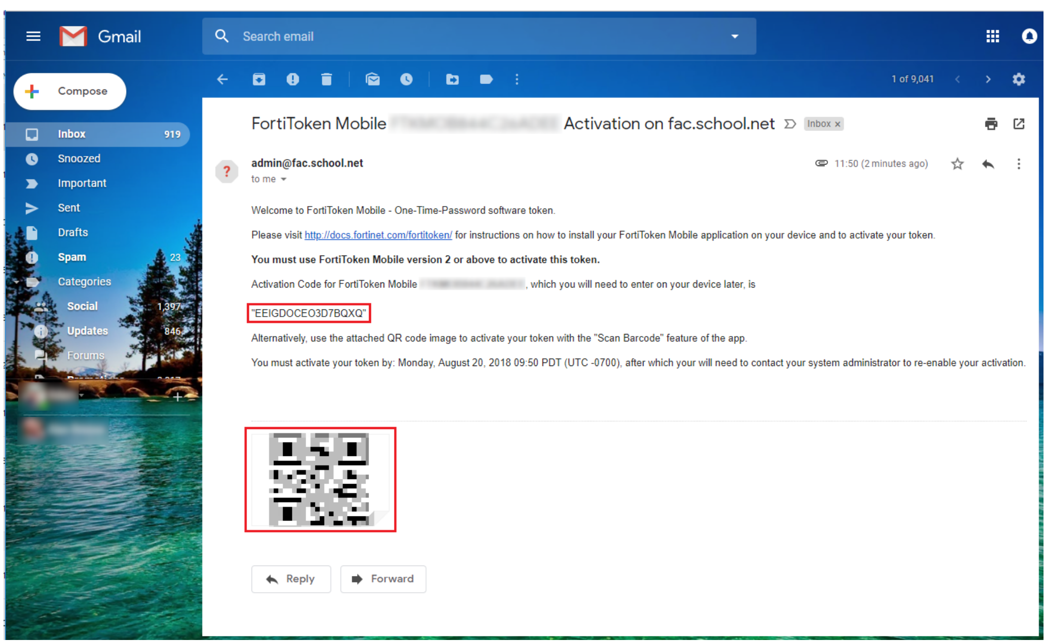


3. Go to *Authentication > User Management > User Groups* and select *Create New*.
   Enter the *Name* (*RemoteFTMUsers*).

Add *gthreepwood* to the group by moving the user from *Available users* to *Selected users*.



4. The FortiAuthenticator sends the FortiToken Mobile activation to the user's email address.
Activate the FortiToken Mobile in the FortiToken Mobile application by entering the activation code or scanning the QR code.

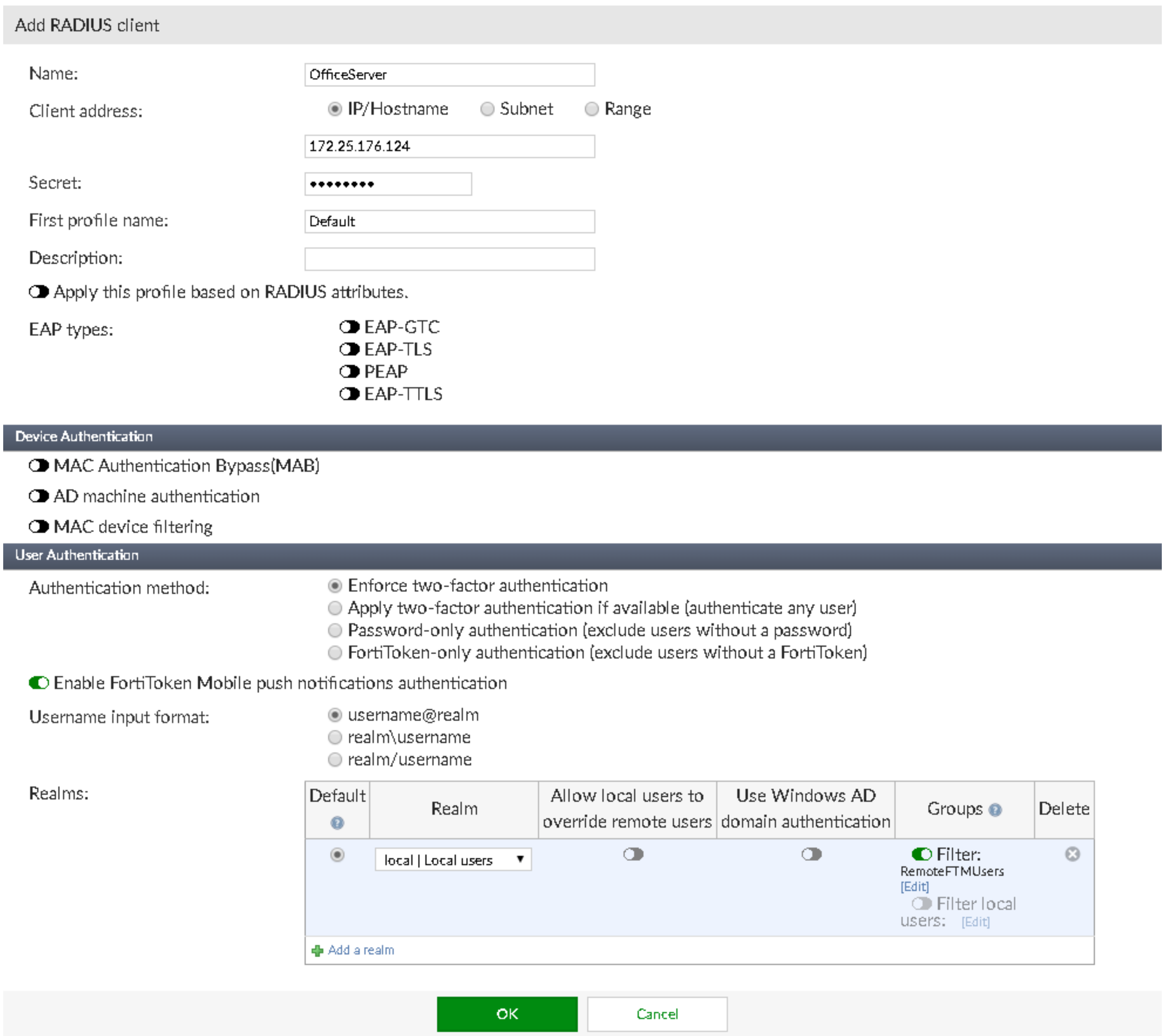


For more information, see the FortiToken Mobile user instructions.

Creating the RADIUS client on the FortiAuthenticator

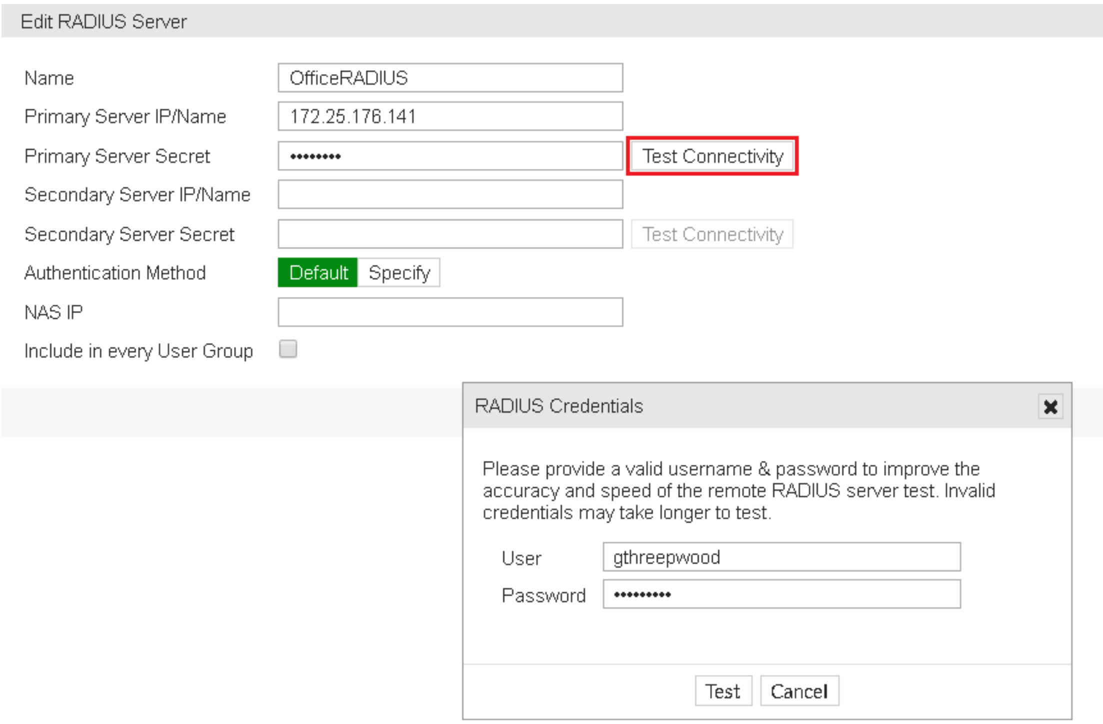
1. On the FortiAuthenticator, go to *Authentication > RADIUS Service > Clients*, and select *Create New* to add the FortiGate as a RADIUS client.
2. Enter a *Name* (*OfficeServer*), the IP address of the FortiGate, and set a *Secret*.
   The secret is a pre-shared password that FortiGate uses to authenticate to the FortiAuthenticator.
3. Set *Authentication method* to *Enforce two-factor authentication* and turn on *Enable FortiToken Mobile push notifications authentication*.
4. Set *Realms* to *local | Local users*, and add *RemoteFTMUsers* to the *Groups* filter.

The *Username input format* is the format that users must use to enter their username in the web portal. This includes the username and realm. In this example, the full username for gthreepwood is *gthreepwood@local*.

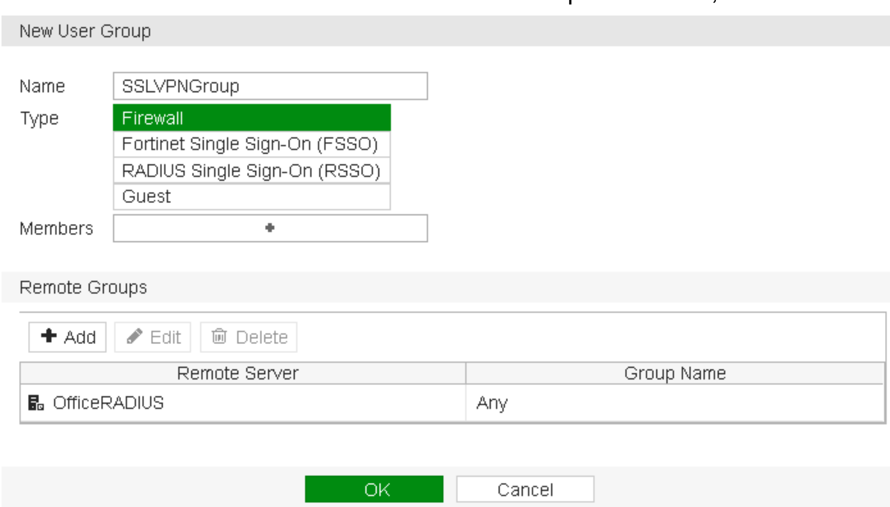


Connecting the FortiGate to the RADIUS server

1. On the FortiGate, go to *User & Device* > *RADIUS Servers*, and select *Create New* to connect to the RADIUS server (FortiAuthenticator).
   Enter a *Name* (*OfficeRADIUS*), the IP address of the FortiAuthenticator, and enter the *Secret* created before.
   Select *Test Connectivity* to be sure you can connect to the RADIUS server. Enter the credentials for *gthreepwood*.



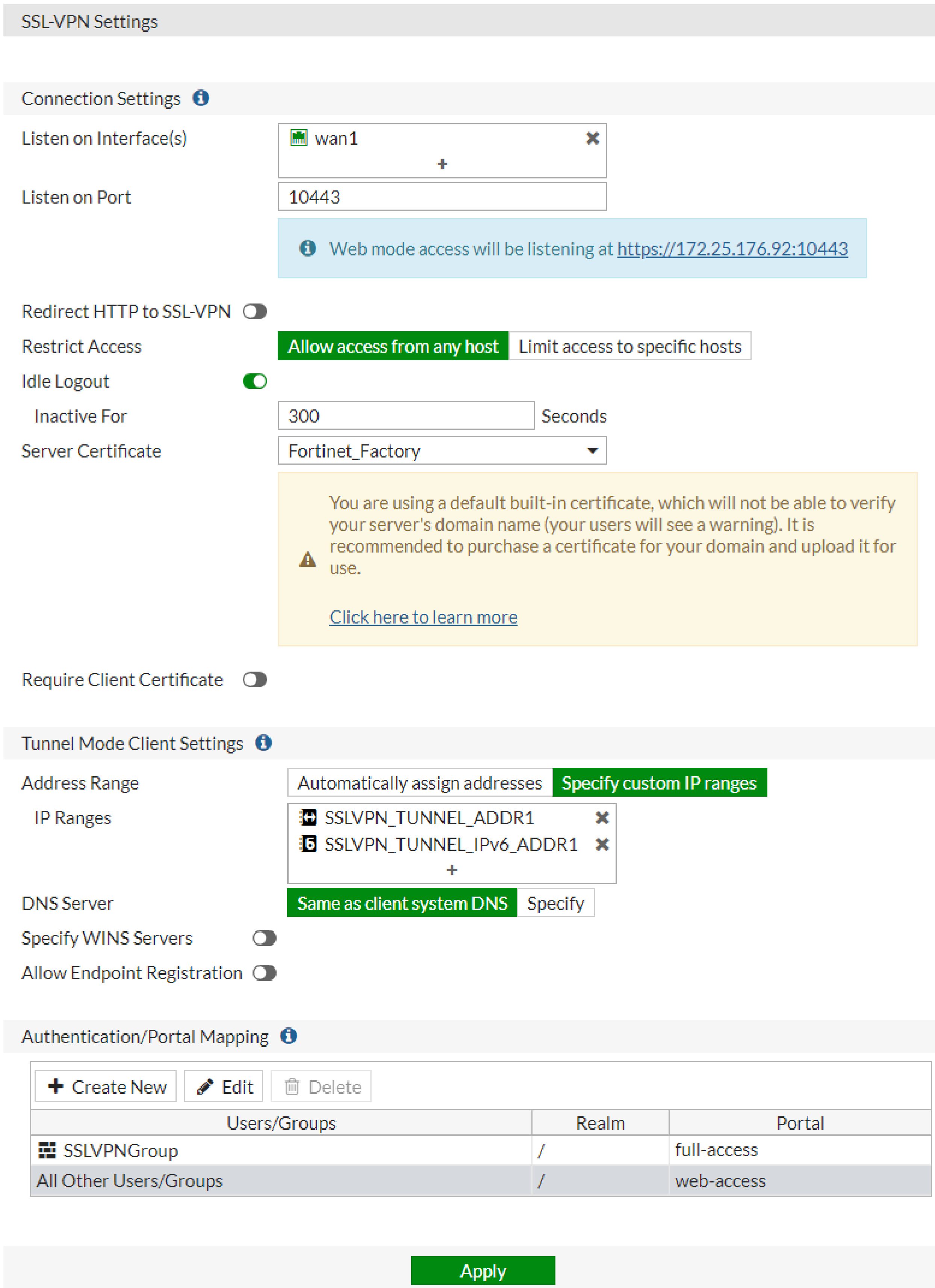
2. Go to *User & Device* > *User Groups*, and select *Create New* to map authenticated remote users to a user group on the FortiGate.
   Enter a *Name* (*SSLVPNGroup*) and select *Add* under *Remote Groups*.
   Select *OfficeRADIUS* under the *Remote Server* dropdown menu, and leave the *Groups* field blank.



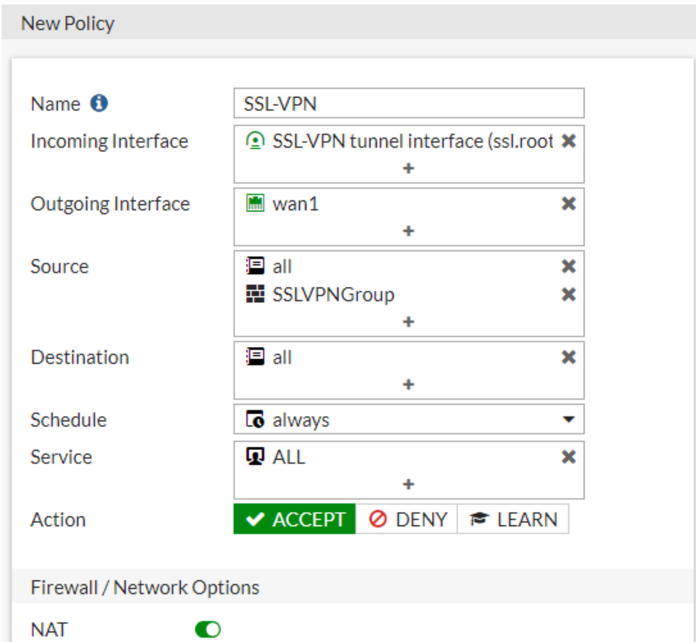
Configuring the SSL VPN

1. On the FortiGate, go to *VPN > SSL-VPN Portals*, and edit the *full-access* portal.
   Turn off *Enable Split Tunneling* so that it is disabled.

2. Go to *VPN > SSL-VPN Settings*.
   Under *Connection Settings*, set *Listen on Interface(s)* to *wan1* and *Listen on Port* to *10443*.
   Under *Tunnel Mode Client Settings*, select *Specify custom IP ranges* and ensure *IP Ranges* is set to the default *SSLVPN_TUNNEL_IPv6_ADDR1*.
   Under *Authentication/Portal Mapping*, select *Create New*.
   Set the *SSLVPNGroup* user group to the *full-access* portal, and assign *All Other Users/Groups* to *web-access*. This gives all other users access to the web portal only.

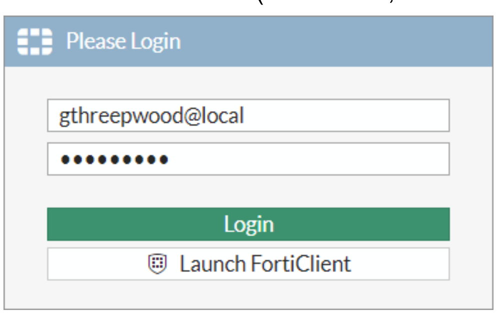

SSL-VPN Settings
Connection Settings
Listen on Interface(s)
wan1
Listen on Port
10443
Web mode access will be listening at https://172.25.176.92:10443
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
300
Seconds
Server Certificate
Fortinet_Factory
You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use.
Click here to learn more
Require Client Certificate
Tunnel Mode Client Settings
Address Range
Automatically assign addresses
Specify custom IP ranges
IP Ranges
SSLVPN_TUNNEL_ADDR1
SSLVPN_TUNNEL_IPv6_ADDR1
DNS Server
Same as client system DNS
Specify
Specify WINS Servers
Allow Endpoint Registration
Authentication/Portal Mapping
Create New
Edit
Delete
Users/Groups
Realm
Portal
SSLVPNGroup
/
full-access
All Other Users/Groups
/
web-access
Apply

3. Go to *Policy & Objects* > *IPv4 Policy* and create a new SSL VPN policy.
Set *Incoming Interface* to the *SSL-VPN tunnel interface*.
Set *Outgoing Interface* to the Internet-facing interface (in this case, *wan1*).
Set *Source* to the *SSLVPNGroup* user group and the *all* address.
Set *Destination* to *all*, *Schedule* to *always*, *Service* to *ALL*.
Enable *NAT*.

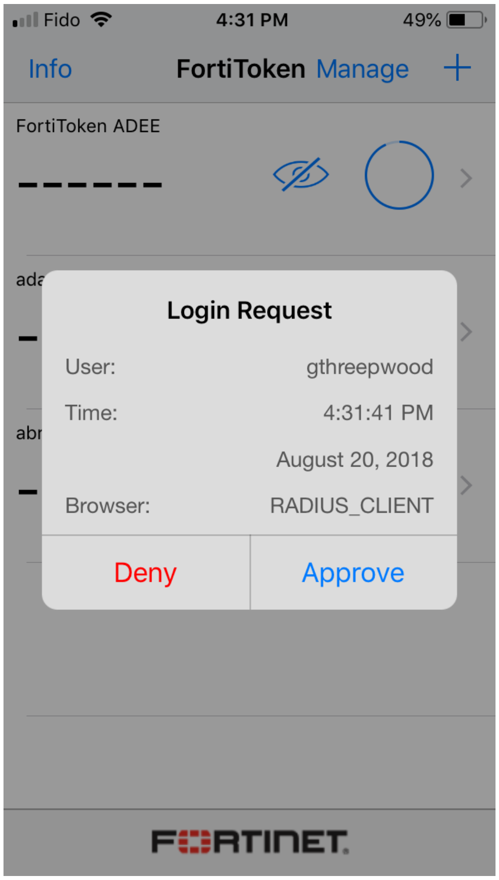


Results

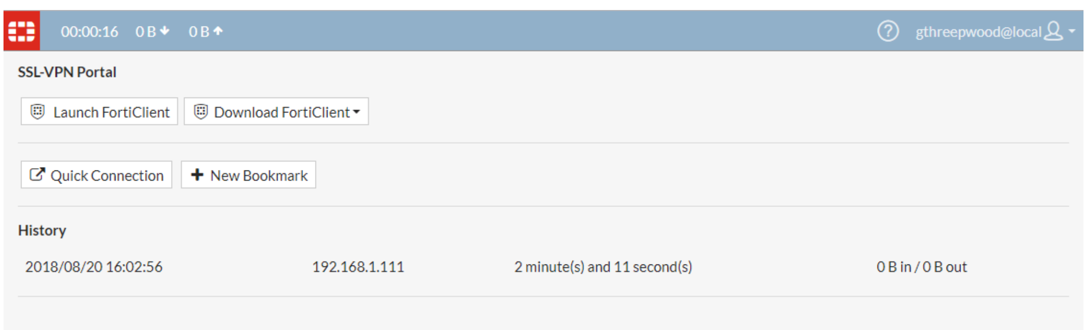
1. From a remote device, open a web browser and go to the SSL VPN web portal *(https://<fortigate-ip>:10443)*.
2. Enter *gthreepwood*'s credentials and select *Login*.
Use the correct format (in this case, username@realm) as configured on the FortiAuthenticator.



3. When the FortiAuthenticator pushes a login request notification through the FortiToken Mobile application, select *Approve*.



When you approve the authentication, *gthreepwood* is logged into the SSL VPN portal.

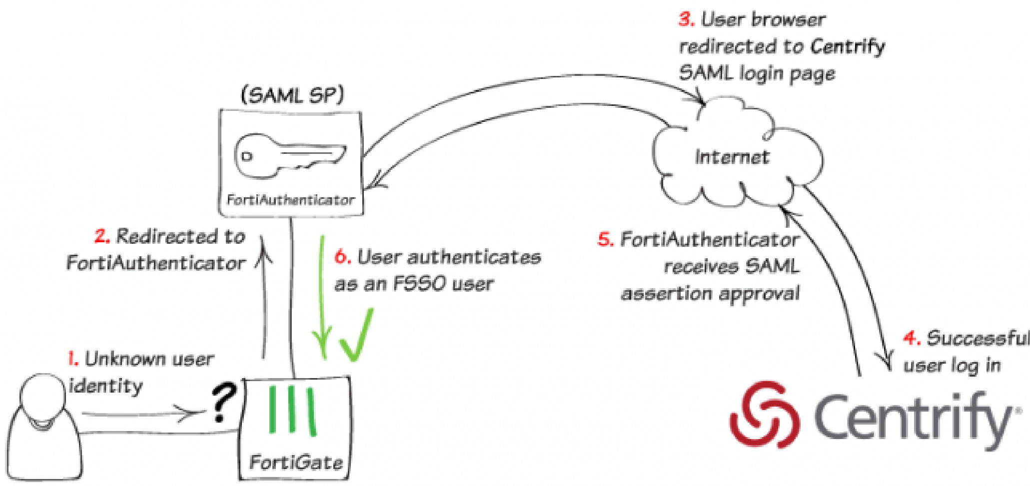


4. On the FortiGate, go to *Monitor* > *SSL-VPN Monitor* to confirm the user's connection.


Refresh

Username	Last Login	Remote Host	Active Connections
gthreepwood@local	2018/08/20 16:32:02	192.168.1.111	

SAML 2.0 FSSO with FortiAuthenticator and Centrify



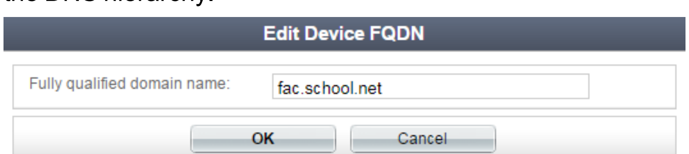
This example shows you how to provide a Security Assertion Markup Language (SAML) FSSO cloud authentication solution using FortiAuthenticator with Centrify Identity Service, a cloud-based or on-premises service. This solution can mitigate one of the leading points of attack in data breaches: compromised credentials. FortiAuthenticator acts as the service provider (SP) and Centrify acts as the identity provider (IdP).

Centrify Identity Service improves end-user productivity and secures access to cloud, mobile, and on-premise apps via SSO, user provisioning, and multi-factor authentication.

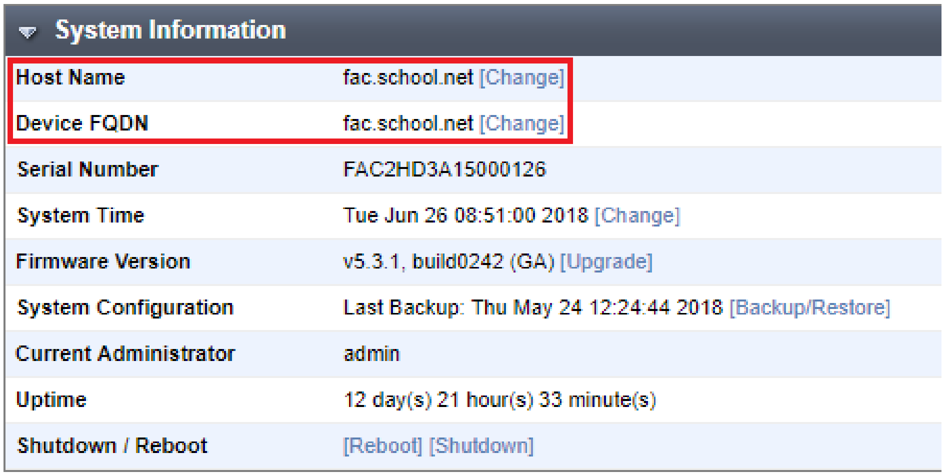
Before you begin:

- Create a Centrify tenant admin account.
- On the FortiAuthenticator, create two user groups (one local user group and one SSO user group). These groups must have identical names, in this example, *saml_users*.

Configuring DNS and FortiAuthenticator's FQDN

1. On the FortiAuthenticator, go to *System* > *Dashboard* > *Status*.
   In the *System Information* widget, select *Change* beside *Device FQDN*.
   Enter a domain name (in this example, *fac.school.net*). This helps identify where the FortiAuthenticator is located in the DNS hierarchy.
   

2. Enter the same name for the *Host Name*. This allows you to add the unit to the FortiGate’s DNS list so that the local DNS lookup of this FQDN can be resolved.

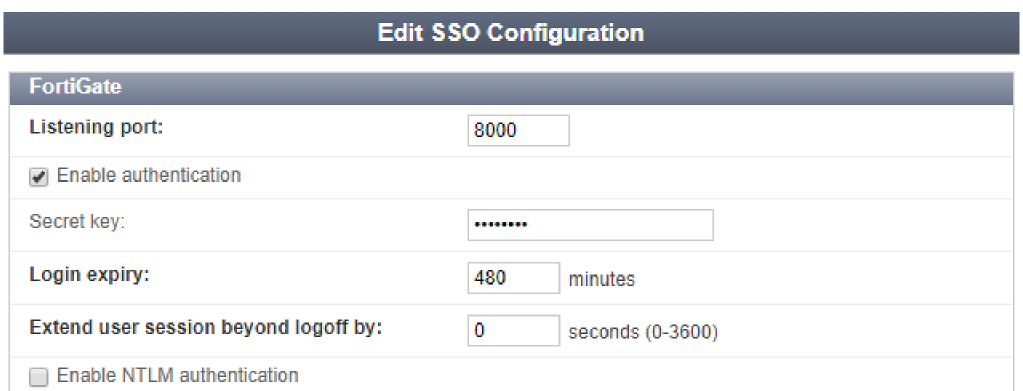


3. On the FortiGate, open the *CLI Console* and enter the following commands using the FortiAuthenticator's host name and Internet-facing IP address:

```
config system dns-database
   edit school.net
      config dns-entry
         edit 1
            set hostname fac.school.net
            set ip 172.25.176.141
         next
      end
      set domain school.net
   next
end
```

Enabling FSSO and SAML on the FortiAuthenticator

1. On the FortiAuthenticator, go to *Fortinet SSO Methods > SSO > General* and set FortiGate SSO options. Make sure to *Enable authentication*.
   Enter a *Secret key* and select *OK* to apply your changes. This *Secret key* is used on the FortiGate to add the FortiAuthenticator as the FSSO server.

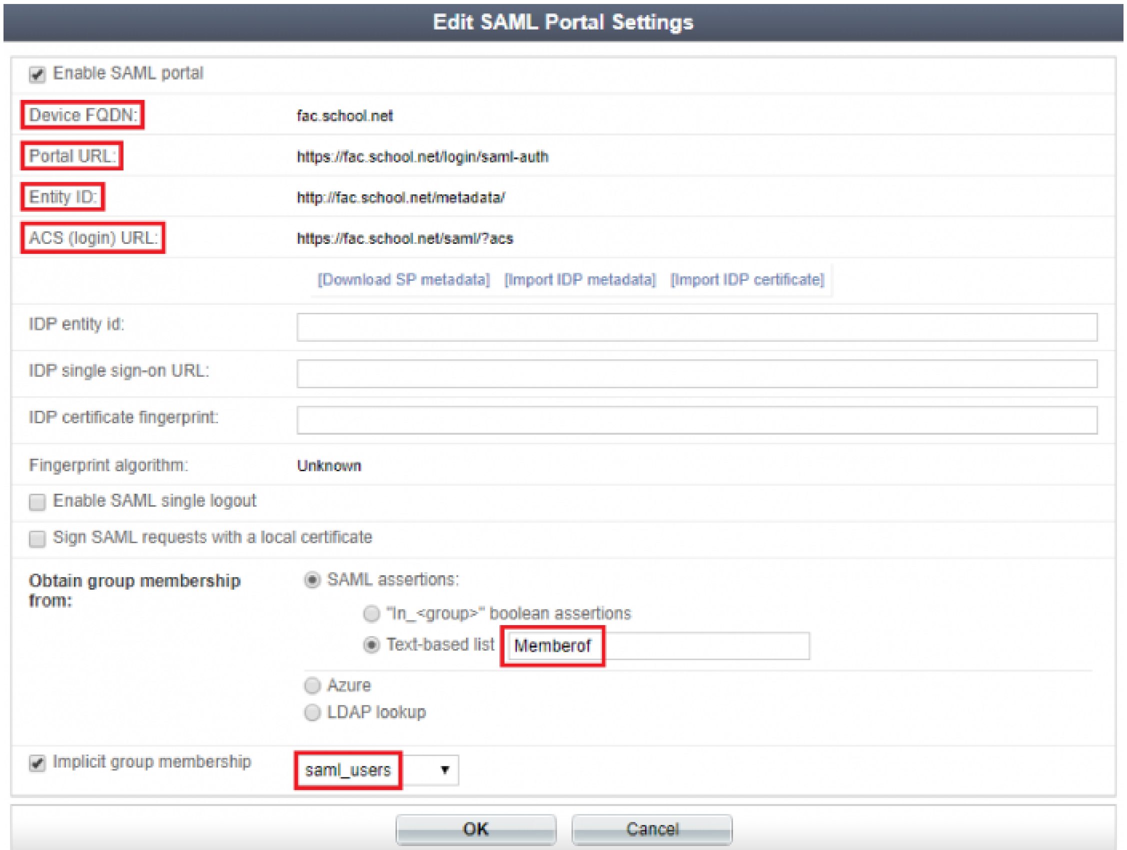


2. Go to *Fortinet SSO Methods > SSO > SAML Authentication* and select *Enable SAML portal*. All necessary URLs are automatically generated:
   - *Portal URL*: captive portal URL for the FortiGate and user.
   - *Entity ID*: used in the Centrify SAML IdP application setup.

- *ACS (login) URL*: assertion POST URL used by the SAML IdP.

Under *SAML assertions*, enable *Text-based list* and enter *Memberof*. This attribute will be configured later on the Centrify tenant to be included in the SAML response to the FortiAuthenticator.

Enable *Implicit group membership* and assign the *saml_users* group. This places SAML authenticated users into this group.

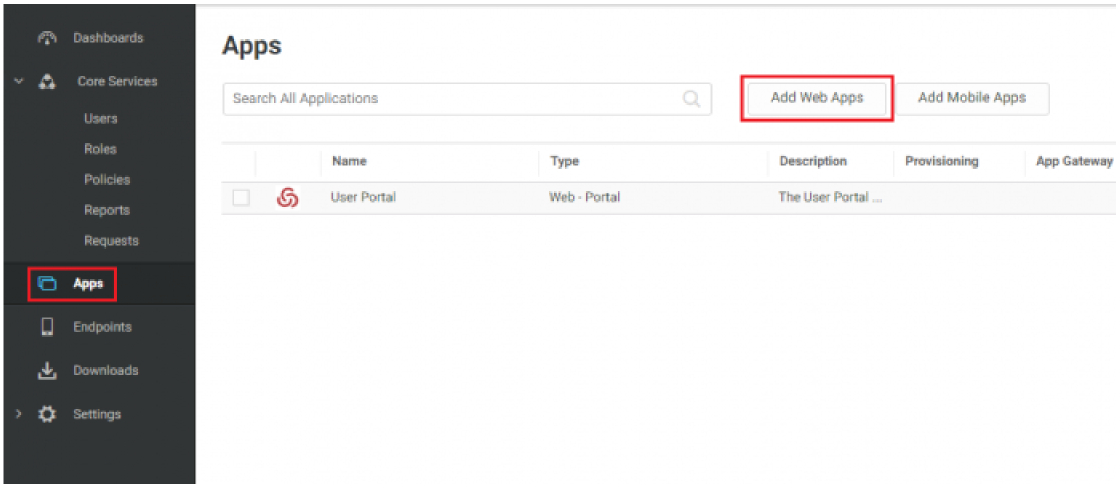


Keep this window open as these URLs are needed to configure the IdP application and for testing.

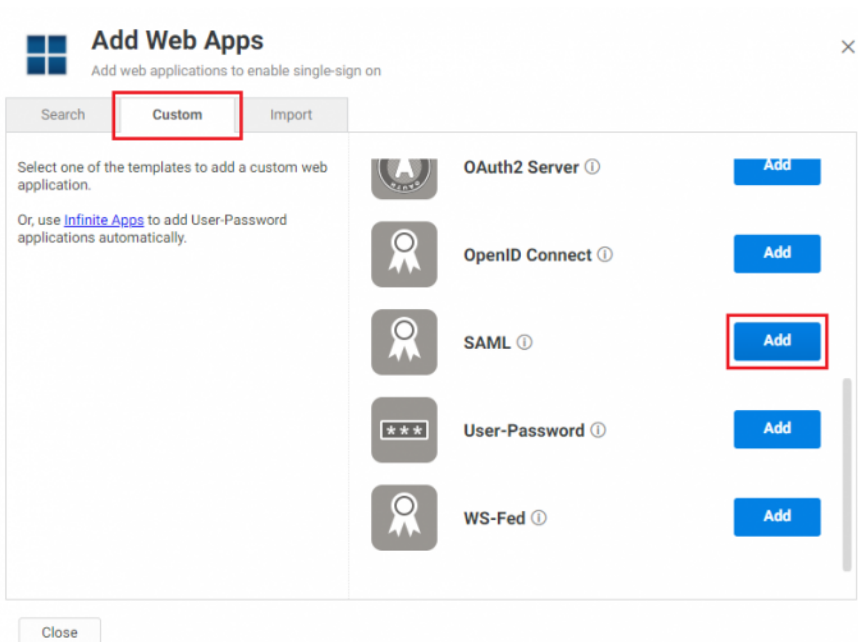
You cannot save these settings yet as the IdP information (*IDP entity id*, *IDP single sign-on URL*, and *IDP certificate fingerprint*) still needs to be entered. These fields will be filled once the IdP application configuration is complete.

Adding SAML connector to Centrify for IdP metadata

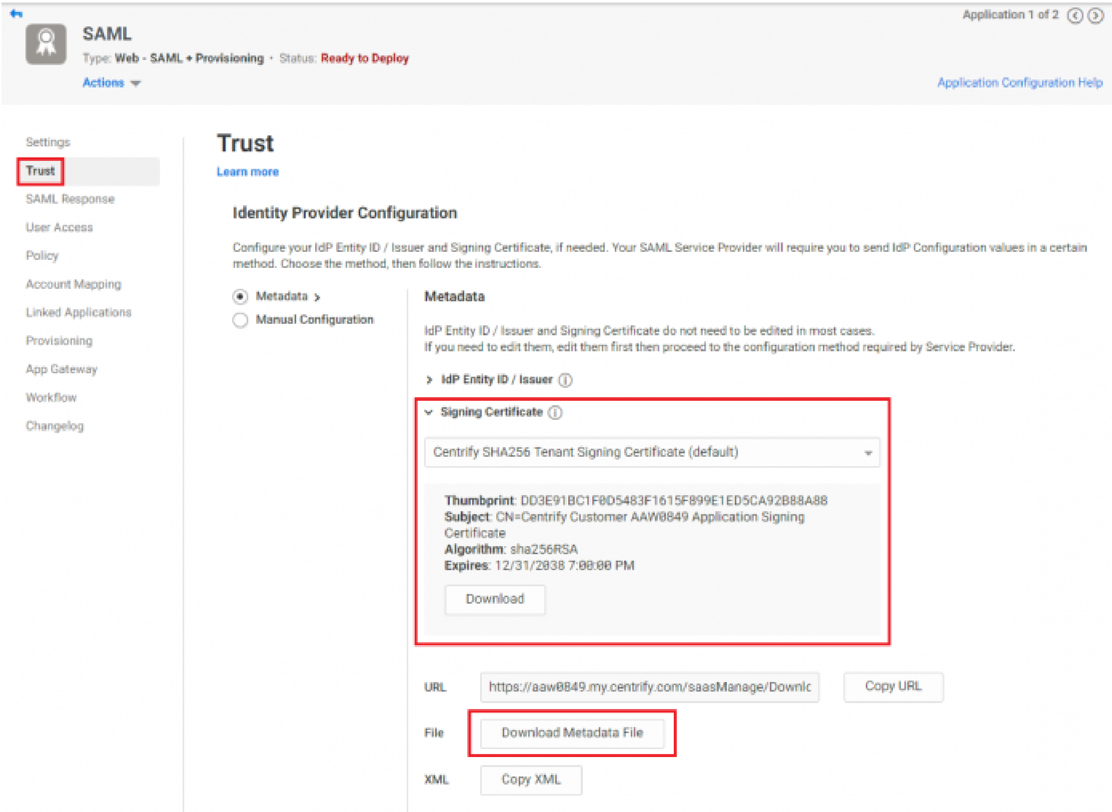
1. Login to the Centrify tenant as an administrator and go to *Apps* > *Add Web Apps*.



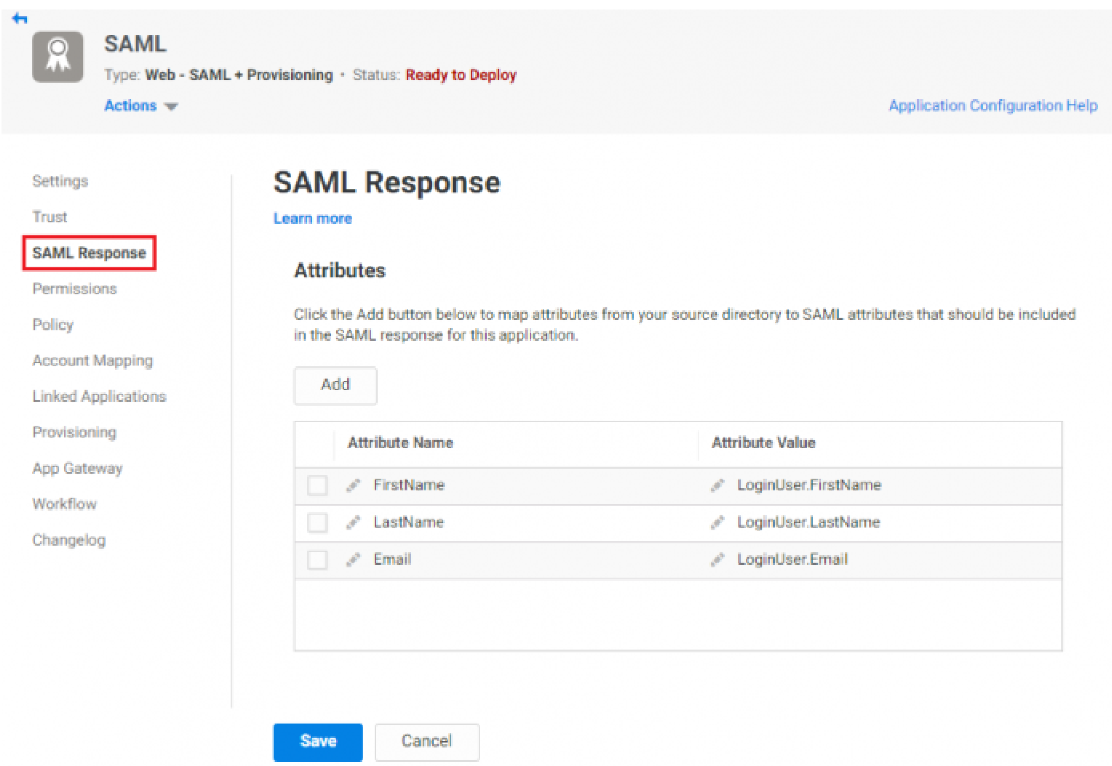
2. Under the *Custom* tab, locate *SAML* and select *Add* beside it. Select *Yes* to agree to add the SAML web app and then select *Close*.



3. The SAML configuration page opens automatically to the *Settings* tab.
Go to *Trust* to view the *Identity Provider Configuration* section.
Select the *Signing Certificate* dropdown menu and click *Download* to download both the Centrify signing certificate and the metadata file. These will be uploaded to the FortiAuthenticator.

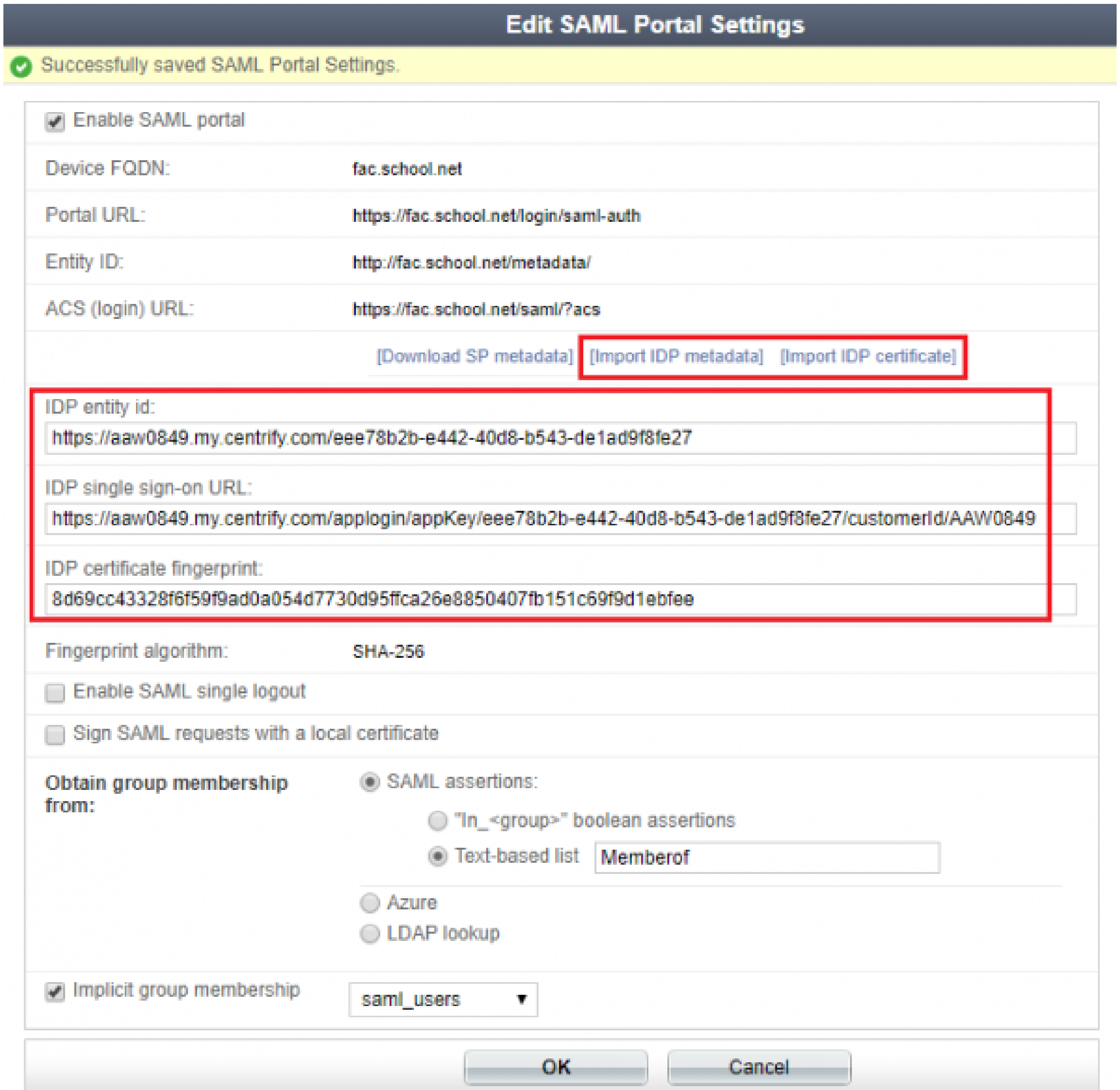


4. Go to *SAML Response* and select *Add*.
Add the *FirstName*, *LastName*, *Email*, and *Memberof* user attributes. Select *Save*.

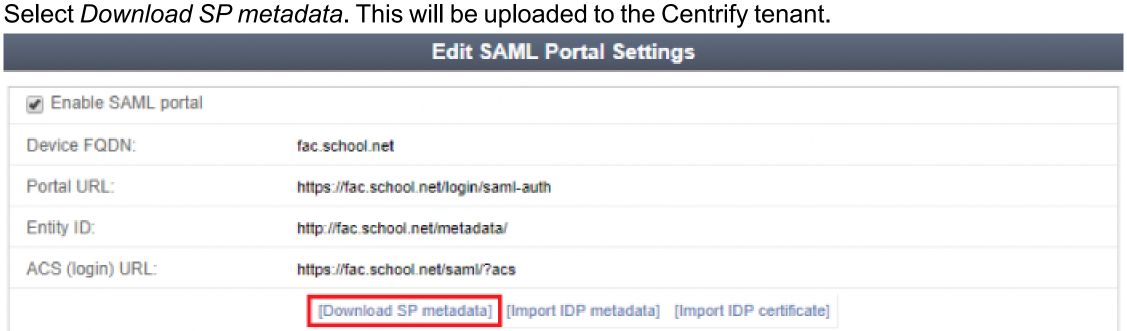


Importing the IdP certificate and metadata on the FortiAuthenticator

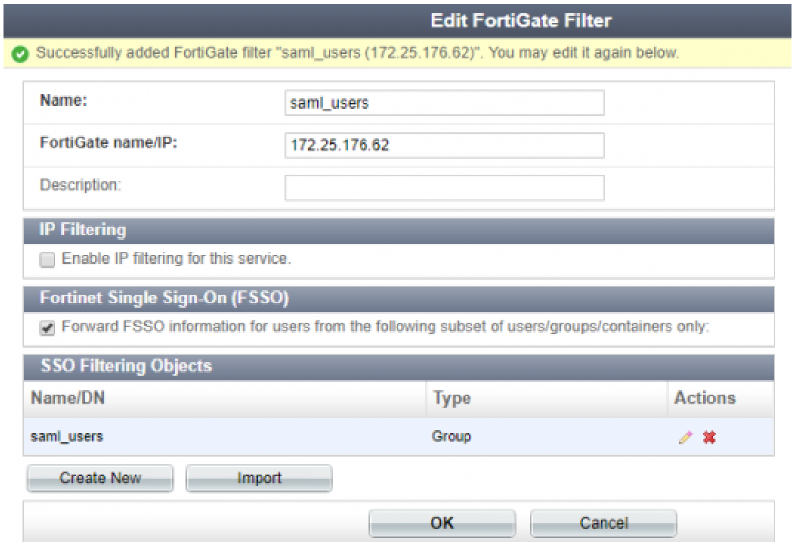
1. On the FortiAuthenticator, go to *Fortinet SSO Methods > SSO > SAML Authentication* and import the IdP metadata and certificate downloaded earlier.
   This automatically fills the IdP fields (as shown in the example). Click *OK* to save these changes.



2. Select *Download SP metadata*. This will be uploaded to the Centrify tenant.

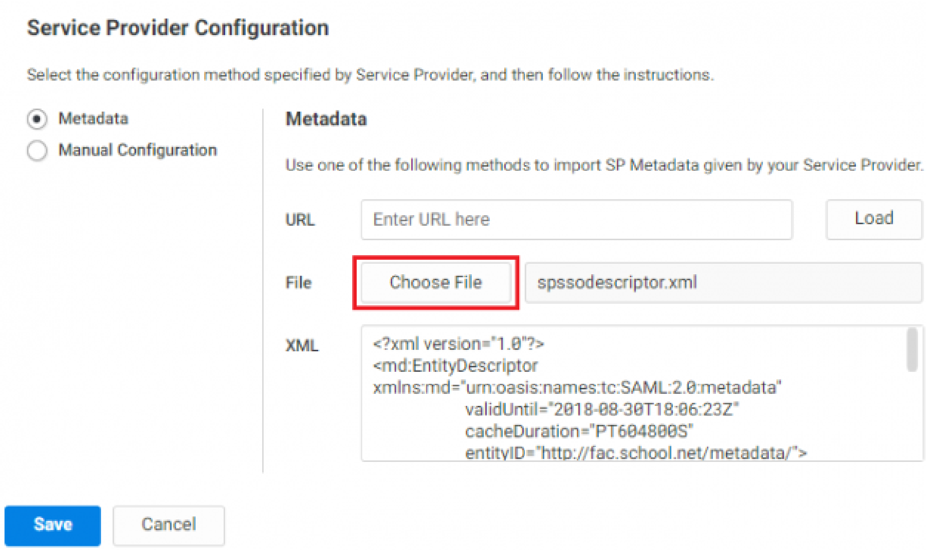


3. Go to *Fortinet SSO Methods > SSO > FortiGate Filtering* and create a new FortiGate filter.
   Enter a name and the FortiGate's wan-interface IP address, and select *OK*.
   Enable *Fortinet Single Sign-On (FSSO)*.
   Select *Create New* to create an SSO group filtering object (as shown in this example).
   The name of the filter must be the same as the group name created for SAML users (*saml_users*). The two user groups must have the exact same name or SSO information will not be pushed to the FortiGate.
   Select *OK* to apply all changes.

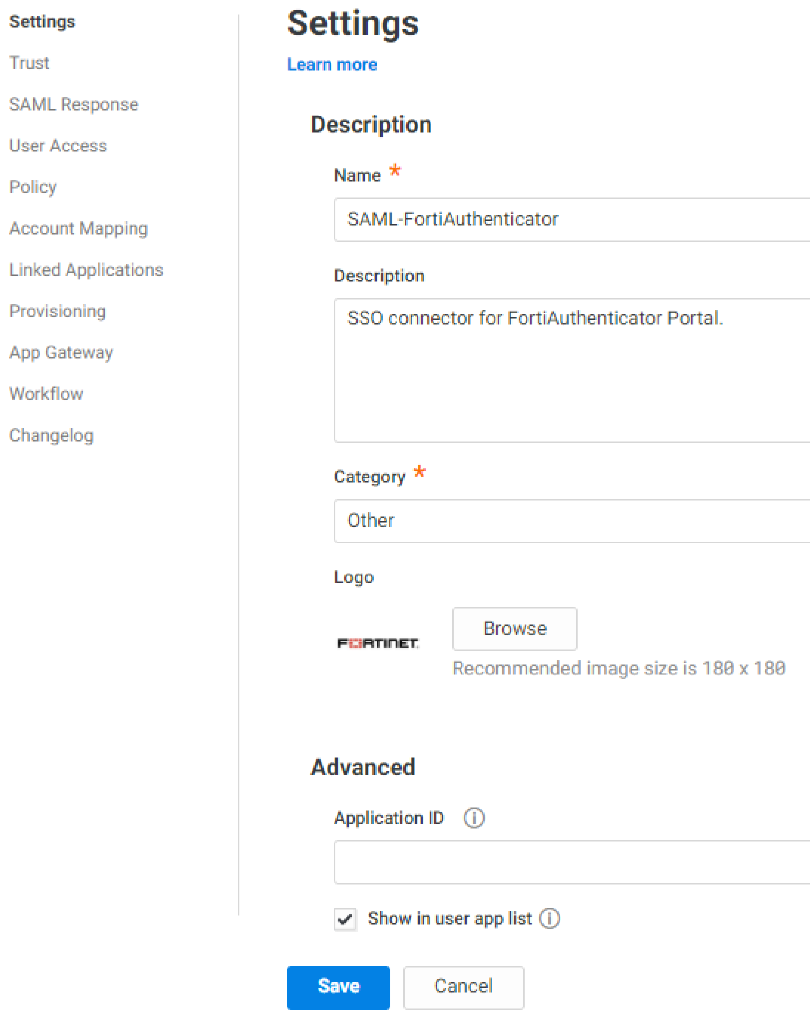


Uploading the SP metadata to the Centrify tenant

1. On the Centrify tenant *Trust* tab, go to the *Service Provider Configuration* section and select *Choose File* to upload the SP metadata from the FortiAuthenticator.
   When the upload is complete, the XML box is automatically filled in. Select *Save*.



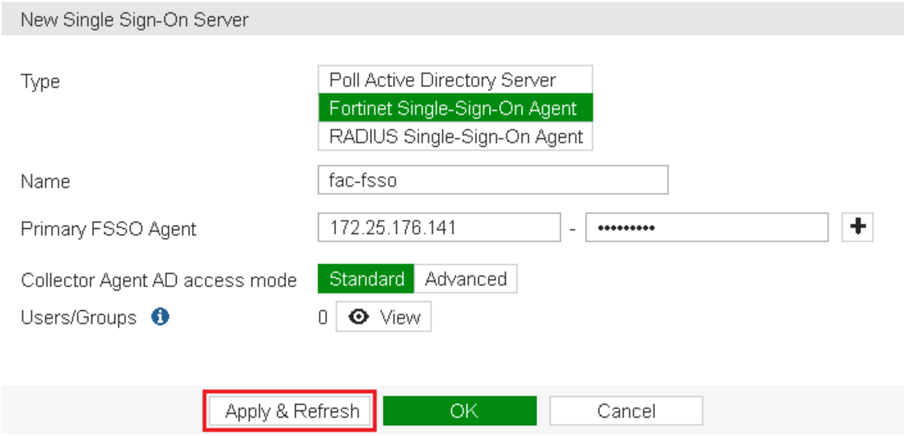
2. Optionally, go to *Settings* and enter a *Name* and *Description*, and upload a custom *Logo*. Select *Save*.



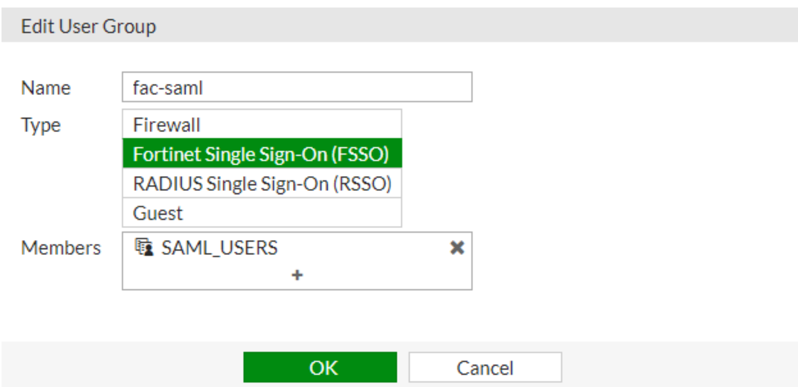
Configuring FSSO on the FortiGate

1. On the FortiGate, go to *User & Device* > *Single Sign-On* and select *Create New*.
   Set Type to *Fortinet Single-Sign-On Agent*, enter a *Name*, the FortiAuthenticator's Internet-interface IP address, and the password, which must match the secret key entered at the beginning of the FortiAuthenticator configuration process.

Select *Apply & Refresh*.

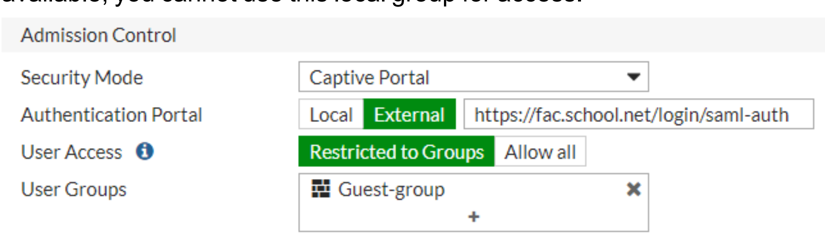


2. The SAML user group name is pushed to the FortiGate from the FortiAuthenticator and appears when you select *View*.
   You might have to wait a few minutes before the user group appears.
3. Go to *User & Device* > *User Groups* and create a new FSSO user group. Users authenticated via SAML FSSO are in this group.
   Enter a *Name*, set *Type* to *Fortinet Single Sign-On (FSSO)*, and add the FSSO group as one of the *Members*.

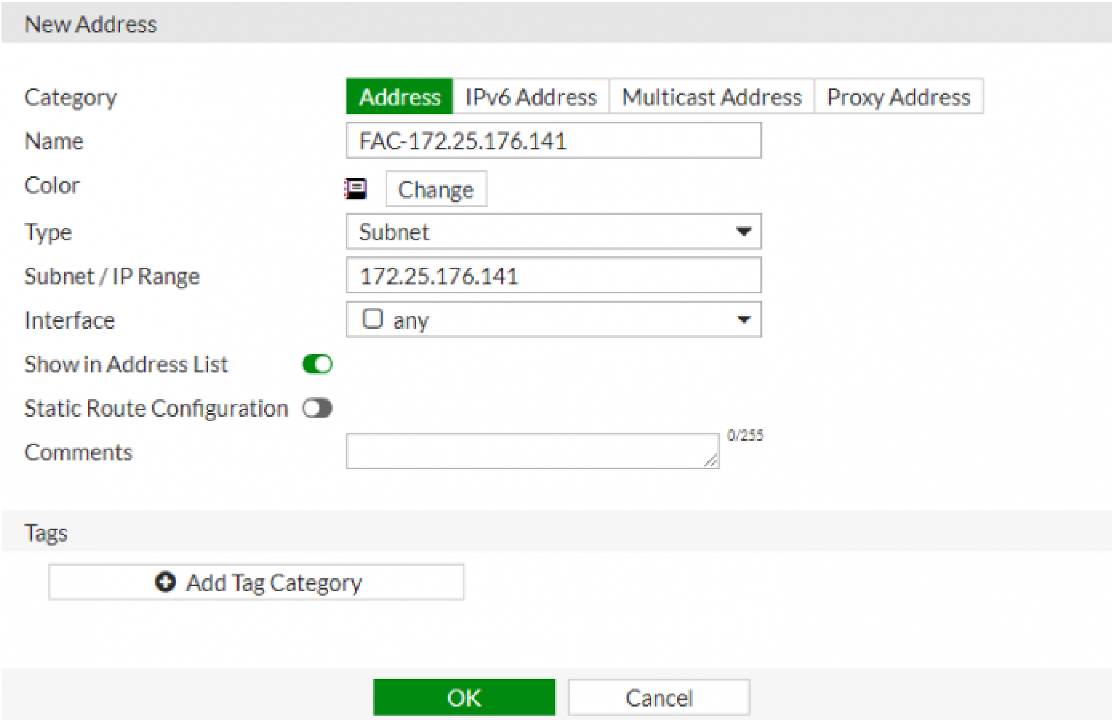


Configuring Captive Portal and security policies

1. On the FortiGate, go to *Network* > *Interfaces* and edit the internal interface.
   Under *Admission Control*, set *Security Mode* to *Captive Portal*.
   Set *Authentication Portal* to *External*, and enter the SAML authentication portal URL.
   Set *User Access* to *Restricted to Groups*, and set *User Groups* to any local group. As the FSSO group is not available, you cannot use this local group for access.

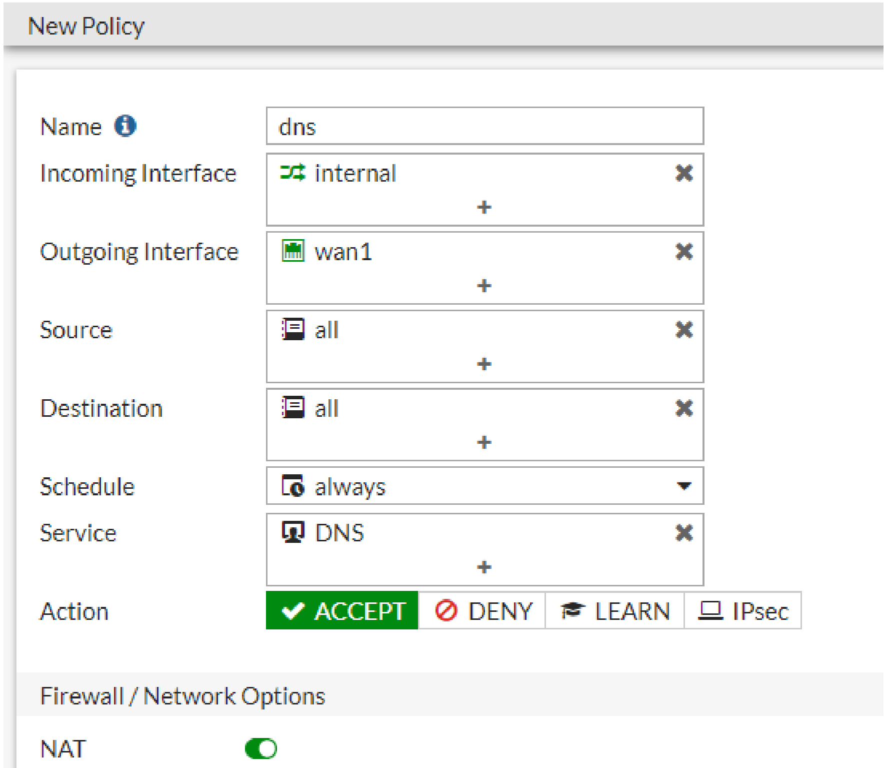


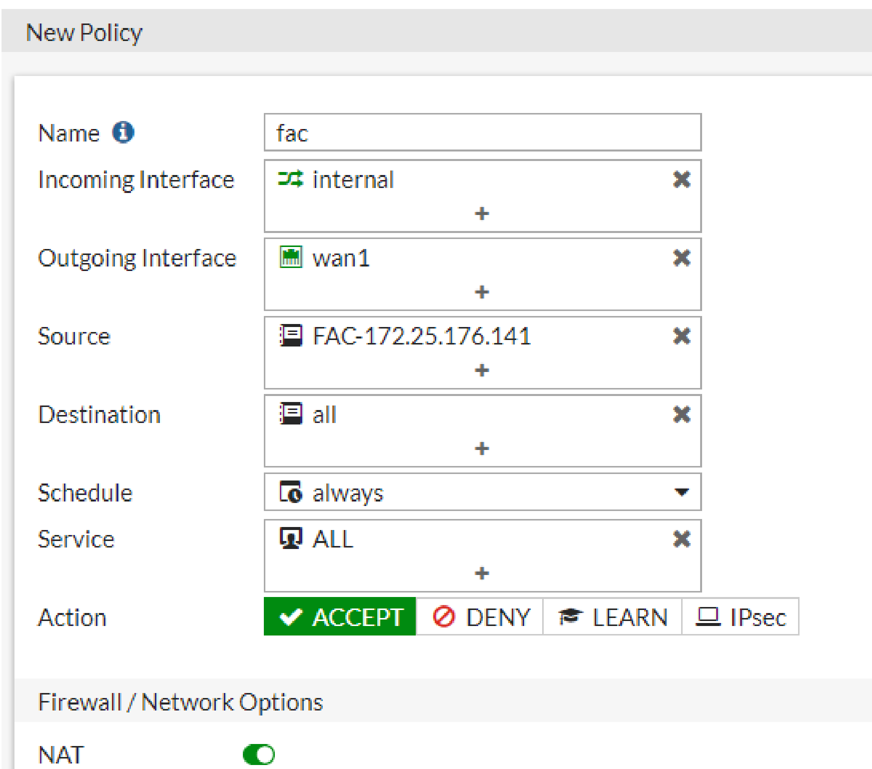
2. Go to *Policy & Objects* > *Addresses* and add the FortiAuthenticator as an address object.

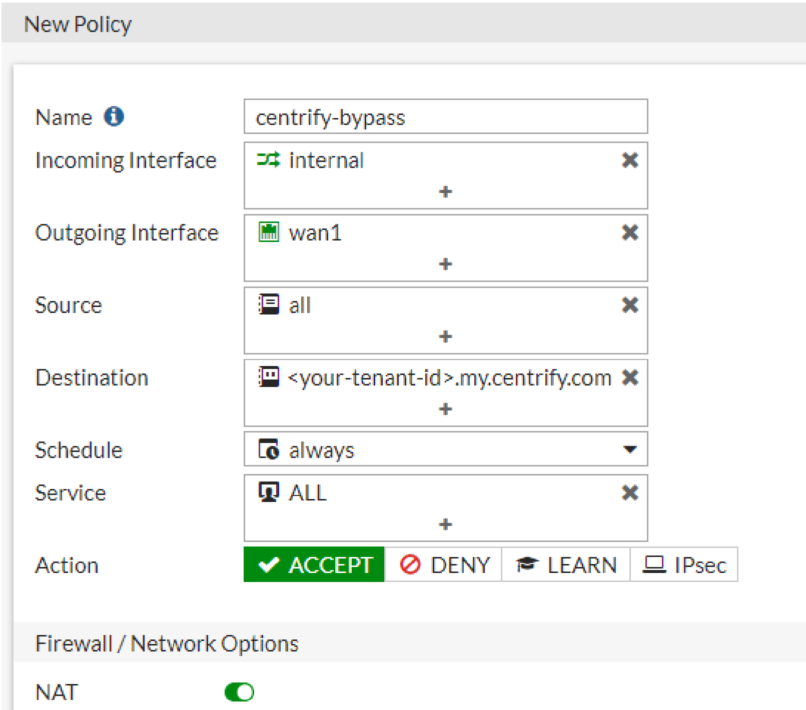


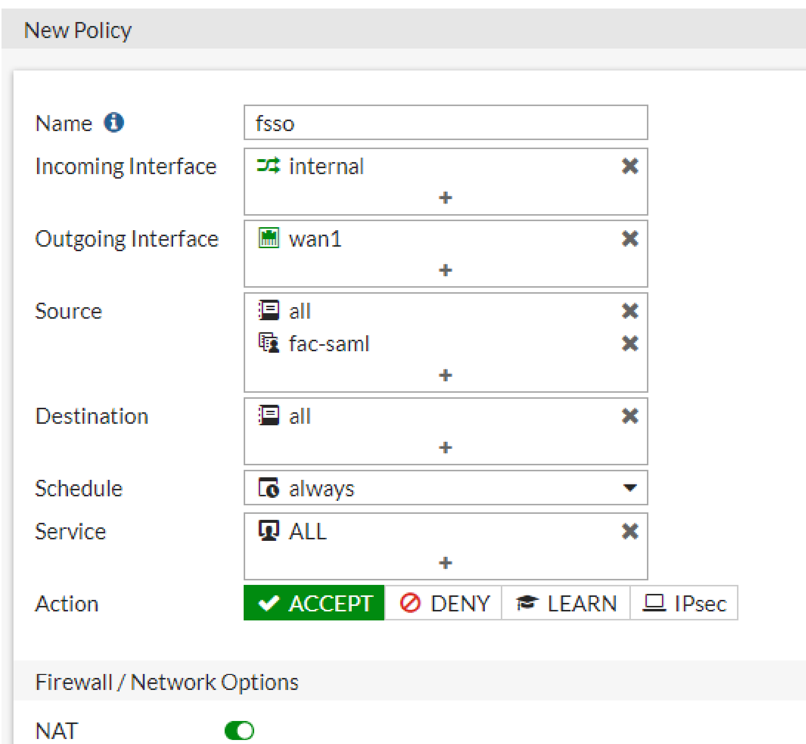
3. Create an FQDN object of your Centrify tenant portal:
   - <your-tenant-id>.my.centrify.com

   As this is an FQDN, make sure to set *Type* to *FQDN*.
4. Go to *Policy & Objects* > *IPv4 Policy* and create the policies in these examples:
   - A policy for DNS.
   - A policy for access from the FortiAuthenticator.
   - A policy for Centrify bypass.
   - A policy for FSSO, including the SAML user group.


New Policy
Name
dns
Incoming Interface
internal
Outgoing Interface
wan1
Source
all
Destination
all
Schedule
always
Service
DNS
Action
ACCEPT
DENY
LEARN
IPsec
Firewall / Network Options
NAT


New Policy
Name
fac
Incoming Interface
internal
Outgoing Interface
wan1
Source
FAC-172.25.176.141
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
LEARN
IPsec
Firewall / Network Options
NAT





5. When finished, right-click each policy except the FSSO policy, select *Edit in CLI*, and enter the following commands for each policy except the FSSO policy:

```
set captive-portal-exempt enable
   next
end
```

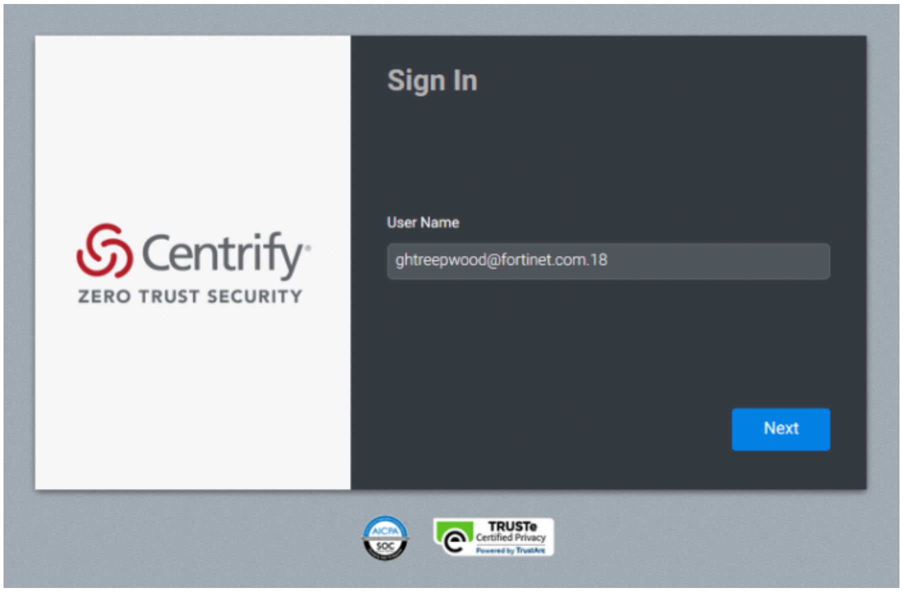
This command exempts users of these policies from the captive portal interface.

Results

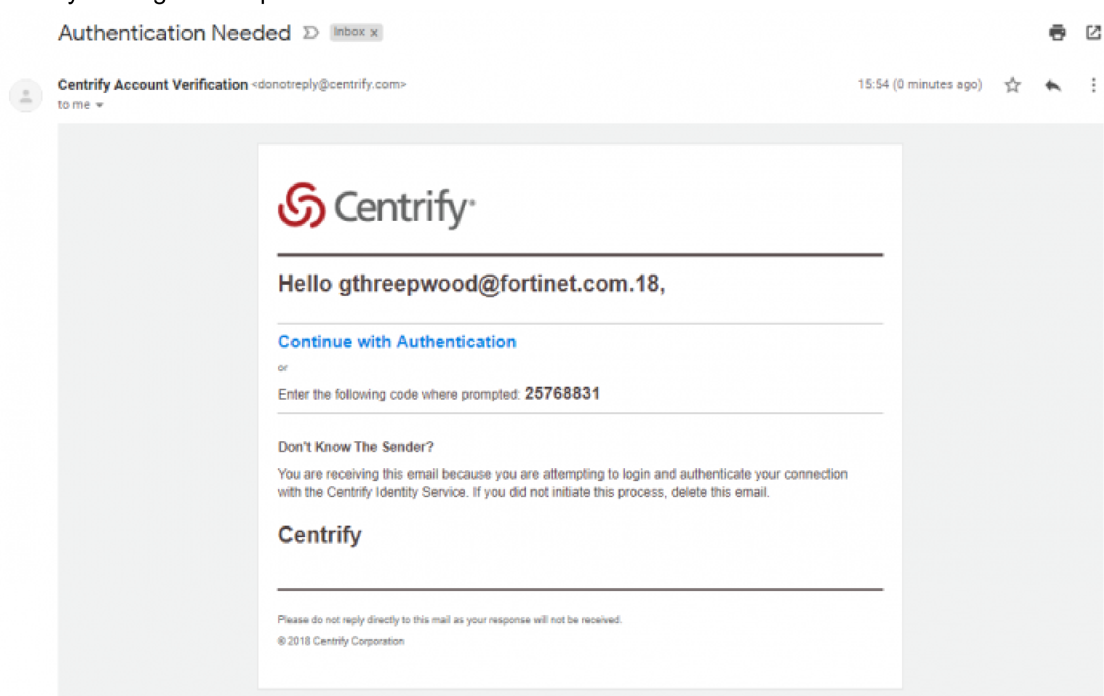
To test the connection, open a browser window and try to browse the Internet. The browser redirects to the FortiAuthenticator SAML portal, which pushes the browser to the SAML IdP.

Alternatively, you can directly navigate to the portal URL.

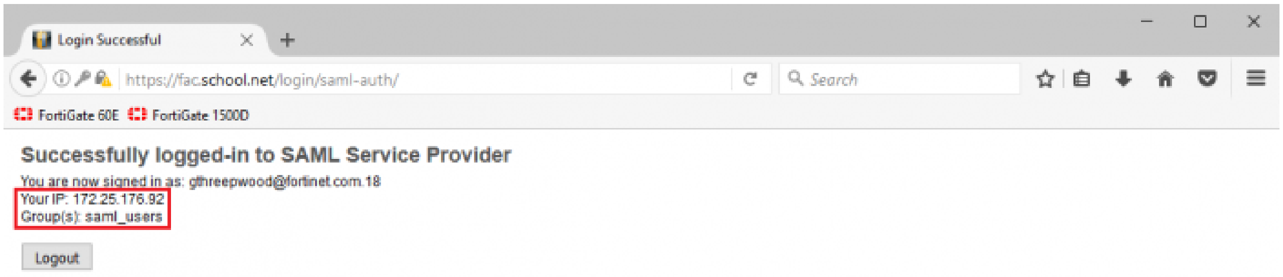
1. Enter the Centrify account credentials and select *Next*.



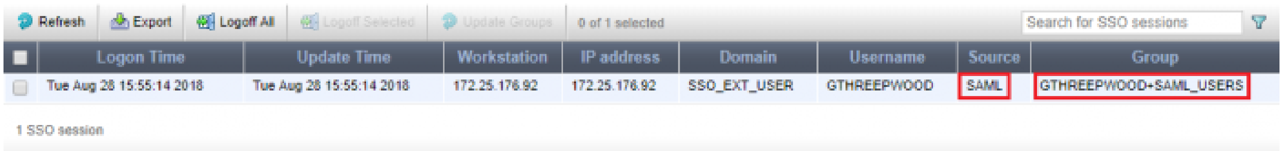
2. You must verify your account on your first login. An eight-digit code is sent to your email. Use the code to verify your identity and log into the portal.



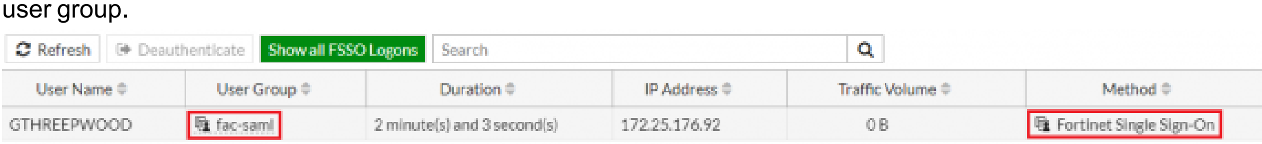
3. The user assertion pushes to the FortiAuthenticator where the user is successfully authenticated. Note the user IP and group name.



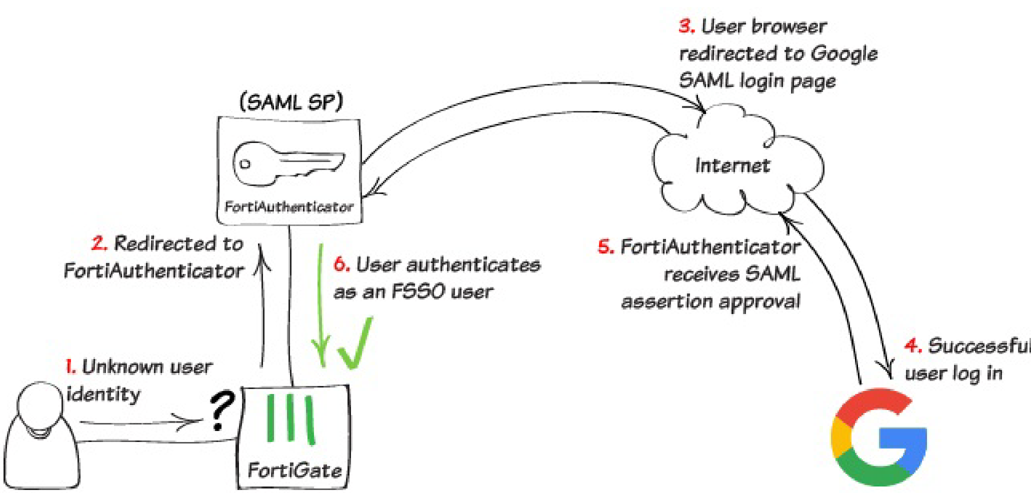
4. In FortiAuthenticator *Monitor* > *SSO* > *SSO Sessions*, you can view user information including the IP address, source, and user group.



5. In FortiGate *Monitor* > *Firewall User Monitor*, confirm that the user is authenticated via FSSO and is in the correct user group.



SAML 2.0 FSSO with FortiAuthenticator and Google G Suite



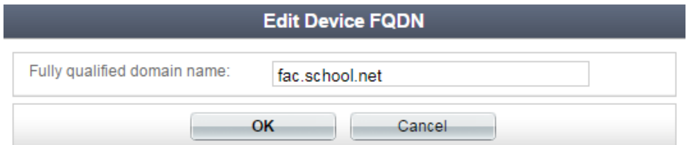
This example shows how to provide a Security Assertion Markup Language (SAML) FSSO cloud authentication solution using FortiAuthenticator with Google G Suite. FortiAuthenticator acts as the authentication Service Provider (SP) and Google as the Identity Provider (IdP).

In this example, the FortiGate has a WAN IP address of *172.25.176.92*, and the FortiAuthenticator has the WAN IP address of *172.25.176.141*.

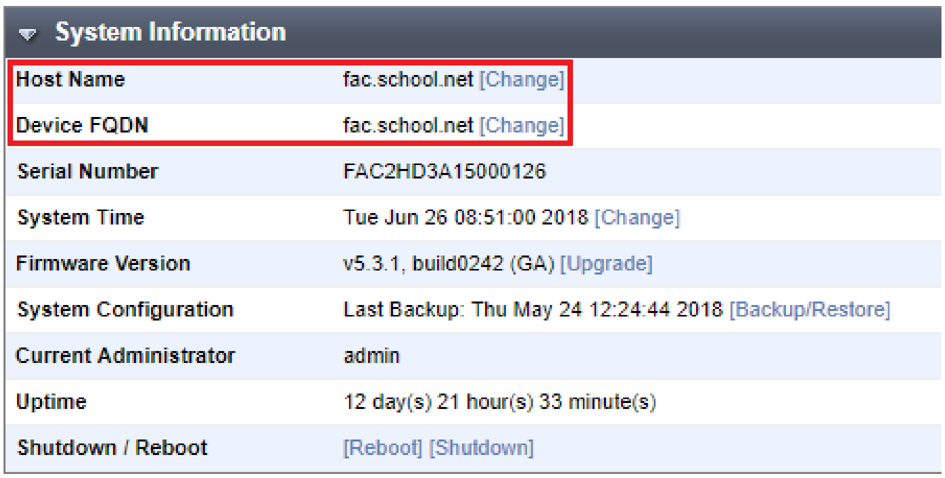
Before you begin, on the FortiAuthenticator, create two user groups (one local user group and one SSO user group). These groups must have identical names, in this example, *saml_users*.

Configuring FSSO and SAML on the FortiAuthenticator

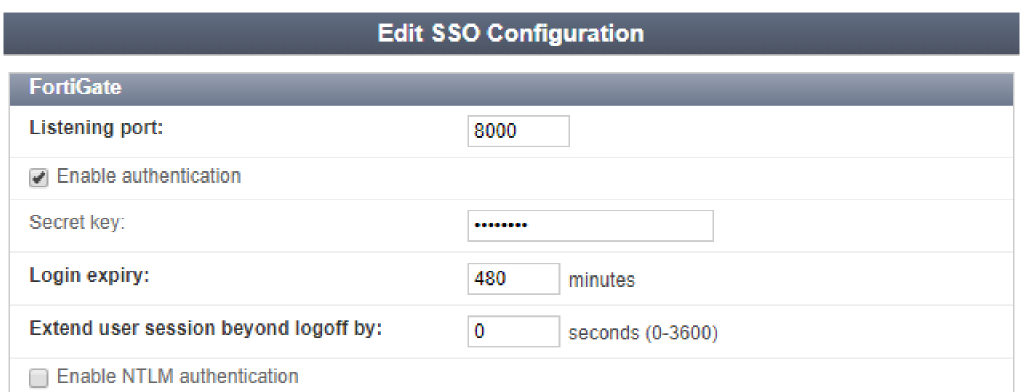
1. On the FortiAuthenticator, go to *System* > *Dashboard* > *Status*.
   In the *System Information* widget, select *Change* beside *Device FQDN*.
   Enter a domain name (in this example, *fac.school.net*). This helps identify where the FortiAuthenticator is located in the DNS hierarchy.



2. Enter the same name for the *Host Name*. This allows you to add the unit to the FortiGate's DNS list so that the local DNS lookup of this FQDN can be resolved.



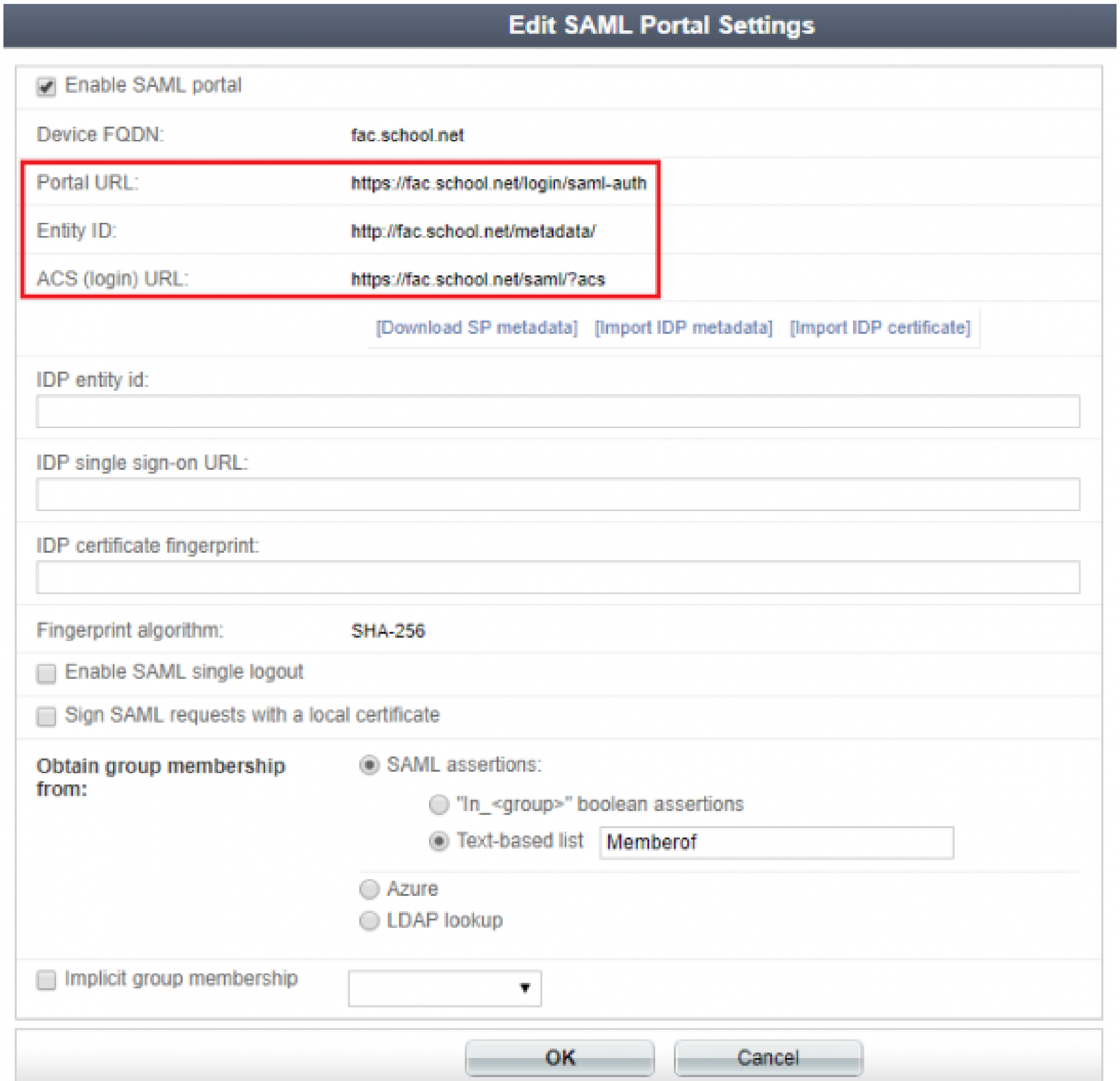
3. On the FortiAuthenticator, go to *Fortinet SSO Methods* > *SSO* > *General* and set FortiGate SSO options. Make sure to *Enable authentication*.
   Enter a *Secret key* and select *OK* to apply your changes. This *Secret key* is used on the FortiGate to add the FortiAuthenticator as the FSSO server.



4. Go to *Fortinet SSO Methods* > *SSO* > *SAML Authentication* and select *Enable SAML portal*. All necessary URLs are automatically generated:

- *Portal URL*: captive portal URL for the FortiGate and user.
- *Entity ID*: used in the Centrify SAML IdP application setup.
- *ACS (login) URL*: assertion POST URL used by the SAML IdP.

Under *SAML assertions*, enable *Text-based list* and enter *Memberof* (this field is case-sensitive).



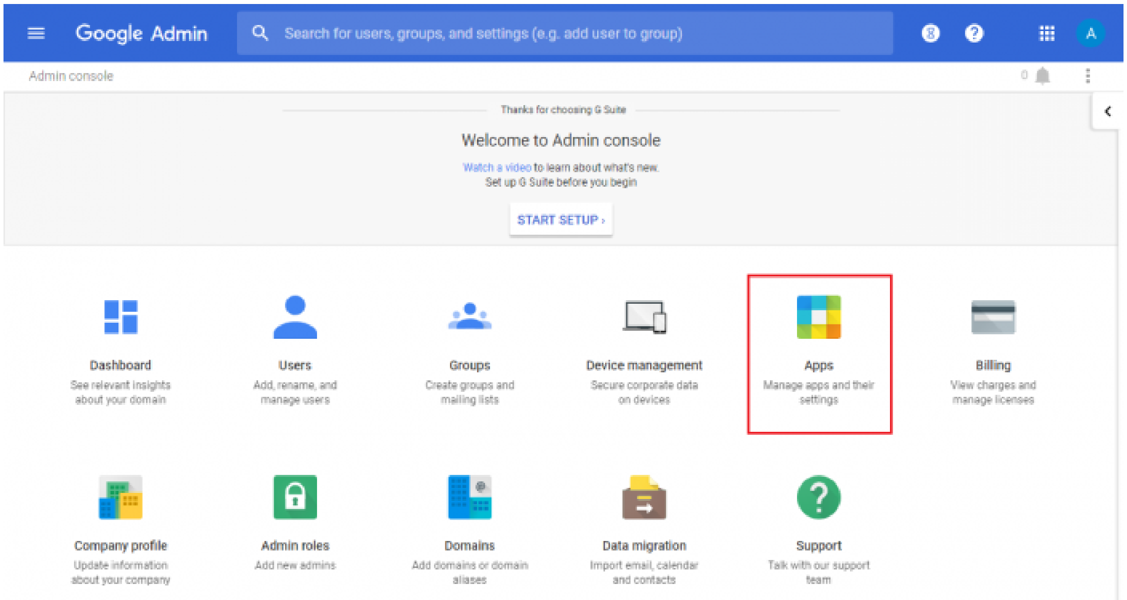
Keep this window open as these URLs are needed to configure the IdP application and for testing.

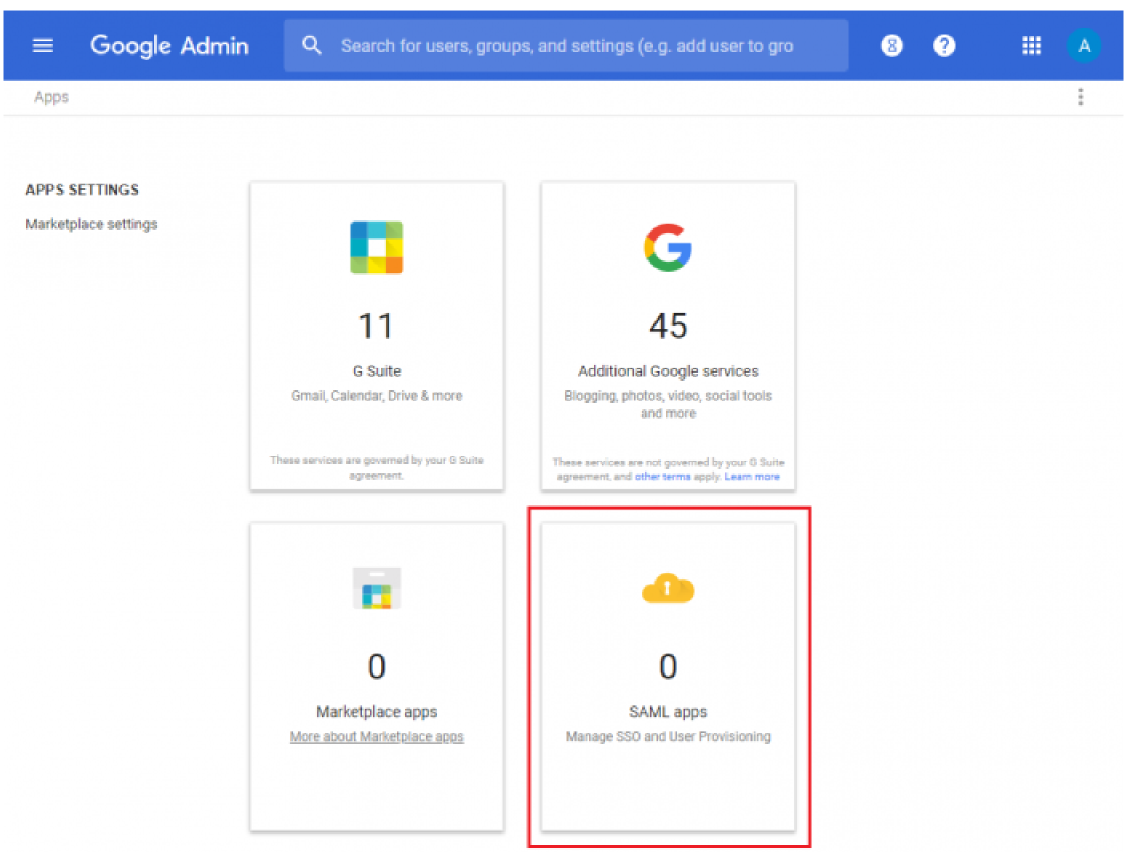
You cannot save these settings yet as the IdP information (*IDP entity id*, *IDP single sign-on URL*, and *IDP certificate fingerprint*) still needs to be entered. These fields will be filled once the IdP application configuration is complete.

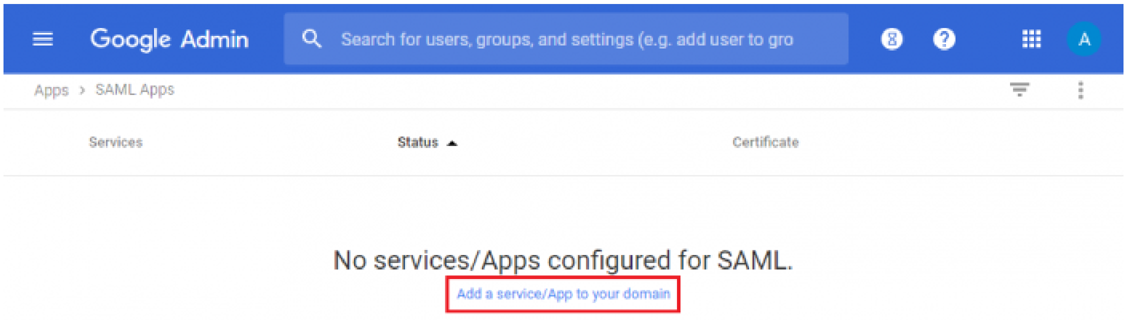
Configuring SAML on G Suite

To configure SAML, log in to your G Suite administrator account:

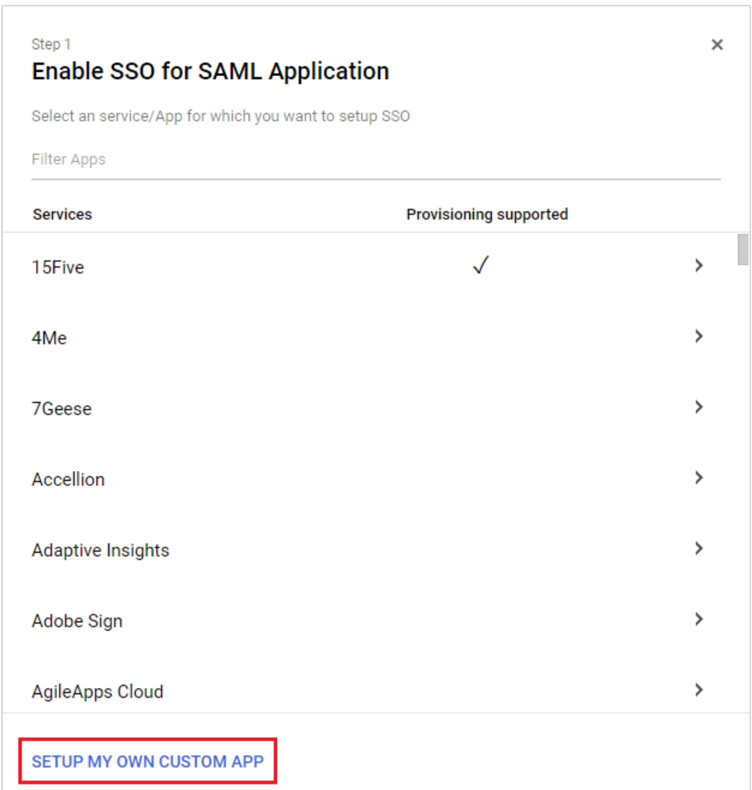
1. In the *Admin console*, select *Apps* > *SAML apps* > *Add a service/App to your domain*.



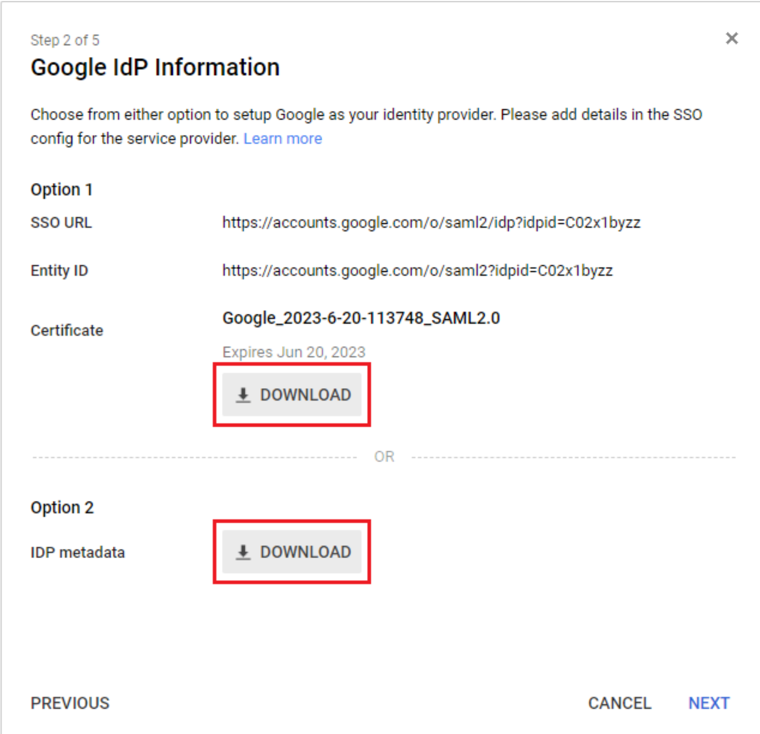




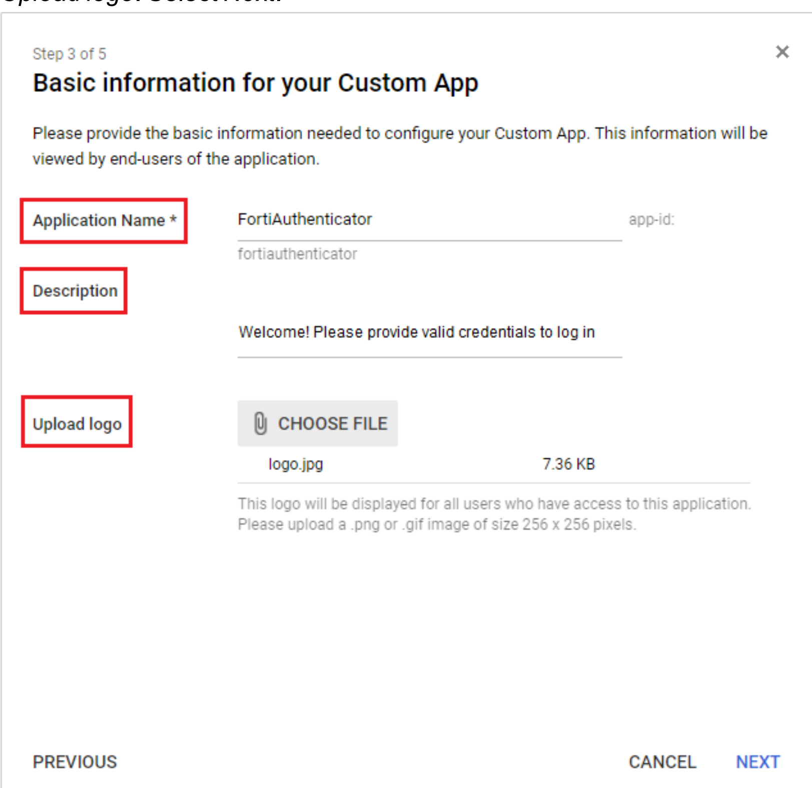
2. In the *Enable SSO for SAML Application* page, select to *SETUP MY OWN CUSTOM APP*.



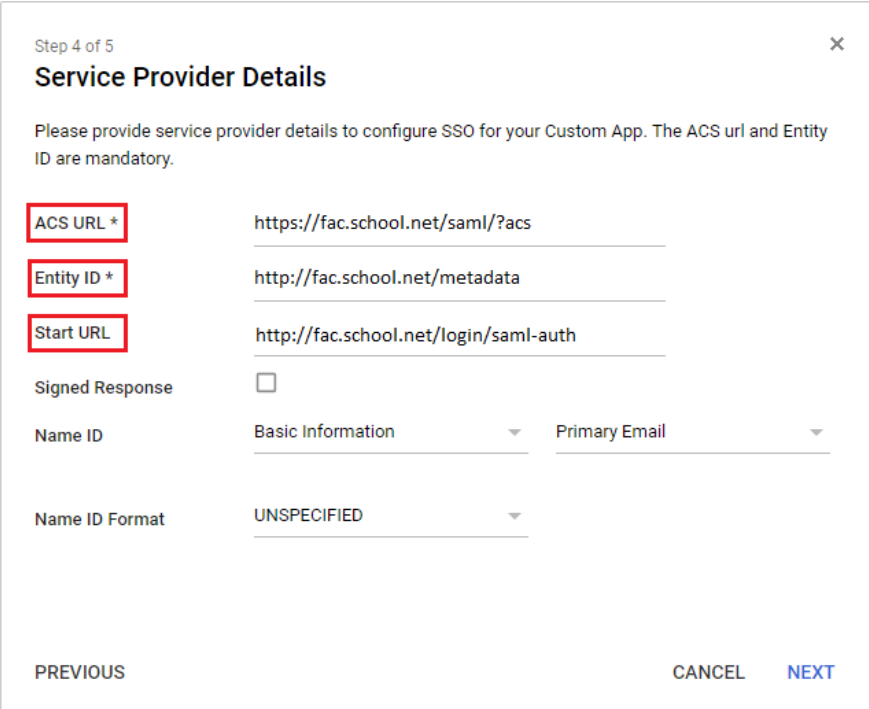
3. In the *Google IdP Information* page, download the *Certificate* and *IDP metadata*. Select *Next*.



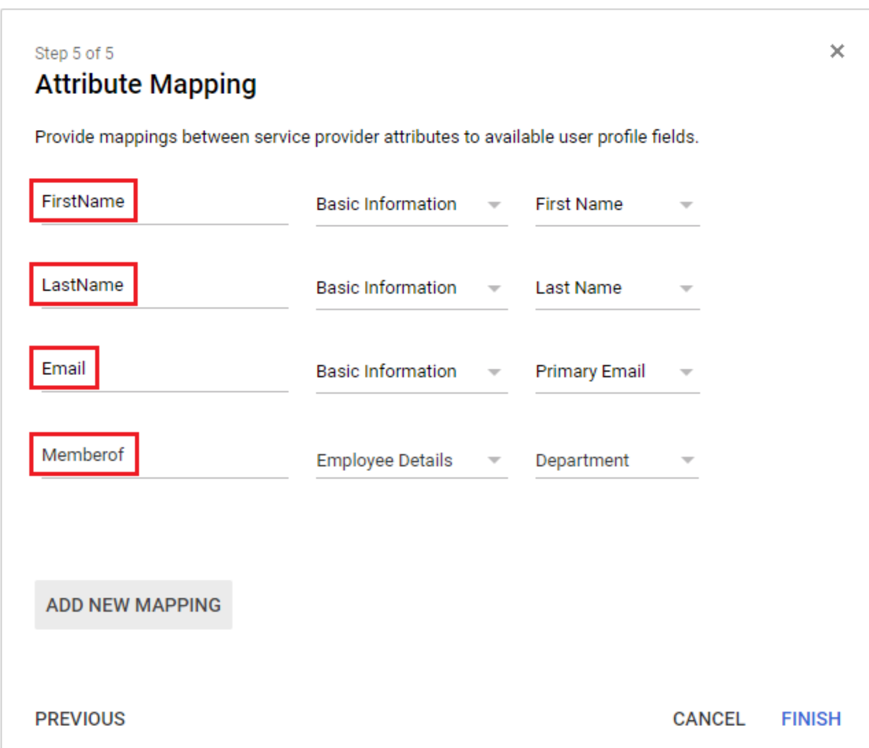
4. In the *Basic information for your Custom App* page, enter an *Application Name*, and, if you want, a *Description* and *Upload logo*. Select *Next*.



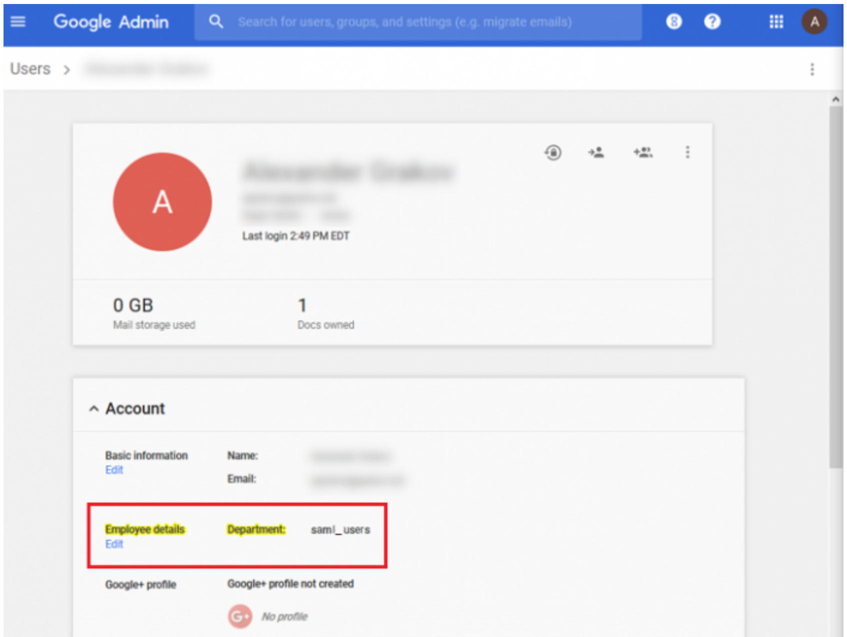
5. In the *Service Provider Details* page, set the *ACS URL*, *Entity ID*, and *Start URL*. These are the *ACS (login) URL*, *Entity ID*, and *Portal URL* from the FortiAuthenticator *Edit SAML Portal Settings* window. Select *Next*.



6. In the *Attribute Mapping* page, add the *FirstName*, *LastName*, *Email*, and *Memberof* user attributes. The *Department* setting for *Memberof* must match the FortiAuthenticator *saml_users* group. Select *Finish*.



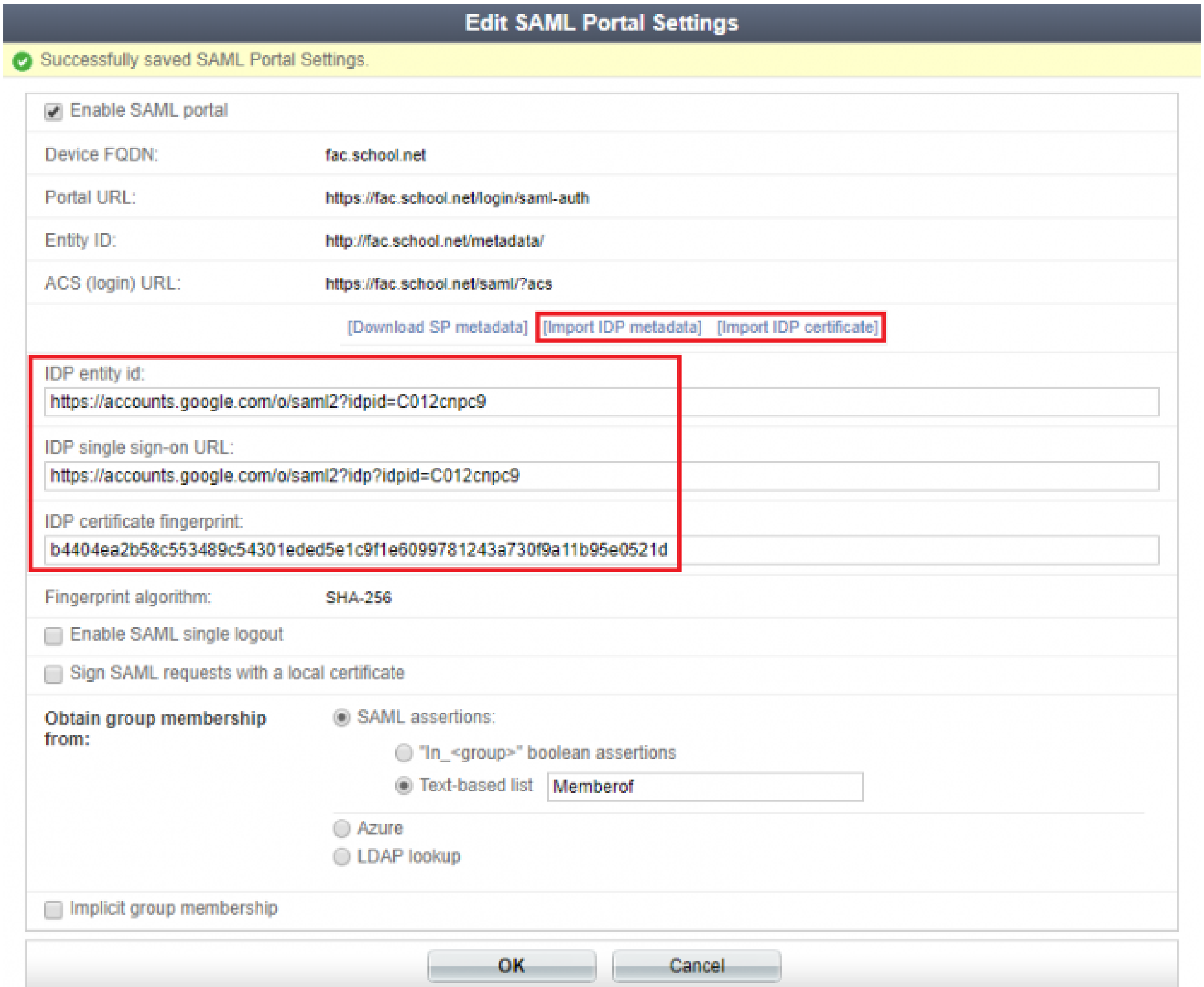
7. Check that the application is *ON* for everyone.
   Go to your user's *Account* information and ensure *Employee details* is *Department*. Set *Department* to the same FortiAuthenticator *saml_users* user group name.



Importing the IdP certificate and metadata on the FortiAuthenticator

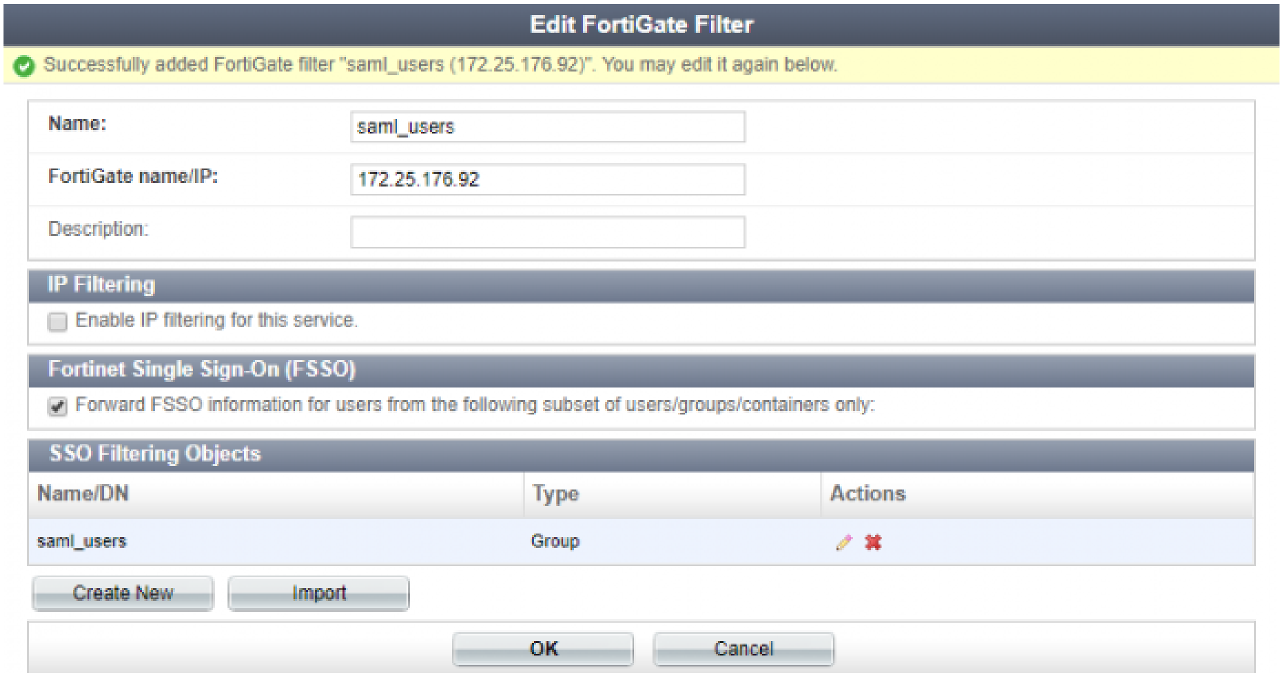
1. On the FortiAuthenticator, go to *Fortinet SSO Methods > SSO > SAML Authentication* and import the IdP metadata and certificate downloaded during the *Google IdP Information* step earlier.

This automatically fills the IdP fields (as shown in the example). Click *OK* to save these changes.



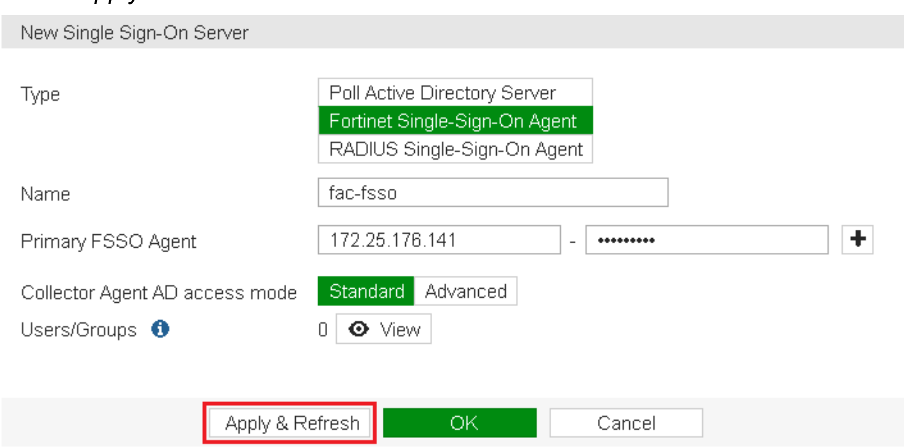
2. Go to *Fortinet SSO Methods* > *SSO* > *FortiGate Filtering* and create a new FortiGate filter.
   Enter a name and the FortiGate's wan-interface IP address, and select *OK*.
   Enable *Fortinet Single Sign-On (FSSO)*.
   Select *Create New* to create an SSO group filtering object (as shown in this example).
   The name of the filter must be the same as the group name created for SAML users (*saml_users*). The two user groups must have the exact same name or SSO information will not be pushed to the FortiGate.

Select *OK* to apply all changes.



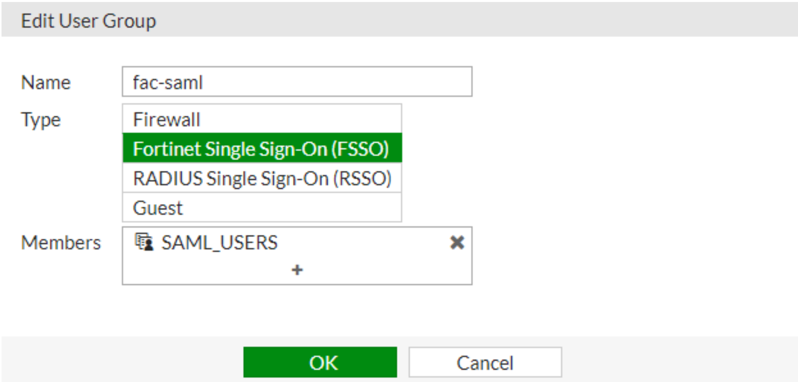
Configuring FSSO on the FortiGate

1. On the FortiGate, go to *User & Device* > *Single Sign-On* and select *Create New*.
   Set Type to *Fortinet Single-Sign-On Agent*, enter a *Name*, the FortiAuthenticator's Internet-interface IP address, and the password, which must match the secret key entered at the beginning of the FortiAuthenticator configuration process.
   Select *Apply & Refresh*.



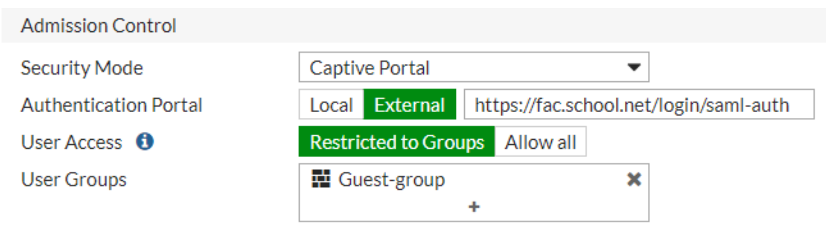
2. The SAML user group name is pushed to the FortiGate from the FortiAuthenticator and appears when you select *View*.
   You might have to wait a few minutes before the user group appears.
3. Go to *User & Device* > *User Groups* and create a new FSSO user group. Users authenticated via SAML FSSO are in this group.

Enter a *Name*, set *Type* to *Fortinet Single Sign-On (FSSO)*, and add the FSSO group as one of the *Members*.

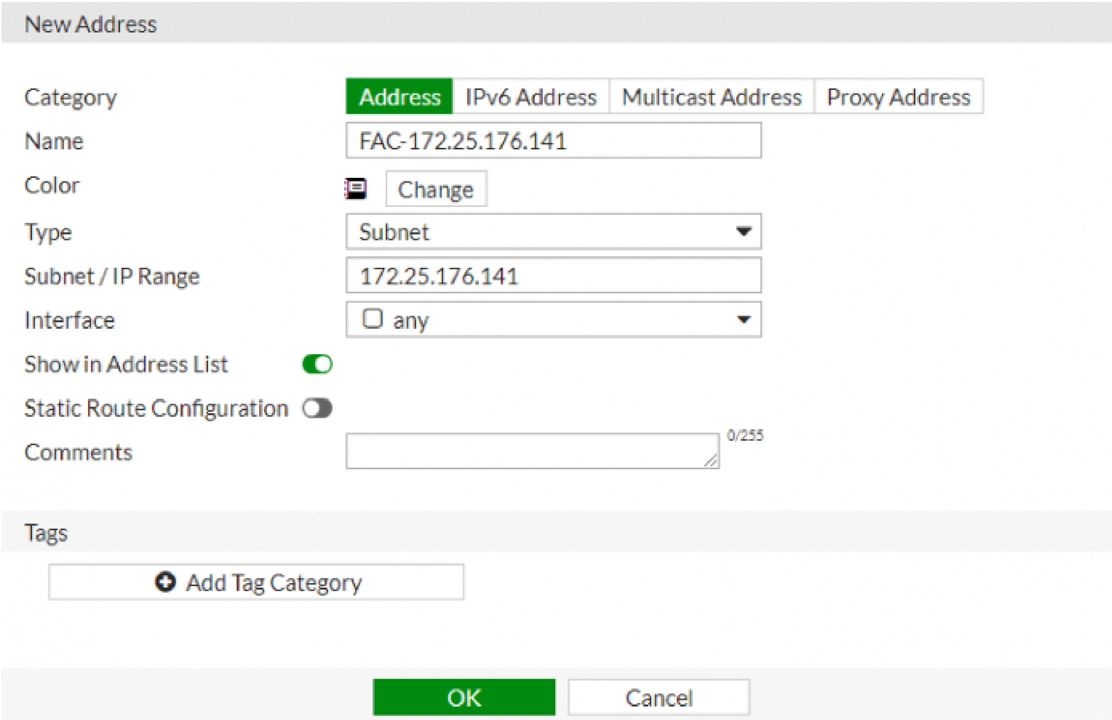


Configuring Captive Portal and security policies

1. On the FortiGate, go to *Network > Interfaces* and edit the internal interface.
   Under *Admission Control*, set *Security Mode* to *Captive Portal*.
   Set *Authentication Portal* to *External*, and enter the SAML authentication portal URL.
   Set *User Access* to *Restricted to Groups*, and set *User Groups* to any local group. As the FSSO group is not available, you cannot use this local group for access.

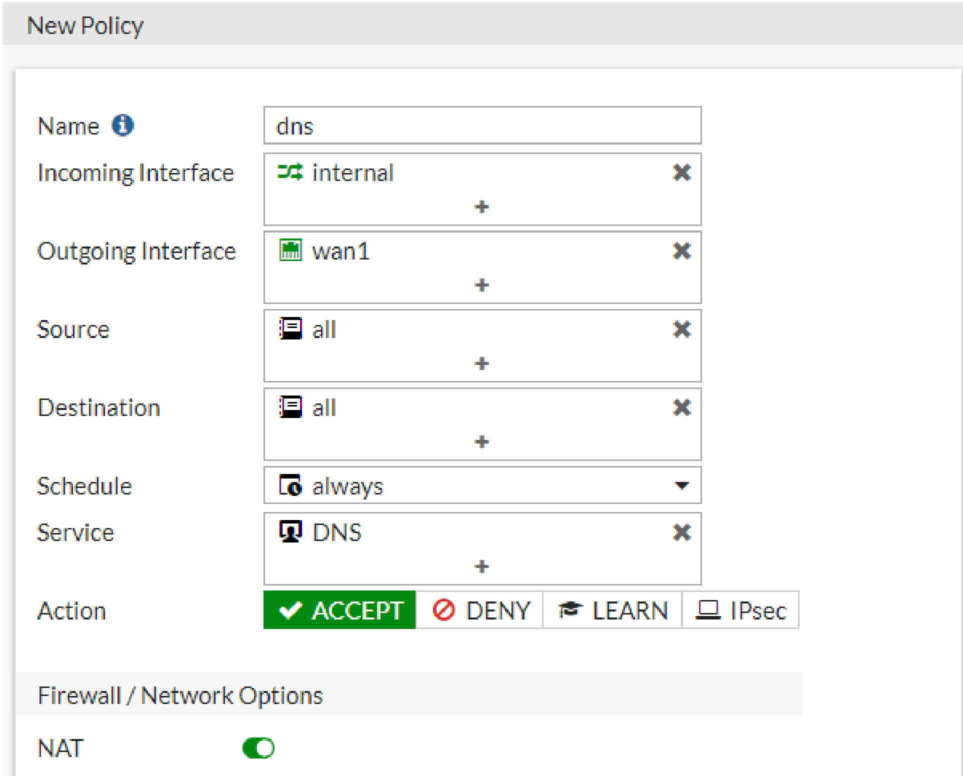


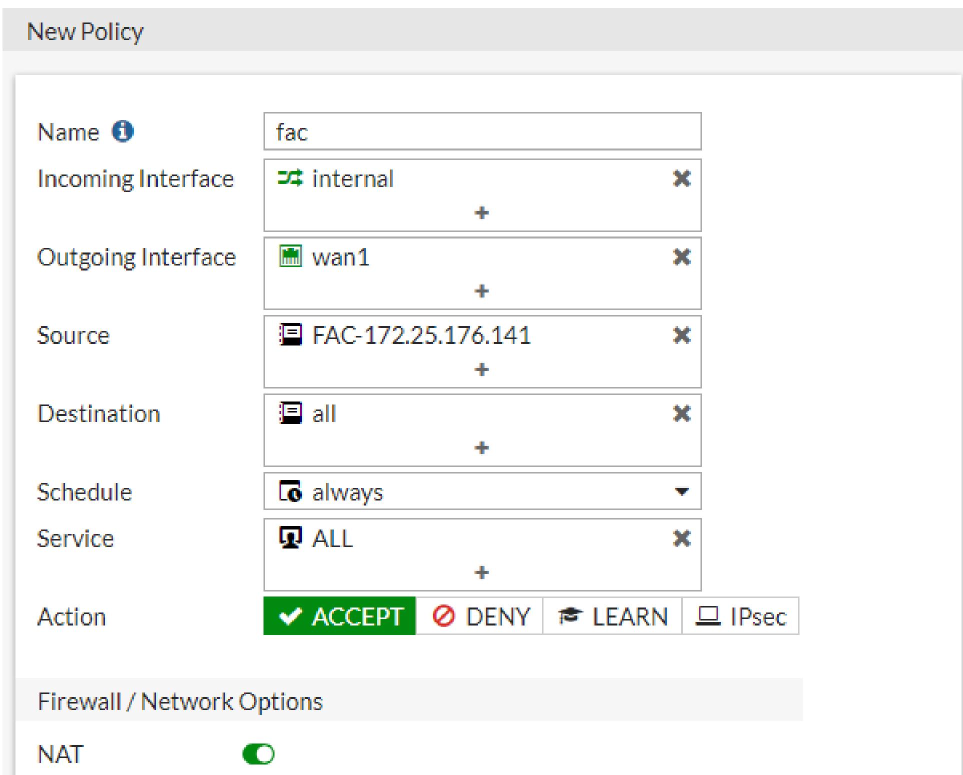
2. Go to *Policy & Objects* > *Addresses* and add the FortiAuthenticator as an address object.

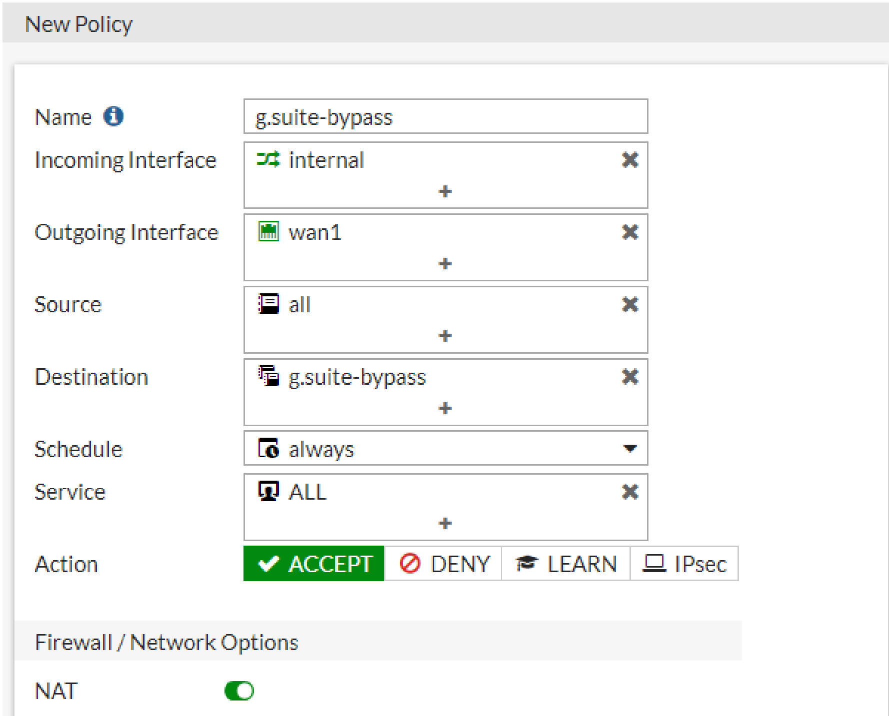


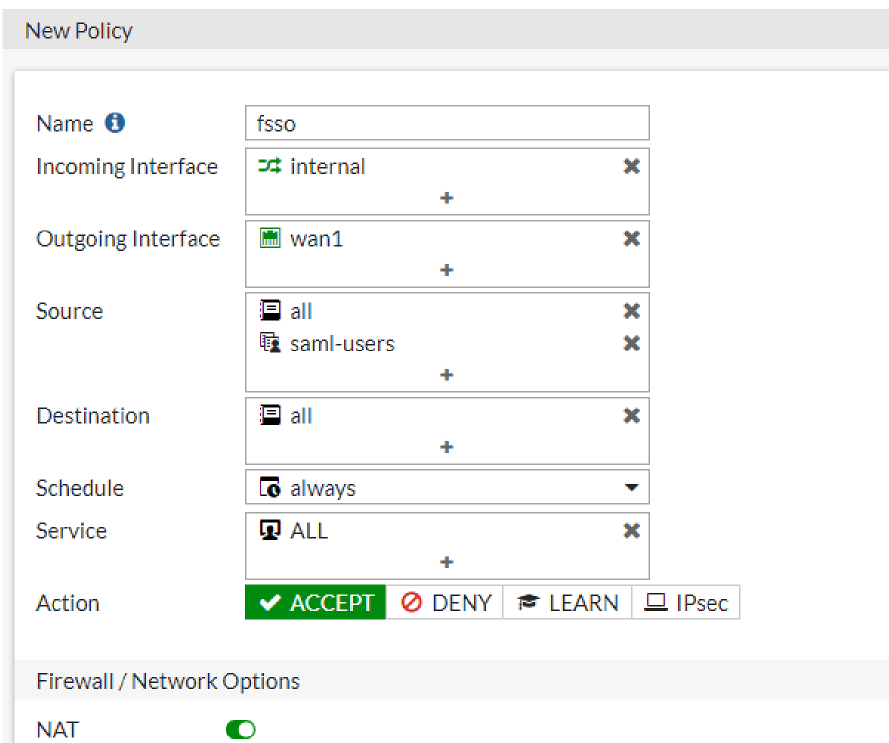
3. Create the following FQDN objects:
   - www.googleapis.com
   - accounts.google.com
   - ssl-gstatic.com
   - fonts.gstatic.com
   - www.gstatic.com
4. Add the following Google subnets:
   - 172.217.9.0/24
   - 216.58.192.0/19
5. Create an address group, adding all created objects as members (in this example, *g.suite-bypass*).
6. Go to *Policy & Objects* > *IPv4 Policy* and create the policies in these examples:
   - A policy for DNS.
   - A policy for access from FortiAuthenticator.
   - A policy for G Suite bypass.

- A policy for FSSO, including the SAML user group.









7. When finished, right-click each policy except the FSSO policy, select *Edit in CLI*, and enter the following commands for each policy except the FSSO policy:

```
set captive-portal-exempt enable
   next
end
```

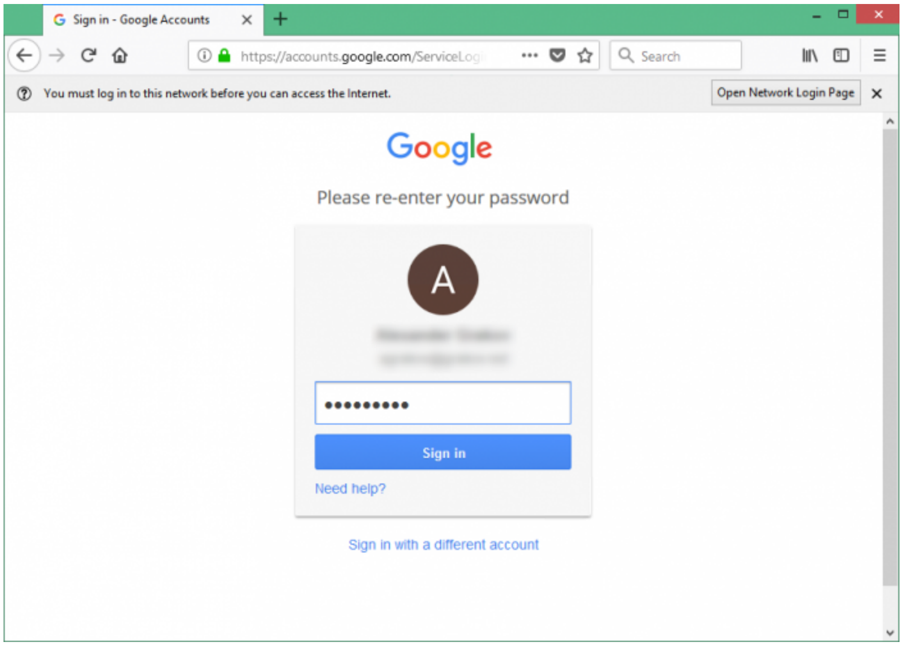
This command exempts users of these policies from the captive portal interface.

Results

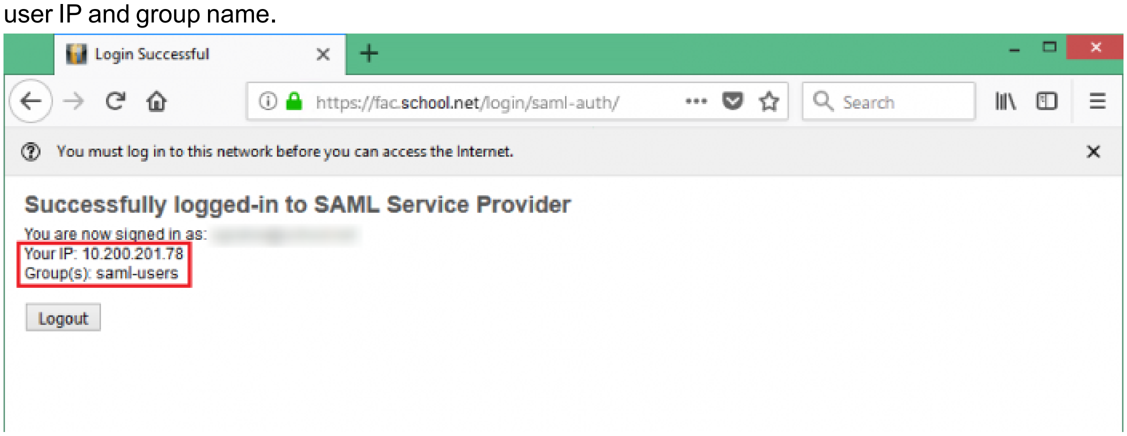
To test the connection, open a browser window and try to browse the Internet. The browser redirects to the FortiAuthenticator SAML portal, which pushes the browser to the SAML IdP.

Alternatively, you can directly navigate to the portal URL.

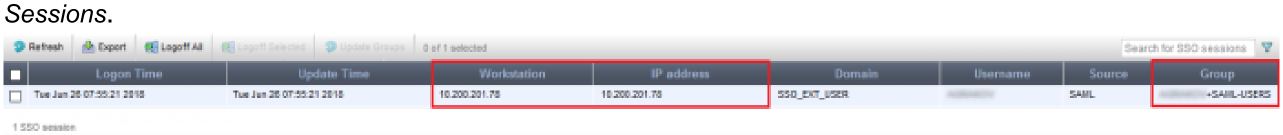
1. Enter a Google account credentials and confirm your password.



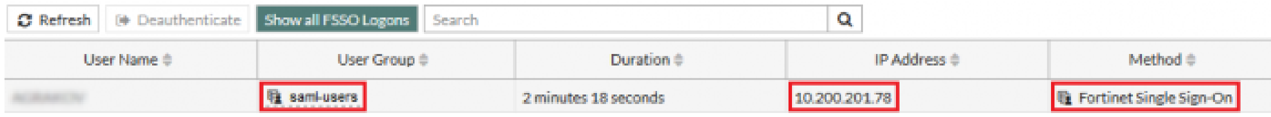
2. The user assertion pushes to the FortiAuthenticator where the user is successfully authenticated. Take note of the user IP and group name.



3. View user information including IP address and user group on the FortiAuthenticator under *Monitor* > *SSO* > *SSO Sessions*.

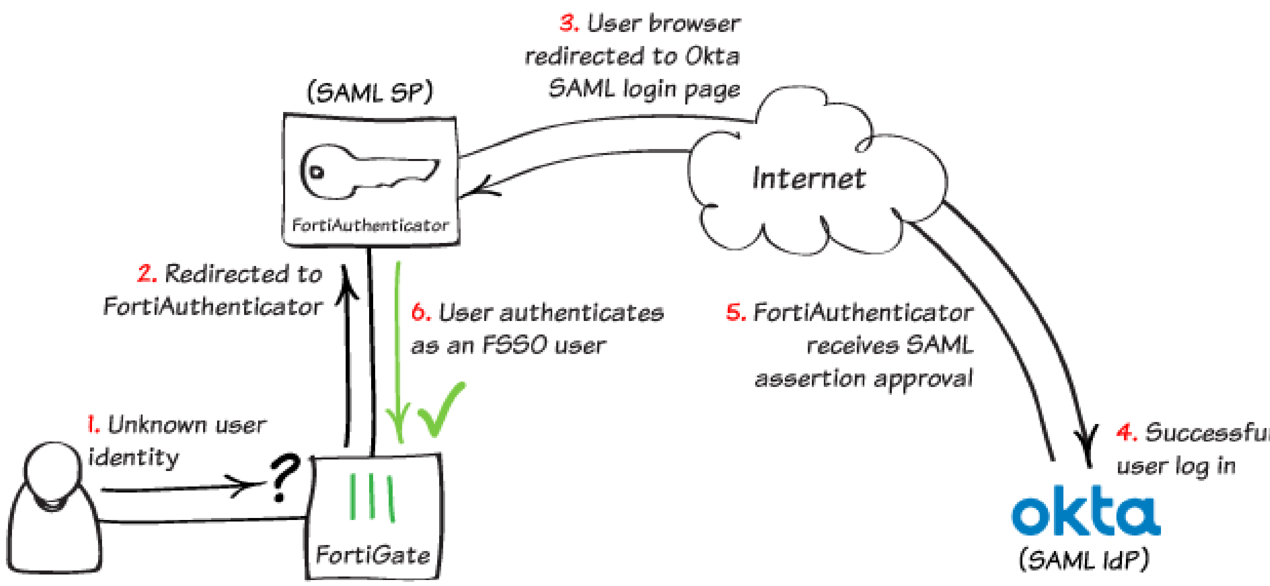


4. Confirm that the user has been authenticated via FSSO on the FortiGate under *Monitor > Firewall User Monitor*.



User Name	User Group	Duration	IP Address	Method
[illegible]	saml-users	2 minutes 18 seconds	10.200.201.78	Fortinet Single Sign-On

SAML 2.0 FSSO with FortiAuthenticator and Okta



This example shows you how to provide a Security Assertion Markup Language (SAML) FSSO cloud authentication solution using FortiAuthenticator as the service provider (SP) and Okta as the identity provider (IdP).

Okta is a cloud-based user directory providing a secure authentication and identity-access management service that offer secure SSO solutions. Okta can be implemented with different technologies and services including Office 365, G Suite, Dropbox, AWS, and others.

In the above sample diagram, a user starts by trying to make an unauthenticated web request (1). The FortiGate's captive portal offloads the authentication request to the FortiAuthenticator's SAML SP portal (2) which in turn redirects that client/browser to the SAML IdP login page (3). If the user successfully logs into the portal (4), a positive SAML assertion is sent back to the FortiAuthenticator (5), converting the user's credentials into those of an FSSO user (6).

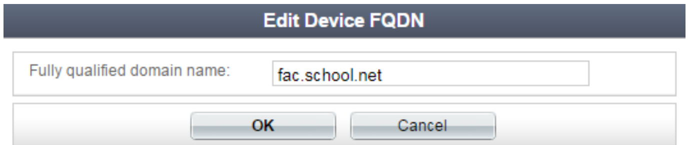
In this example, the FortiGate has a WAN IP address of *172.25.176.92*, and the FortiAuthenticator has the WAN IP address of *172.25.176.141*. For testing purposes, the FortiAuthenticator's IP and FQDN are added to the host's file of trusted host names; this is not necessary for a typical network.

Before you begin:

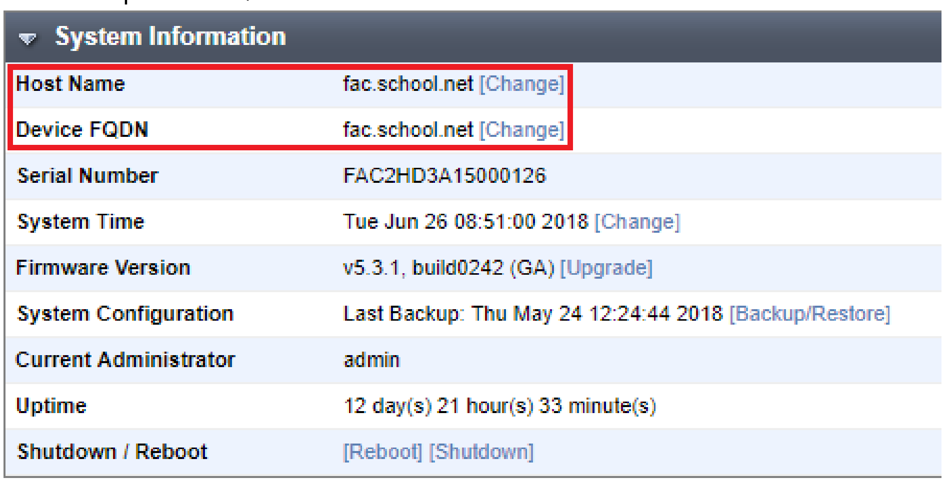
- Create an Okta developer account.
- On the FortiAuthenticator, create two user groups (one local user group and one SSO user group). These groups must have identical names, in this example, *saml_users*.

Configuring DNS and FortiAuthenticator's FQDN

1. On the FortiAuthenticator, go to *System* > *Dashboard* > *Status*.
   In the *System Information* widget, select *Change* beside *Device FQDN*.
   Enter a domain name (in this example, *fac.school.net*). This helps identify where the FortiAuthenticator is located in the DNS hierarchy.



2. Enter the same name for the *Host Name*. This allows you to add the unit to the FortiGate's DNS list so that the local DNS lookup of this FQDN can be resolved.



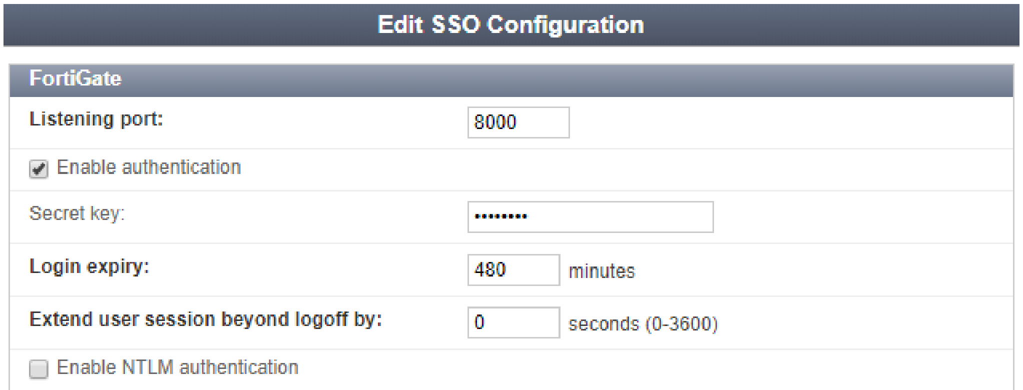
3. On the FortiGate, open the *CLI Console* and enter the following commands using the FortiAuthenticator's host name and Internet-facing IP address:

```
config system dns-database
   edit school.net
      config dns-entry
         edit 1
            set hostname fac.school.net
            set ip 172.25.176.141
         next
      end
      set domain school.net
   next
end
```

Enabling FSSO and SAML on the FortiAuthenticator

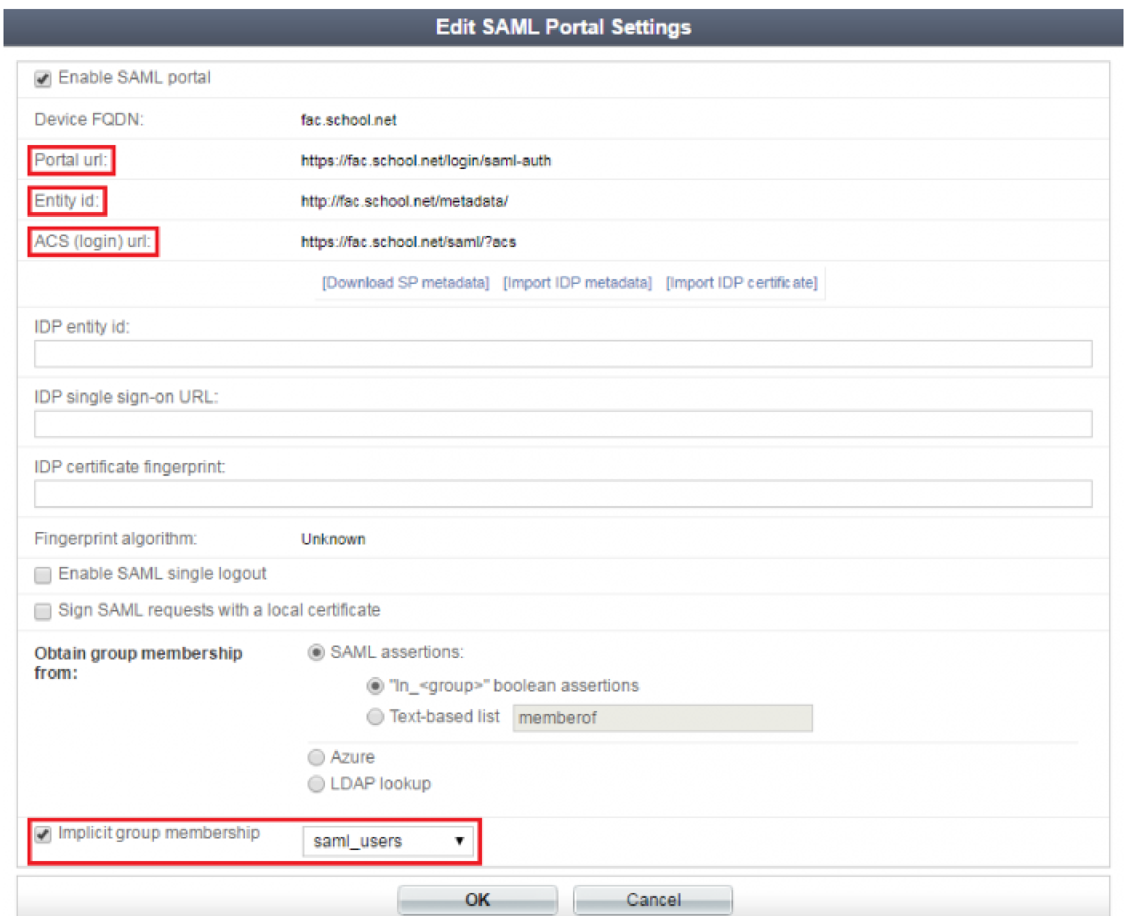
1. On the FortiAuthenticator, go to *Fortinet SSO Methods* > *SSO* > *General* and set FortiGate SSO options. Make sure to *Enable authentication*.

Enter a *Secret key* and select *OK* to apply your changes. This *Secret key* is used on the FortiGate to add the FortiAuthenticator as the FSSO server.



2. Go to *Fortinet SSO Methods* > *SSO* > *SAML Authentication* and select *Enable SAML portal*. All necessary URLs are automatically generated:
   - *Portal URL*: captive portal URL for the FortiGate and user.
   - *Entity ID*: used in the Centrify SAML IdP application setup.
   - *ACS (login) URL*: assertion POST URL used by the SAML IdP.

   Enable *Implicit group membership* and assign the *saml_users* group. This places SAML authenticated users into this group.

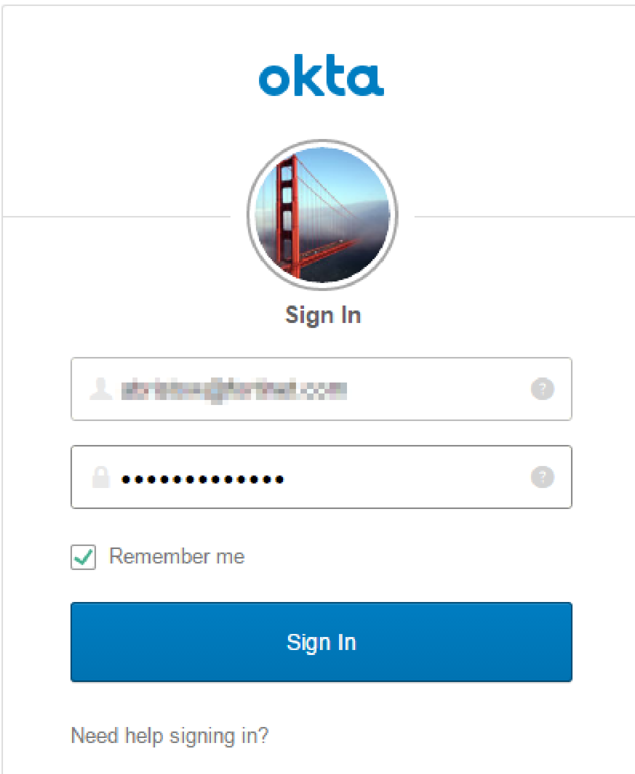


Keep this window open as these URLs are needed to configure the IdP application and for testing.

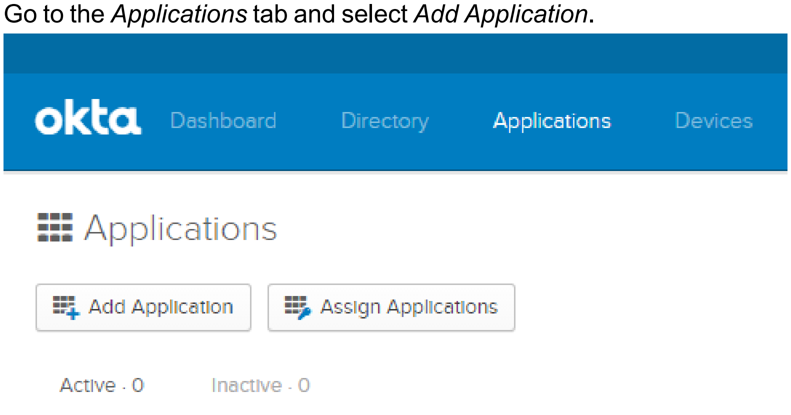
You cannot save these settings yet as the IdP information (*IDP entity id*, *IDP single sign-on URL*, and *IDP certificate fingerprint*) still needs to be entered. These fields will be filled once the IdP application configuration is complete.

Configuring the Okta developer account IDP application

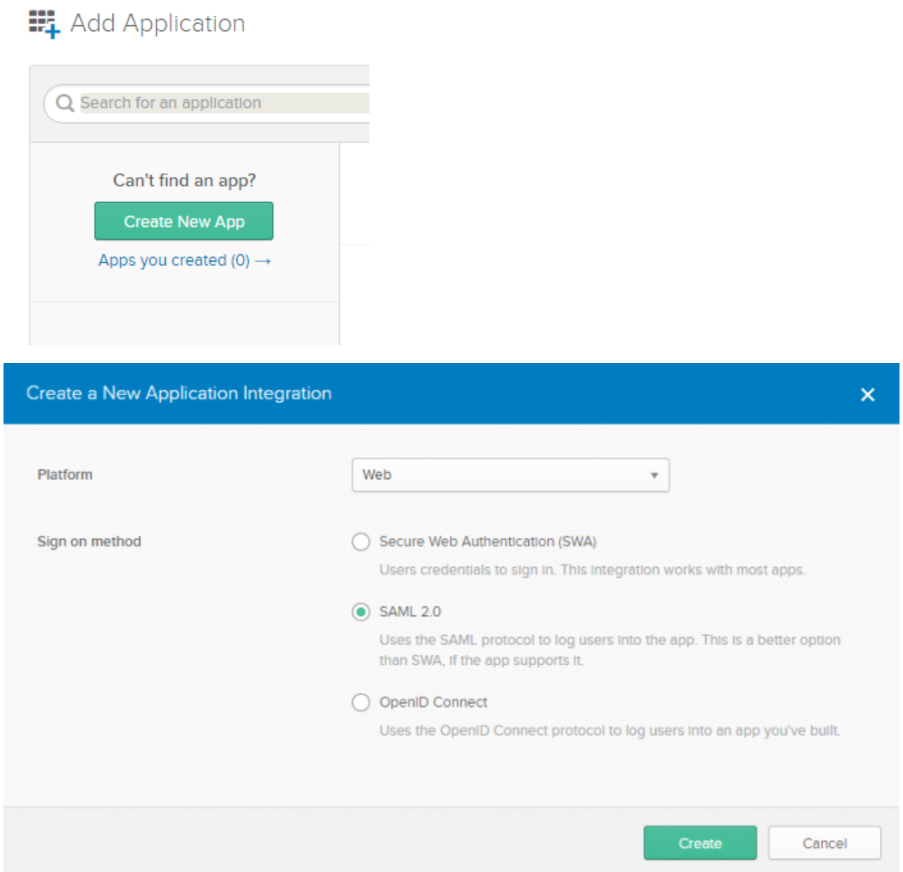
1. Open a browser, log in to your Okta developer account, and select *Admin* under your user settings.



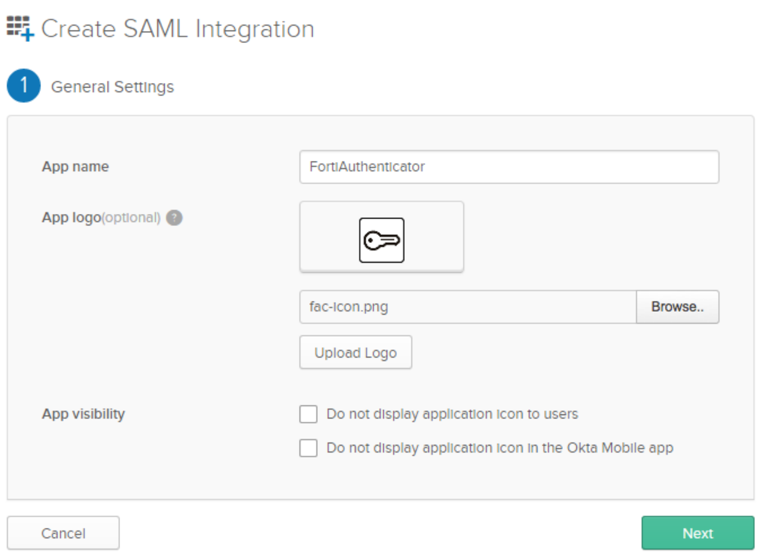
2. Go to the *Applications* tab and select *Add Application*.



3. Select *Create New App* and create a new application with the *SAML 2.0* sign on method.

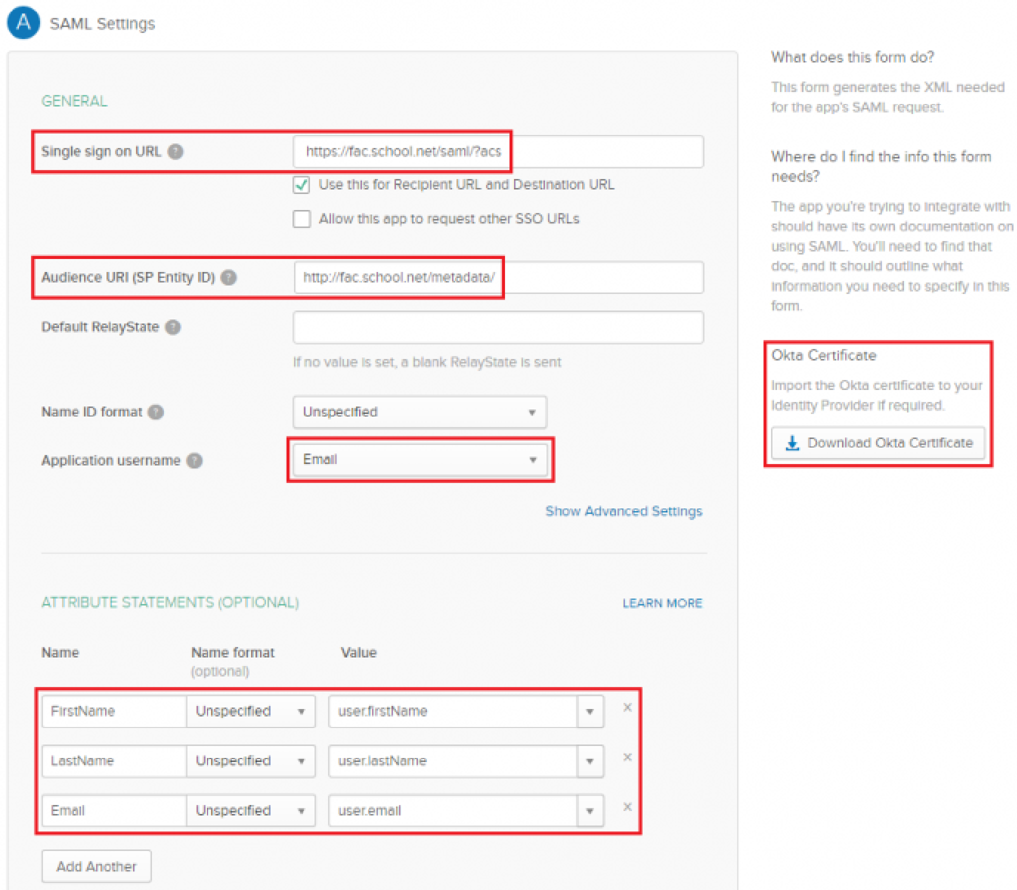


4. Enter an *App name*. The *App name* is the name of the portal the user logs into.
   If you want, you can upload a logo.
   Select *Next*.



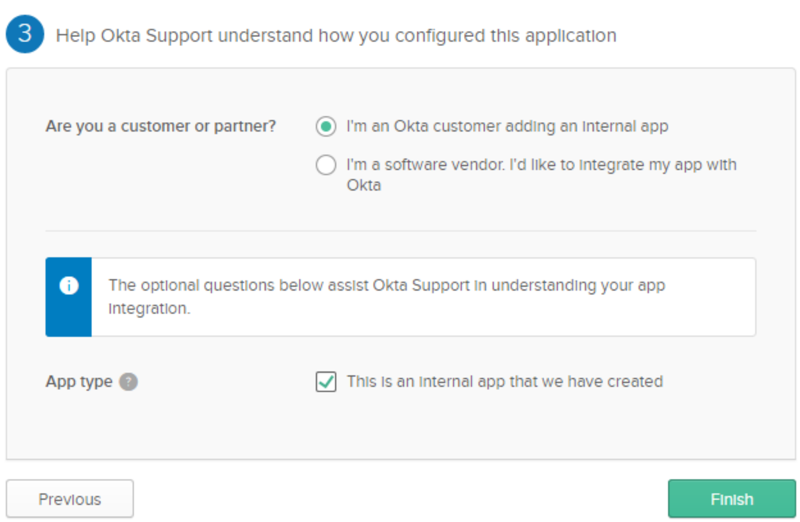
5. In the *A – SAML Settings* page, set *Single sign on URL* to the *ACS (login) URL* from the *Edit SAML Portal Settings* page on the FortiAuthenticator.

Set *Audience URI (SP Entity ID)* to the *Entity ID* URLs from the *Edit SAML Portal Settings* page.
Users must use their email address as the username and their first and last names (see example).
Select *Download Okta Certificate*. This will be imported to the FortiAuthenticator later.

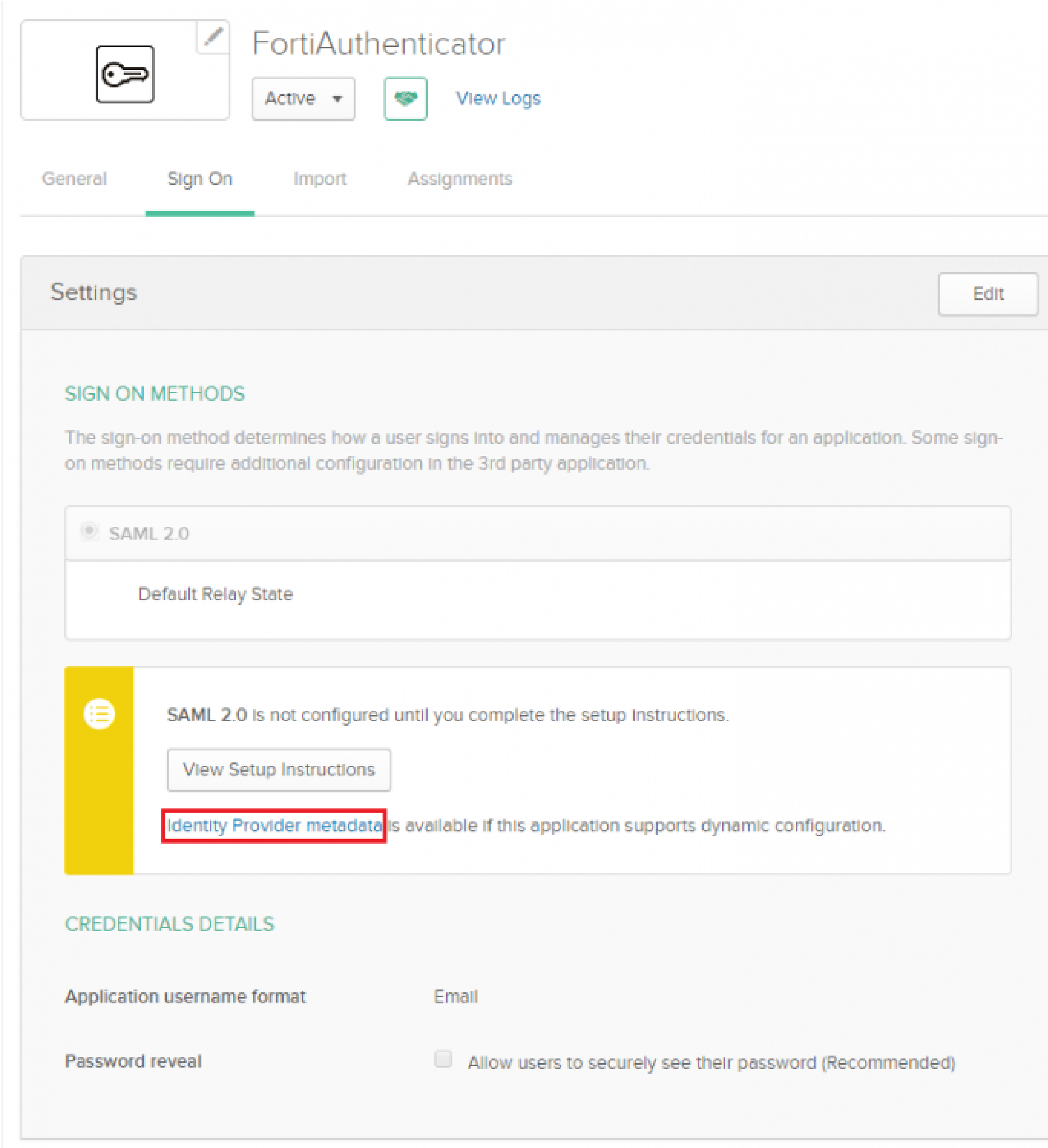


You do not need to configure group attributes or section *B*.

6. Confirm that you are an Okta customer and set the *App type* to an internal app. Then select *Finish*.

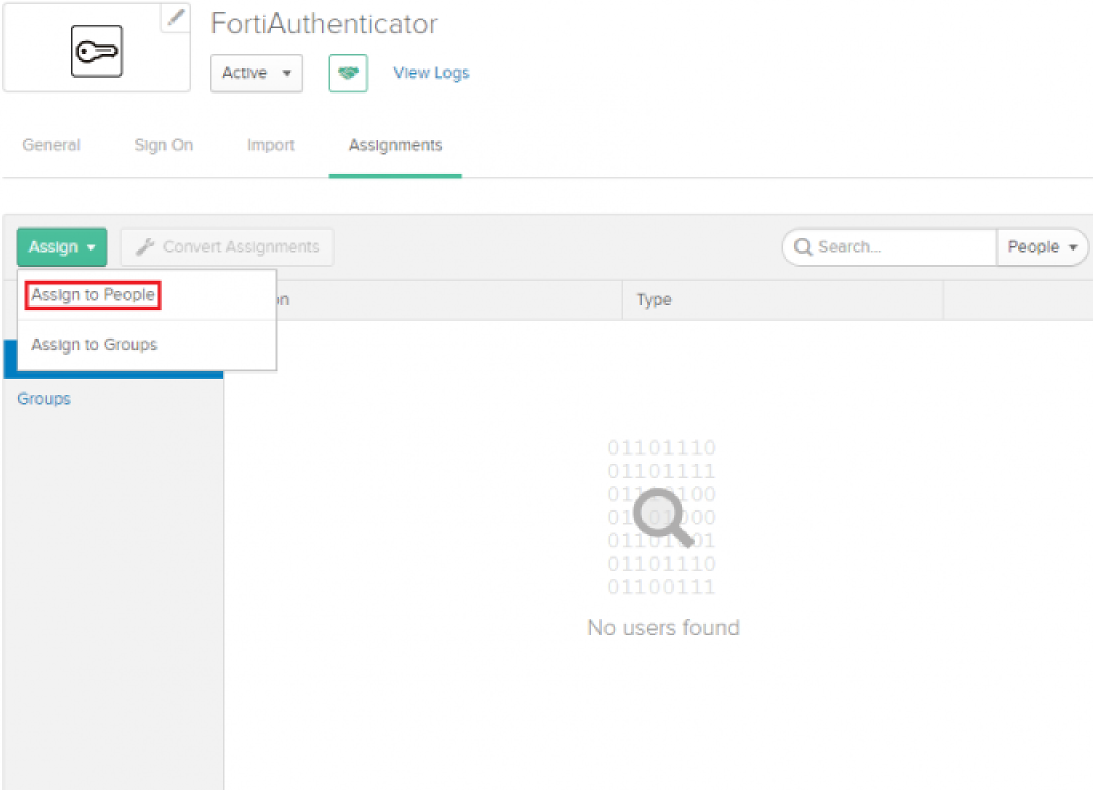


7. In the *Sign On* tab, download the *Identity Provider metadata*.

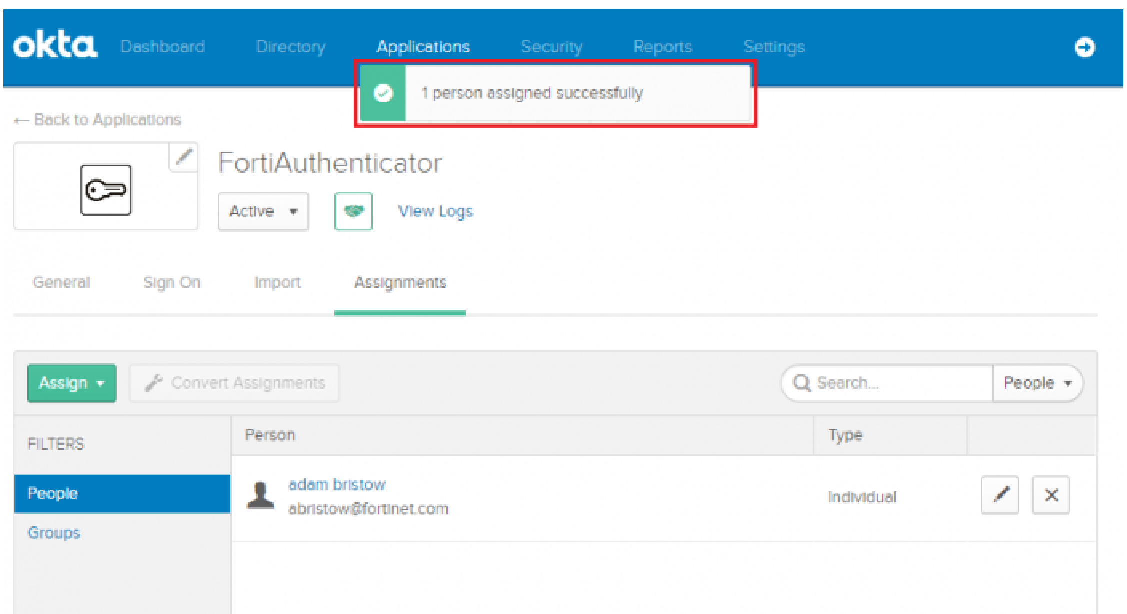


8. In the *Assignments* tab, select *Assign* > *Assign to People*.
   Assign the users you want to add to the application. This allows the user to log in to the application's portal.

Save your changes and select *Done*.

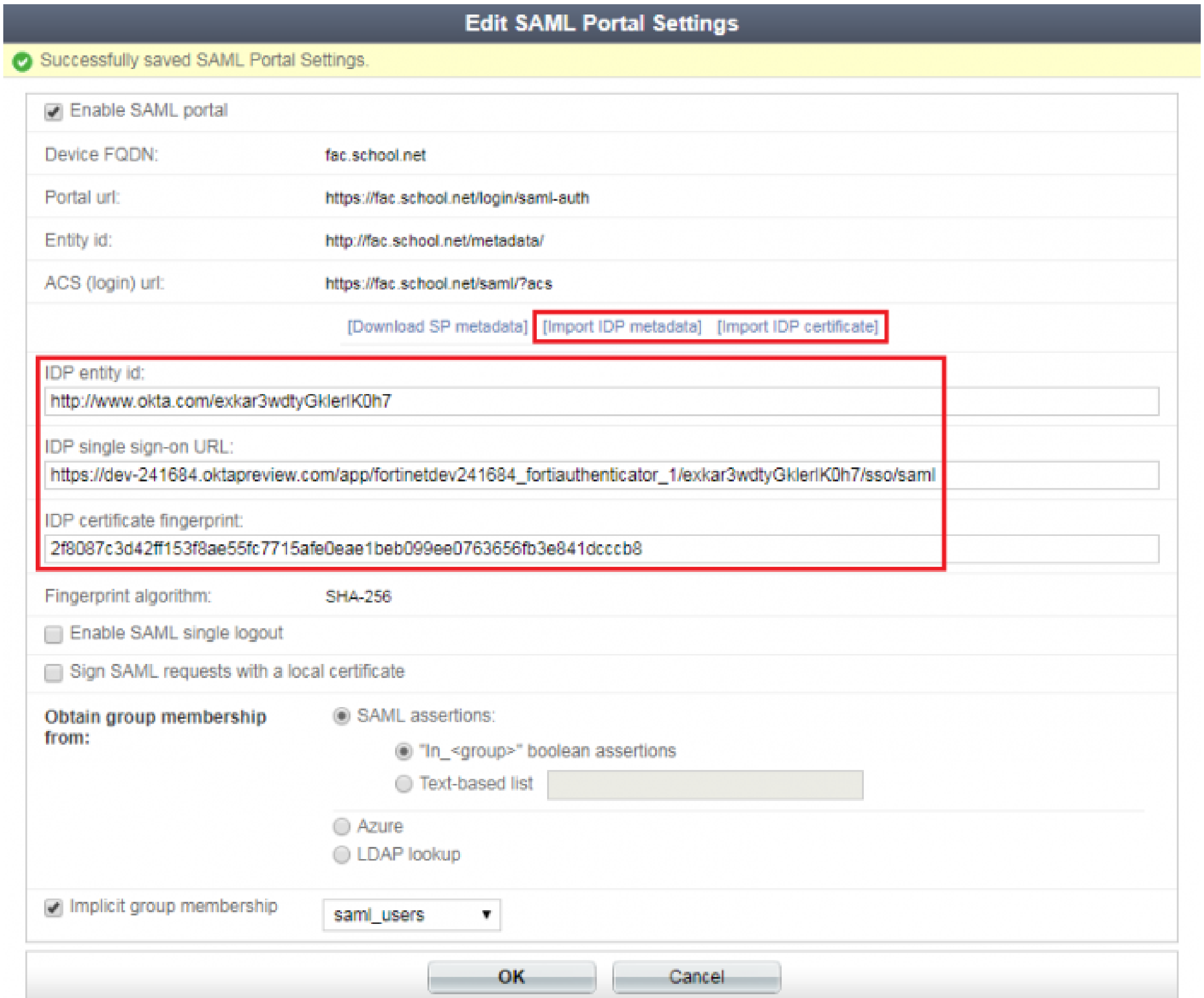


The user is assigned.



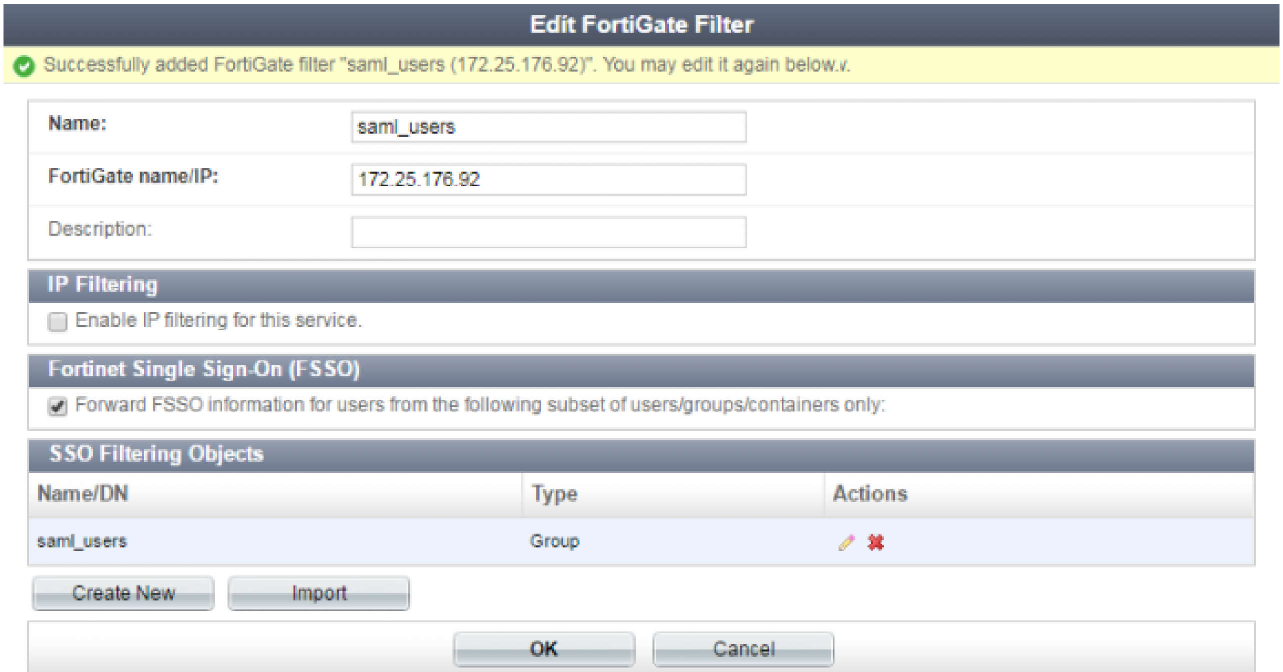
Importing the IDP certificate and metadata on the FortiAuthenticator

1. In FortiAuthenticator, go to *Fortinet SSO Methods > SSO > SAML Authentication* and import the IDP metadata and certificate downloaded earlier.
   This automatically fills the IdP fields (as shown in the example). Click *OK* to save these changes.



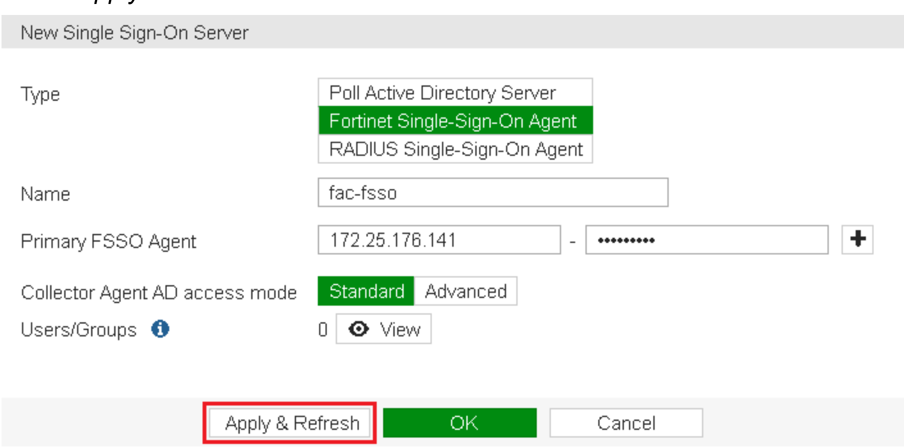
2. Go to *Fortinet SSO Methods > SSO > FortiGate Filtering* and create a new FortiGate filter.
   Enter a name and the FortiGate's wan-interface IP address, and select *OK*.
   Enable *Fortinet Single Sign-On (FSSO)*.
   Select *Create New* to create an SSO group filtering object (as shown in this example).
   The name of the filter must be the same as the group name created for SAML users (*saml_users*). The two user groups must have the exact same name or SSO information will not be pushed to the FortiGate.

Select *OK* to apply all changes.

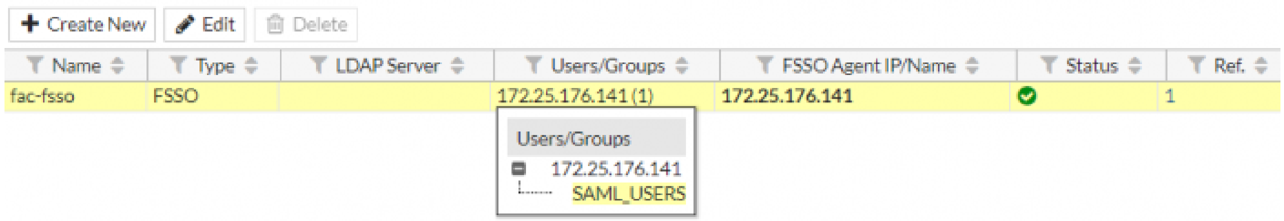


Configuring FSSO on the FortiGate

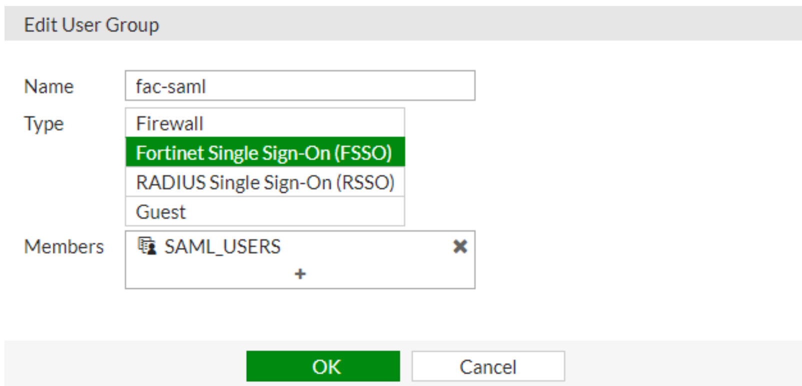
1. On the FortiGate, go to *User & Device* > *Single Sign-On* and select *Create New*.
   Set Type to *Fortinet Single-Sign-On Agent*, enter a *Name*, the FortiAuthenticator's Internet-interface IP address, and the password, which must match the secret key entered at the beginning of the FortiAuthenticator configuration process.
   Select *Apply & Refresh*.



2. The SAML user group name is pushed to the FortiGate from the FortiAuthenticator and appears when you select *View*.
   You might have to wait a few minutes before the user group appears.
3. In the list showing the server, hover over the entry under the *Users/Groups* column and check that the FSSO group has been pushed down.

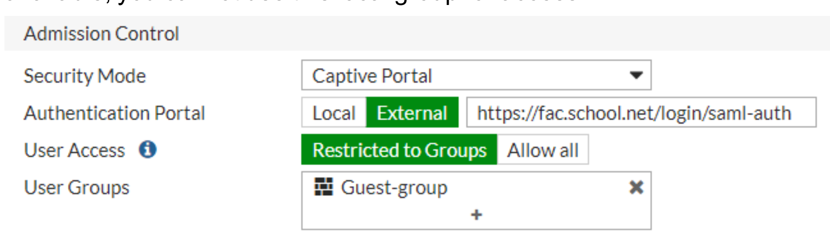


4. Go to *User & Device* > *User Groups* and create a new FSSO user group. Users authenticated via SAML FSSO are in this group.
   Enter a *Name*, set *Type* to *Fortinet Single Sign-On (FSSO)*, and add the FSSO group as one of the *Members*.

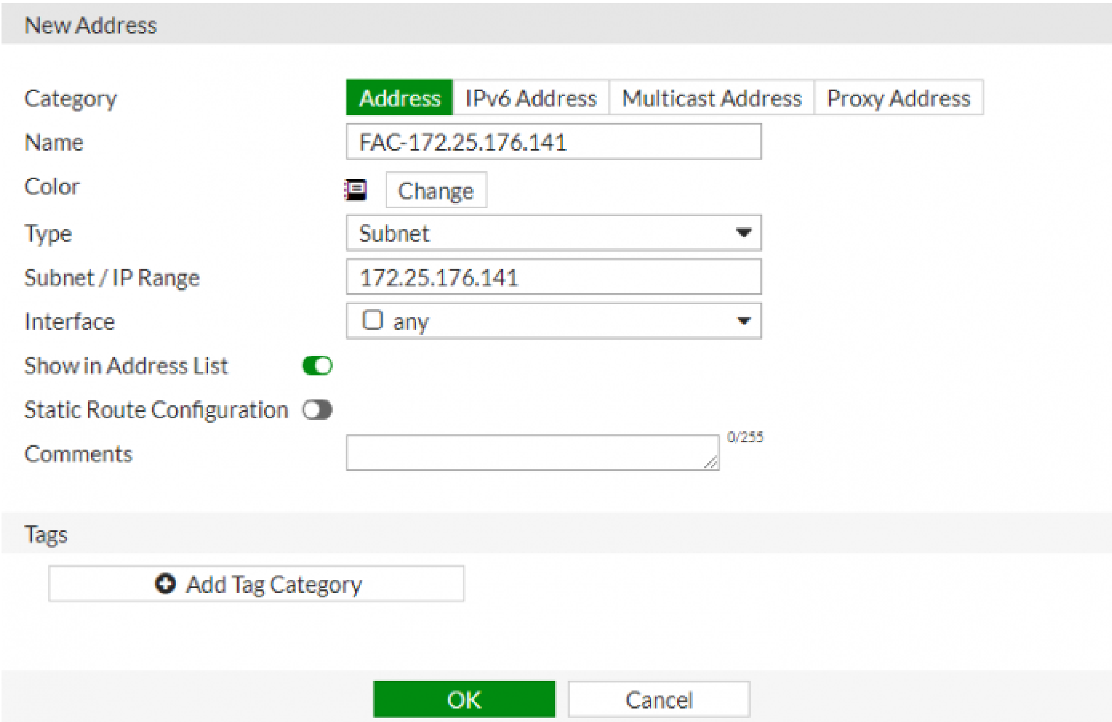


Configuring Captive Portal and security policies

1. On the FortiGate, go to *Network* > *Interfaces* and edit the internal interface.
   Under *Admission Control*, set *Security Mode* to *Captive Portal*.
   Set *Authentication Portal* to *External*, and enter the SAML authentication portal URL.
   Set *User Access* to *Restricted to Groups*, and set *User Groups* to any local group. As the FSSO group is not available, you cannot use this local group for access.



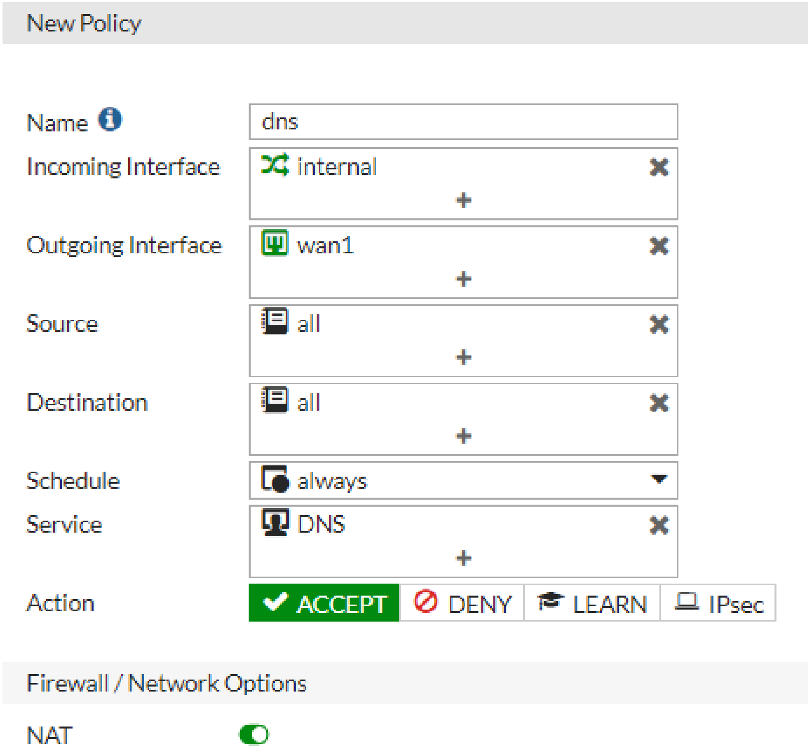
2. Go to *Policy & Objects* > *Addresses* and add the FortiAuthenticator as an address object.

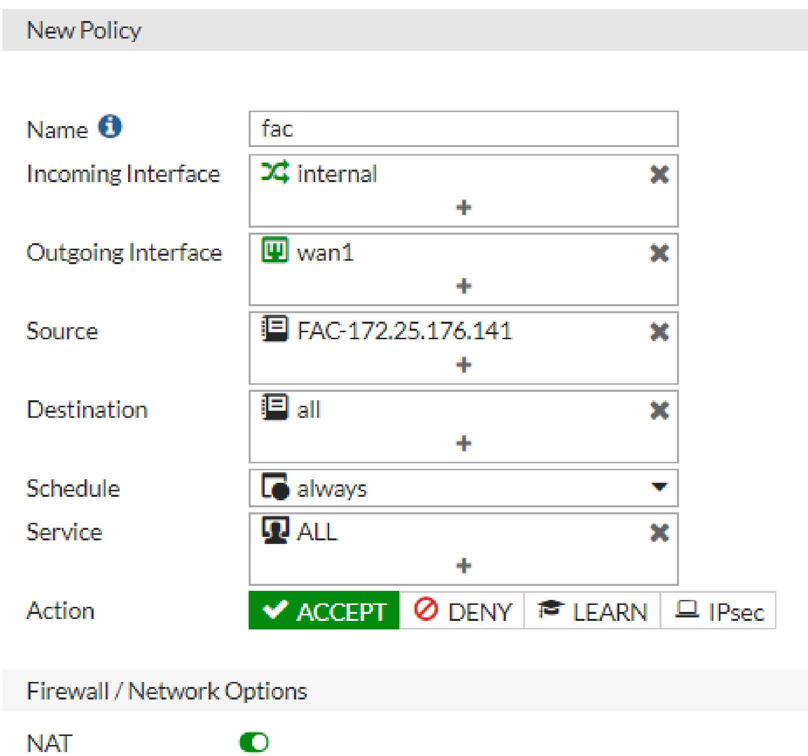


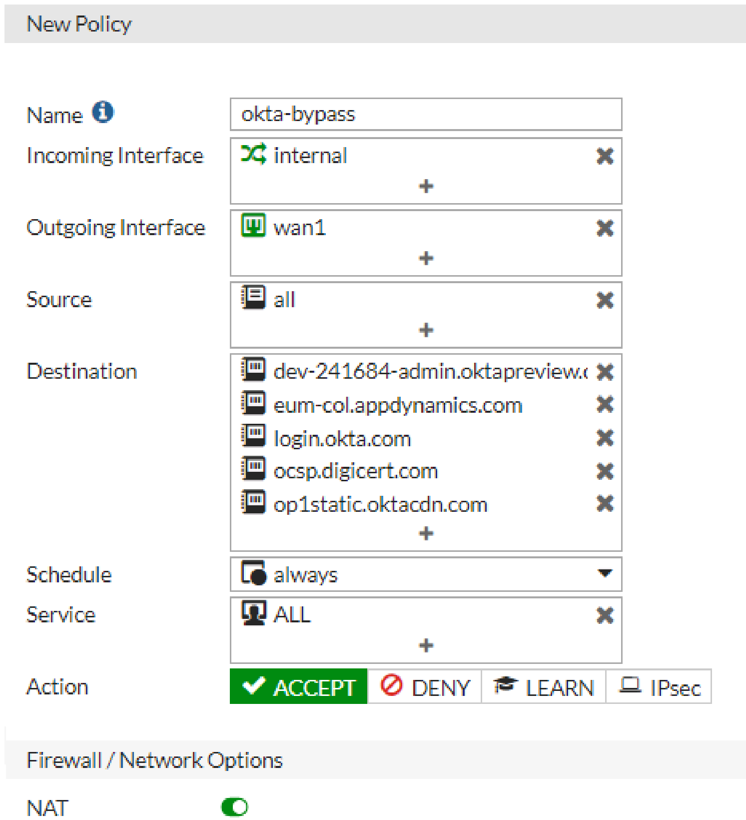
3. Create the following FQDN objects:
   - eum-col.appdynamics.com
   - login.okta.com
   - ocsp.digicert.com
   - op1static.oktacdn.com

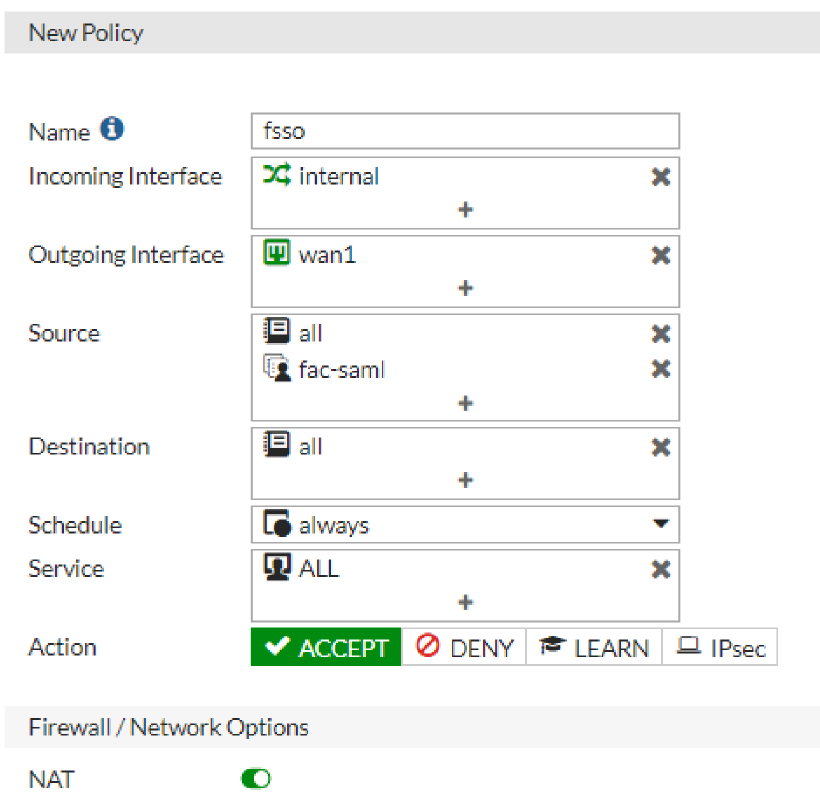
   As these are FQDNs, make sure to set *Type* to *FQDN*.
4. Go to *Policy & Objects* > *IPv4 Policy* and create the policies in these examples:
   - A policy for DNS.
   - A policy for access from FortiAuthenticator.
   - A policy for Okta bypass.

- A policy for FSSO, including the SAML user group.






New Policy
Name
okta-bypass
Incoming Interface
internal
Outgoing Interface
wan1
Source
all
Destination
dev-241684-admin.oktapreview.c
eum-col.appdynamics.com
login.okta.com
ocsp.digicert.com
op1static.oktacdn.com
Schedule
always
Service
ALL
Action
ACCEPT
DENY
LEARN
IPsec
Firewall / Network Options
NAT


New Policy
Name
fsso
Incoming Interface
internal
Outgoing Interface
wan1
Source
all
fac-saml
Destination
all
Schedule
always
Service
ALL
Action
ACCEPT
DENY
LEARN
IPsec
Firewall / Network Options
NAT

5. When finished, right-click each policy except the FSSO policy, select *Edit in CLI*, and enter the following commands for each policy except the FSSO policy:

```
set captive-portal-exempt enable
   next
end
```

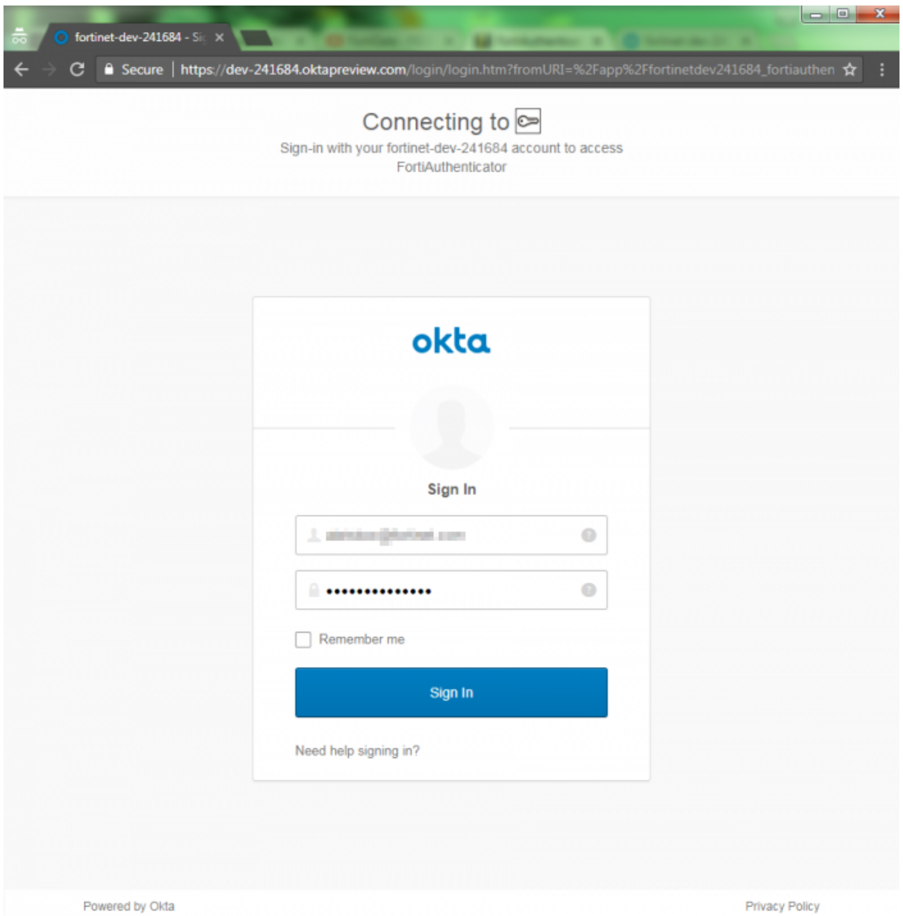
This command exempts users of these policies from the captive portal interface.

Results

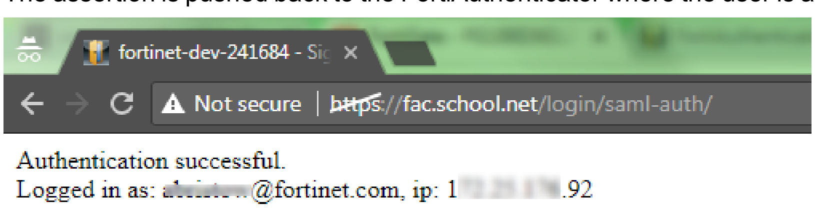
To test the connection, open a browser window and try to browse the Internet. The browser redirects to the FortiAuthenticator SAML portal, which pushes the browser to the SAML IdP.

Alternatively, you can directly navigate to the portal URL.

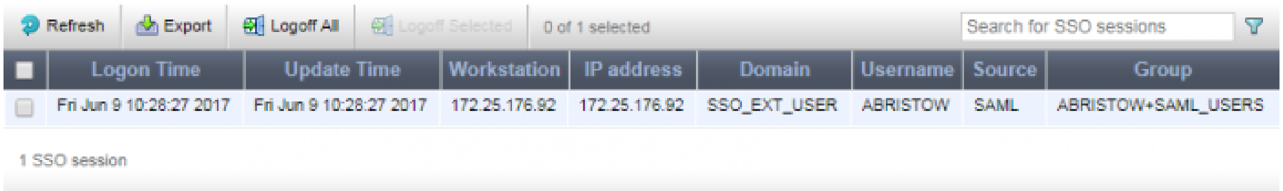
1. Enter the user's credentials and select *Sign In*.



The assertion is pushed back to the FortiAuthenticator where the user is authenticated.



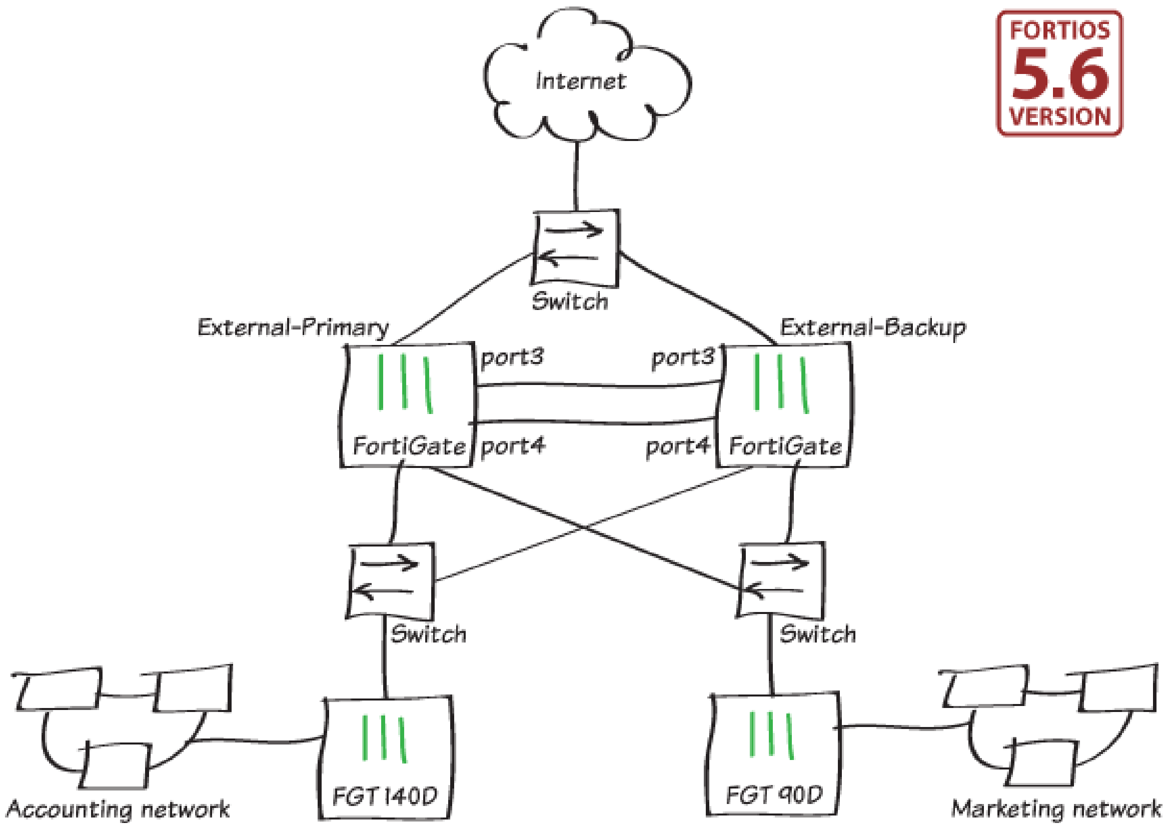
2. On the FortiAuthenticator, go to *Monitor* > *SSO* > *SSO Sessions* to view the user and assigned user group.



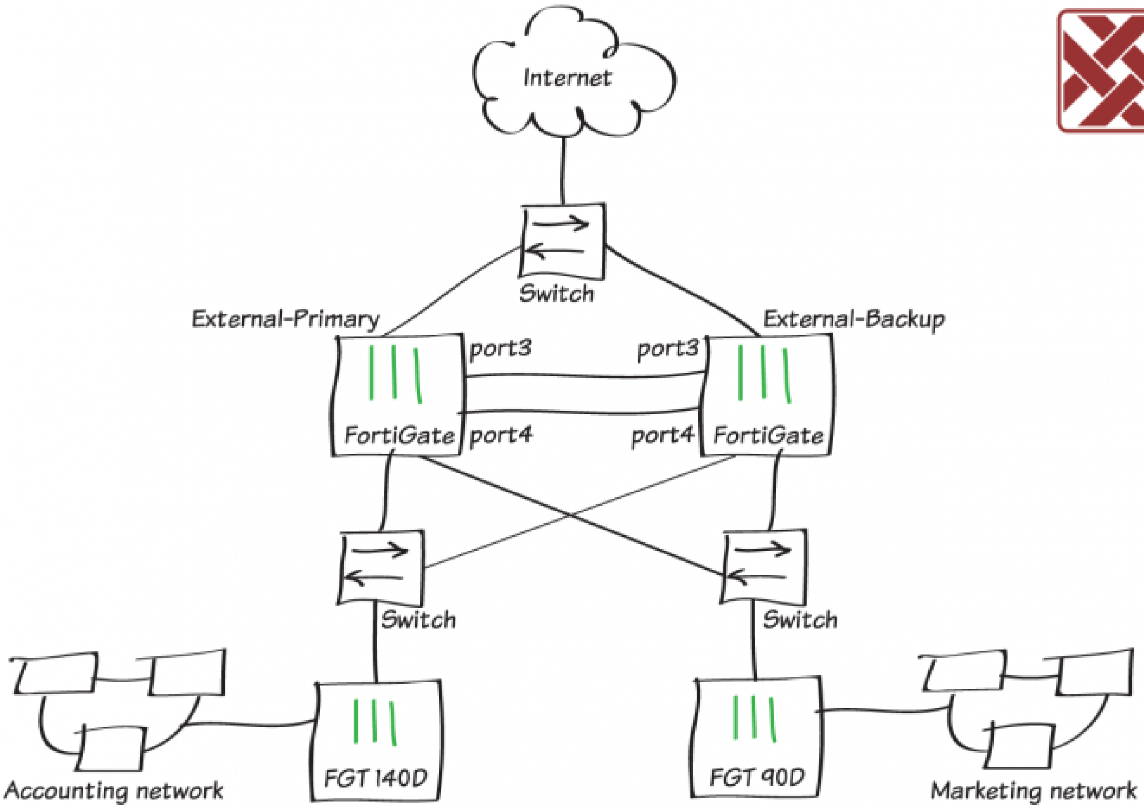
3. On the FortiGate, go to *Monitor* > *Firewall User Monitor* to view user information and confirm that the user has been authenticated via FSSO.

High availability

This section includes recipes about how you can use high availability (HA) with your FortiGate.



High availability with two FortiGates



This example describes how to add a backup FortiGate to a previously installed FortiGate, to form a high availability (HA) cluster to improve network reliability.

Before you begin, check the following:

- The FortiGates are running the same FortiOS firmware version.
- Interfaces are **not** configured to get their addresses from DHCP or PPPoE.
- A switch port is **not** used as an HA heartbeat interface. If necessary, convert the switch port to individual interfaces.

This example is in the Fortinet Security Fabric collection. It can also be used as a standalone recipe.

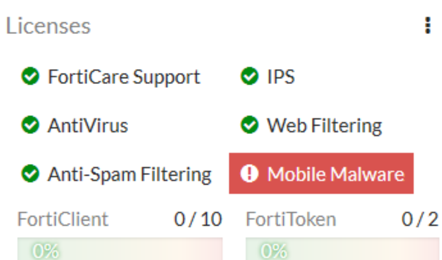
This example uses the FortiGate Clustering Protocol (FGCP) for HA. After you complete this example, the original FortiGate continues to operate as the primary FortiGate and the new FortiGate operates as the backup FortiGate.

For a more advanced HA example that includes CLI steps and involves using advanced options such as override to maintain the same primary FortiGate, see High availability with FGCP (expert) on page 133.

Setting up registration and licensing

1. Make sure both FortiGates are running the same FortiOS firmware version.
   Register and apply licenses to the primary FortiGate before configuring it for HA operation. This includes licensing for *FortiCare Support*, *IPS*, *AntiVirus*, *Web Filtering*, *Mobile Malware*, *FortiClient*, *FortiCloud*, and additional *virtual domains* (VDOMs).
   All FortiGates in the cluster must have the same level of licensing for FortiGuard, FortiCloud, FortiClient, and VDOMs. You can add *FortiToken* licenses at any time because they're synchronized with all cluster members.

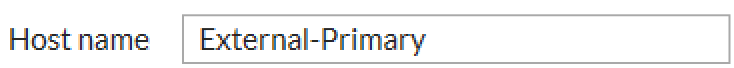
   If the FortiGates in the cluster will run FortiOS Carrier, apply the FortiOS Carrier license before you apply other licenses and before you configure the cluster. When you apply the FortiOS Carrier license, the FortiGate resets its configuration to factory defaults, requiring you to repeat steps performed before applying the license.

2. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is running, the FGCP synchronizes third-party certificates with the backup FortiGate.

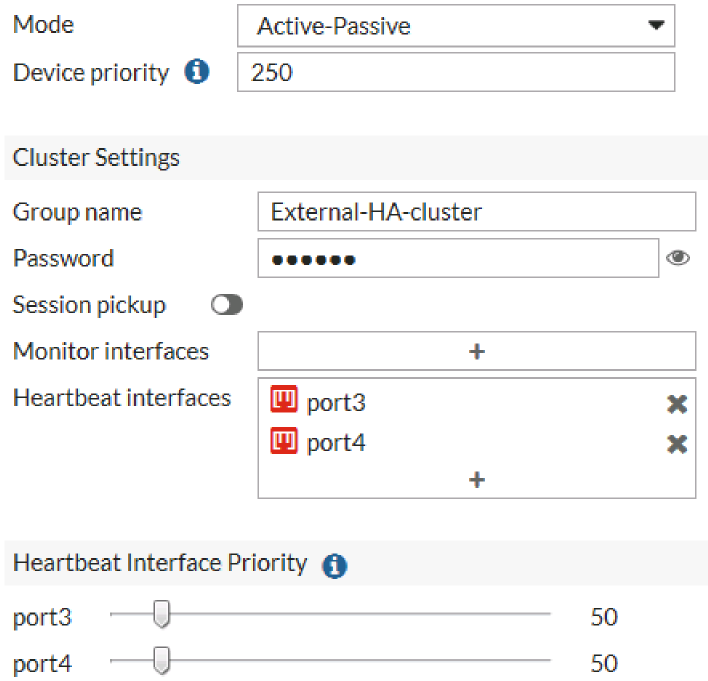
Configuring the primary FortiGate for HA

1. On the primary FortiGate, go to *System* > *Settings* and change the *Host name* to identify this as the primary FortiGate in the HA cluster.

2. Go to *System* > *HA* and set the *Mode*.
   Set the *Mode* to *Active-Passive*.
   Set the *Device priority* to a higher value than the default (in this example, 250) to ensure this FortiGate is always the primary FortiGate.
   Set a *Group name* and *Password*.

Check that the *Heartbeat interfaces* (in this example, *port3* and *port4*) are selected and the *Heartbeat Interface Priority* for each is set to 50.



Since the backup FortiGate isn't available yet, when you save the HA configuration, the primary FortiGate operates normally as a cluster of one.

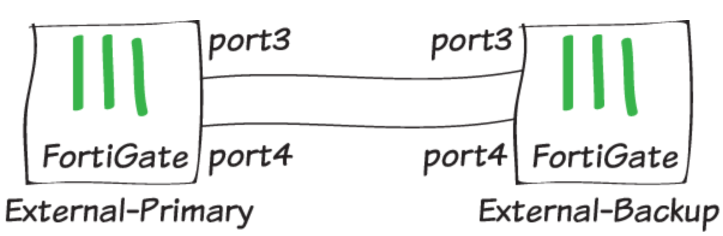
If these steps don't start HA mode, make sure that none of the FortiGate interfaces use DHCP or PPPoE addressing.

If there are other FortiOS HA clusters on your network, you might need to change the cluster group ID using this CLI command:

```
config system ha
   set group-id 25
end
```

Connecting the backup FortiGate

Connect the backup FortiGate to the primary FortiGate and to the network, as shown in the network diagram at the start of this example.



Since making these connections disrupt traffic, make these connections when network traffic is low. If possible, make direct Ethernet connections between the heartbeat interfaces of the two FortiGate units.

This example uses two FortiGate-600Ds and the default heartbeat interfaces (port3 and port4). You can use any interfaces for HA heartbeat interfaces. A best practice is to use interfaces that don't process traffic but this is not a requirement.

If you set up HA between two FortiGates in a VM environment (for example, VMware or Hyper-V), you must enable promiscuous mode and allow MAC address changes for heartbeat communication to work. Since the HA heartbeat interfaces must be on the same broadcast domain, for HA between remote data centers (distributed clustering), you must support layer 2 extensions between the remote data centers using technology such as MPLS or VXLAN.

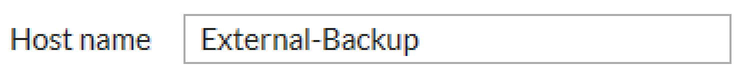
You must use switches between the cluster and the Internet, and between the cluster and the internal networks, as shown in the network diagram. You can use any good quality switches to make these connections. You can also use one switch for all these connections as long as you configure the switch to separate traffic from different networks.

Configuring the backup FortiGate for HA

1. Ensure the backup FortiGate is running the same version firmware as the primary FortiGate.
2. If this is a new FortiGate that has never been used, you can skip this step.
   Reset the backup FortiGate to factory default settings using the following CLI command:
   ```
   execute factoryreset
   ```

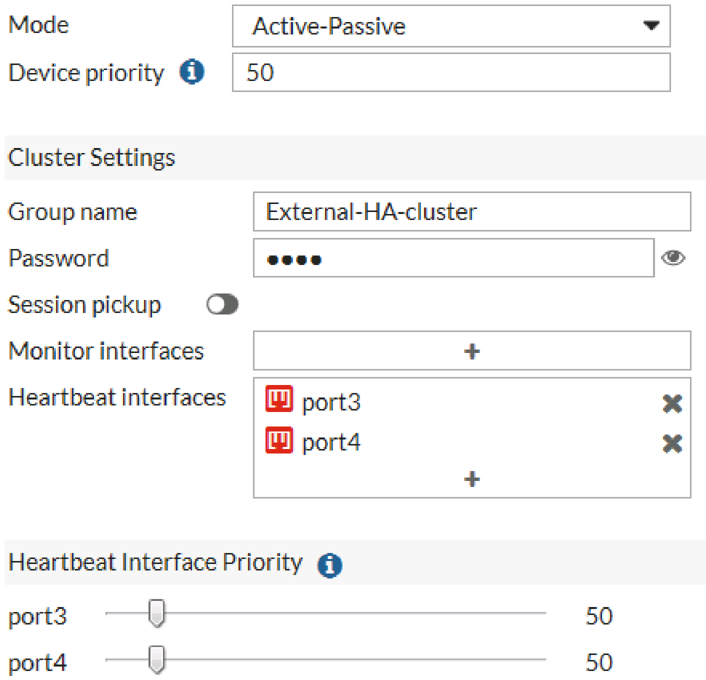
   If the FortiGates in the cluster will run FortiOS Carrier, apply the FortiOS Carrier license before you apply other licenses and before you configure the cluster. When you apply the FortiOS Carrier license, the FortiGate resets its configuration to factory defaults, requiring you to repeat steps performed before applying the license.

3. On the backup FortiGate, go to *System* > *Settings* and change the *Host name* to identify this as the backup FortiGate.



4. Go to *System* > *HA* and duplicate the HA configuration of the primary FortiGate (except for *Device priority*).
   Set *Mode* to *Active-Passive*.
   Set the *Device Priority* to a lower value than the default to ensure this FortiGate is always the backup FortiGate.
   Set the same *Group name* and *Password* as the primary FortiGate.

Check that the same two *Heartbeat interfaces* (port3 and port4) are selected and the *Heartbeat Interface Priority* for each is set to 50.



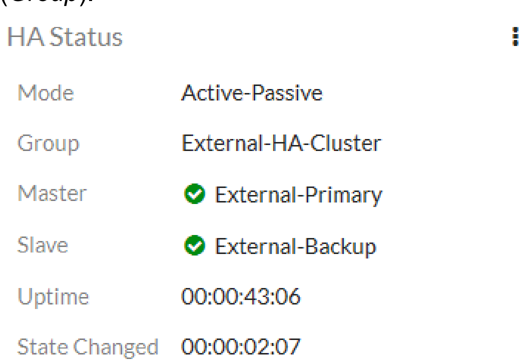
5. If you changed the cluster group ID of the primary FortiGate, change the cluster group ID for the backup FortiGate to match it, using this CLI command:

```
config system ha
   set group-id 25
end
```

When you save the HA configuration of the backup FortiGate, if the heartbeat interfaces are connected, the FortiGates will find each other and form an HA cluster. Network traffic might be disrupted when the cluster negotiates the connection.

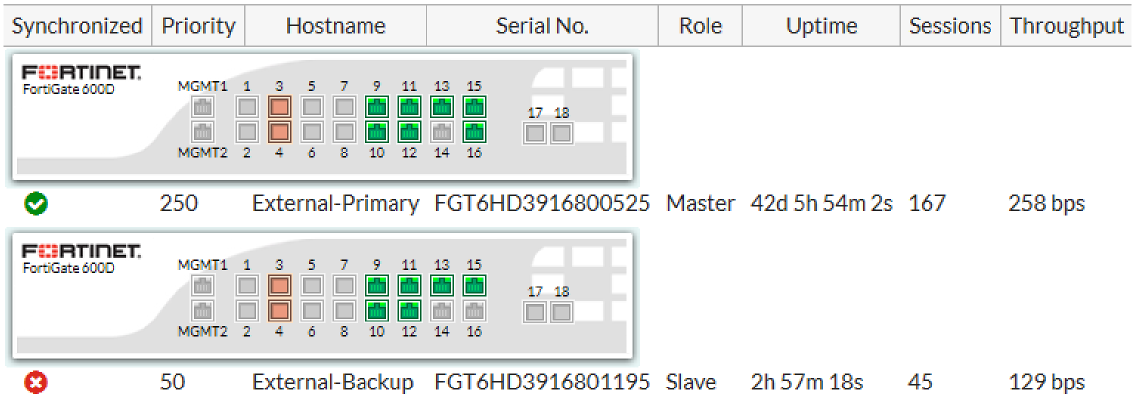
Viewing the status of the HA cluster

1. In the primary FortiGate *Dashboard*, the *HA Status* widget shows the cluster mode (*Mode*) and group name (*Group*).



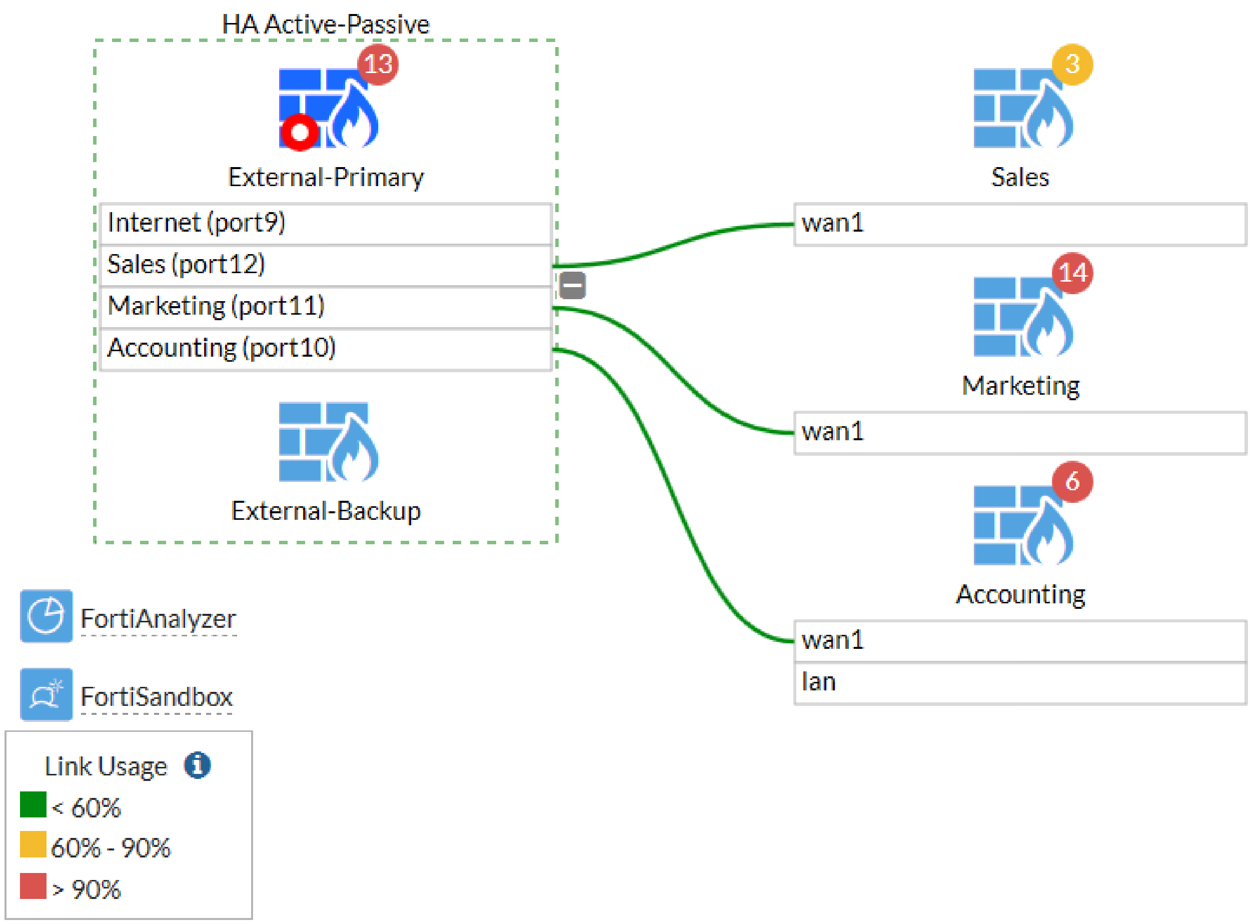
It also shows the host name of the primary FortiGate (*Master*), which you can hover over to verify that the cluster is synchronized and operating normally. You can click on the widget to change the HA configuration or view a list of recently recorded cluster events such as members joining or leaving the cluster.

2. Click the *HA Status* widget and select *Configure settings in System* > *HA* (or go to *System* > *HA*) to view the cluster status.



Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
✔	250	External-Primary	FGT6HD3916800525	Master	42d 5h 54m 2s	167	258 bps
✖	50	External-Backup	FGT6HD3916801195	Slave	2h 57m 18s	45	129 bps

If the cluster is part of a Security Fabric, the FortiView Physical and Logical Topology views show information about the cluster status.



Results

All traffic should flow through the primary FortiGate. If the primary FortiGate becomes unavailable, traffic fails over to the backup FortiGate. When the primary FortiGate rejoins the cluster, the backup FortiGate should continue to operate as the primary FortiGate.

To test this, ping a reliable IP address from a PC on the internal network. After a moment, power off the primary FortiGate.

If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover.

You see a momentary pause in the ping results until traffic diverts to the backup FortiGate, allowing the ping traffic to continue.

```
64 bytes from 184.25.76.114: icmp_seq=69 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=70 ttl=52 time=8.822 ms\
64 bytes from 184.25.76.114: icmp_seq=71 ttl=52 time=9.034 ms\
64 bytes from 184.25.76.114: icmp_seq=72 ttl=52 time=9.536 ms\
64 bytes from 184.25.76.114: icmp_seq=73 ttl=52 time=8.877 ms\
64 bytes from 184.25.76.114: icmp_seq=74 ttl=52 time=8.901 ms\
Request timeout for icmp_seq 75\
64 bytes from 184.25.76.114: icmp_seq=76 ttl=52 time=8.860 ms\
64 bytes from 184.25.76.114: icmp_seq=77 ttl=52 time=9.174 ms\
64 bytes from 184.25.76.114: icmp_seq=78 ttl=52 time=10.108 ms\
64 bytes from 184.25.76.114: icmp_seq=79 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=80 ttl=52 time=10.861 ms\
64 bytes from 184.25.76.114: icmp_seq=81 ttl=52 time=10.757 ms\
64 bytes from 184.25.76.114: icmp_seq=82 ttl=52 time=8.158 ms\
64 bytes from 184.25.76.114: icmp_seq=83 ttl=52 time=8.639 ms}
```

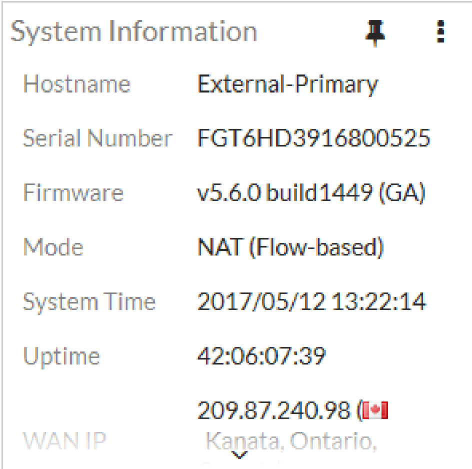
You can log into the cluster GUI or CLI using the same IP address as you had been using to the log into the primary FortiGate. If the primary FortiGate is powered off, you will be logging into the backup FortiGate. Check the host name to verify the FortiGate that you have logged into. The FortiGate continues to operate in HA mode and if you restart the primary FortiGate, after a few minutes it should rejoin the cluster and operate as the backup FortiGate. Traffic should not be disrupted when the restarted primary unit rejoins the cluster.

(Optional) Upgrading the firmware for the HA cluster

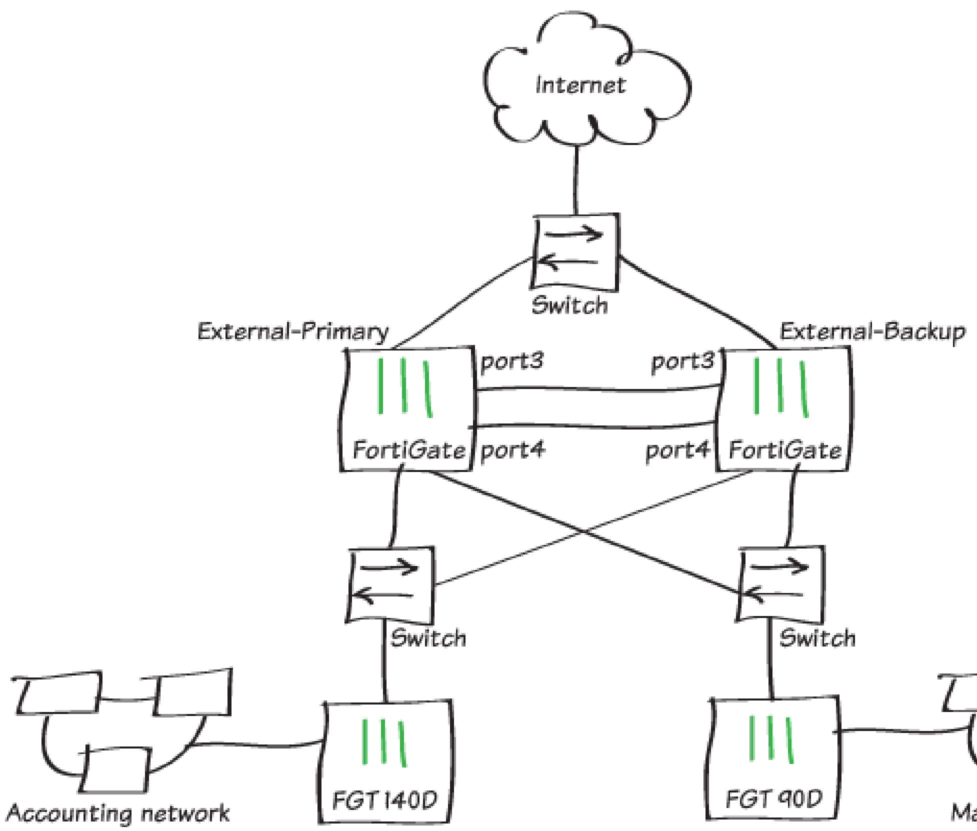
Upgrading the firmware on the primary FortiGate automatically upgrades the firmware on the backup FortiGate. Upgrading firmware causes minimal traffic disruption. Before upgrading firmware, always review the Release Notes first.

1. Click the *System Information* widget and select *Update firmware in System > Firmware*.
2. Back up the configuration and update the firmware from FortiGuard or upload a firmware image file.
   The firmware installs onto both the primary and backup FortiGates.

3. After the upgrade is complete, verify that the *System Information* widget shows the new firmware version.



High availability with FGCP (expert)



This example describes how to enhance the reliability of a network protected by a FortiGate by adding a second FortiGate and setting up a FortiGate Clustering Protocol (FGCP) high availability (HA) cluster.

First, configure the FortiGate already on the network to become the primary FortiGate by:

1. Licensing the FortiGate if required.
2. Enabling HA.
3. Increasing its device priority.
4. Enabling override.

Then prepare the new FortiGate by:

1. Setting it to factory defaults to reset any configuration changes.
2. Licensing the FortiGate if required.
3. Enabling HA without changing the device priority and without enabling override.
4. Connecting it to the FortiGate already on the network.

The new FortiGate becomes the backup FortiGate and its configuration is overwritten by the primary FortiGate.

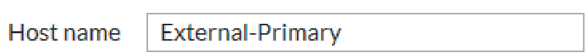
This example describes best practices for configuring HA and includes extra steps that are not required for a basic HA setup. For an example of setting up a basic HA, see High availability with two FortiGates on page 126.

Before you start, ensure the FortiGates are running the same FortiOS firmware version and their interfaces are not configured to get addresses from DHCP or PPPoE.

The FGCP does not support using a switch interface for the HA heartbeat. As an alternative to using the lan4 and lan5 interfaces as described in this example, you can use the wan1 and wan2 interfaces for the HA heartbeat.

Configuring the primary FortiGate

1. On the primary FortiGate, go to *System* > *Settings* and change the *Host name* to identify this as the primary FortiGate in the HA cluster.

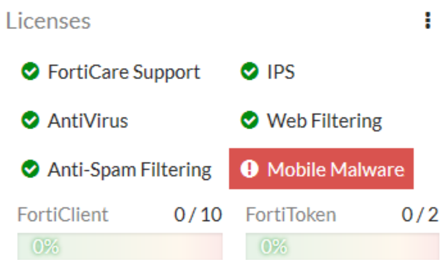
   

   You can also enter this CLI command:

   ```
   config system global
      set hostname External-Primary
   end
   ```

2. Register and apply licenses to the primary FortiGate before configuring it for HA operation. This includes licensing for *FortiCare Support*, *IPS*, *AntiVirus*, *Web Filtering*, *Mobile Malware*, *FortiClient*, *FortiCloud*, and additional *virtual domains* (VDOMs).
   All FortiGates in the cluster must have the same level of licensing for FortiGuard, FortiCloud, FortiClient, and VDOMs. You can add *FortiToken* licenses at any time because they're synchronized with all cluster members.

   If the FortiGates in the cluster will run FortiOS Carrier, apply the FortiOS Carrier license before you apply other licenses and before you configure the cluster. When you apply the FortiOS Carrier license, the FortiGate resets its configuration to factory defaults, requiring you to repeat steps performed before applying the license.



3. You can also install any third-party certificates on the primary FortiGate before forming the cluster. Once the cluster is formed, third-party certificates are synchronized with the backup FortiGate(s).
4. Enter these CLI commands to set the HA mode to active-passive, set a group id, group name and password, set a higher device priority (for example, 250), and enable override.

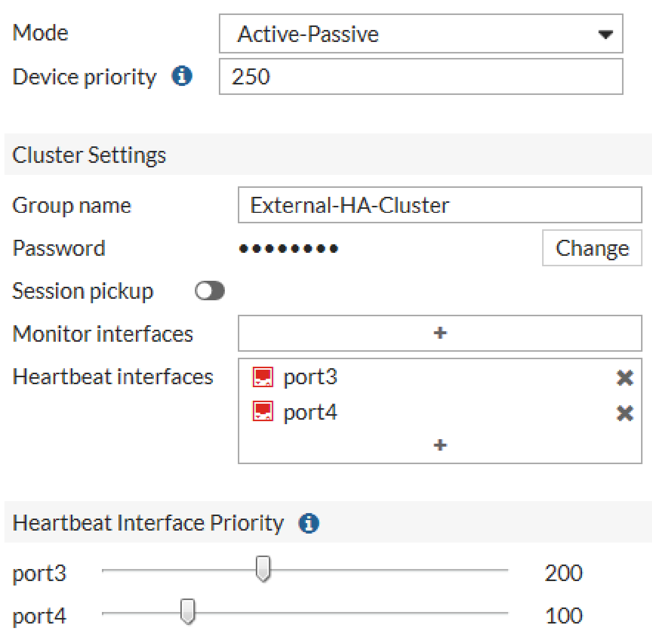
```
config system ha
   set mode a-p
   set group-id 25
   set group-name External-HA-Cluster
   set password <password>
   set priority 250
   set override enable
   set hbdev port3 200 port4 100
end
```

Enabling override and increasing the device priority sets this FortiGate to always be the primary unit.

If you have more than one cluster on the same network, set a different group id for each cluster. Changing the group id changes the cluster interface virtual MAC addresses. If your group id causes a MAC address conflict on your network, you can select a different group id.

This command also selects `port3` and `port4` to be the heartbeat interfaces and sets their priorities to 200 and 100. Although not required, a best practice is to set different priorities for the heartbeat interfaces.

You can configure most of these settings using the GUI in *System* > *HA*. You must configure the group-id and override using the CLI.



When you enable HA, each FortiGate negotiates to establish an HA cluster. You might temporarily lose connectivity during FGCP negotiation and the MAC addresses of the FortiGate interfaces change to HA virtual MAC addresses.

If these steps don't start HA mode, make sure that none of the FortiGate's interfaces use DHCP or PPPoE addressing.

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or deleting all ARP table entries). You can usually delete the ARP table from a command prompt using a command similar to `arp -d`.

The FGCP uses virtual MAC addresses for failover. The virtual MAC address assigned to each FortiGate interface depends on the HA group ID. A group ID of 100 sets FortiGate interfaces to the following MAC addresses: 00:09:0f:09:64:00, 00:09:0f:09:64:01, 00:09:0f:09:64:02 and so on. For details, see Cluster virtual MAC addresses.

You can verify that the FGCP has set the virtual MAC addresses by viewing the configuration of each FortiGate interface from the GUI (in *Network* > *Interfaces*) or by entering the following CLI command:

```
get hardware nic port3
...
Current_HWaddr 00:09:0f:09:64:01
Permanent_HWaddr 70:4c:a5:98:11:54
...
```

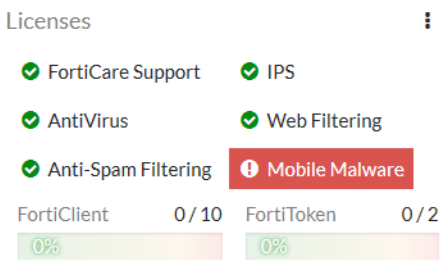
You can also use the `diagnose hardware deviceinfo nic port3` command to display this information.

The output shows the current hardware (MAC) address (the virtual MAC set by the FGCP) and the permanent hardware (MAC) address for the interface.

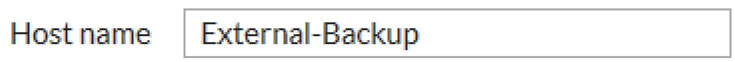
Configuring the backup FortiGate

1. Ensure the backup FortiGate is running the same version firmware as the primary FortiGate.
2. If this is a new FortiGate that has never been used, you can skip this step.
   Reset the backup FortiGate to factory default settings using the following CLI command:
   `execute factoryreset`
3. Register and apply licenses to the primary FortiGate before configuring it for HA operation. This includes licensing for *FortiCare Support*, *IPS*, *AntiVirus*, *Web Filtering*, *Mobile Malware*, *FortiClient*, *FortiCloud*, and additional *virtual domains* (VDOMs).
   All FortiGates in the cluster must have the same level of licensing for FortiGuard, FortiCloud, FortiClient, and VDOMs. You can add *FortiToken* licenses at any time because they're synchronized with all cluster members.

If the FortiGates in the cluster will run FortiOS Carrier, apply the FortiOS Carrier license before you apply other licenses and before you configure the cluster. When you apply the FortiOS Carrier license, the FortiGate resets its configuration to factory defaults, requiring you to repeat steps performed before applying the license.



4. On the backup FortiGate, go to *System > Settings* and change the *Host name* to identify this as the backup FortiGate.



You can also enter this CLI command:

```
config system global
   set hostname External-Backup
end
```

5. Duplicate the primary FortiGate HA settings, except set the *Device priority* to a lower value (for example, 50) and do not enable override.

```
config system ha
   set mode a-p
   set group-id 25
   set group-name External-HA-Cluster
   set password <password>
   set priority 50
   set hbdev port3 200 port4 100
end
```

When you enable HA, each FortiGate negotiates to establish an HA cluster. You might temporarily lose connectivity during FGCP negotiation and the MAC addresses of the FortiGate interfaces change to HA virtual MAC addresses.

If these steps don't start HA mode, make sure that none of the FortiGate's interfaces use DHCP or PPPoE addressing.

If the group ID is the same, the backup FortiGate interfaces get the same virtual MAC addresses as the primary FortiGate. You can check *Network > Interfaces* on the GUI or use the `get hardware nic` command to verify.

Connecting the primary and backup FortiGates

Connect the backup FortiGate to the primary FortiGate and to the network as shown in the network diagram at the start of this example. Making these connections disrupts network traffic as you disconnect and reconnect cables.

You must use switches between the cluster and the Internet, and between the cluster and the internal networks, as shown in the network diagram. You can use any good quality switches to make these connections. You can also use one switch for all these connections as long as you configure the switch to separate traffic from different networks.

This example shows the recommended configuration of direct connections between the port3 heartbeat interfaces and between the port4 heartbeat interfaces. A best practice is to use interfaces that don't process traffic but this is not a requirement.

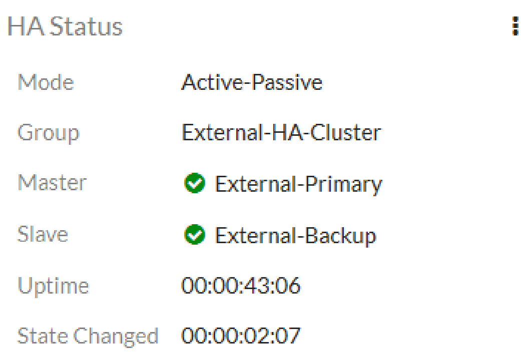
When you connect the heartbeat interfaces and power on the FortiGates, they find each other and negotiate to form a cluster. The primary FortiGate synchronizes its configuration to the backup FortiGate. The cluster forms automatically with minimal or no additional disruption to network traffic.

The cluster has the same IP addresses as the primary FortiGate. You can log into the cluster by logging into the primary FortiGate CLI or GUI using one of the original IP addresses of the primary FortiGate.

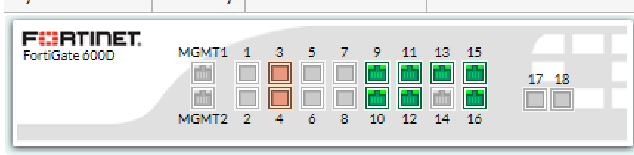
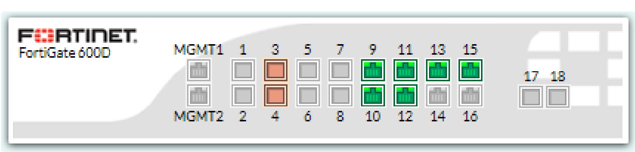
Checking cluster operation

Check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration.

1. Log into the primary FortiGate CLI and enter this command:
   `diagnose sys ha checksum cluster`
   The command output lists all cluster members' configuration checksums. If both cluster members have identical checksums, you can be sure that their configurations are synchronized. If the checksums are different, wait a short while and enter the command again. Repeat until the checksums are identical. It may take a while for configurations to synchronize.
   If the checksums never become identical, troubleshoot using Synchronizing the configuration or Fortinet Support.
2. The *HA Status* dashboard widget also shows synchronization status. Hover over the host names of each FortiGate in the widget to verify that they are synchronized and both have the same checksum.



3. To view more information about the cluster status, go to the *HA Status* widget and select *Configure Settings in System > HA*, or go to *System > HA*.

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
							
✓	250	External-Primary	FGT6HD3916800525	Master	42d 5h 54m 2s	167	258 bps
							
✗	50	External-Backup	FGT6HD3916801195	Slave	2h 57m 18s	45	129 bps

Disabling override (recommended)

When the checksums are identical, disable override on the primary FortiGate by entering the following command:

```
config system ha
   set override disable
end
```

Results

All traffic should flow through the primary FortiGate. If the primary FortiGate becomes unavailable, traffic fails over to the backup FortiGate. When the primary FortiGate rejoins the cluster, the backup FortiGate should continue to operate as the primary FortiGate.

To test this, ping a reliable IP address from a PC on the internal network. After a moment, power off the primary FortiGate.

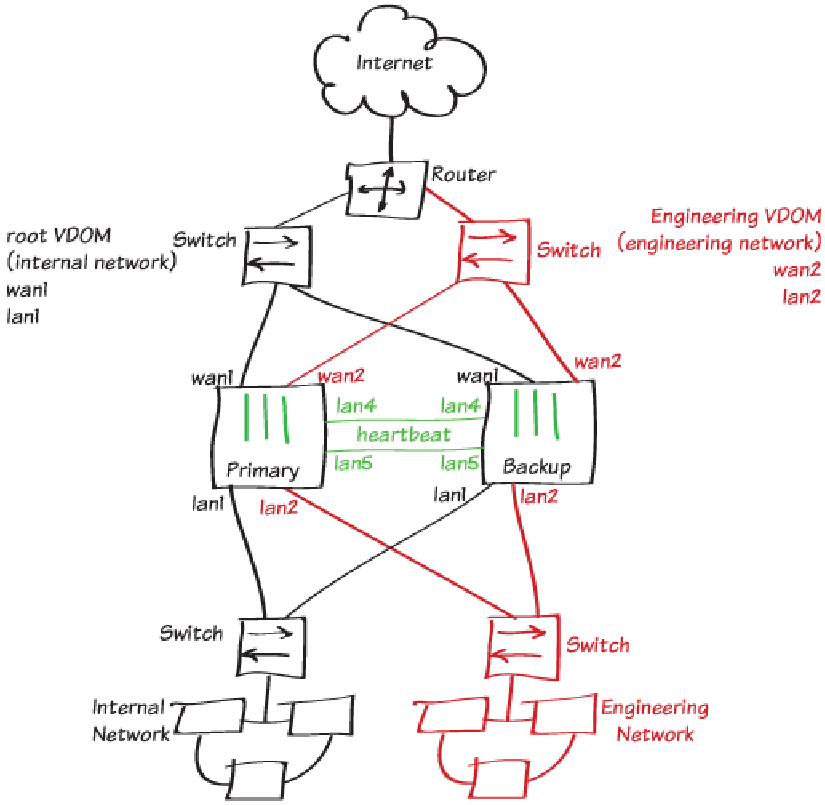
If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover.

You see a momentary pause in the ping results until traffic diverts to the backup FortiGate, allowing the ping traffic to continue.

```
64 bytes from 184.25.76.114: icmp_seq=69 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=70 ttl=52 time=8.822 ms\
64 bytes from 184.25.76.114: icmp_seq=71 ttl=52 time=9.034 ms\
64 bytes from 184.25.76.114: icmp_seq=72 ttl=52 time=9.536 ms\
64 bytes from 184.25.76.114: icmp_seq=73 ttl=52 time=8.877 ms\
64 bytes from 184.25.76.114: icmp_seq=74 ttl=52 time=8.901 ms\
Request timeout for icmp_seq 75\
64 bytes from 184.25.76.114: icmp_seq=76 ttl=52 time=8.860 ms\
64 bytes from 184.25.76.114: icmp_seq=77 ttl=52 time=9.174 ms\
64 bytes from 184.25.76.114: icmp_seq=78 ttl=52 time=10.108 ms\
64 bytes from 184.25.76.114: icmp_seq=79 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=80 ttl=52 time=10.861 ms\
64 bytes from 184.25.76.114: icmp_seq=81 ttl=52 time=10.757 ms\
64 bytes from 184.25.76.114: icmp_seq=82 ttl=52 time=8.158 ms\
64 bytes from 184.25.76.114: icmp_seq=83 ttl=52 time=8.639 ms}
```

You can log into the cluster GUI or CLI using the same IP address as you had been using to the log into the primary FortiGate. If the primary FortiGate is powered off, you will be logging into the backup FortiGate. Check the host name to verify the FortiGate that you have logged into. The FortiGate continues to operate in HA mode and if you restart the primary FortiGate, after a few minutes it should rejoin the cluster and operate as the backup FortiGate. Traffic should not be disrupted when the restarted primary unit rejoins the cluster.

FGCP Virtual Clustering with two FortiGates (expert)



This example describes how to set up a FortiGate Clustering Protocol (FGCP) virtual clustering configuration with two FortiGates to provide redundancy and failover protection for two networks. The FortiGate configuration includes two VDOMs. The root VDOM handles internal network traffic and the engineering VDOM handles engineering network traffic. This example shows a simple two-VDOM configuration. The same principles apply to a virtual cluster with more VDOMs.

In this virtual cluster configuration, the primary FortiGate processes all internal network traffic and the backup FortiGate processes all engineering network traffic. Virtual clustering enables override and uses device priorities to distribute traffic between the primary and backup FortiGates. For details, see Configuring virtual clustering.

This example uses two FortiGate-51Es. FortiGate-51Es have a 5-port switch LAN interface. Before configuring HA, the LAN interface was converted to five separate interfaces (lan1 to lan5).

Before adding the management VDOM to virtual cluster 2, ensure you have added all the backup FortiGates and they have joined the cluster; otherwise the configuration of the primary FortiGate might be overwritten by the backup FortiGate.

Before you start, ensure the FortiGates are running the same FortiOS firmware version and their interfaces are not configured to get addresses from DHCP or PPPoE.

The FGCP does not support using a switch interface for the HA heartbeat. As an alternative to using the lan4 and lan5 interfaces as described in this example, you can use the wan1 and wan2 interfaces for the HA heartbeat.

For an example of how to configure virtual clustering by converting a FortiGate with VDOMs to HA mode and then adding another FortiGate to form a cluster, see High availability with FGCP (expert) on page 133.

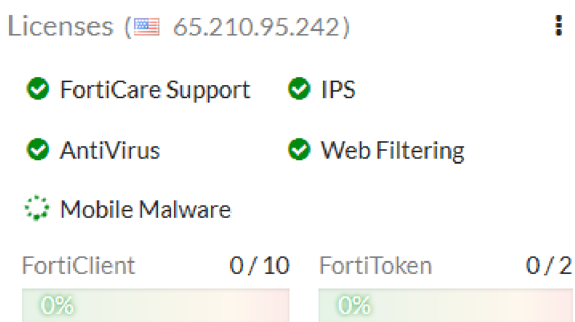
Preparing the FortiGates

1. If required, upgrade the firmware running on the FortiGates. All FortiGates must be running the same version of FortiOS.
2. If this is a new FortiGate that has never been used, you can skip this step.
   Reset the backup FortiGate to factory default settings using the following CLI command:
   ```
   execute factoryreset
   ```
3. In some cases, after resetting to factory defaults, you might want to make some initial configuration changes to connect the FortiGates to the network. In this example, the LAN switch on the FortiGate-51Es was converted to separate lan1 to lan5 interfaces.
4. On the primary FortiGate, go to *System* > *Settings* and change the *Host name* to identify this as the primary FortiGate in the HA cluster.
   

5. On the backup FortiGate, go to *System* > *Settings* and change the *Host name* to identify this as the backup FortiGate.
   

   You can also use the CLI to change the host name. From the Primary FortiGate:
   ```
   config system global
     set hostname Primary
   end
   ```
   From the Backup-1 FortiGate:
   ```
   config system global
     set hostname Backup
   end
   ```
6. Register and apply licenses to the primary FortiGate before configuring it for HA operation. This includes licensing for *FortiCare Support*, *IPS*, *AntiVirus*, *Web Filtering*, *Mobile Malware*, *FortiClient*, *FortiCloud*, and additional *virtual domains* (VDOMs).
   All FortiGates in the cluster must have the same level of licensing for FortiGuard, FortiCloud, FortiClient, and VDOMs. You can add *FortiToken* licenses at any time because they're synchronized with all cluster members.

   If the FortiGates in the cluster will run FortiOS Carrier, apply the FortiOS Carrier license before you apply other licenses and before you configure the cluster. When you apply the FortiOS Carrier license, the FortiGate resets its configuration to factory defaults, requiring you to repeat steps performed before applying the license.



Configuring clustering

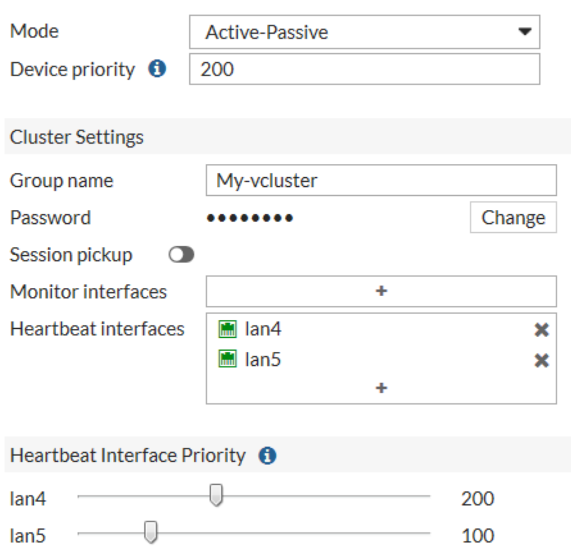
1. On the primary FortiGate, enter the following CLI command to set the HA mode to active-passive, set a group-id, group name and password, increase the device priority to 200, enable override, and configure the heartbeat interfaces (lan4 and lan5 in this example).

```
config system ha
   set mode a-p
   set group-id 88
   set group-name My-vcluster
   set password <password>
   set priority 200
   set override enable
   set hbdev lan4 200 lan5 100
end
```

Enabling override and increasing the device priority sets this FortiGate to always be the primary unit.

If you have more than one cluster on the same network, set a different group id for each cluster. Changing the group id changes the cluster interface virtual MAC addresses. If your group id causes a MAC address conflict on your network, you can select a different group id.

You can configure most of these settings using the GUI in *Global* > *System* > *HA*. You must configure the group-id and override using the CLI.



2. On the backup FortiGate, duplicate the primary FortiGate HA mode, group-id, group-name, password, override, and heartbeat device settings. Set the device priority to 50.

```
config system ha
   set mode a-p
   set group-id 88
   set group-name My-vcluster
   set password <password>
   set priority 50
   set override enable
   set hbdev lan4 200 lan5 100
end
```

When you enable HA, each FortiGate negotiates to establish an HA cluster. You might temporarily lose connectivity during FGCP negotiation and the MAC addresses of the FortiGate interfaces change to HA virtual MAC addresses.

If these steps don't start HA mode, make sure that none of the FortiGate's interfaces use DHCP or PPPoE addressing.

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or deleting all ARP table entries). You can usually delete the ARP table from a command prompt using a command similar to `arp -d`.

The FGCP uses virtual MAC addresses for failover. The virtual MAC address assigned to each FortiGate interface depends on the HA group ID. A group ID of 88 sets FortiGate interfaces to the following MAC addresses: 00:09:0f:09:58:00, 00:09:0f:09:58:01, 00:09:0f:09:58:02 and so on. For details, see Cluster virtual MAC addresses.

You can verify that the FGCP has set the virtual MAC addresses by viewing the configuration of each FortiGate interface from the GUI (in *Network > Interfaces*) or by entering the following CLI command (shown below for lan2 on a FortiGate-51E):

```
get hardware nic lan2
...
Current_HWaddr 00:09:0f:09:58:01
Permanent_HWaddr 70:4c:a5:98:11:54
...
```

You can also use the `diagnose hardware deviceinfo nic lan2` command to display this information.

The output shows the current hardware (MAC) address (the virtual MAC set by the FGCP) and the permanent hardware (MAC) address for the interface.

Connecting and verifying cluster operation

Connect the FortiGates together and to your networks as shown in the network diagram at the start of this example. Making these connections disrupts network traffic as you disconnect and re-connect cables.

You must use switches between the cluster and the Internet, between the cluster and the internal networks, and between the cluster and the engineering network as shown in the network diagram. You can use any good quality switches to make these connections. You can use fewer switches for all these connections as long as you configure the switch to separate traffic from different networks.

To make HA heartbeat connections, connect all of the lan4 interfaces to the same switch and all of the lan5 interfaces to another switch.

When you connect the heartbeat interfaces and power on the FortiGates, they find each other and negotiate to form a cluster. The cluster has the same IP addresses as the primary FortiGate. You can log into the cluster by logging into the primary FortiGate GUI or CLI using one of the original IP addresses of the primary FortiGate.

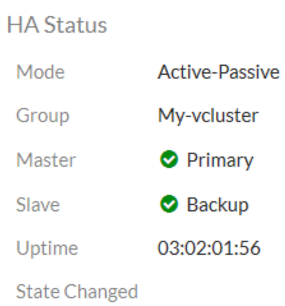
Check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration. Log into the primary FortiGate CLI and enter this command:

```
diagnose sys ha checksum cluster
```

The command output lists all cluster members' configuration checksums. If both cluster members have identical checksums you can be sure that their configurations are synchronized. If the checksums are different, wait a short while and enter the command again. Repeat until the checksums are identical. It may take a while for some parts of the configuration to be synchronized. If the checksums never become identical you can use the information in Synchronizing the configuration to troubleshoot the problem or visit the Fortinet Support website for assistance.

You can also use the `get system ha status` command to display detailed information about the cluster. For information about this command, see Viewing cluster status from the CLI for details.

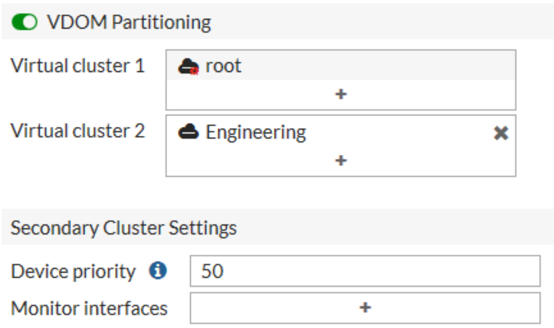
The *HA Status* dashboard widget also shows synchronization status. Hover over the host names of each FortiGate in the widget to verify that they are synchronized and both have the same checksum.



Adding VDOMs and setting up virtual clustering

1. Go to *System* > *Settings* > *System Operation Settings* and enable *Virtual Domains*.
   Or use the following CLI commands:
   ```
   config system global
      set vdom-admin enable
   end
   ```
2. Go to *Global* > *System* > *VDOM* and select *Create New* to add VDOMs.
   Or use the following CLI commands to add the Engineering VDOM:
   ```
   config global
      edit Engineering
   end
   ```
3. Configure virtual clustering and VDOM partitioning on the primary FortiGate. The following commands enable virtual cluster 2, add the Engineering VDOM to virtual cluster 2, and set the virtual cluster 2 device priority of the primary FortiGate to 50.
   ```
   config global
      config system ha
         set vcluster2 enable
            config secondary-vcluster
               set vdom Engineering
               set priority 50
            end
   ```

You can also configure virtual clustering and VDOM partitioning from the GUI in *Global > System > HA*.



4. Set the virtual cluster 2 priority of the backup FortiGate to a relatively high value (in this example, 200) so that this FortiGate processes traffic for the VDOMs in virtual cluster 2. The FGCP synchronizes all other HA settings from the primary FortiGate.
   You must use CLI to configure the virtual cluster 2 priority of the backup FortiGate. Use `execute ha manage` to access the backup FortiGate CLI.

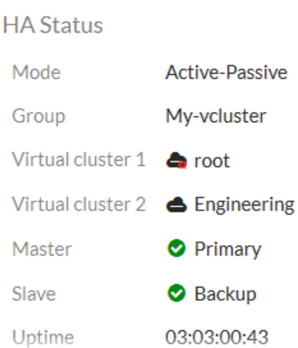
```
config global
   config system ha
      config secondary-vcluster
         set priority 200
   end
```

Checking virtual cluster operation

1. To check the cluster synchronization status to ensure the primary and backup FortiGates both have the same configuration, use the following CLI commands:

```
diagnose sys ha checksum
get system ha status
```

2. The *HA Status* dashboard widget shows the VDOMs in the virtual clusters. Hover over VDOM names to see their status information. Hover over the host names of each FortiGate to verify that they are synchronized and both have the same checksum.



3. To view more information about the cluster status, go to the *HA Status* widget and select *Configure Settings in System > HA*, or go to *System > HA*.
   The HA status page shows both FortiGates in the cluster. It also shows that Primary is the primary (master) FortiGate for the root VDOM (so the primary FortiGate processes all root VDOM traffic). The page also shows that Backup is the primary (master) FortiGate for the engineering VDOM (so the backup FortiGate processes all engineering VDOM traffic).

Synchronized	Priority	Hostname	Virtual Domains	Serial No.	Role
Virtual cluster 1 (2)					
					
✔	200	Primary	• root	FGT51E5618000206	Master
					
✔	50	Backup	• root	FGT51E5618000259	Slave
Virtual cluster 2 (2)					
					
	50	Primary	• Engineering	FGT51E5618000206	Slave
					
	200	Backup	• Engineering	FGT51E5618000259	Master

Results

All traffic should flow through the primary FortiGate. If the primary FortiGate becomes unavailable, traffic fails over to the backup FortiGate. When the primary FortiGate rejoins the cluster, the backup FortiGate should continue to operate as the primary FortiGate.

To test this, ping a reliable IP address from a PC on the internal network. After a moment, power off the primary FortiGate.

If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover.

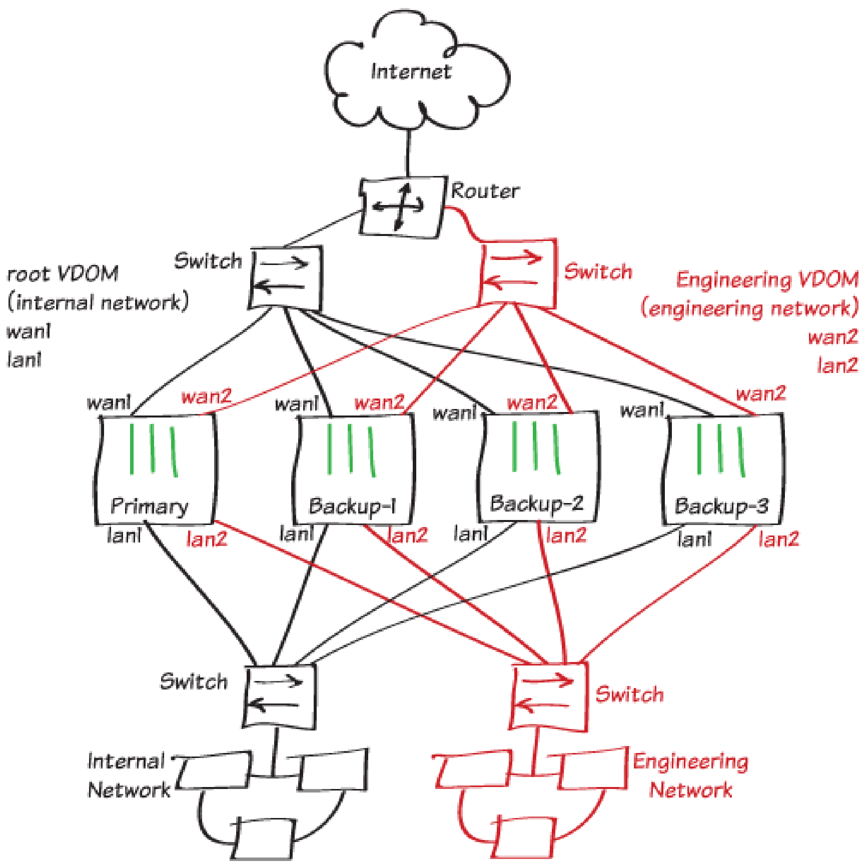
You see a momentary pause in the ping results until traffic diverts to the backup FortiGate, allowing the ping traffic to continue.

```
64 bytes from 184.25.76.114: icmp_seq=69 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=70 ttl=52 time=8.822 ms\
64 bytes from 184.25.76.114: icmp_seq=71 ttl=52 time=9.034 ms\
64 bytes from 184.25.76.114: icmp_seq=72 ttl=52 time=9.536 ms\
64 bytes from 184.25.76.114: icmp_seq=73 ttl=52 time=8.877 ms\
64 bytes from 184.25.76.114: icmp_seq=74 ttl=52 time=8.901 ms\
Request timeout for icmp_seq 75\
64 bytes from 184.25.76.114: icmp_seq=76 ttl=52 time=8.860 ms\
```

```
64 bytes from 184.25.76.114: icmp_seq=77 ttl=52 time=9.174 ms\
64 bytes from 184.25.76.114: icmp_seq=78 ttl=52 time=10.108 ms\
64 bytes from 184.25.76.114: icmp_seq=79 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=80 ttl=52 time=10.861 ms\
64 bytes from 184.25.76.114: icmp_seq=81 ttl=52 time=10.757 ms\
64 bytes from 184.25.76.114: icmp_seq=82 ttl=52 time=8.158 ms\
64 bytes from 184.25.76.114: icmp_seq=83 ttl=52 time=8.639 ms}
```

You can log into the cluster GUI or CLI using the same IP address as you had been using to the log into the primary FortiGate. If the primary FortiGate is powered off, you will be logging into the backup FortiGate. Check the host name to verify the FortiGate that you have logged into. The FortiGate continues to operate in HA mode and if you restart the primary FortiGate, after a few minutes it should rejoin the cluster and operate as the backup FortiGate. Traffic should not be disrupted when the restarted primary unit rejoins the cluster.

FGCP Virtual Clustering with four FortiGates (expert)



This example describes how to set up a FortiGate Clustering Protocol (FGCP) virtual clustering configuration with two FortiGates to provide redundancy and failover protection for two networks. The FortiGate configuration includes two VDOMs. The root VDOM handles internal network traffic and the engineering VDOM handles engineering network traffic. This example shows a simple two-VDOM configuration. The same principles apply to a virtual cluster with more VDOMs.

In this virtual cluster configuration, the primary FortiGate processes all internal network traffic and the backup FortiGate processes all engineering network traffic. Virtual clustering enables override and uses device priorities to distribute traffic between the primary and backup FortiGates. For details, see Configuring virtual clustering.

This example uses four FortiGate-51Es. FortiGate-51Es have a 5-port switch LAN interface. Before configuring HA, the LAN interface was converted to five separate interfaces (lan1 to lan5).

The third FortiGate (this example names it Backup-2) acts as a backup to the primary FortiGate. If the primary FortiGate fails, all primary FortiGate network traffic transfers to the Backup-2 FortiGate as it becomes the new primary FortiGate.

The fourth FortiGate (Backup-3) acts as a backup to the backup FortiGate. If the backup FortiGate fails, all backup FortiGate network traffic transfers to the Backup-3 FortiGate as it becomes the new backup FortiGate.

Before adding the management VDOM to virtual cluster 2, ensure you have added all the backup FortiGates and they have joined the cluster; otherwise the configuration of the primary FortiGate might be overwritten by the backup FortiGate.

Before you start, ensure the FortiGates are running the same FortiOS firmware version and their interfaces are not configured to get addresses from DHCP or PPPoE.

The FGCP does not support using a switch interface for the HA heartbeat. As an alternative to using the lan4 and lan5 interfaces as described in this example, you can use the wan1 and wan2 interfaces for the HA heartbeat.

For an example of how to configure virtual clustering by converting a FortiGate with VDOMs to HA mode and then adding another FortiGate to form a cluster, see High availability with FGCP (expert) on page 133.

Preparing the FortiGates

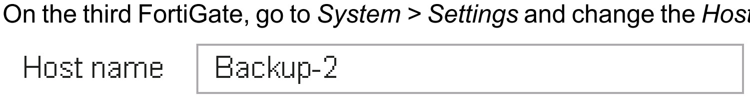
1. If required, upgrade the firmware running on the FortiGates. All FortiGates must be running the same version of FortiOS.
2. If this is a new FortiGate that has never been used, you can skip this step.
   Reset the backup FortiGate to factory default settings using the following CLI command:
   ```
   execute factoryreset
   ```
3. In some cases, after resetting to factory defaults, you might want to make some initial configuration changes to connect the FortiGates to the network. In this example, the LAN switch on the FortiGate-51Es was converted to separate lan1 to lan5 interfaces.
4. On the primary FortiGate, go to *System > Settings* and change the *Host name* to identify this as the primary FortiGate in the HA cluster.

5. On the backup FortiGate, go to *System > Settings* and change the *Host name* to identify this as Backup-1.

6. On the third FortiGate, go to *System > Settings* and change the *Host name* to identify this as Backup-2.

7. On the fourth FortiGate, go to *System* > *Settings* and change the *Host name* to identify this as Backup-3.

You can also use the CLI to change the host name. From the Primary FortiGate:

```
config system global
   set hostname Primary
end
```

From the Backup-1 FortiGate:

```
config system global
   set hostname Backup-1
end
```

From the Backup-2 FortiGate:

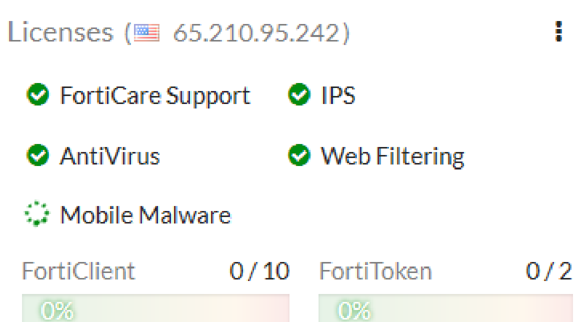
```
config system global
   set hostname Backup-2
end
```

From the Backup-3 FortiGate:

```
config system global
   set hostname Backup-3
end
```

8. Register and apply licenses to the primary FortiGate before configuring it for HA operation. This includes licensing for *FortiCare Support*, *IPS*, *AntiVirus*, *Web Filtering*, *Mobile Malware*, *FortiClient*, *FortiCloud*, and additional *virtual domains* (VDOMs).
All FortiGates in the cluster must have the same level of licensing for FortiGuard, FortiCloud, FortiClient, and VDOMs. You can add *FortiToken* licenses at any time because they're synchronized with all cluster members.

If the FortiGates in the cluster will run FortiOS Carrier, apply the FortiOS Carrier license before you apply other licenses and before you configure the cluster. When you apply the FortiOS Carrier license, the FortiGate resets its configuration to factory defaults, requiring you to repeat steps performed before applying the license.



Configuring clustering

1. On the primary FortiGate, enter the following CLI command to set the HA mode to active-passive, set a group-id, group name, and password, increase the device priority to 200, enable override, and configure the heartbeat interfaces (lan4 and lan5 in this example).

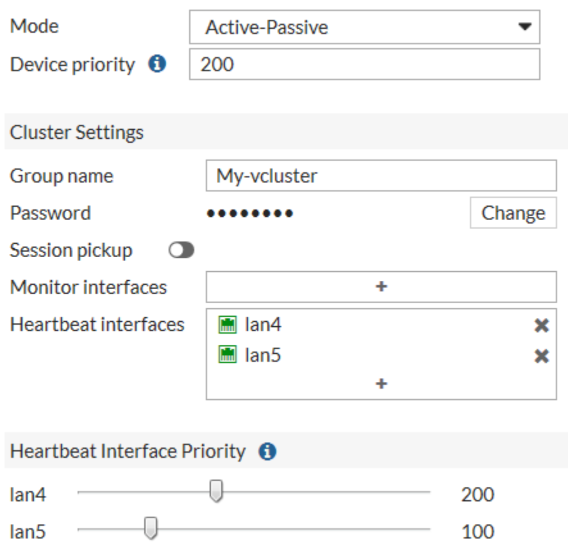
```
config system ha
   set mode a-p
   set group-id 88
```

```
   set group-name My-vcluster
   set password <password>
   set priority 200
   set override enable
   set hbdev lan4 200 lan5 100
end
```

Enabling override and increasing the device priority sets this FortiGate to always be the primary unit.

If you have more than one cluster on the same network, set a different group id for each cluster. Changing the group id changes the cluster interface virtual MAC addresses. If your group id causes a MAC address conflict on your network, you can select a different group id.

You can configure most of these settings using the GUI in *Global* > *System* > *HA*. You must configure the group-id and override using the CLI.



2. On the Backup-1 FortiGate, duplicate the primary FortiGate HA mode, group-id, group-name, password, override, and heartbeat device settings. Set the device priority to 50. Setting the device priority to a lower value means the Backup-1 FortiGate will most likely always be the backup FortiGate.

```
config system ha
   set mode a-p
   set group-id 88
   set group-name My-vcluster
   set password <password>
   set priority 50
   set override enable
   set hbdev lan4 200 lan5 100
end
```

3. On the Backup-2 FortiGate, duplicate the primary FortiGate HA mode, group-id, group-name, password, override, and heartbeat device settings. Set the device priority to 150. A device priority of 150 is almost as high as the device priority of the primary FortiGate. So if the primary FortiGate fails, the Backup-2 FortiGate should become the new primary FortiGate.

```
config system ha
   set mode a-p
   set group-id 88
   set group-name My-vcluster
   set password <password>
   set priority 150
   set override enable
```

```
   set hbdev lan4 200 lan5 100
end
```

4. On the Backup-3 FortiGate, duplicate the primary FortiGate HA mode, group-id, group-name, password, override, and heartbeat device settings. Set the device priority to 100. A device priority of 100 means that if the backup FortiGate fails, the Backup-3 FortiGate will have the lowest device priority so will become the new backup FortiGate.

```
config system ha
   set mode a-p
   set group-id 88
   set group-name My-vcluster
   set password <password>
   set priority 100
   set override enable
   set hbdev lan4 200 lan5 100
end
```

When you enable HA, each FortiGate negotiates to establish an HA cluster. You might temporarily lose connectivity during FGCP negotiation and the MAC addresses of the FortiGate interfaces change to HA virtual MAC addresses.

If these steps don't start HA mode, make sure that none of the FortiGate's interfaces use DHCP or PPPoE addressing.

To reconnect sooner, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or deleting all ARP table entries). You can usually delete the ARP table from a command prompt using a command similar to `arp -d`.

The FGCP uses virtual MAC addresses for failover. The virtual MAC address assigned to each FortiGate interface depends on the HA group ID. A group ID of 88 sets FortiGate interfaces to the following MAC addresses: 00:09:0f:09:58:00, 00:09:0f:09:58:01, 00:09:0f:09:58:02 and so on. For details, see Cluster virtual MAC addresses.

You can verify that the FGCP has set the virtual MAC addresses by viewing the configuration of each FortiGate interface from the GUI (in *Network* > *Interfaces*) or by entering the following CLI command (shown below for lan2 on a FortiGate-51E):

```
get hardware nic lan2
...
Current_HWaddr 00:09:0f:09:58:01
Permanent_HWaddr 70:4c:a5:98:11:54
...
```

You can also use the `diagnose hardware deviceinfo nic lan2` command to display this information.

The output shows the current hardware (MAC) address (the virtual MAC set by the FGCP) and the permanent hardware (MAC) address for the interface.

Connecting and verifying cluster operation

Connect the FortiGates together and to your networks as shown in the network diagram at the start of this example Making these connections disrupts network traffic as you disconnect and re-connect cables.

You must use switches between the cluster and the Internet, between the cluster and the internal networks, and between the cluster and the engineering network as shown in the network diagram. You can use any good quality switches to make these connections. You can use fewer switches for all these connections as long as you configure the switch to separate traffic from different networks.

To make HA heartbeat connections, connect all of the lan4 interfaces to the same switch and all of the lan5 interfaces to another switch.

When you connect the heartbeat interfaces and power on the FortiGates, they find each other and negotiate to form a cluster. The cluster will have the same IP addresses as the primary FortiGate. You can log into the cluster by logging into the primary FortiGate GUI or CLI using one of the original IP addresses of the primary FortiGate.

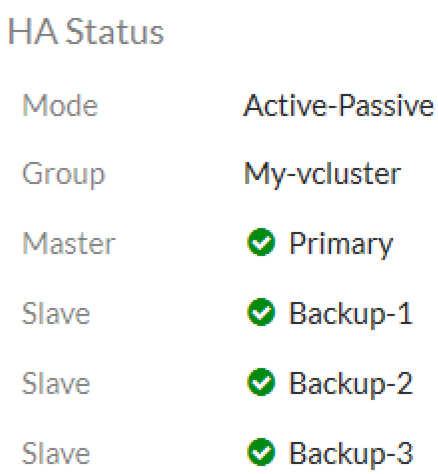
Check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration. Log into the primary FortiGate CLI and enter this command:

```
diagnose sys ha checksum cluster
```

The command output lists all cluster members' configuration checksums. If both cluster members have identical checksums you can be sure that their configurations are synchronized. If the checksums are different, wait a short while and enter the command again. Repeat until the checksums are identical. It may take a while for some parts of the configuration to be synchronized. If the checksums never become identical you can use the information in Synchronizing the configuration to troubleshoot the problem or visit the Fortinet Support website for assistance.

You can also use the `get system ha status` command to display detailed information about the cluster. For information about this command, see Viewing cluster status from the CLI for details.

The *HA Status* dashboard widget also shows synchronization status. Hover over the host names of each FortiGate in the widget to verify that they are synchronized and both have the same checksum.



Adding VDOMs and setting up virtual clustering

1. Go to *System* > *Settings* > *System Operation Settings* and enable *Virtual Domains*.

   Or use the following CLI commands:

   ```
   config system global
      set vdom-admin enable
   end
   ```

2. Go to *Global* > *System* > *VDOM* and select *Create New* to add VDOMs.

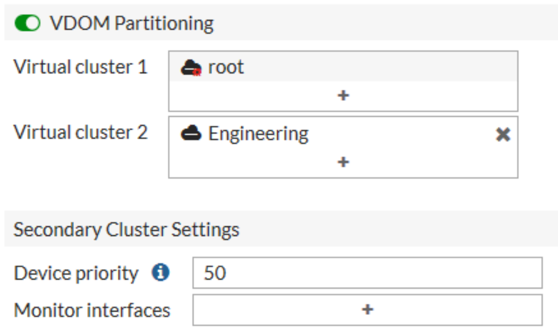
   Or use the following CLI commands to add the Engineering VDOM:

   ```
   config global
      edit Engineering
   end
   ```

3. Configure virtual clustering and VDOM partitioning on the primary FortiGate. The following commands enables virtual cluster 2, add the Engineering VDOM to virtual cluster 2, and set the virtual cluster 2 device priority of the primary FortiGate to 50.

```
config global
   config system ha
      set vcluster2 enable
         config secondary-vcluster
            set vdom Engineering
            set priority 50
         end
```

You can also configure virtual clustering and VDOM partitioning from the GUI in *Global* > *System* > *HA*.



4. Set the virtual cluster 2 priority of the Backup-1 FortiGate to a relatively high value (in this example, 200) so that this FortiGate processes traffic for the VDOMs in virtual cluster 2. The FGCP synchronizes all other HA settings from the primary FortiGate.
   You must use CLI to configure the virtual cluster 2 priority of the backup FortiGate. Use `execute ha manage` to access the backup FortiGate CLI.

```
config global
   config system ha
      config secondary-vcluster
         set priority 200
   end
```

5. Set the virtual cluster 2 priority of the Backup-2 FortiGate to 100 so that if the primary FortiGate fails, Backup-2 will become the primary FortiGate but will have the lowest virtual cluster 2 priority. The FGCP synchronizes all other HA settings from the primary FortiGate.
   You must use CLI to configure the virtual cluster 2 priority of the Backup-2 FortiGate. Use `execute ha manage` to access the backup FortiGate CLI.

```
config global
   config system ha
      config secondary-vcluster
         set priority 100
      end
```

6. Set the virtual cluster 2 priority of the Backup-3 FortiGate to 150 so that if the backup FortiGate fails, Backup-3 will have the highest virtual cluster 2 device priority. The FGCP synchronizes all other HA settings from the primary FortiGate.
   You must use CLI to configure the virtual cluster 2 priority of the backup FortiGate. Use `execute ha manage` to access the backup FortiGate CLI.

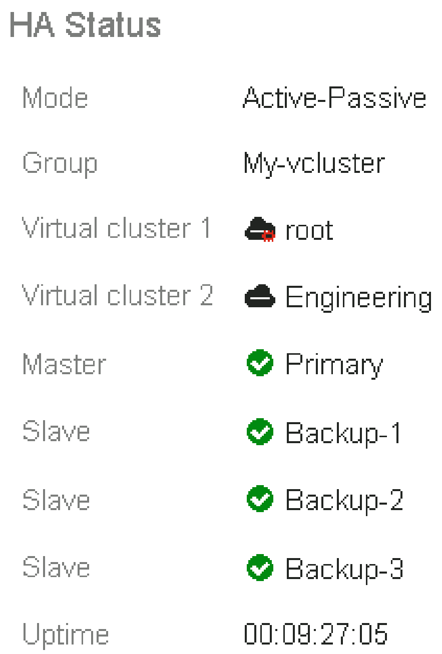
```
config global
   config system ha
      config secondary-vcluster
         set priority 150
      end
```

Checking virtual cluster operation

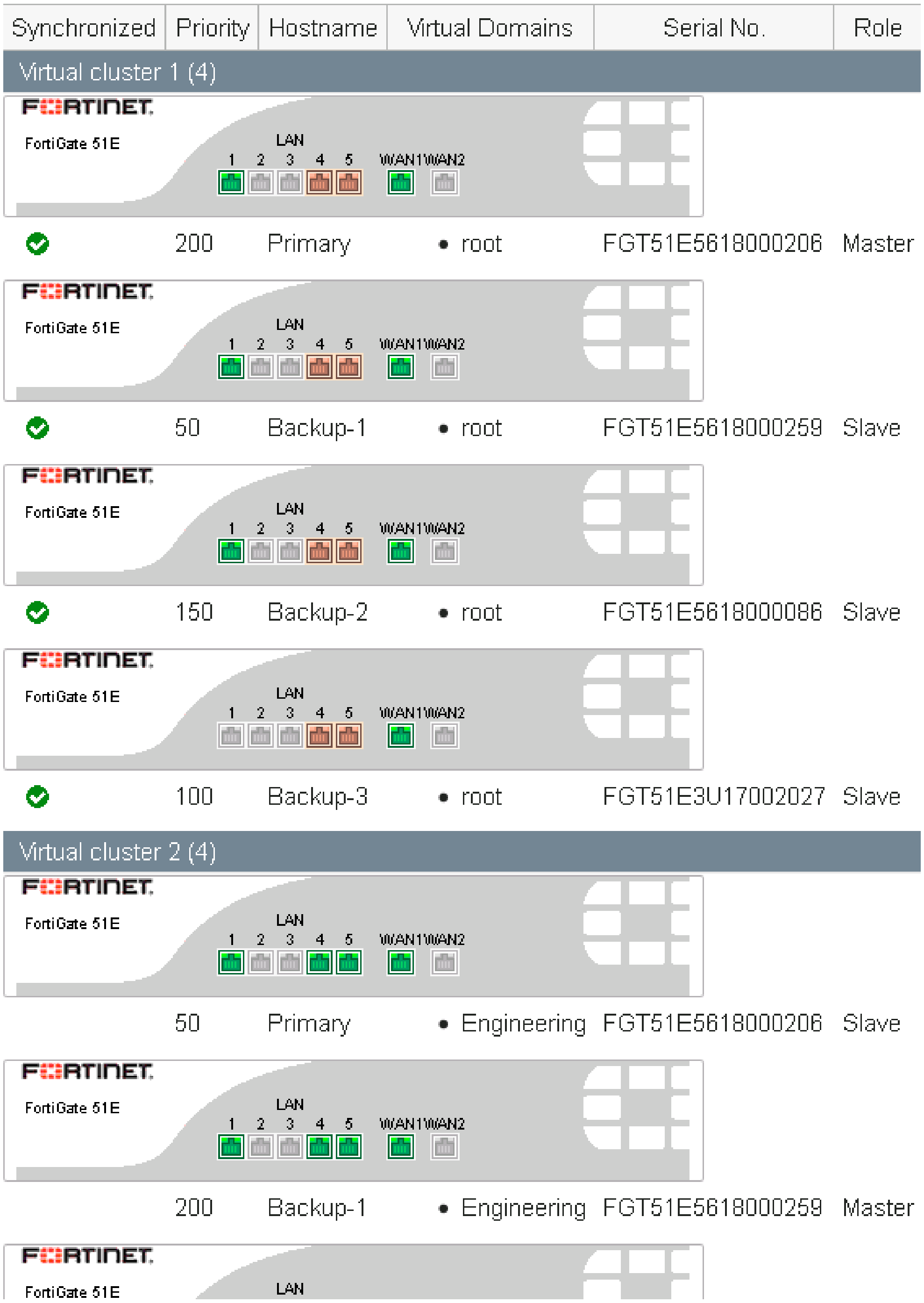
1. To check the cluster synchronization status to ensure the primary and backup FortiGates both have the same configuration, use the following CLI commands:

```
diagnose sys ha checksum
get system ha status
```

2. The *HA Status* dashboard widget shows the VDOMs in the virtual clusters. Hover over VDOM names to see their status information. Hover over the host names of each FortiGate to verify that they are synchronized and both have the same checksum.



3. To view more information about the cluster status, go to the *HA Status* widget and select *Configure Settings in System* > *HA*, or go to *System* > *HA*.
The HA status page shows all four FortiGates in the cluster. It also shows that Primary is the primary (master) FortiGate for the root VDOM (so the primary FortiGate processes all root VDOM traffic). The page also shows that Backup-1 is the primary (master) FortiGate for the engineering VDOM (so the backup FortiGate processes all engineering VDOM traffic).



Synchronized	Priority	Hostname	Virtual Domains	Serial No.	Role
Virtual cluster 1 (4)					
✔	200	Primary	• root	FGT51E5618000206	Master
✔	50	Backup-1	• root	FGT51E5618000259	Slave
✔	150	Backup-2	• root	FGT51E5618000086	Slave
✔	100	Backup-3	• root	FGT51E3U17002027	Slave
Virtual cluster 2 (4)					
	50	Primary	• Engineering	FGT51E5618000206	Slave
	200	Backup-1	• Engineering	FGT51E5618000259	Master

Results

All root VDOM traffic should flow through the primary FortiGate and engineering VDOM traffic should flow through the backup FortiGate. If the primary FortiGate becomes unavailable, the cluster negotiates and traffic fails over and all traffic would be processed by the backup FortiGate.

To test this, ping a reliable IP address from a PC on the internal network. After a moment, power off the primary FortiGate.

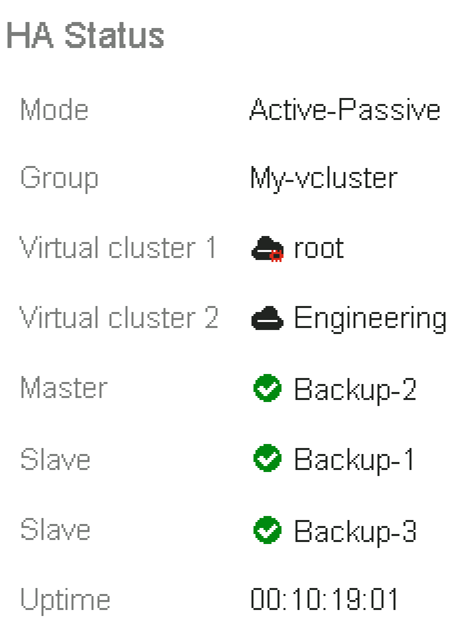
If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover.

You see a momentary pause in the ping results until traffic diverts to the backup FortiGate, allowing the ping traffic to continue.

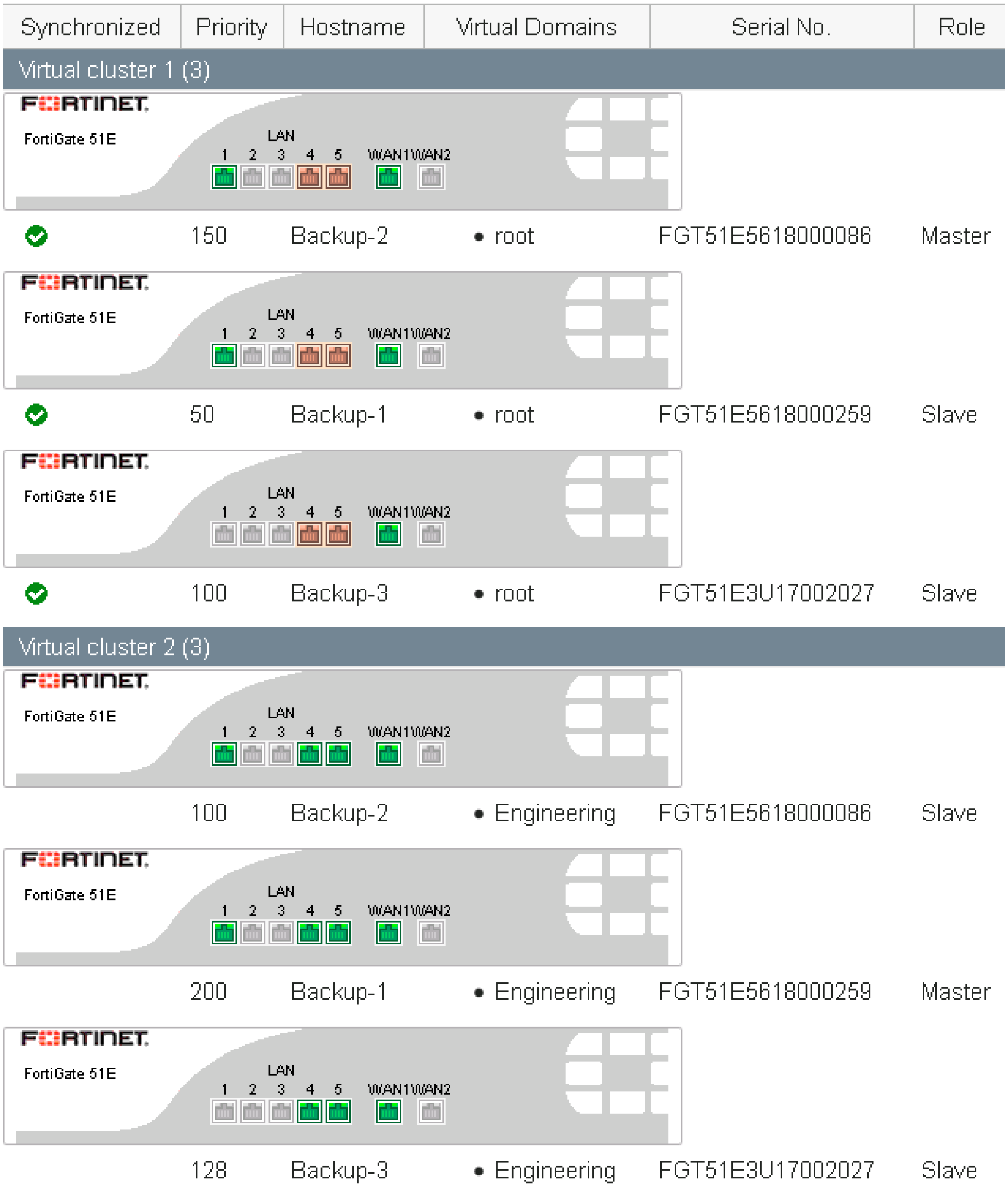
```
64 bytes from 184.25.76.114: icmp_seq=69 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=70 ttl=52 time=8.822 ms\
64 bytes from 184.25.76.114: icmp_seq=71 ttl=52 time=9.034 ms\
64 bytes from 184.25.76.114: icmp_seq=72 ttl=52 time=9.536 ms\
64 bytes from 184.25.76.114: icmp_seq=73 ttl=52 time=8.877 ms\
64 bytes from 184.25.76.114: icmp_seq=74 ttl=52 time=8.901 ms\
Request timeout for icmp_seq 75\
64 bytes from 184.25.76.114: icmp_seq=76 ttl=52 time=8.860 ms\
64 bytes from 184.25.76.114: icmp_seq=77 ttl=52 time=9.174 ms\
64 bytes from 184.25.76.114: icmp_seq=78 ttl=52 time=10.108 ms\
64 bytes from 184.25.76.114: icmp_seq=79 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=80 ttl=52 time=10.861 ms\
64 bytes from 184.25.76.114: icmp_seq=81 ttl=52 time=10.757 ms\
64 bytes from 184.25.76.114: icmp_seq=82 ttl=52 time=8.158 ms\
64 bytes from 184.25.76.114: icmp_seq=83 ttl=52 time=8.639 ms}
```

You can log into the cluster GUI or CLI using the same IP address as you had been using to the log into the primary FortiGate. If the primary FortiGate is powered off, you will be logging into the Backup-1 FortiGate. Check the host name to verify the FortiGate that you have logged into.

After the primary FortiGate fails the *HA Status* dashboard widget shows that the Backup-2 has become the primary (master) FortiGate.



System > HA shows that the Backup-2 FortiGate has become the primary FortiGate for virtual cluster 1. This page also shows that the Backup-1 FortiGate continues to process virtual cluster 2 traffic.

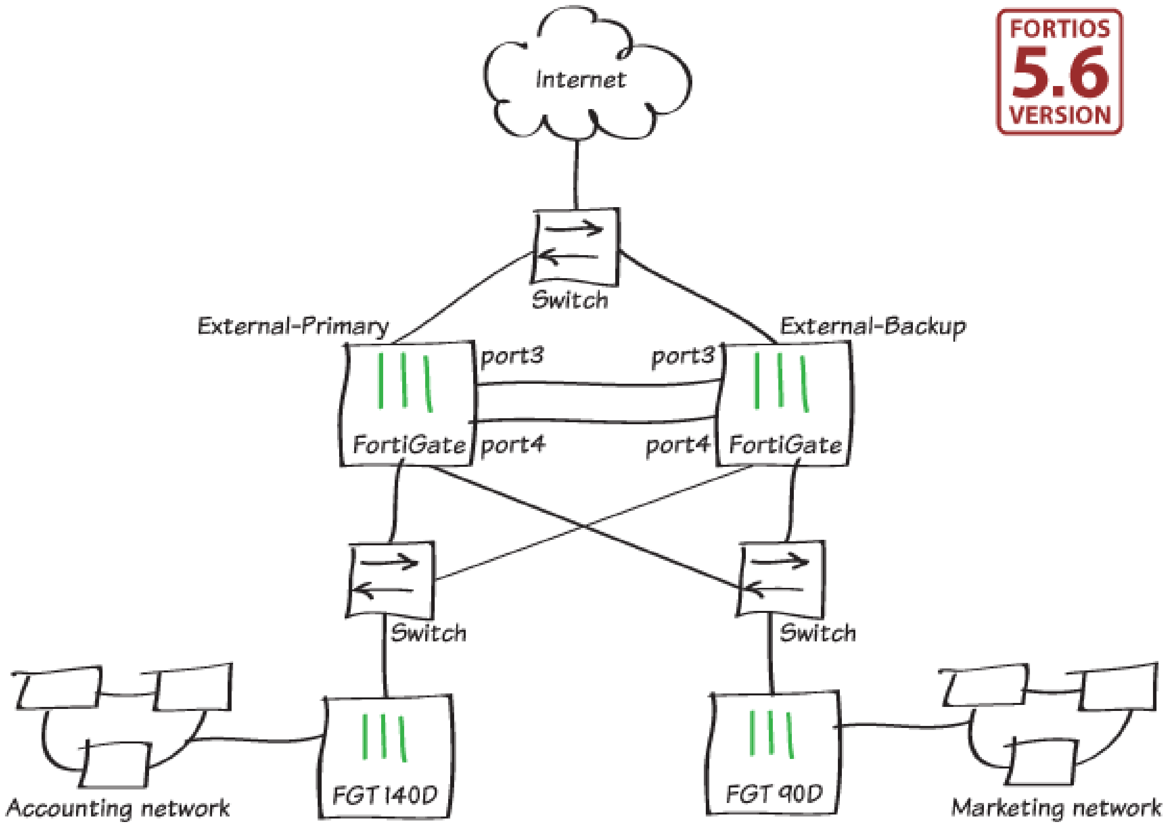


Synchronized	Priority	Hostname	Virtual Domains	Serial No.	Role
Virtual cluster 1 (3)					
	150	Backup-2	• root	FGT51E5618000086	Master
	50	Backup-1	• root	FGT51E5618000259	Slave
	100	Backup-3	• root	FGT51E3U17002027	Slave
Virtual cluster 2 (3)					
	100	Backup-2	• Engineering	FGT51E5618000086	Slave
	200	Backup-1	• Engineering	FGT51E5618000259	Master
	128	Backup-3	• Engineering	FGT51E3U17002027	Slave

If you restart the primary FortiGate, after a few minutes it should rejoin the cluster and because override is enabled, the original virtual cluster configuration should be re-established. Traffic may be temporarily disrupted when the restarted primary FortiGate rejoins the cluster.

You can also try powering off other FortiGates in the virtual cluster to see how the cluster adapts to the failover. Because of the device priority configuration, if two FortiGates are operating, virtual cluster 1 and virtual cluster 2 traffic is distributed between them.

FGCP high availability troubleshooting



This example shows you how to find and fix some common FortiGate Clustering Protocol (FGCP) HA problems.

Before you set up a cluster

Before you set up an FortiGate FGCP cluster, ensure the following:

- All the FortiGates have the same hardware version and the same hardware configuration.
- All the FortiGates have the same firmware build.
- All the FortiGates are set to the same operating mode (NAT or Transparent).
- All the FortiGates are operating in single VDOM mode.
- If the FortiGates are operating in multiple VDOM mode, they all have the same VDOM configuration.

In some cases, you might be able to form a cluster if your FortiGates have different firmware builds, different VDOM configurations, and are in different operating modes. However, if you encounter problems when forming a cluster you might be able to resolve them by installing the same firmware build on each unit and giving them the same VDOM configuration and operating mode. If possible, you could also reset them all to factory defaults and start over.

If the FortiGates in the cluster have different licenses, the cluster that is formed but it will operate at the lowest licensing level.

Troubleshooting licensing

All the FortiGates in a cluster must have the same level of licensing. This includes FortiGuard, FortiCloud, FortiClient, VDOMs (if applicable), and FortiOS Carrier (if applicable).

If one of the FortiGates has a lower level of licensing, then all the FortiGates in the cluster operate at the lowest licensing level. For example, if you only purchase FortiGuard Web Filtering for one of the FortiGates in a cluster, when the cluster is established, none of the cluster units supports FortiGuard Web Filtering.

An exception is FortiToken licensing. FortiToken activations are completed in one FortiGate unit and synchronized with all of the FortiGates in the cluster.

Troubleshooting hardware revisions

Many FortiGate platforms have gone through multiple hardware versions and in some cases these hardware changes might prevent cluster formation. If you run into this problem, you can use the following command on each FortiGate to set the cluster to ignore different hardware versions:

```
execute ha ignore-hardware-revision enable
```

This command is only available on FortiGates that have had multiple hardware revisions. If this command isn't available, then hardware version issues should not prevent cluster formation.

By default the command is set to prevent cluster formation between FortiGates with different hardware revisions. You can enter the following command to view its status:

```
execute ha ignore-hardware-revision status
```

Usually the incompatibility is caused by different hardware versions having different hard disks. Enabling this command disables each FortiGate's hard disks. As a result of disabling hard disks, the cluster will not support logging to the hard disk or WAN Optimization.

If the FortiGates have compatible hardware versions or if you want to run a FortiGate in standalone mode, enter the following command to disable ignoring the hardware revision and enable hard disks:

```
execute ha ignore-hardware-revision disable
```

Affected models include but are not limited to:

- FortiGate-100D
- FortiGate-300C
- FortiGate-600C
- FortiGate-800C
- FortiGate-80C and FortiWiFi-80C
- FortiGate-60C

Troubleshooting the initial cluster configuration

This section describes how to check a cluster when it first starts up to make sure that it is configured and operating correctly. This section assumes you have already configured your HA cluster and it appears to be up and running normally.

To verify that a cluster can process traffic and react to a failure:

1. Add a basic security policy configuration and send network traffic through the cluster to confirm connectivity.
   For example, if the cluster is installed between the Internet and an internal network, set up a basic internal to external security policy that accepts all traffic. Then from a PC on the internal network, browse to a website on the Internet or ping a server on the Internet to confirm connectivity.
2. From your management PC, continuously ping the cluster and then start a large download or use another way to establish ongoing traffic through the cluster.
3. While traffic is going through the cluster, disconnect the power from one of the cluster units. You could also shut down or restart a cluster unit. Traffic should continue with minimal interruption.
4. Start up or reconnect the cluster unit that you disconnected. The FortiGate should re-join the cluster with little or no effect on traffic.
5. Disconnect a cable from one of the HA heartbeat interfaces. The cluster should keep functioning using the other heartbeat interface.
6. If you have port monitoring enabled, disconnect a network cable from a monitored interface. Traffic should continue with minimal interruption.

Verifying the cluster configuration from the GUI

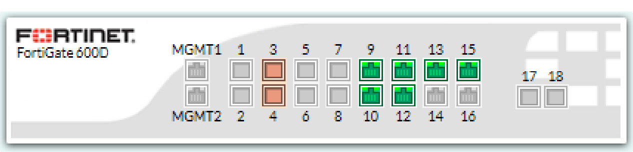
To verify the cluster's status and configuration:

1. Log into the cluster GUI. Verify that the *HA Status* dashboard widget lists all the cluster units.

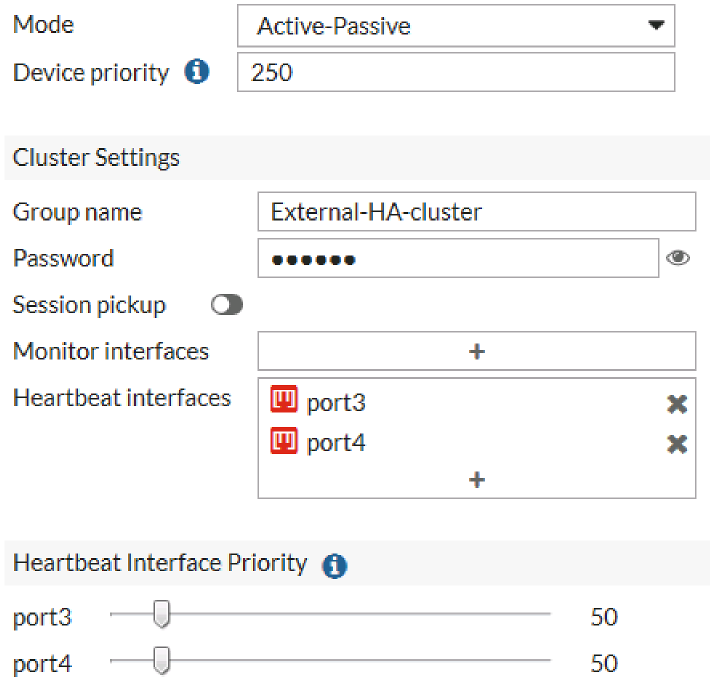
HA Status

Mode	Active-Passive
Group	External-HA-Cluster
Master	External-Primary
Slave	External-Backup
Uptime	00:00:43:06
State Changed	00:00:02:07

2. Go to *System* > *HA* and verify that all cluster units are displayed in the HA Cluster list. You can also verify that the correct cluster unit interfaces are connected and display their status information. See Cluster members list for more information.

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput
							
	250	External-Primary	FGT6HD3916800525	Master	42d 5h 54m 2s	167	258 bps
							
	50	External-Backup	FGT6HD3916801195	Slave	2h 57m 18s	45	129 bps

3. From the cluster members list, edit the primary unit (master) and verify the cluster configuration.



Troubleshooting the cluster configuration from the GUI

If the FortiGates do not form a cluster, try the following:

1. Connect to each cluster unit's GUI and verify that the HA configurations are the same. The HA configurations of all cluster units must be identical – even a small discrepancy can prevent a FortiGate from joining a cluster.
2. If the configurations are the same, try re-entering the HA password on each cluster unit in case you made an error typing the password when configuring one of the cluster units.
3. Check the cables and interface LEDs.
4. Check that the correct interfaces of each cluster unit are connected. Use the cluster members list to verify that each interface that should be connected actually is connected. If a link is down, re-verify the physical connection.
5. Try replacing network cables or switches.

Verifying the cluster configuration from the CLI

If a cluster is formed, do the following to verify its status and configuration:

1. Log into each cluster unit's CLI. You can use the GUI CLI console, SSH, or a direct console port connection.
2. Enter the command `get system status`. Look for the current HA mode in the command output. If the cluster is operating correctly and you have connected to the primary unit, you see something like this:
   `Current HA mode: a-a, master`
3. Connect to the backup unit using the `execute ha manage` command or connect directly to the console port of the backup FortiGate. If the cluster is operating correctly, you see something like this:
   `Current HA mode: a-a, backup`
4. If the FortiGate is not operating in HA mode, the `get system status command` output is something like this:
   `Current HA mode: standalone`

5. Verify that the `get system ha status` command displays all cluster units. For example, in a cluster of three FortiGate units, the command output is something like this:
```
Master: 5001d-slot3 , FG-5KD3914800344
Slave : 5001d-slot5 , FG-5KD3914800353
Slave : 5001d-slot4 , FG-5KD3914800284
```
6. To verify that the HA configuration is correct and the same for each cluster unit, enter the `get system ha` command.
```
get system ha
group-id : 0
group-name : External-HA-cluster
mode : a-p
password : *
hbdev : "port3" 50 "port4" 50
.
.
.
```

Troubleshooting the cluster configuration from the CLI

1. If the FortiGates don't form a cluster, use the following command to re-enter the cluster password. Do this for each cluster unit in case you made an error typing the password when configuring one of the cluster units.
```
config system ha
   set password <password>
end
```
2. Check that the correct interfaces of each cluster unit are connected. Check the cables and interface LEDs. Use the `get hardware nic <interface_name>` command to confirm that each interface is connected.
   If the interface is connected, the output should contain a `Link: up` entry similar to the following:
```
get hardware nic port1
.
.
.
Link: up
.
.
.
```
3. If the link is down, re-verify the physical connection. Try replacing network cables or switches.

More troubleshooting information

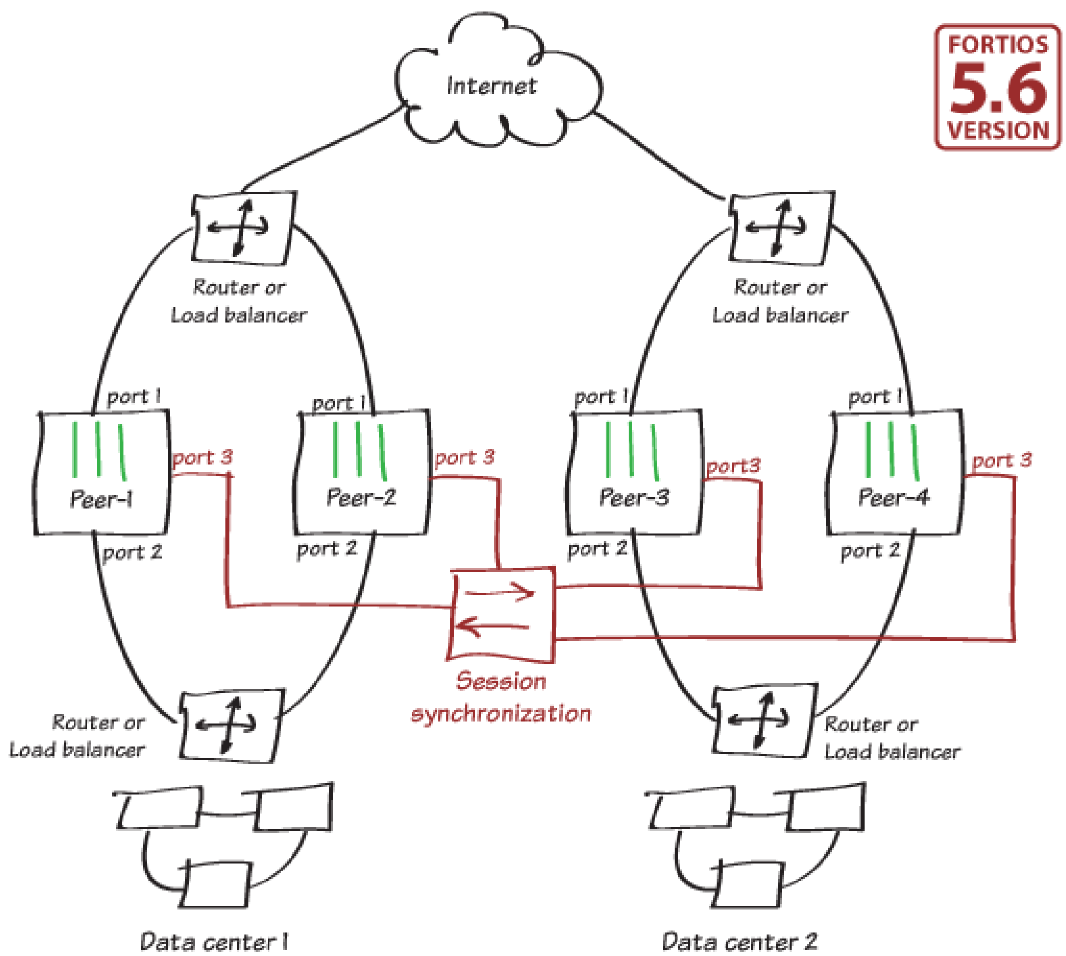
The HA guide is useful for troubleshooting HA clusters. The following are links to sections with more information.

- If sessions are lost after a failover, you may need to change `route-ttl` to keep synchronized routes active longer. See Synchronizing kernel routing tables.
- In rare cases, sometimes after a cluster unit has been replaced, a cluster might not form because the disk partition sizes of the cluster units are different. Use the following command to check the disk storage checksum of each cluster unit. If the checksums are different, then contact Fortinet support for help in setting up compatible storage partitions.
```
diagnose sys ha showcsum 1 system | grep storage
```
- To control which cluster unit becomes the primary unit, you can change the device priority and enable override. See Controlling primary unit selection using device priority and override.

- Changes made to a cluster can be lost if override is enabled. See Configuration changes can be lost if override is enabled.
- When override is enabled, after a failover, traffic might be disrupted if the primary unit rejoins the cluster before the session tables are synchronized or for other reasons such as if the primary unit is configured for DHCP or PPPoE. See Delaying how quickly the primary unit rejoins the cluster when override is enabled.
- In some cases, age differences among cluster units can result in the wrong cluster unit becoming the primary unit. For example, if a cluster unit set to a high priority reboots, that unit will have a lower age than other cluster units. You can resolve this problem by resetting the age of one or more cluster units. See Primary unit selection and age. You can also adjust how sensitive the cluster is to age differences. This can be useful if large age differences cause problems. See Cluster age difference margin (grace period) and Changing the cluster age difference margin.
- If one cluster unit needs to be serviced or removed from the cluster, you can do so without affecting the operation of the cluster. See Disconnecting a cluster unit from a cluster.
- If FGSP is enabled, the web-based manager and CLI do not allow you to configure HA. See FortiGate Session Life Support Protocol (FGSP).
- If one or more FortiGate unit interfaces is configured as a PPTP or L2TP client, the GUI and CLI do not allow you to configure HA.
- FGCP is compatible with DHCP and PPPoE but be careful when configuring a cluster that includes a FortiGate interface configured to get its IP address with DHCP or PPPoE. Fortinet recommends turning on DHCP or PPPoE addressing for an interface after the cluster has been configured. See FortiGate HA compatibility with DHCP and PPPoE.
- Some third-party network equipment may prevent HA heartbeat communication resulting in the failure of the cluster or the creation of a split brain scenario. For example, some switches use packets with the same Ethertype as HA heartbeat packets used for internal functions and when used for HA heartbeat communication, the switch generates CRC errors and the packets are not forwarded. See Heartbeat packet Ethertypes.
- Very busy clusters might not be able to send HA heartbeat packets quickly enough resulting in a split brain scenario. You might be able to resolve this problem by modifying HA heartbeat timing. See Modifying heartbeat timing.
- Very busy clusters might have performance degradation if session pickup is enabled. If possible, you can disable this feature to improve performance. If you require session pickup for your cluster, there are options for improving session pickup performance. See Improving session synchronization performance.
- If it takes longer than expected for a cluster to fail over, try changing how the primary unit sends gratuitous ARP packets. See Changing how the primary unit sends gratuitous ARP packets after a failover on page 1.
- You can improve failover times by configuring the cluster for subsecond failover. See Subsecond failover and Failover performance.
- When you first put a FortiGate unit in HA mode, you might lose connectivity to the unit because HA changes the MAC addresses of all FortiGate unit interfaces including the one that you are connecting to. The cluster MAC addresses also change if you change some HA settings such as the cluster group ID. The connection will be restored in a moment as your network and PC updates to the new MAC address. To reconnect more quickly, you can update the ARP table of your management PC by deleting the ARP table entry for the FortiGate unit (or just deleting all ARP table entries). You might be able to delete the ARP table of your management PC using a command similar to `arp -d`.
- Since HA changes all cluster unit MAC addresses, if your network uses MAC address filtering, you might have to make configuration changes to account for the HA MAC addresses.
- A network might experience packet loss when two FortiGate HA clusters have been deployed in the same broadcast domain. Deploying two HA clusters in the same broadcast domain can result in packet loss because of MAC address conflicts. Diagnose packet loss by pinging from one cluster to the other or by pinging both of the clusters from a device in the broadcast domain. You can resolve the MAC address conflict by changing the HA Group ID configuration of the two clusters. The HA Group ID is sometimes called the Cluster ID. See Diagnosing packet loss with two FortiGate HA clusters in the same broadcast domain.
- If there is a synchronization problem between the primary unit and one or more subordinate units, the cluster CLI displays `slave is not in sync` messages. See How to diagnose HA out of sync messages.

- If you have configured dynamic routing and the new primary unit takes too long to update its routing table after a failover, you can configure a graceful restart and also optimize how routing updates are synchronized. See Configuring graceful restart for dynamic routing failover and Synchronizing kernel routing tables.
- Some switches might not be able to detect that the primary unit has become a backup unit and will keep sending packets to the former primary unit. This can occur after a link failover if the switch does not detect the failure and does not clear its MAC forwarding table. See Updating MAC forwarding tables when a link failover occurs.
- If a link not directly connected to a cluster unit fails, such as between a switch connected to a cluster interface and the network, you can enable remote link failover to maintain communication. See Remote link failover.
- If you find that some cluster units are not running the same firmware build, reinstall the correct firmware build on the cluster to upgrade all cluster units to the same firmware build. See Synchronizing the firmware build running on a new cluster unit.

Using FGSP to load balance access to two active-active data centers



This advanced scenario describes how to configure FortiGate Session Life Support Protocol (FGSP) with four peer FortiGates protecting two active-active data centers.

FGSP supports up to 16 peer FortiGates.

In this example, two redundant active-active data centers process traffic from the Internet, distributing traffic to the FortiGates (named Peer-1, Peer-2, Peer-3 and Peer-4) by routers or load balancers. All the FortiGates are configured with two virtual domains: root and vdom1. All sessions processed by vdom1 are synchronized with all the FortiGates. The synchronization link interface is port 3 in the root virtual domain. The IP addresses of port 3 are different for each FortiGate:

- For Peer-1, the port 3 IP address is 10.10.10.1
- For Peer-2, the port 3 IP address is 10.10.10.2
- For Peer-3, the port 3 IP address is 10.10.10.3
- For Peer-4, the port 3 IP address is 10.10.10.4

The port 1 and port 2 interfaces are added to vdom1. To keep the configuration simple and applicable to different networks, port 1 and port 2 are added to a virtual wire pair so these interfaces do not have IP addresses. This example includes a policy that allows all traffic across the virtual wire pair. This example policy applies the default VoIP profile to all VoIP traffic and applies virus scanning and application control.

Although this architecture can support different configurations on each FortiGate, it is not recommended. Usually, all FortiGates in an FGSP deployment have the same configuration. This example assumes configuration synchronization is disabled in FortiOS and you are using FortiManager to keep the FortiGate configurations synchronized.

Configuring the first FortiGate (Peer-1)

Configure Peer-1 with the following settings:

1. Enable virtual domain configuration, add vdom1, set vdom1 to proxy mode (to support VoIP profiles), and add port1 and port2 to vdom1.

```
config system global
   set vdom-admin enable
end

config vdom
   edit vdom1
      config system settings
         set inspection-mode proxy
   end
end

config system global
   config system interface
      edit port1
         set vdom vdom1
      next
      edit port2
         set vdom vdom1
      end
   end
```

2. Create a virtual wire pair between port1 and port2.
```
config vdom
   edit vdom1
      config system virtual-wire-pair
         edit my-wire-pair
            set member port1 port2
         end
      end
```
3. Create a virtual wire pair policy to allow all traffic between port 1 and port 2. This example policy applies antivirus scanning, application control, and VoIP profiles.
```
config vdom
   edit vdom1
      config firewall policy
         edit 1
         set srcintf port1 port2
            set dstintf port1 port2
            set srcaddr all
            set dstaddr all
            set service ALL
            set schedule always
            set action allow
            set utm-status enable
            set av-profile default
            set application-list default
            set voip-profile default
         end
```
4. Configure Peer-1 for FGSP.
```
config system cluster-sync
   edit 1
      set peerip 10.10.10.2
      set peervd root
      set syncvd vdom1
   next
   edit 2
      set peerip 10.10.10.3
      set peervd root
      set syncvd vdom1
   next
   edit 3
      set peerip 10.10.10.4
      set peervd root
      set syncvd vdom1
   end
```

Configuring the second FortiGate (Peer-2)

1. Configure Peer-2 with the same configuration as Peer-1:
   a. Enable virtual domain configuration, add vdom1, set vdom1 to proxy mode, and add port 1 and port 2 to vdom1.
   b. Create a virtual wire pair between port 1 and port 2.
   c. Create a virtual wire pair policy to allow all traffic between port 1 and port 2. This example policy applies antivirus scanning, application control, and VoIP profiles.
2. Configure Peer-2 for FGSP.
```
config system cluster-sync
```

```
    edit 1
        set peerip 10.10.10.1
        set peervd root
        set syncvd vdom1
    next
    edit 2
        set peerip 10.10.10.3
        set peervd root
        set syncvd vdom1
    next
    edit 3
        set peerip 10.10.10.4
        set peervd root
        set syncvd vdom1
    end
```

Configuring the third FortiGate (Peer-3)

1. Configure Peer-3 with the same configuration as Peer-1:
   a. Enable virtual domain configuration, add vdom1, set vdom1 to proxy mode, and add port 1 and port 2 to vdom1.
   b. Create a virtual wire pair between port 1 and port 2.
   c. Create a virtual wire pair policy to allow all traffic between port 1 and port 2. This example policy applies antivirus scanning, application control, and VoIP profiles.
2. Configure Peer-3 for FGSP.

```
config system cluster-sync
    edit 1
        set peerip 10.10.10.1
        set peervd root
        set syncvd vdom1
    next
    edit 2
        set peerip 10.10.10.2
        set peervd root
        set syncvd vdom1
    next
    edit 3
        set peerip 10.10.10.4
        set peervd root
        set syncvd vdom1
    end
```

Configuring the fourth FortiGate (Peer-4)

1. Configure Peer-4 with the same configuration as Peer-1:
   a. Enable virtual domain configuration, add vdom1, set vdom1 to proxy mode, and add port 1 and port 2 to vdom1.
   b. Create a virtual wire pair between port 1 and port 2.
   c. Create a virtual wire pair policy to allow all traffic between port 1 and port 2. This example policy applies antivirus scanning, application control, and VoIP profiles.
2. Configure Peer-4 for FGSP.

```
config system cluster-sync
    edit 1
```

```
        set peerip 10.10.10.1
        set peervd root
        set syncvd vdom1
    next
    edit 2
        set peerip 10.10.10.2
        set peervd root
        set syncvd vdom1
    next
    edit 3
        set peerip 10.10.10.3
        set peervd root
        set syncvd vdom1
    end
```

Synchronizing TCP sessions

Synchronize TCP sessions so that if one FortiGate fails, the TCP sessions it was processing can continue to be processed by the remaining FortiGates. After the FortiGate fails, the router or load balancer re-distributes sessions to the FortiGates that are still running. The remaining FortiGates can continue to process these sessions because the sessions have been synchronized with the session tables of all the FortiGates in the deployment.

Enter the following commands on each FortiGate to synchronize TCP sessions with all FortiGates:

```
config system ha
    set session-pickup enable
end
```

Synchronizing UDP and ICMP sessions

Enter the following commands on each FortiGate to synchronize UDP and ICMP (or connectionless) sessions with all the FortiGates. You must enable TCP session synchronization to synchronize other types of sessions.

```
config system ha
    set session-pickup enable
    set session-pickup-connectionless enable
end
```

Synchronizing VoIP sessions

Synchronizing VoIP sessions requires the FortiGates to automatically allow RTP sessions created by a previous SIP session even if the SIP session was received by a different FortiGate. FortiOS calls these created sessions expectation sessions and synchronizing VoIP sessions requires expectation session synchronization.

Use the `diagnose sys session list expectation` command on each FortiGate to display the synchronization state of expectation sessions.

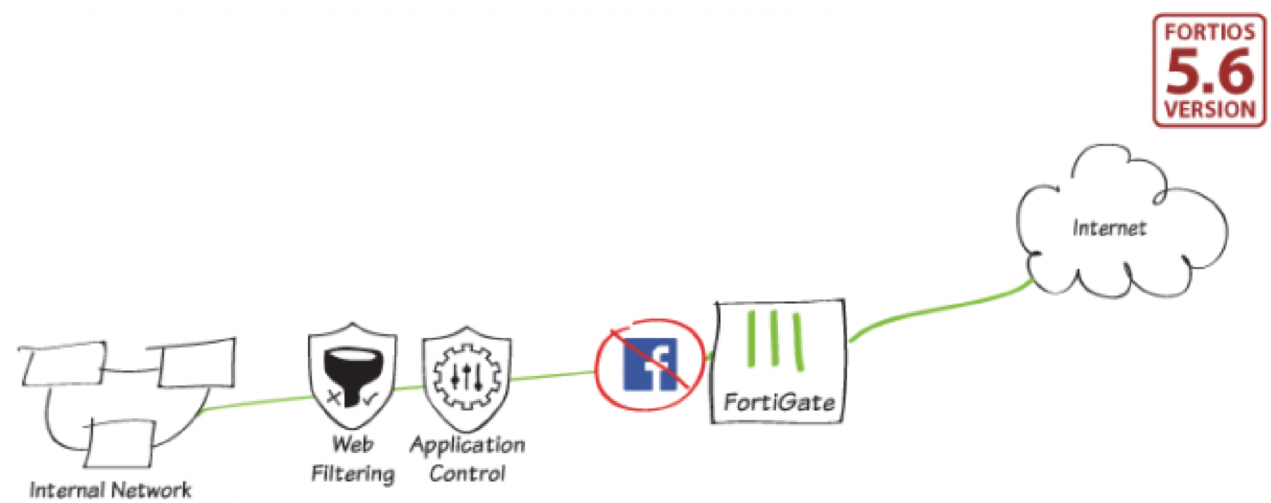
Enter the following commands on each FortiGate to synchronize expectation sessions to support VoIP. You must enable TCP session synchronization to synchronize other types of sessions.

```
config system ha
    set session-pickup enable
    set session-pickup-expectation enable
end
```

Security profiles

This section contains examples about using FortiOS security features to protect your network.

Blocking Facebook



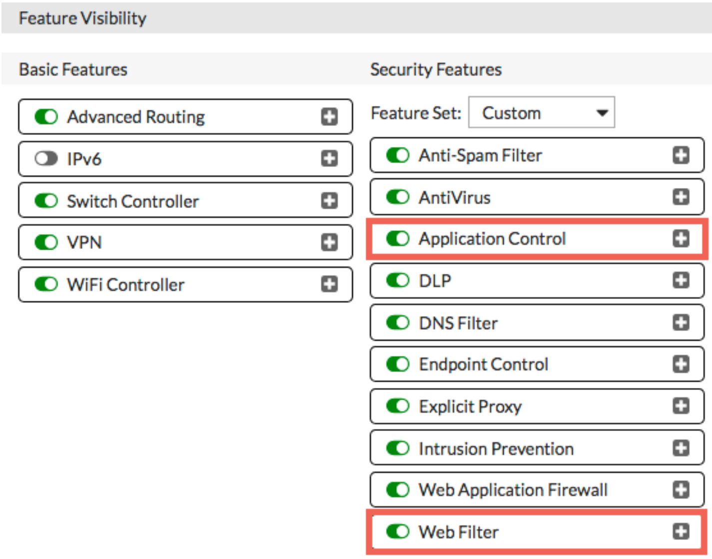
This example explains how to block access to Facebook on your network with a Web Filter security profile and an Application Control security profile. This example works on FortiGates operating in flow-based profile inspection mode or proxy-based inspection mode.

Your FortiGate must have a WiFi network. See Setting up WiFi with a FortiAP or Setting up a WiFi Bridge with a FortiAP.

Next Generation Firewall Policies

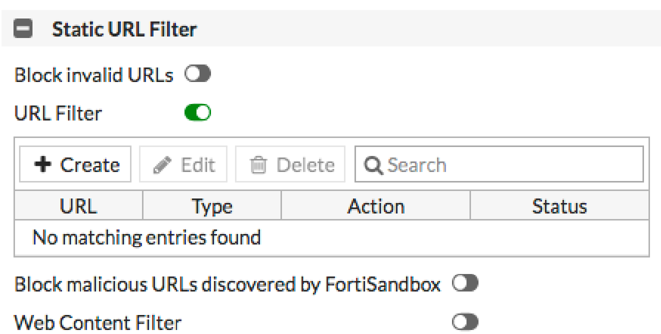
Enabling Web Filtering and Application Control

1. Go to *System* > *Feature Visibility* and enable *Application Control* and *Web Filter*.

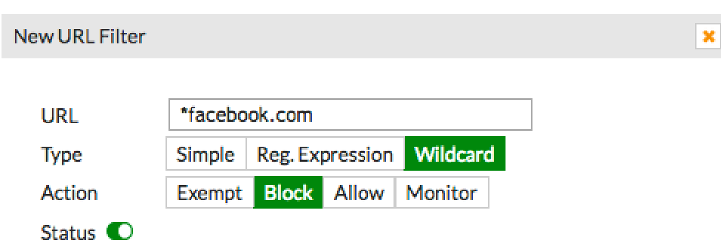


Edit the default Web Filter profile

1. Go to *Security Profiles* > *Web Filter* and edit the default profile.
2. In the *Static URL filter* section, enable *URL Filter*, and click *Create*.



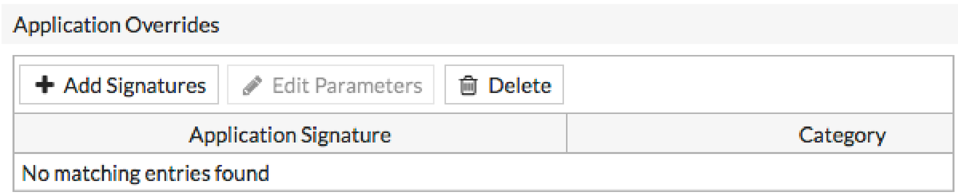
3. Set *URL* to **facebook.com*.
   Set *Type* to *Wildcard*.
   Set *Action* to *Block*.
   Enable *Status*.



4. Click *Apply*.

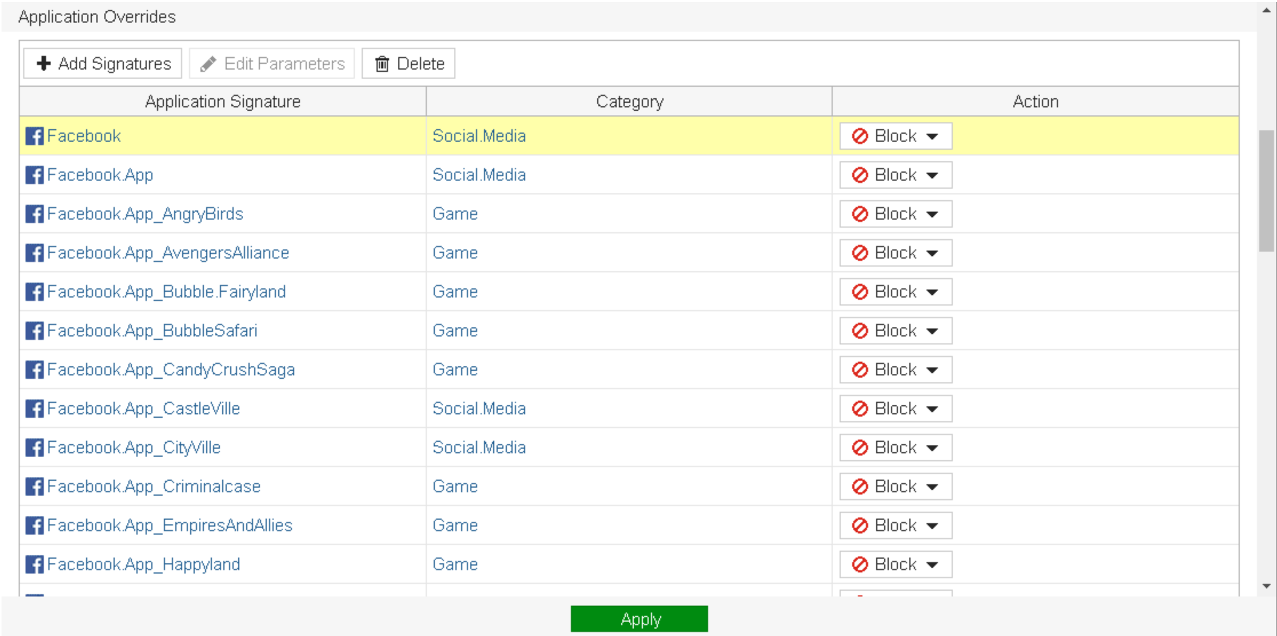
Edit the default Application Control profile

1. Go to *Security Profiles > Application Control* and edit the default profile.
2. In the *Application Overrides* section, click *Add Signatures*.



3. Click *Add Filter* and select *Name*.
   Enter *Facebook* to see a list of all signatures for Facebook applications.
   Click *Select All* and then click *Use Selected Signatures*.

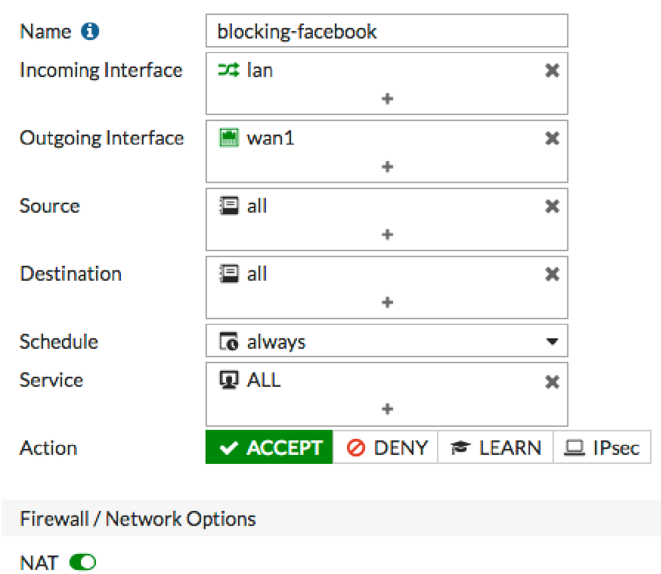
4. In the *Action* column, check that all Facebook application signatures are set to *Block*.



5. Click *Apply*.

Creating the security policy

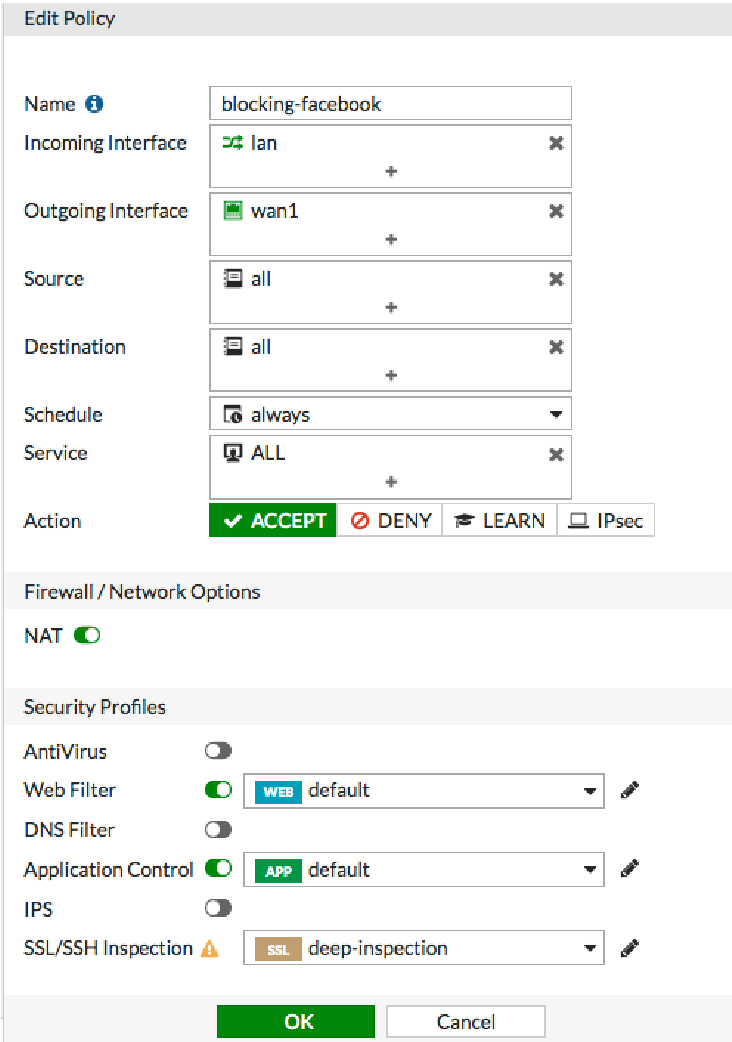
1. Go to *Policy & Objects > IPv4 Policy* and click *Create New*.
2. Give the policy an identifying name, in this example, *blocking-facebook*.
   Set *Incoming Interface* to the internal network.
   Set *Outgoing Interface* to the Internet-facing interface.
   Enable *NAT*.



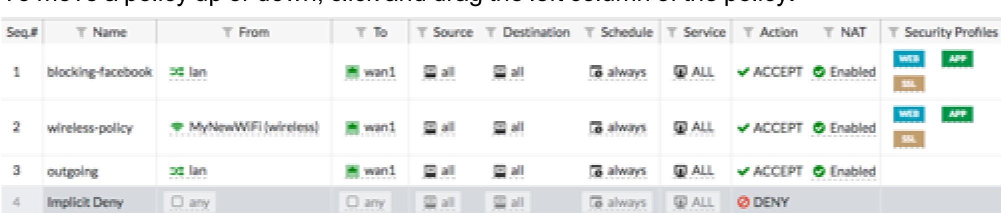
3. In the *Security Profiles* section, enable *Web Filter* and *Application Control*, and use the default web filter and application control profiles.

When you select these profiles, *SSL/SSH Inspection* is enabled by default. If you are using proxy-based inspection mode, then *Proxy Options* is also be enabled by default.

To inspect all traffic, set *SSL/SSH Inspection* to *deep-inspection*.



4. The new policy must be first in the list in order to be applied to Internet traffic. Confirm this by viewing policies *By Sequence*.
   To move a policy up or down, click and drag the left column of the policy.



If your FortiAP is configured in tunnel mode, you must edit the wireless policy and apply the web filter and application control security profiles to that policy.

Results

1. Visit facebook.com.
   HTTPS is automatically applied to facebook.com even if it is not entered in the address bar.
   A *Web Page Blocked!* message appears.
   A FortiGuard warning message appears, stating that the application was blocked.

   Web Page Blocked!

   The page you have requested has been blocked, because the URL is banned.

   URL: https://www.facebook.com/

   Client IP: 192.168.100.1
   Server IP: 157.240.14.35
   User name:
   Group name:

2. Visit a subdomain of Facebook, for example, attachments.facebook.com.
   A *Web Page Blocked!* message appears, blocking the subdomain.

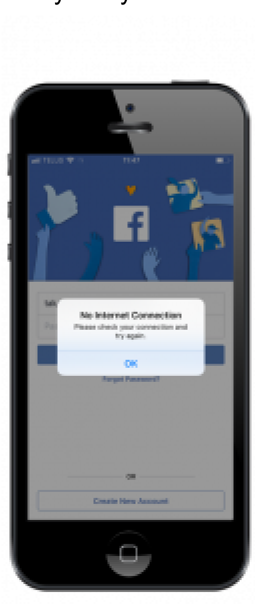
   Web Page Blocked!

   The page you have requested has been blocked, because the URL is banned.

   URL: https://attachments.facebook.com/

   Client IP: 192.168.100.1
   Server IP: 157.240.14.15
   User name:
   Group name:

3. Using a mobile device or any device that has the Facebook app installed, ensure that you are connected to the Internet.
   Open the Facebook app and try to log in.
   Verify that you cannot connect.



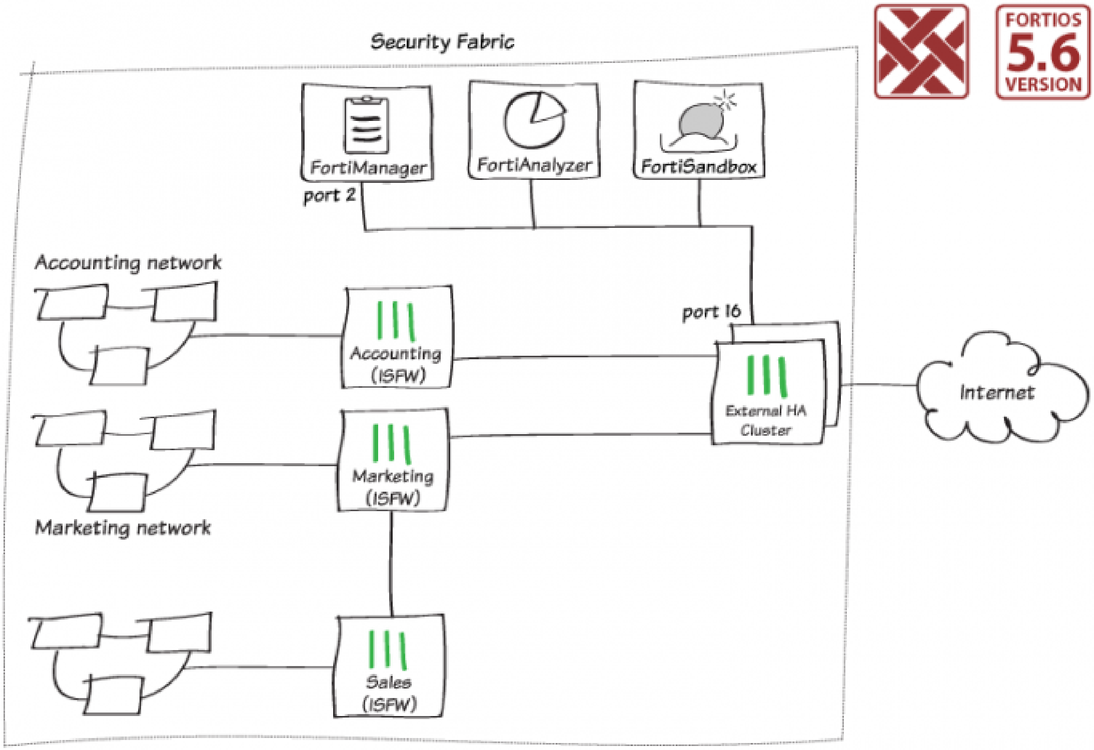
4. Go to *Log & Report* > *Web Filter* and check that facebook.com and attachments.facebook.com are blocked by FortiGate.

#	Date/Time	User	Source	Action	URL	Category Description	Initiator	Sent / Received
1	09:07:24		192.168.100.1	blocked	www.facebook.com/favicon.ico			350 B / 0 B
2	09:06:54		192.168.100.1	blocked	www.facebook.com/			391 B / 0 B
3	09:06:45		192.168.100.1	blocked	www.google.ca/complete/search?client=chrome-omni&gs_ri=c...			860 B / 0 B
4	09:05:23		192.168.100.1	blocked	attachments.facebook.com/favicon.ico			373 B / 0 B
5	09:05:23		192.168.100.1	blocked	attachments.facebook.com/			438 B / 0 B
6	09:05:20		192.168.100.1	blocked	www.google.ca/complete/search?client=chrome-omni&gs_ri=c...			6.18 kB / 198.29 kB
7	09:03:00		192.168.100.1	blocked	www.facebook.com/favicon.ico			359 B / 52 B

5. Go to *Log & Report* > *Application Control* and check that the Facebook application is blocked by FortiGate.

#		Date/Time	Source	Destination	Application Name	Action
1		11:52:17	192.168.100.1	172.217.7.3 (www.gstatic.com)	QUIC	block
2		11:52:14	192.168.100.1	208.91.114.47 (cli.fortinet.com)	HTTP.BROWSER_Firefox	pass
3		11:52:13	192.168.100.1	172.217.7.3 (www.gstatic.com)	QUIC	block
4		11:52:12	192.168.100.1	157.240.14.35 (star-mini.c10r.facebook.com)	Facebook	block
5		11:52:12	192.168.100.1	172.217.7.3 (www.gstatic.com)	Google.Services	pass
6		11:52:12	192.168.100.1	172.217.7.3 (www.gstatic.com)	QUIC	block
7		11:52:09	192.168.100.1	172.217.7.3 (www.gstatic.com)	QUIC	block

FortiManager in the Fortinet Security Fabric



This example shows you how to add a FortiManager to the Fortinet Security Fabric. This scenario simplifies network administration because you can manage all the FortiGates in the network from FortiManager.

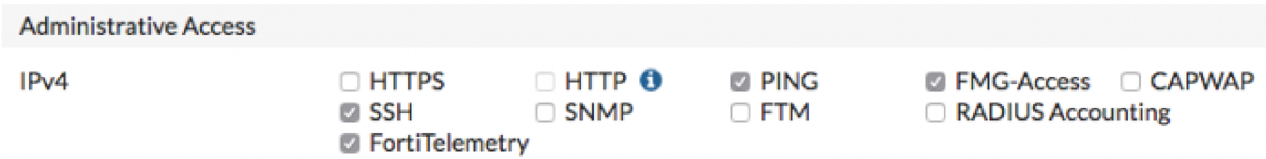
In this example, FortiManager is added to an existing Security Fabric with an HA cluster, called Edge, configured as the root FortiGate. In this network, the subnet 192.168.55.0 is used for external devices such as a FortiAnalyzer. The FortiManager is added to this subnet.

Security Fabric Installation

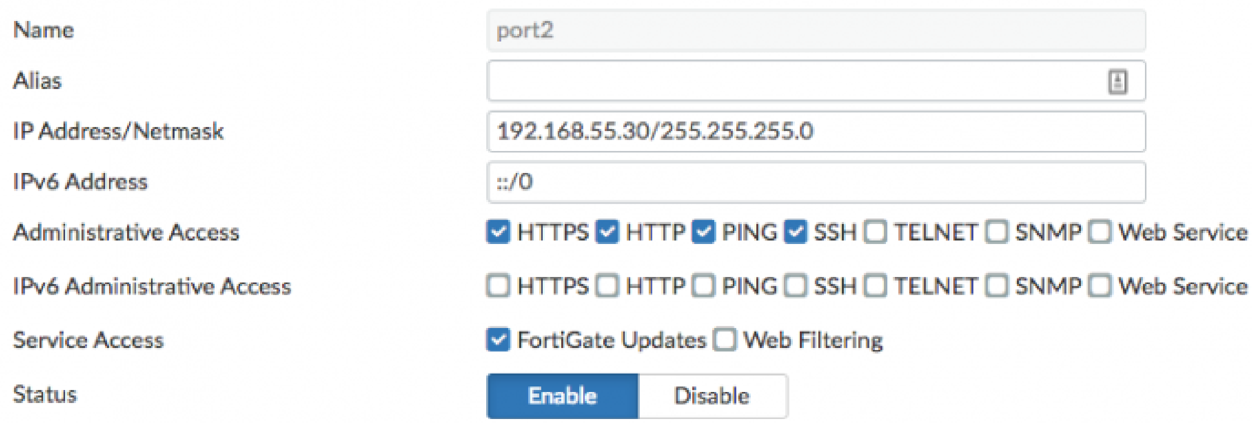
Connecting FortiManager and Edge

In this example, Edge's port 16 connects to port 2 on the FortiManager.

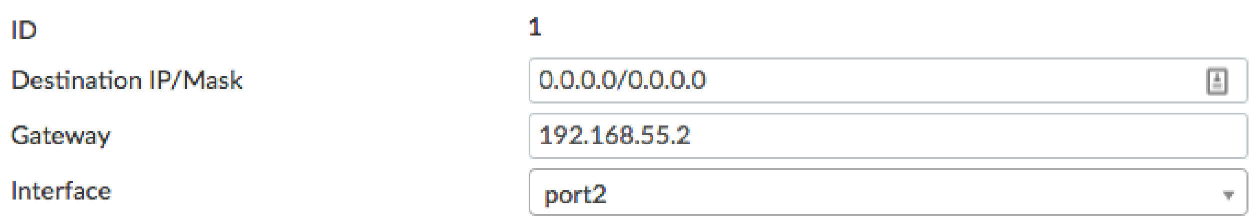
1. On Edge, go to *Network* > *Interfaces* and edit port 16.
2. Configure *Administrative Access* to allow *FMG-Access* and *FortiTelemetry*.



3. On the FortiManager, go to *System Settings* > *Network*, select *All Interfaces*, and edit port 2.
4. Set *IP Address/Netmask* to an internal IP address (in this example, *192.168.55.30/255.255.255.0*), and set the following administrative and service access options.



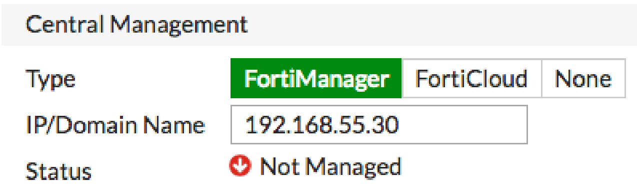
5. Go to *System Settings* > *Network*, select *Routing Table*, and add a default route for port 2.
6. Set *Gateway* to the IP address of Edge's port 16.



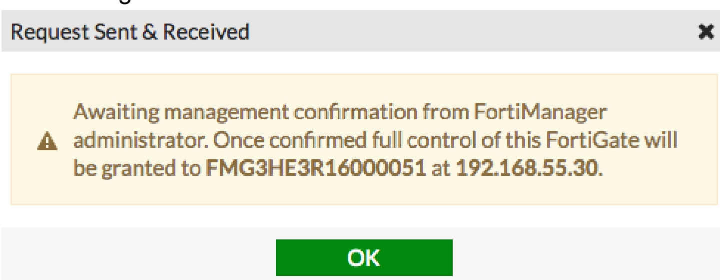
7. Connect port 2 on the FortiManager to port 16 on Edge.

Configuring central management on Edge

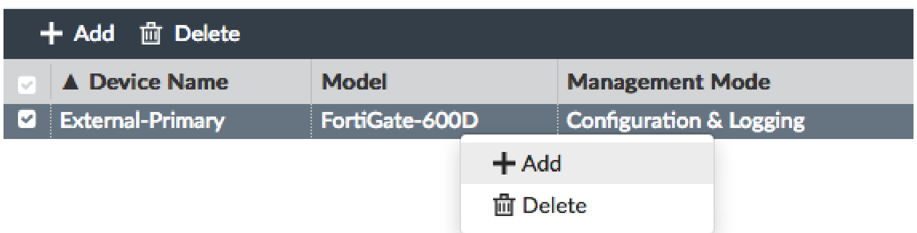
1. On Edge, go to *System > Settings*.
2. In the *Central Management* section, select *FortiManager* and enter the *IP/Domain Name*.



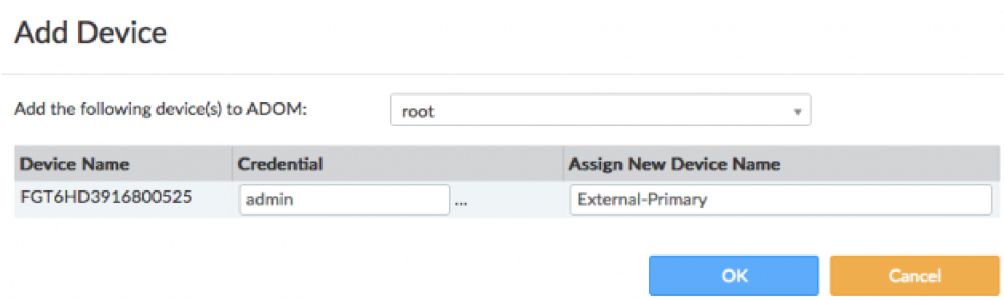
3. Click *Apply* and a message appears stating that the FortiGate's message was received by the FortiManager and is now waiting for confirmation.



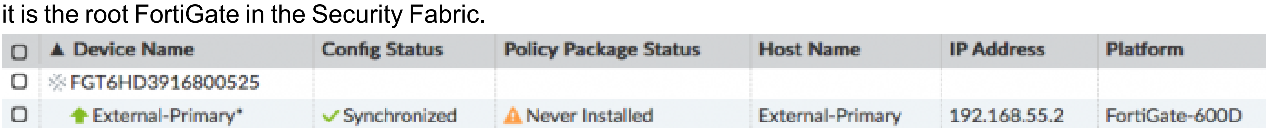
4. On the FortiManager, go to *Device Manager > Unregistered Devices*.
5. Select *External* and then select *Add*.



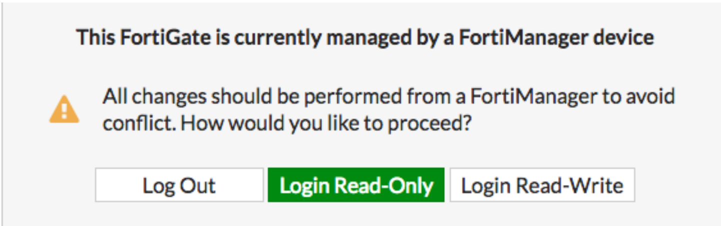
6. Add Edge to the root ADOM.



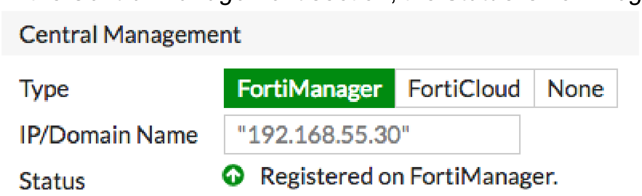
7. Edge is now on the *Managed FortiGates* list and is part of a Security Fabric group. The * beside Edge indicates that it is the root FortiGate in the Security Fabric.



8. Connect to Edge. A message indicates that the FortiGate is now managed by a FortiManager. Click *Login Read-Only*.



9. On Edge, go to *System > Settings*.
10. In the *Central Management* section, the *Status* is now *Registered on FortiManager*.

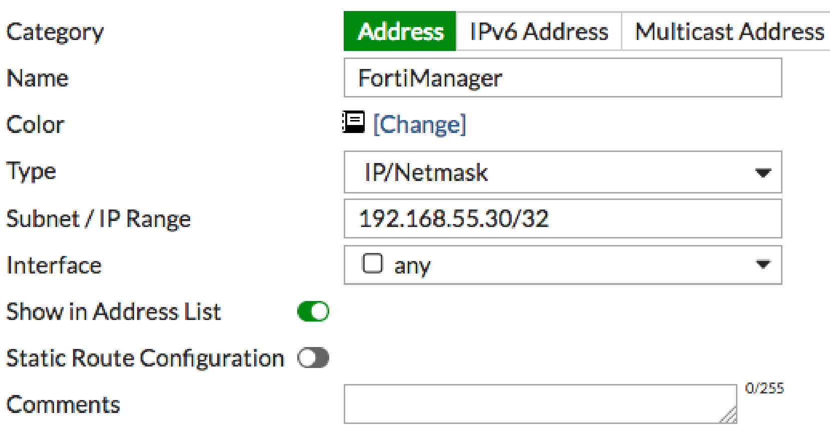


11. For each FortiGate in the Security Fabric, ensure the interface connected to Edge allows *FMG-Access*.
12. Configure central management for all the other FortiGates in the Security Fabric.

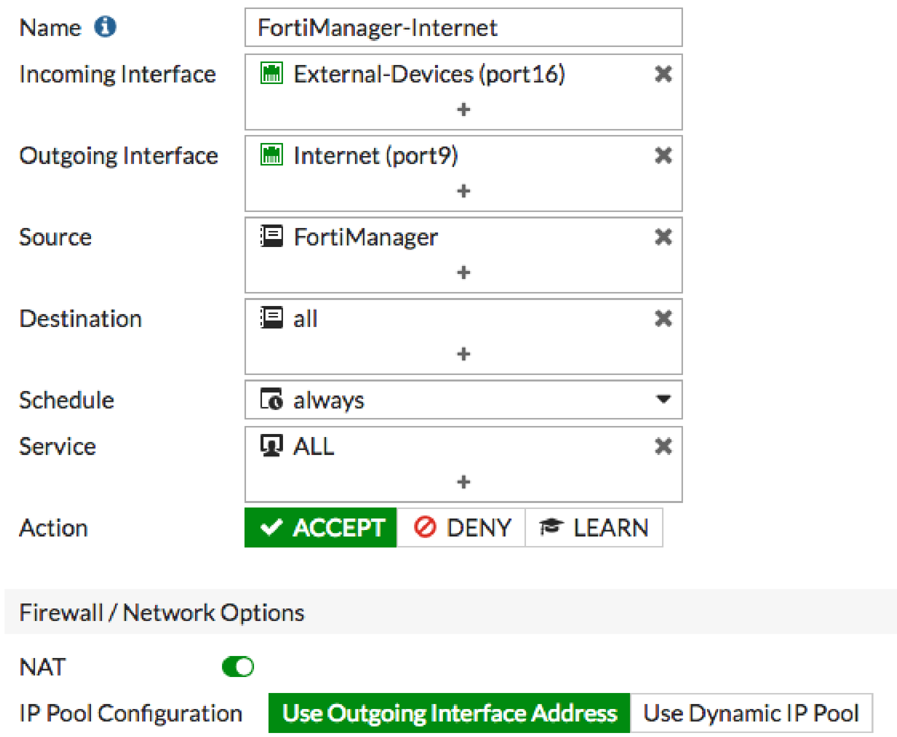
Allowing FortiManager to have Internet access

To communicate with FortiGuard, FortiManager requires Internet access.

1. On Edge, go to *Policy & Objects > Addresses* and create an address the FortiManager.

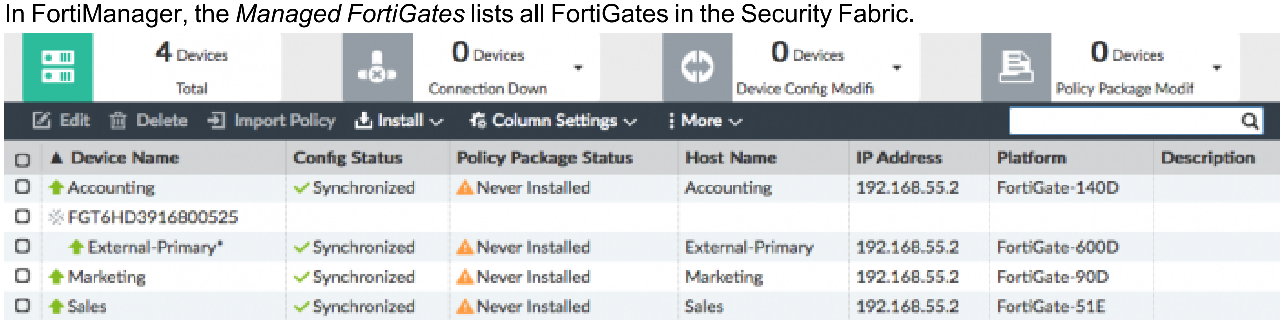


2. Go to *Policy & Objects > IPv4 Policy* and create a policy that allows FortiManager to access the Internet.

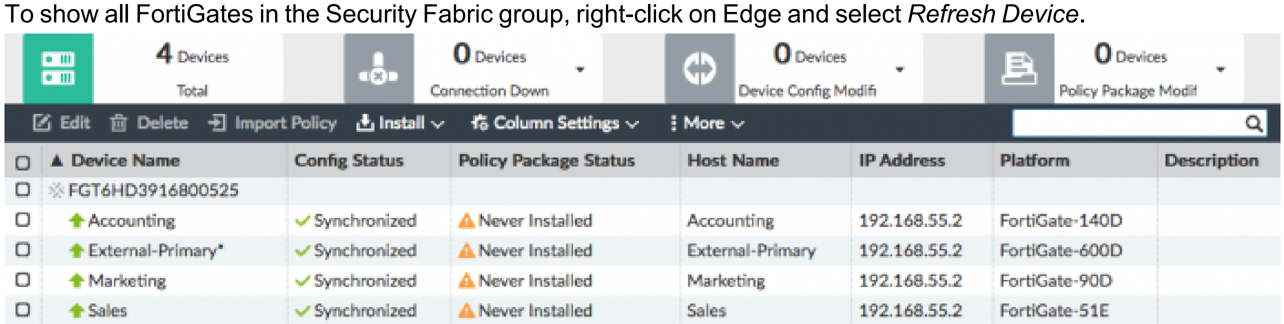


Results

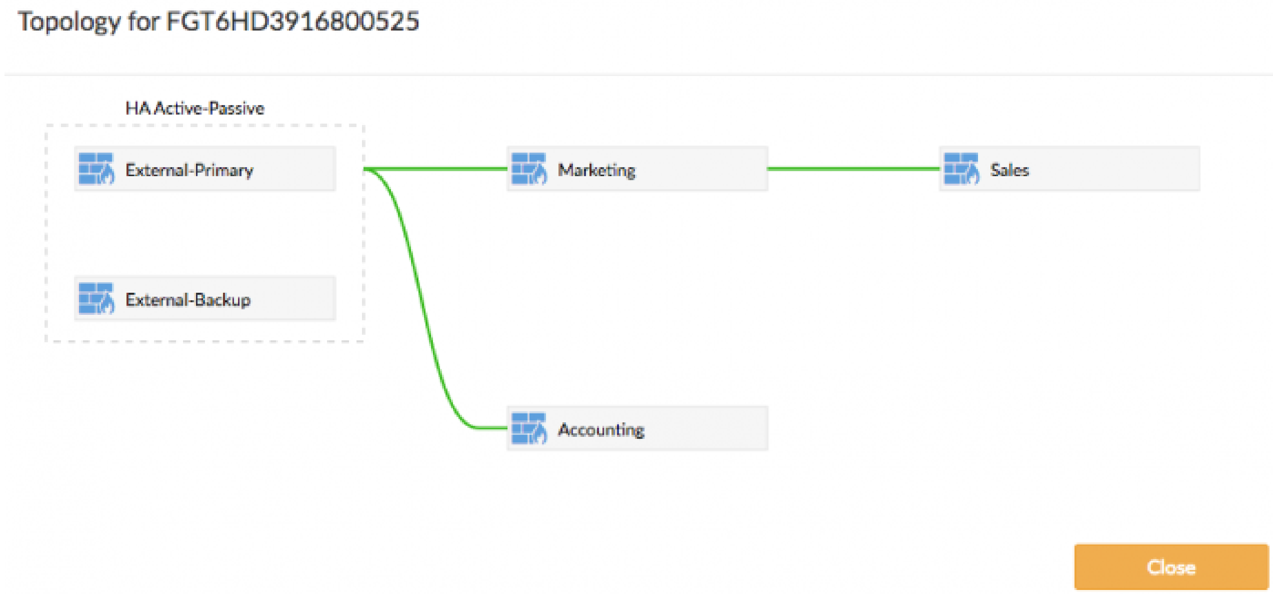
1. In FortiManager, the *Managed FortiGates* lists all FortiGates in the Security Fabric.



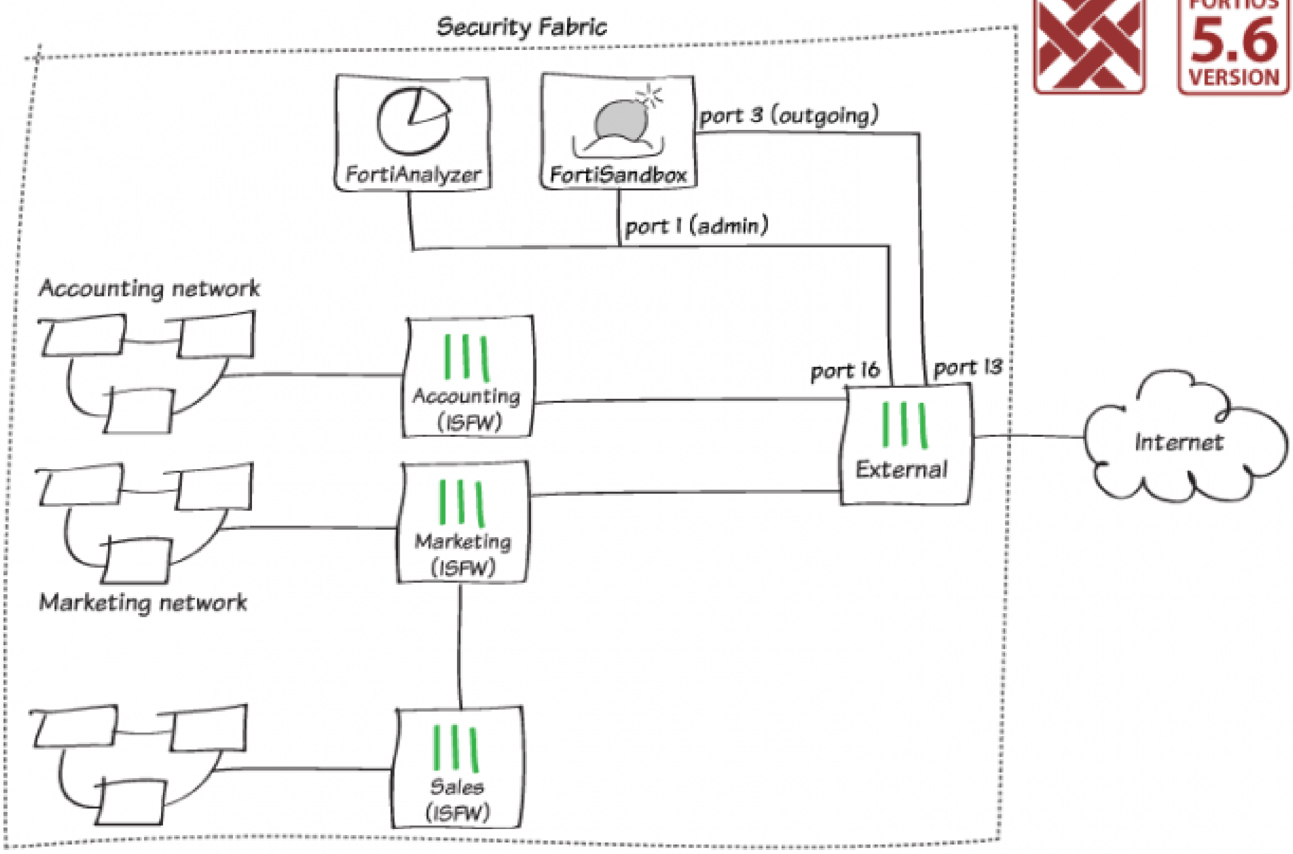
2. To show all FortiGates in the Security Fabric group, right-click on Edge and select *Refresh Device*.



3. Right-click on the Security Fabric group and select *Fabric Topology* to display the topology of the Security Fabric.



FortiSandbox in the Fortinet Security Fabric



This example shows you how to add a FortiSandbox to the Fortinet Security Fabric and configure each FortiGate in the network to send suspicious files to FortiSandbox for sandbox inspection. FortiSandbox scans and tests these files in isolation from your network.

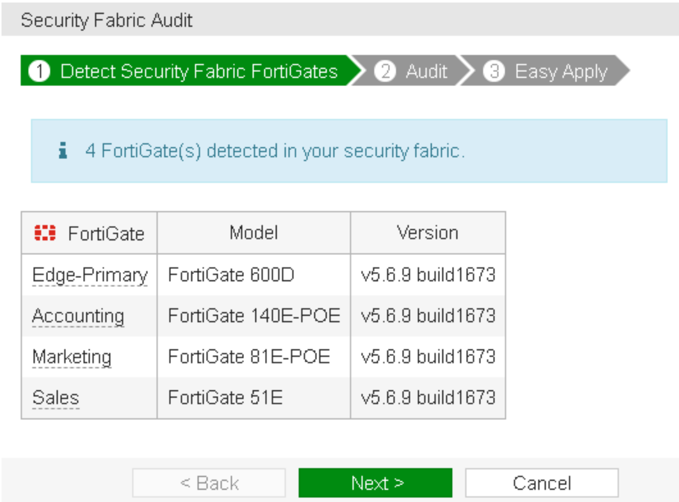
This example uses the Security Fabric example configuration created in the Fortinet Security Fabric collection. The FortiSandbox connects to the external root FortiGate in the Security Fabric, known as Edge. There are two connections between the devices:

- FortiSandbox port 1 (administration port) connects to External port 16.
- FortiSandbox port 3 (VM outgoing port) connects to External port 13.

You can use a separate Internet connection for FortiSandbox port 3 rather than connect through the external FortiGate to use your main Internet connection. This configuration avoids getting IP addresses from your main network blacklisted if malware tested on the FortiSandbox generates an attack. If you use this configuration, you can skip the steps listed for FortiSandbox port 3.

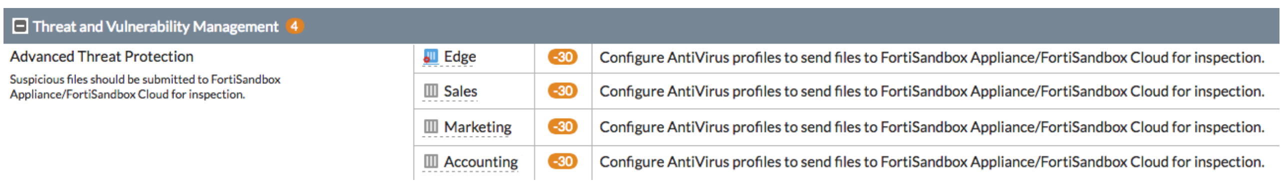
Checking the Security Rating

1. On Edge, go to *Security Fabric > Audit* and run an audit for the Security Fabric.



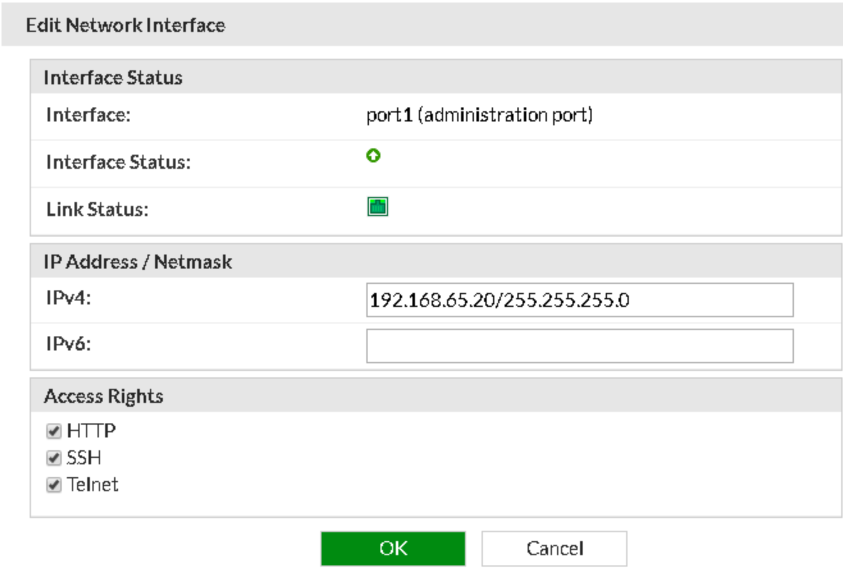
Since you have not installed a FortiSandbox, the Security Fabric fails the *Advanced Threat Protection*. See *Threat and Vulnerability Management* section.

In this example, the *Security Rating Score* decreases by 30 points for each of the four FortiGates in the Security Fabric.

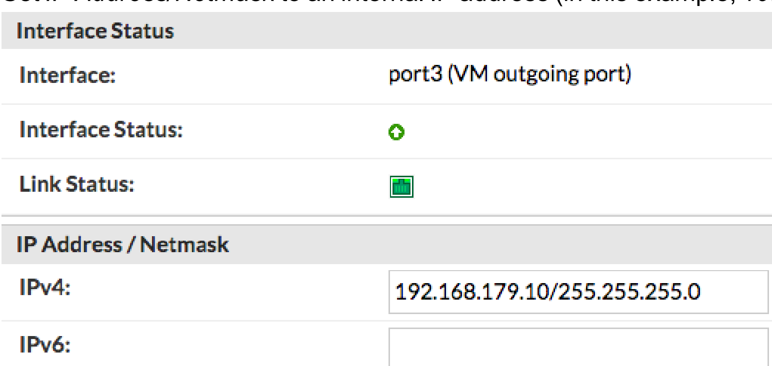


Connecting FortiSandbox and Edge

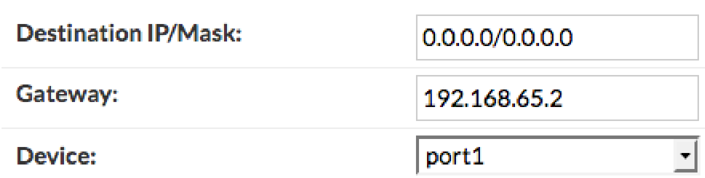
1. Connect to the FortiSandbox.
2. Go to *Network > Interfaces* and edit *port1*.
   This port is used for communication between FortiSandbox and the rest of the Security Fabric.
3. Set *IP Address/Netmask* to an internal IP address.
   In this example, FortiSandbox connects to the same subnet as the Security Fabric's FortiAnalyzer, using the IP address *192.168.65.20*.



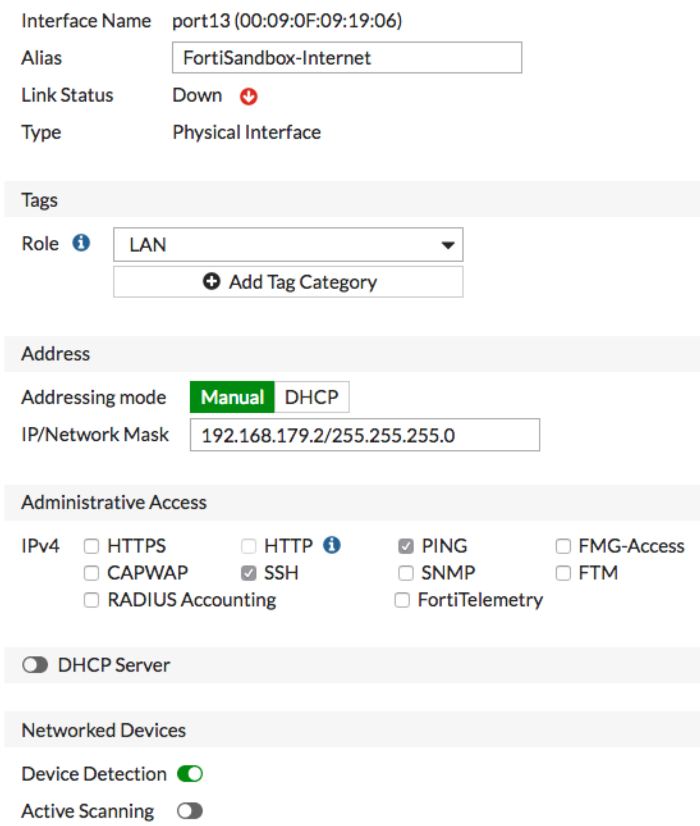
4. Edit *port3*.
   This port is used for outgoing communication by virtual machines (VMs) running on FortiSandbox. It's recommended that you connect this port to a dedicated interface on your FortiGate to protect the rest of the network from threats that FortiSandbox is currently investigating.
5. Set *IP Address/Netmask* to an internal IP address (in this example, *192.168.179.10/255.255.255.0*).



6. Go to *Network > System Routing* to add a static route.
   Set *Gateway* to the IP address of the FortiGate interface that port 1 connects to (in the example, *192.168.65.2*).



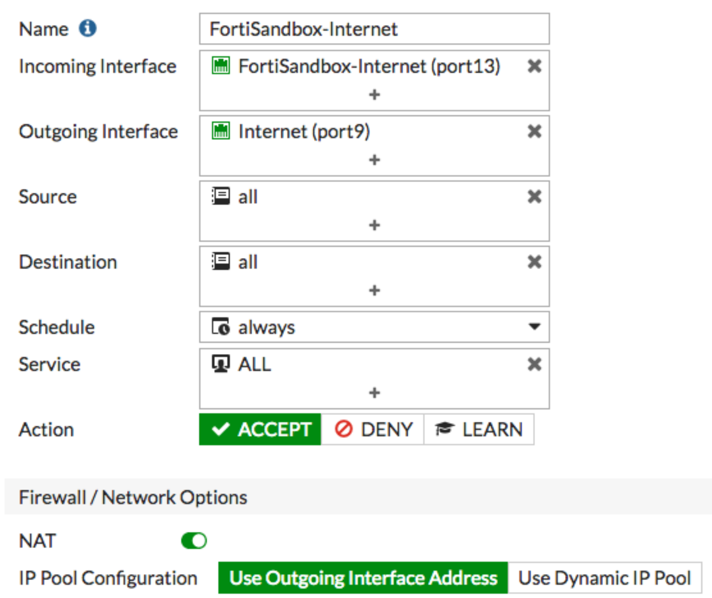
7. Connect to Edge.
8. Go to *Network > Interfaces* to configure the port that connects to port3 on the FortiSandbox (in this example, *port13*).
   Set *IP/Network Mask* to an address in the same subnet as port 3 on the FortiSandbox (in this example, *192.168.179.2/255.255.255.0*).



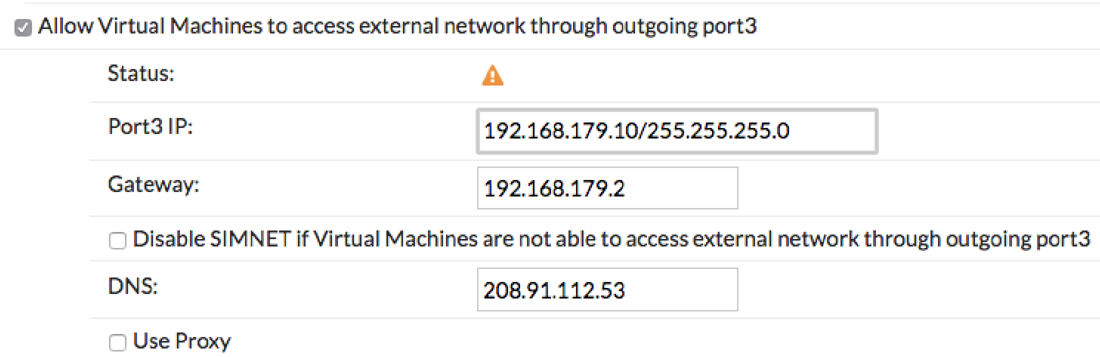
9. Connect the FortiSandbox to the Security Fabric.

Allowing VM Internet access

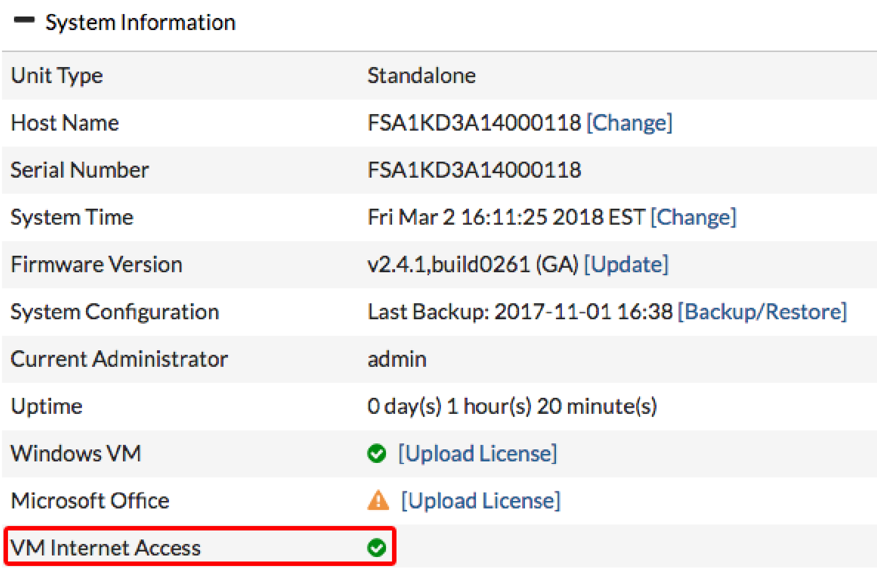
1. On Edge, go to *Policy & Objects* > *IPv4 Policy* and create a policy that allows connections from the FortiSandbox to the Internet.



2. In FortiSandbox, go to *Scan Policy > General* and select *Allow Virtual Machines to access external network through outgoing port3*.
   Set *Gateway* to the IP address of port 13 on the FortiGate.

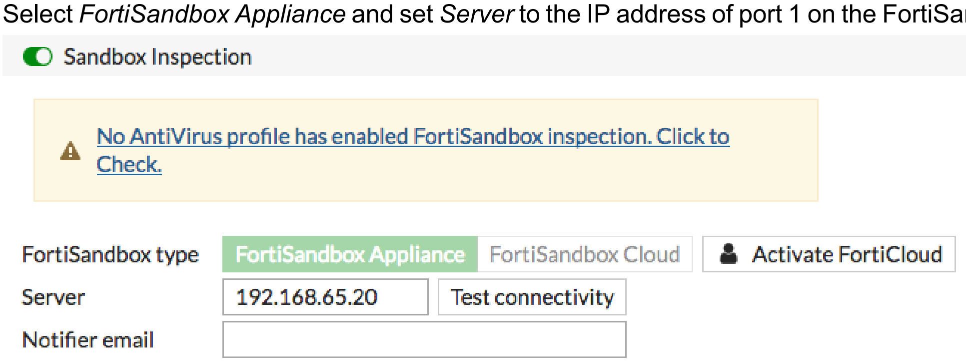


3. Go to *Dashboard System Information* widget and verify that *VM Internet Access* has a green checkmark beside it.

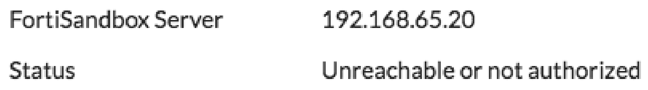


Adding FortiSandbox to Security Fabric

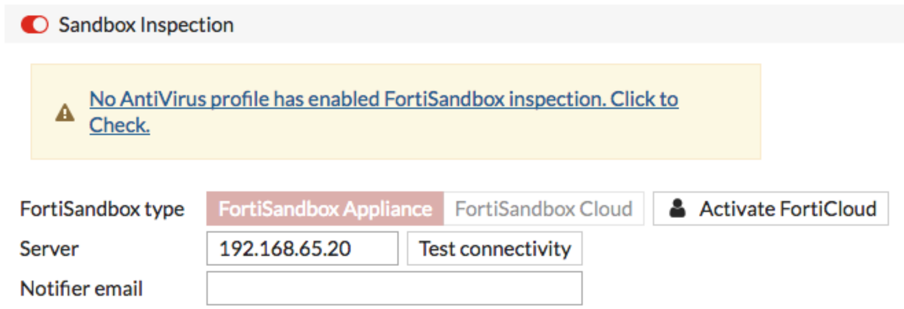
1. On Edge, go to *Security Fabric > Settings* and enable *Sandbox Inspection*.
2. Select *FortiSandbox Appliance* and set *Server* to the IP address of port 1 on the FortiSandbox.



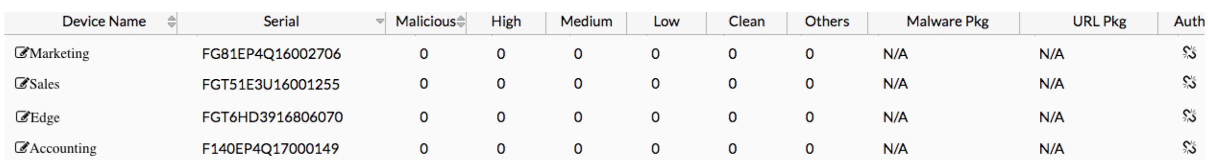
3. Click *Test Connectivity*.
   An error message appears because Edge hasn't been authorized on FortiSandbox.



   External, as the root FortiGate, pushes FortiSandbox settings to the other FortiGates in the Security Fabric.
4. To verify this, on Accounting, go to *Security Fabric > Settings*.

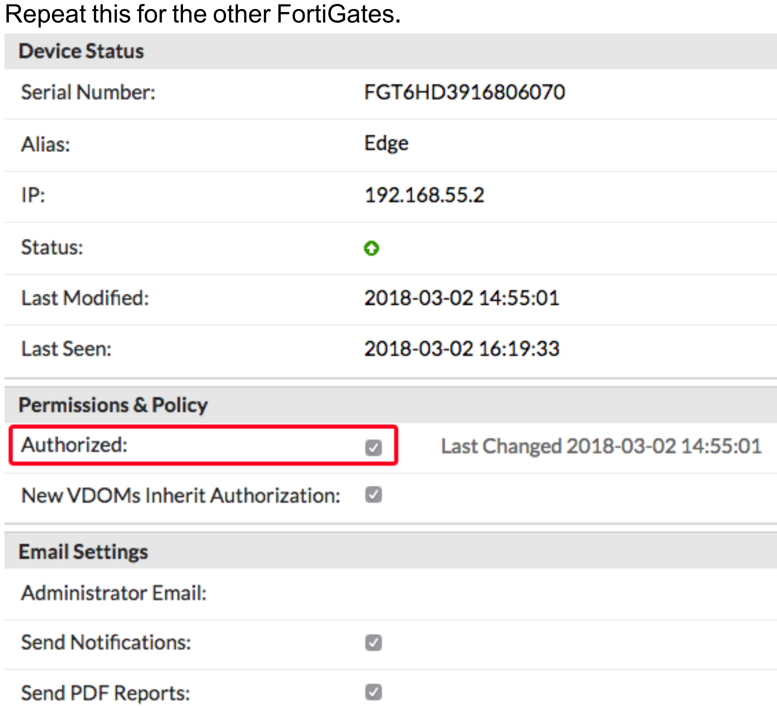


5. In FortiSandbox, go to *Scan Input > Device*.
   The FortiGates in the Security Fabric (Edge, Accounting, Marketing, and Sales) are listed but the *Auth* column indicates that the devices are unauthorized.

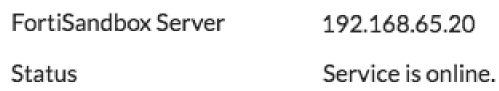


Device Name	Serial	Malicious	High	Medium	Low	Clean	Others	Malware Pkg	URL Pkg	Auth
Marketing	FG81EP4Q16002706	0	0	0	0	0	0	N/A	N/A	
Sales	FGT51E3U16001255	0	0	0	0	0	0	N/A	N/A	
Edge	FGT6HD3916806070	0	0	0	0	0	0	N/A	N/A	
Accounting	F140EP4Q17000149	0	0	0	0	0	0	N/A	N/A	

6. Edit Edge.
7. In the *Permissions & Policy* section, select *Authorized*.
8. Repeat this for the other FortiGates.



9. On Edge, go to *Security Fabric* > *Settings* and test the *Sandbox Inspection* connectivity again. Edge is now connected to the FortiSandbox.



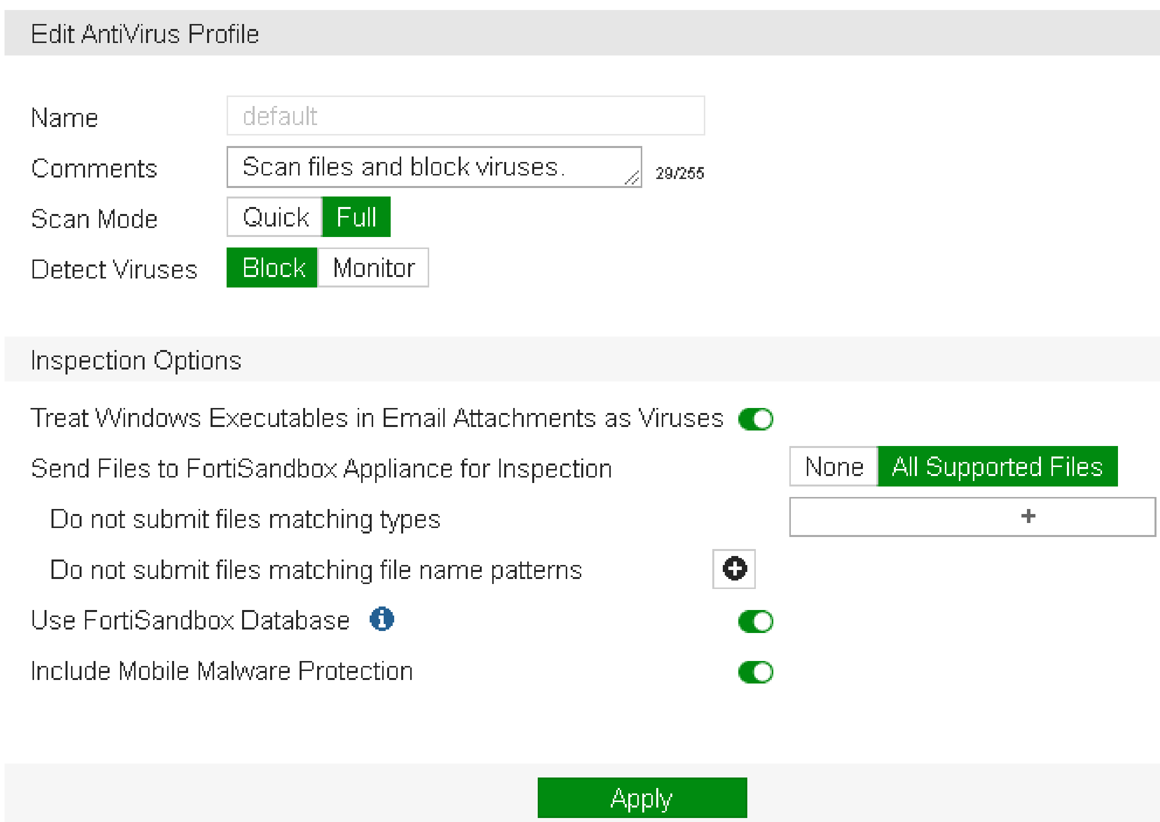
Adding sandbox inspection to security profiles

You can apply sandbox inspection with three types of security inspection: antivirus, web filter, and FortiClient compliance profiles.

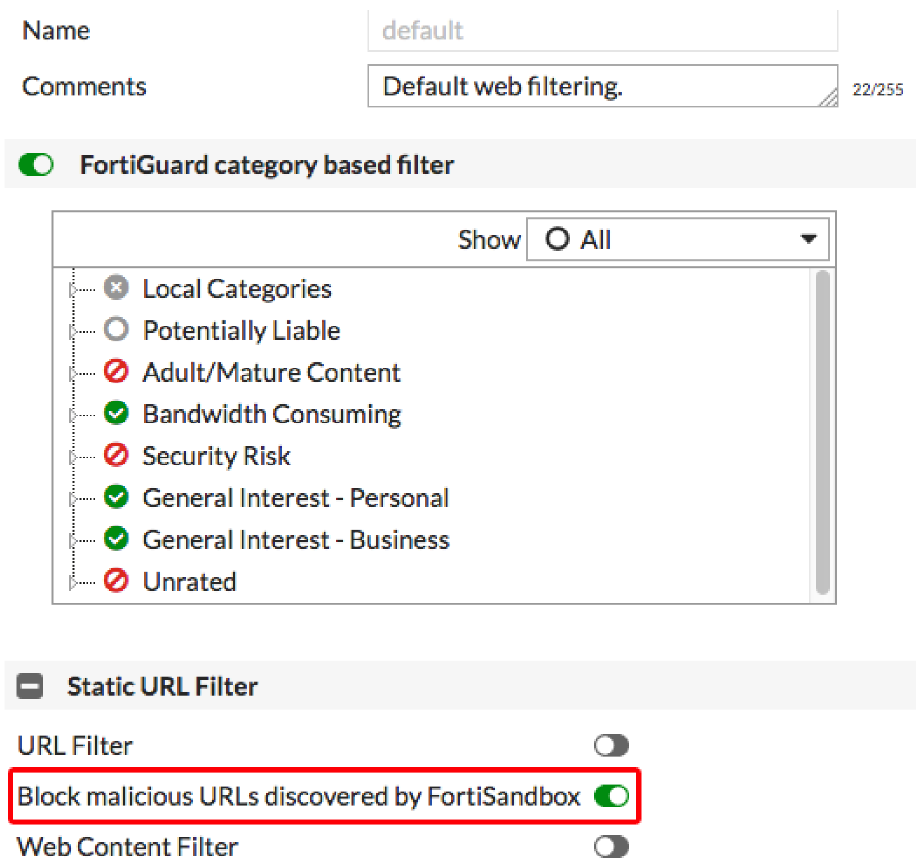
This example shows you how to add sandbox inspection to all FortiGates in the Security Fabric individually using the profiles that each FortiGate applies to network traffic.

To pass the *Advanced Threat Protection* check, add sandbox inspection to antivirus profiles for all FortiGates in the Security Fabric.

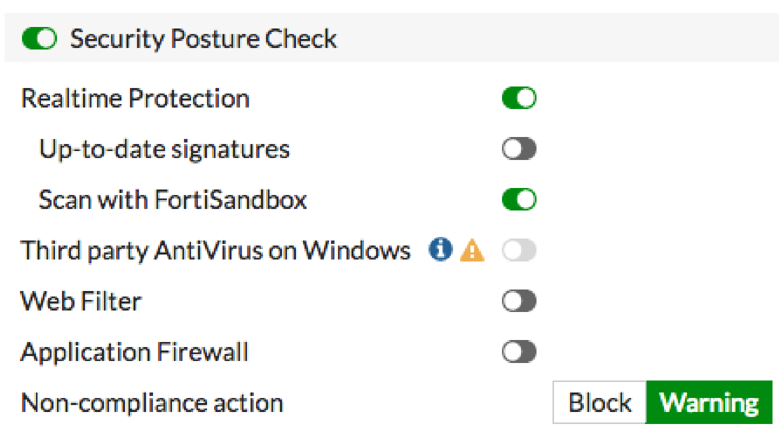
1. On Edge, go to *Security Profiles* > *AntiVirus* and edit the *default* profile.
2. In the *Inspection Options* section, set *Send Files to FortiSandbox Appliance for Inspection* to *All Supported Files*. Enable *Use FortiSandbox Database* so that if FortiSandbox discovers a threat, it adds a signature for that file to the antivirus signature database on the FortiGate.
   Click *Apply*.



3. Go to *Security Profiles* > *Web Filter* and edit the *default* profile.
4. In the *Static URL Filter* section, enable *Block malicious URLs discovered by FortiSandbox* so that if FortiSandbox discovers a threat, it adds the URL to the list of URLs that are blocked by the FortiGate.



5. Go to *Security Profiles > FortiClient Compliance Profiles* and edit the *default* profile.
6. Enable *Security Posture Check*
   Enable *Realtime Protection*.
   Enable *Scan with FortiSandbox*.

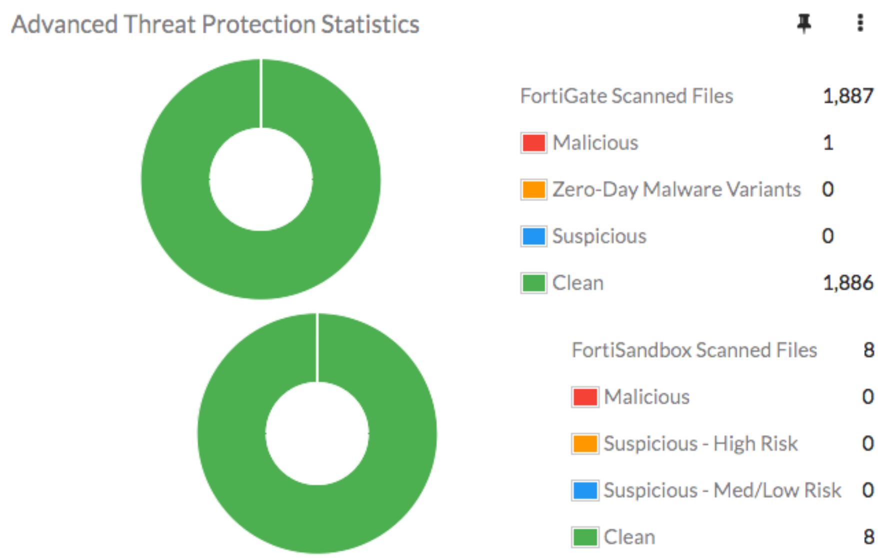


Results

If a FortiGate in the Security Fabric discovers a suspicious file, it sends the file to FortiSandbox.

You can view information about scanned files on either the FortiGate that sent the file or on FortiSandbox.

1. On FortiGate, go to *Dashboard > Main* and locate the *Advanced Threat Protection Statistics* widget. This widget shows files that both the FortiGate and FortiSandbox scan.

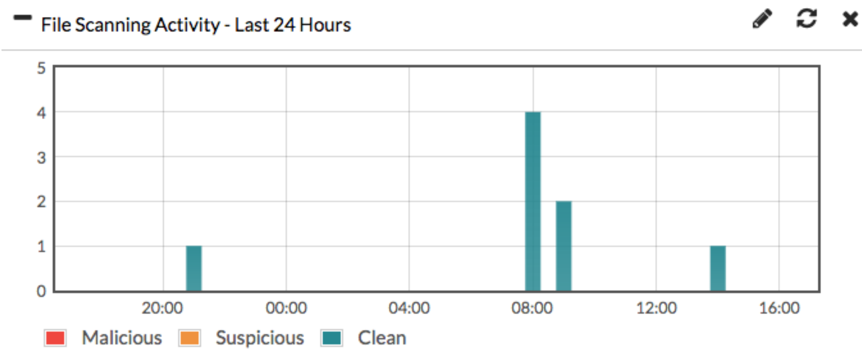


2. On FortiSandbox, go to *Dashboard* and view the *Scanning Statistics* widget for a summary of scanned files.

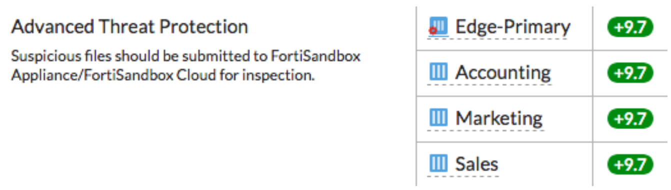
Scanning Statistics - Last 24 Hours

Rating	Sniffer	Device(s)	On Demand	Network	Adapter	URL	All
Malicious	0	0	0	0	0	0	0
Suspicious - High Risk	0	0	0	0	0	0	0
Suspicious - Medium Risk	0	0	0	0	0	0	0
Suspicious - Low Risk	0	0	0	0	0	0	0
Clean	0	8	0	0	0	0	8
Other	0	0	0	0	0	0	0
Processed	0	8	0	0	0	0	8
Pending	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Processing	*0*	*0*	*0*	*0*	*0*	*0*	*0*
Total	*0*	*8*	*0*	*0*	*0*	*0*	*8*

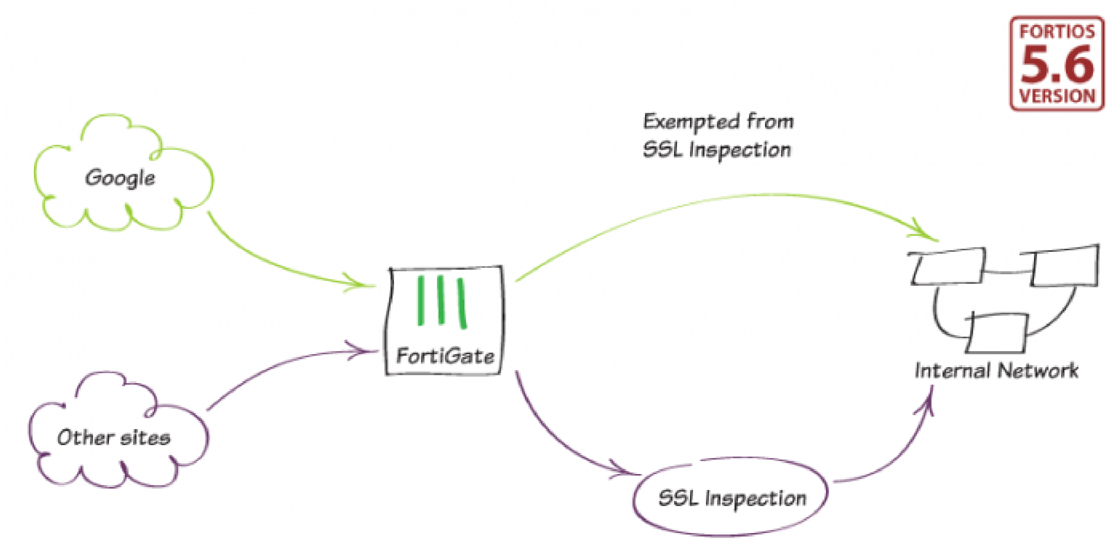
You can also view a timeline of scanning in the *File Scanning Activity* widget.



3. On Edge, go to *Security Fabric* > *Audit* and run a new audit.
   When it is finished, select the *All Results* view.
   In this example, all four FortiGates in the Security Fabric pass the *Advanced Threat Protection* check and the Security Rating Score increases by 9.7 points for each FortiGate.



Exempting Google from SSL inspection



This example shows you how to exempt Google websites from deep SSL inspection. Exempting these websites allows Google Chrome to access them without errors.

Be careful when exempting websites. In general, exempt only websites you can trust. You might consider exempting websites that do not function properly when subjected to SSL inspection, such as a site (or application) that uses certificate/public key pinning.

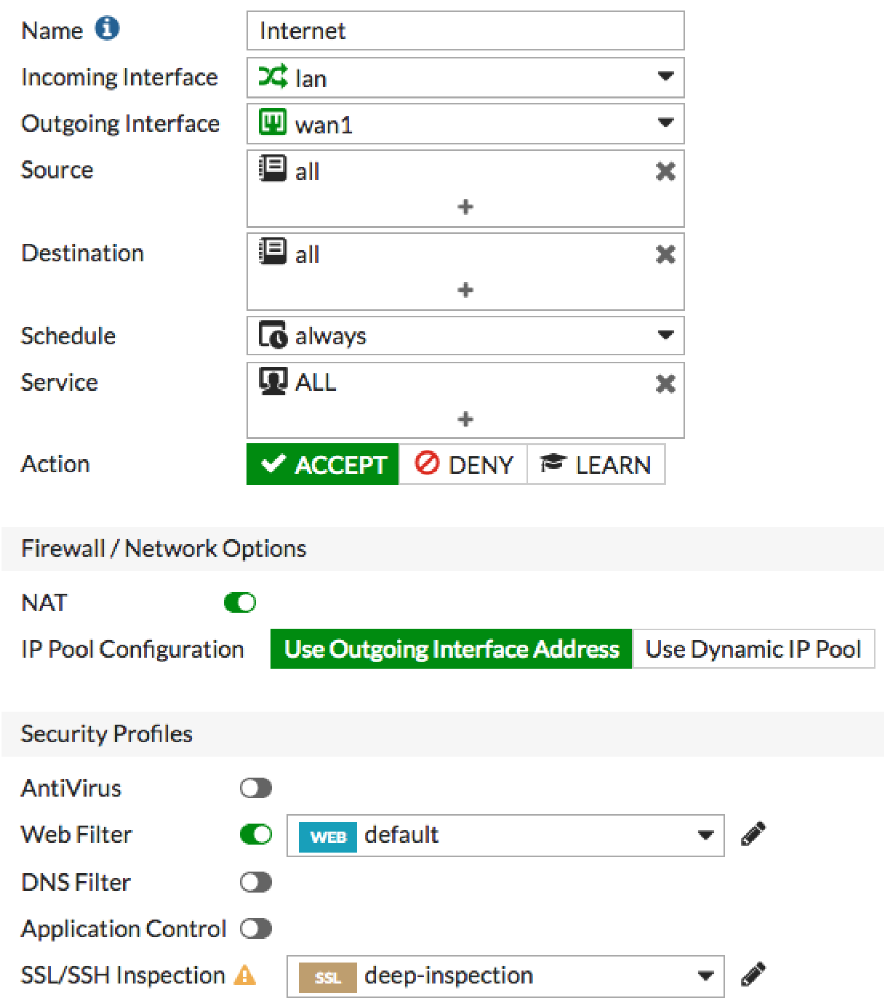
This example shows exempting google.ca from SSL inspection. You can substitute your local Google search domain.

Using the default deep-inspection profile

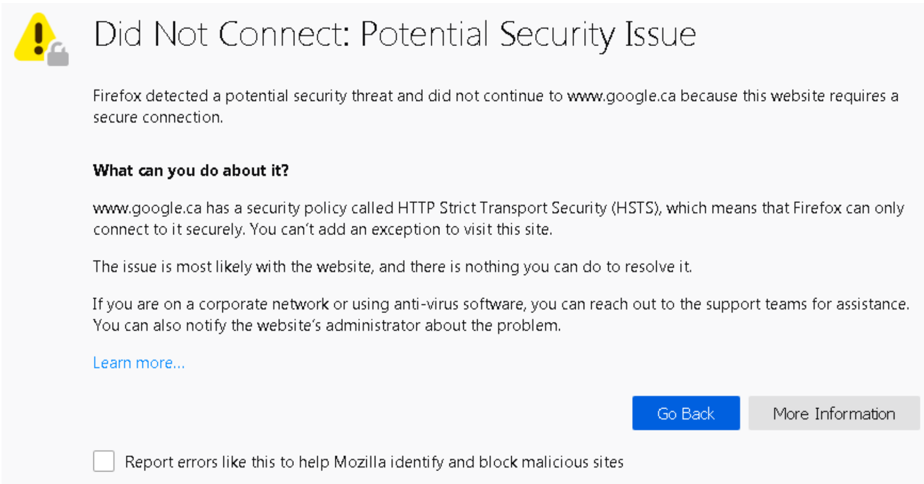
1. Go to *System* > *Feature Visibility* and ensure *Multiple Security Profiles* is enabled.

2. Go to *Policy & Objects* > *IPv4 Policy* and edit the policy that allows users on the internal network to access the Internet.
3. In the *Security Profiles* section, enable *Web Filter* and use the default profile.
   SSL/SSH Inspection is enabled by default. Select the *deep-inspection* profile.

   Using the *deep-inspection* profile, FortiGate impersonates the recipient of the originating SSL session, then decrypts and inspects the content. FortiGate then re-encrypts the content, creates a new SSL session between FortiGate and the recipient by impersonating the sender, and sends the content to the sender.



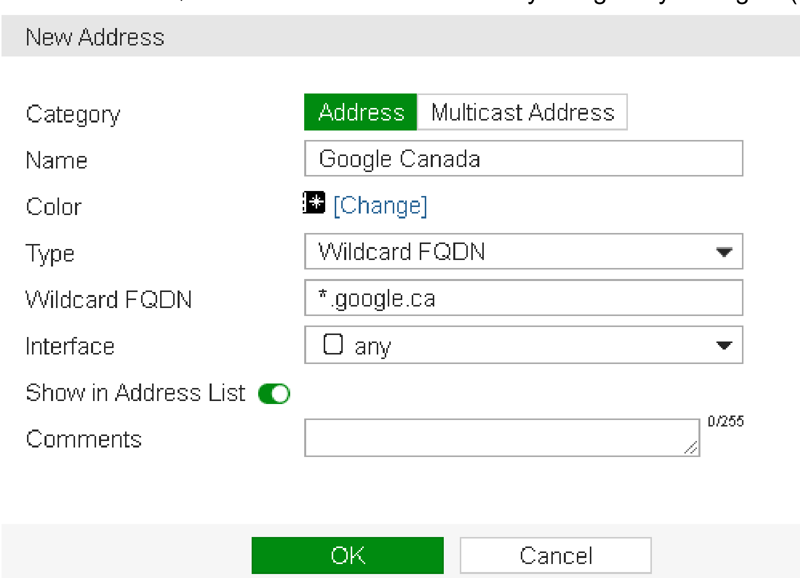
4. Browse to google.ca.
   This example uses Mozilla Firefox. An error appears that you cannot bypass.
   This error occurs because Firefox uses certificate pinning (also called SSL pinning or public key pinning). This allows Firefox to determine that the certificate from the website does not match one belonging to Google. Because of this, Firefox believes that a “man in the middle” attack is occurring and blocks you from the compromised website.



Creating an SSL/SSH profile that exempts Google

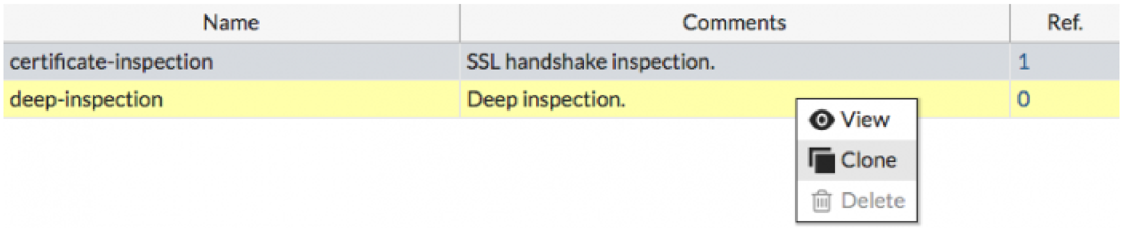
The two default SSL/SSH inspection profiles, *certificate-inspection* and *deep-inspection*, are read-only. To exempt Google, you must create a new profile.

1. Go to *Policy & Objects* > *Addresses* and create a new address.
   Set *Type* to *Wildcard FQDN*.
   Set *Wildcard FQDN* to the domain name used by Google in your region (in this example, **.google.ca*).

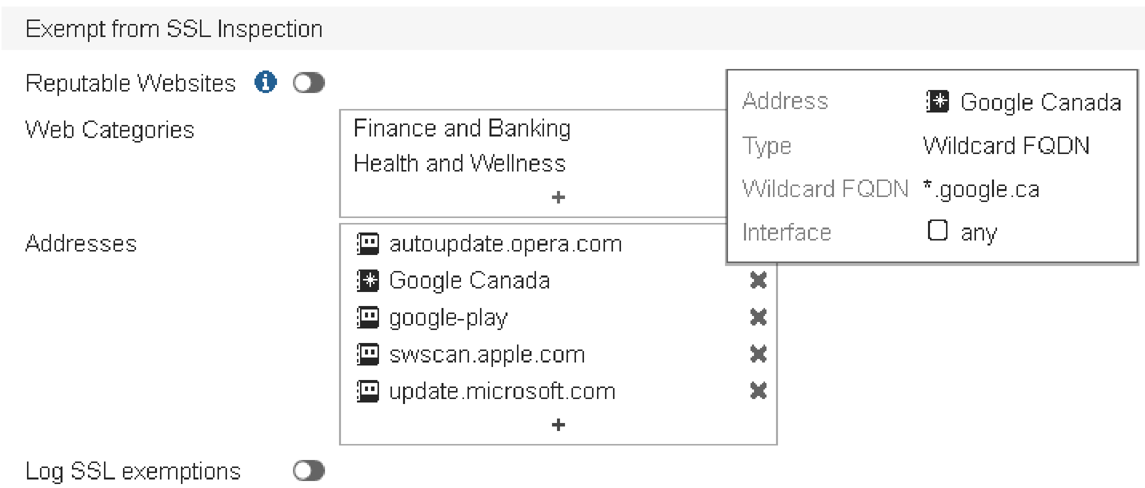


2. Go to *Security Profiles* > *SSL/SSH Inspection* and select the list view in the top right to view all profiles.

3. Select the *deep-inspection* profile and then select *Clone* to create a copy of this profile.
   This copy has the same settings as the default profile but is read-write so that you can modify it.

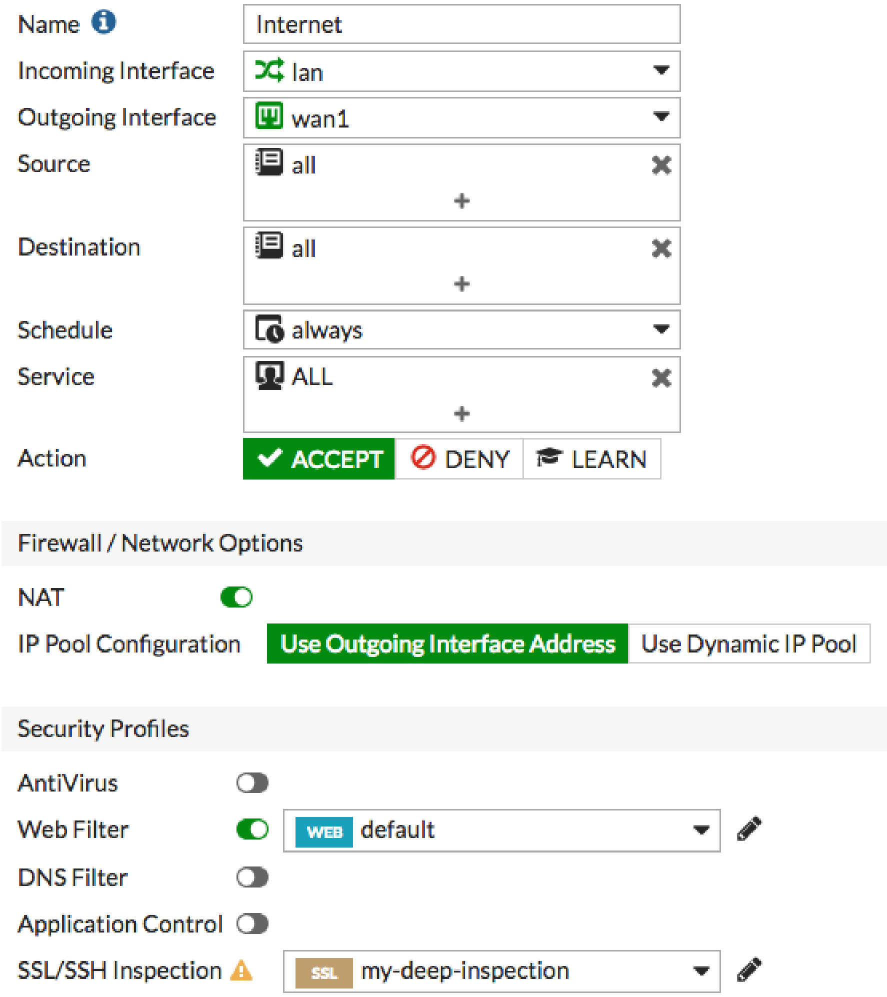


4. Edit the new profile and change its name (in this example, *my-deep-inspection*).
   The *Exempt from SSL Inspection* section shows the exempt web categories and addresses.
   Add the address for Google to the list of exempt *Addresses*.



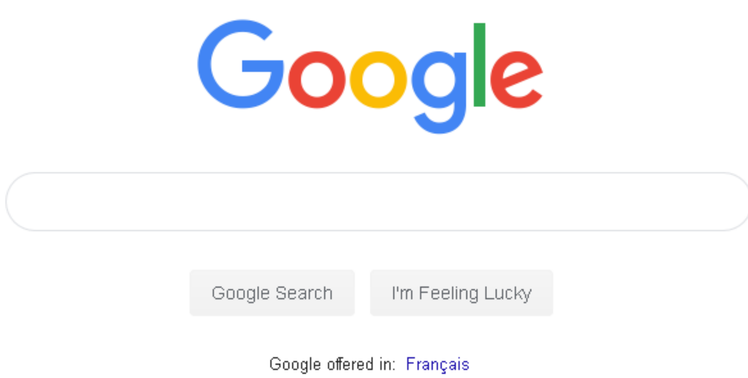
5. Go to *Policy & Objects > IPv4 Policy* and edit the policy that allows users on the internal network to access the Internet.

Set *SSL/SSH Inspection* to use the new profile.

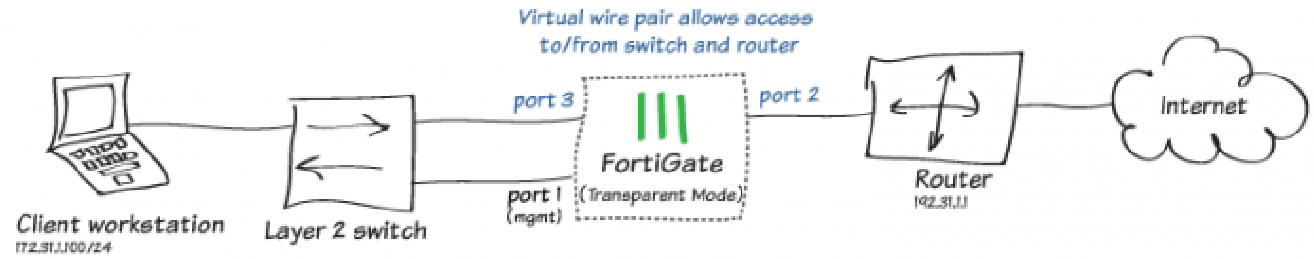


Results

1. Use Chrome to browse to google.ca. The site loads properly.



Transparent web filtering using a virtual wire pair



This example shows how to insert FortiGate transparent web filtering between two network devices. The FortiGate is configured with a management interface and Virtual Wire (V-Wire) pair connected between a network switch and router. Once inserted between the network devices, V-Wire policy and web-filtering are configured to allow and inspect traffic.

In this example, port 1 is used for management, while ports 2 and 3 are configured as the virtual wire pair.

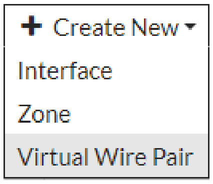
Configure the management interface

Port 1 is the management interface. If the management interface isn't configured, use the CLI to configure it.

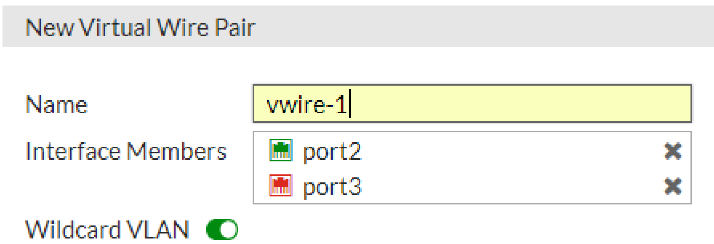
1. Using a console cable, access the Fortinet command line interface and configure the management port IP address, default gateway, and DNS.
   At the CLI prompt, enter the following:
```
config system interface
   edit port1
      set ip 172.31.1.254/24
end

config router static
   edit 1
      set gateway 172.31.1.1
      set device port1
end

config system dns
   set primary 208.91.112.53
   set secondary 208.91.112.52
end
```
2. When the management IP address is set, access the FortiGate login screen using the new management IP address.

Configure the virtual wire pair

1. On the FortiGate, go to *Network* > *Interfaces*.
   Select *Create New* > *Virtual Wire Pair*.



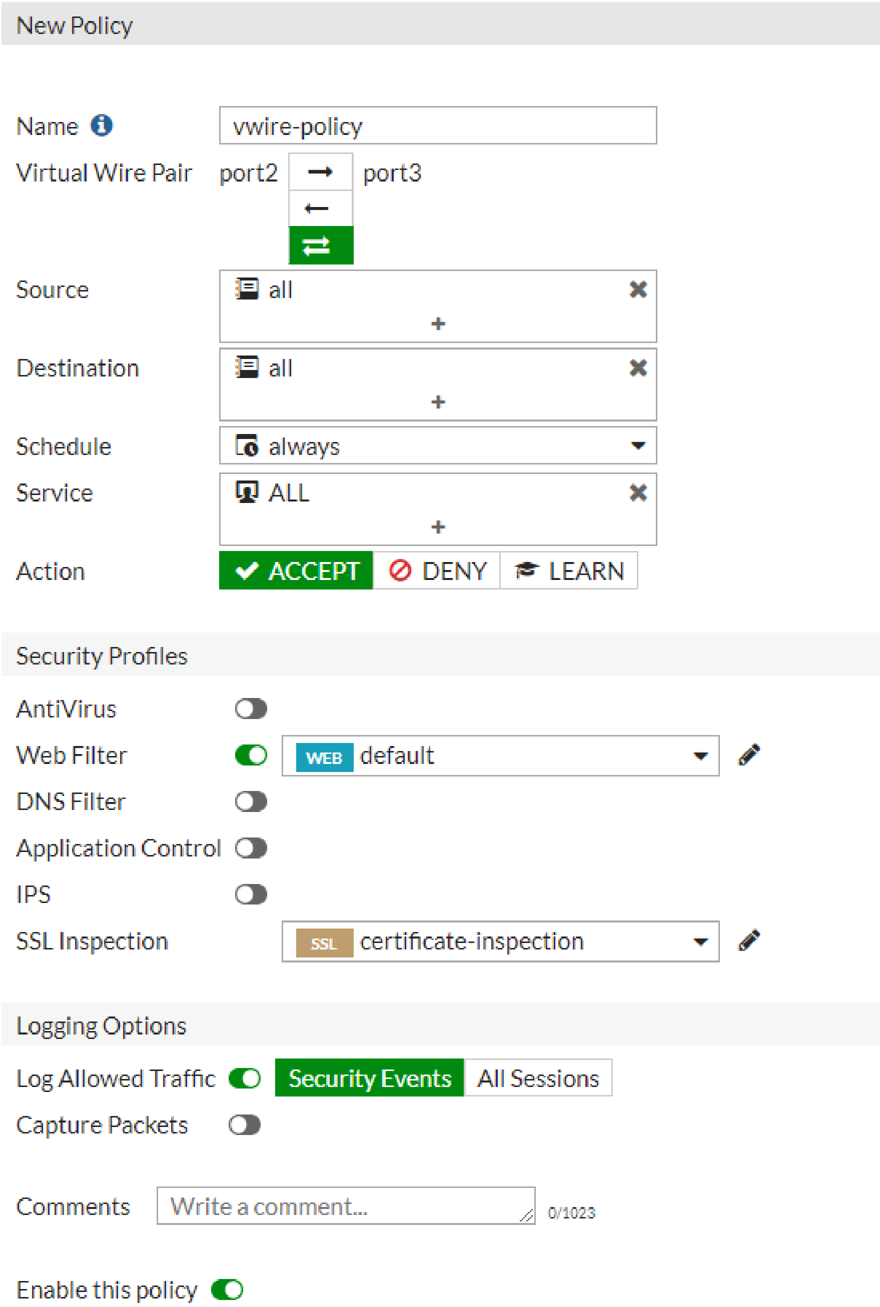
2. In the *New Virtual Wire Pair* page, enter the interface name and add the interface members.
   If multiple VLANs are used on the connection, enable *Wildcard VLAN*.



Configure the virtual wire pair policy and enable web filtering

1. On The FortiGate, go to *Policy & Objects* > *IPv4 Virtual Wire Pair Policy*.
2. Click *Create New*.
3. Enter the policy *Name*.
   For *Virtual Wire Pair*, select bidirectional traffic flow (double arrows).
   Specify the *Source*, *Destination*, *Schedule*, *Service*, and *Action*.

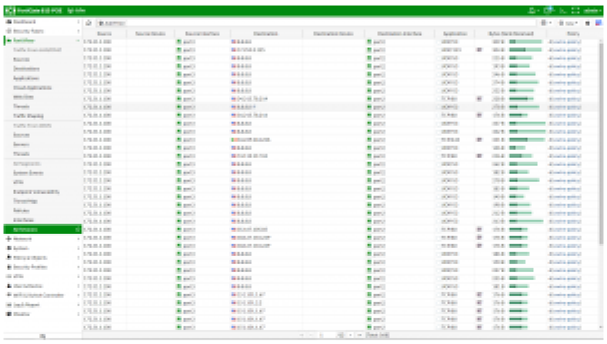
In the *Security Profiles* section, enable *Web Filter* and select a policy.



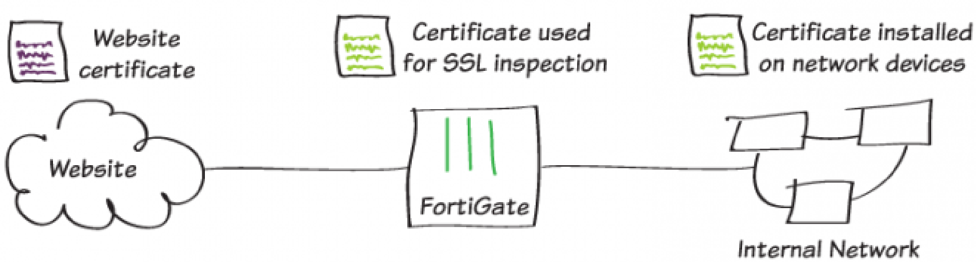
Results

When the virtual wire policy is created, traffic flows through the virtual wire pair and web filtering is enabled.

To verify traffic, go to *FortiView > All Sessions* and review the source and destination ports. Check that traffic is flowing across ports 2 and 3.



Preventing certificate warnings (CA-signed certificate)



This example shows how to prevent users from receiving a security certificate warning when FortiGate performs full SSL inspection on incoming traffic. When you enable full SSL inspection, FortiGate impersonates the recipient of the originating SSL session and then decrypts and inspects the content. FortiGate then re-encrypts the content, creates a new SSL session between FortiGate and the recipient by impersonating the sender, and sends the content to the user. "Man-in-the-middle" attacks use a similar process which is why a user's device might show a security certificate warning.

When users receive security certificate warnings, they usually click *Continue* without understanding why the error occurs. To avoid encouraging this habit, you can prevent the warning from appearing in the first place.

For more information about SSL inspection, see Why you should use SSL inspection on page 215.

Using a CA-signed certificate

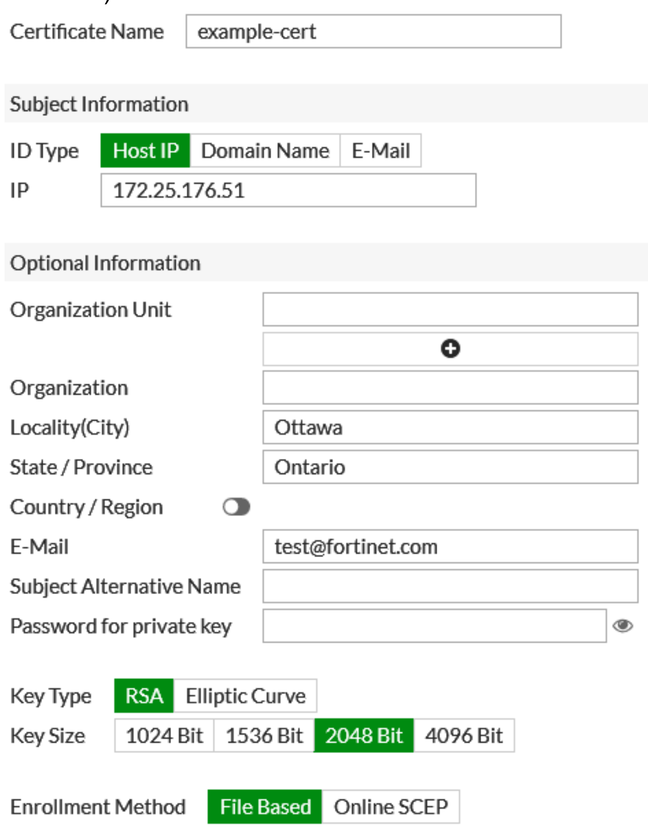
Obtain and install a CA-signed certificate on FortiGate to use with SSL inspection. To implement SSL inspection, add another security profile to the policy that controls Internet traffic. You can use either FortiAuthenticator as your CA or a trusted private CA.

If you use FortiAuthenticator as a CA, generate a certificate signing request (CSR) on your FortiGate, have it signed on FortiAuthenticator, import the certificate into FortiGate, and configure FortiGate to use the certificate for SSL deep inspection of HTTPS traffic.

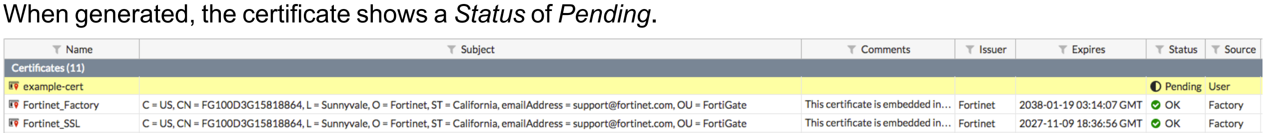
If you use a trusted private CA, generate a CSR on your FortiGate, apply for an SSL certificate from the trusted private CA, import the certificate into FortiGate, and configure FortiGate to use the certificate for SSL deep inspection of HTTPS traffic.

Generating a CSR on a FortiGate

1. Go to *System* > *Certificates* and select *Generate*.
2. Enter a *Certificate Name*, the external *IP* address of your FortiGate, and an *E-Mail* address.
3. To ensure the certificate is securely encrypted, set *Key Type* to *RSA* and *Key Size* to *2048 Bit* (the industry standard).



When generated, the certificate shows a *Status* of *Pending*.



4. To save the .csr file to your local drive, highlight the certificate and select *Download*.

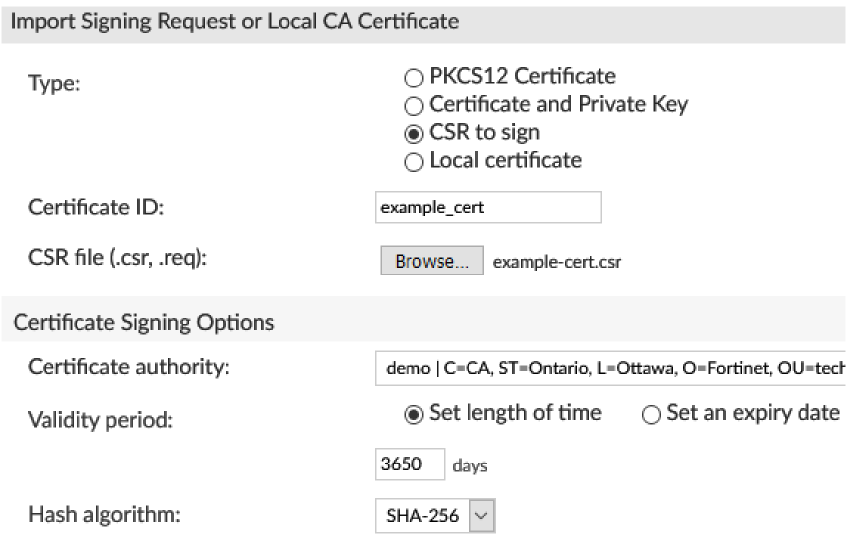
Getting the certificate signed by a CA

Trusted private CA:

If you want to use a trusted private CA to sign the certificate, use the CSR to apply for an SSL certificate with your trusted private CA.

FortiAuthenticator:

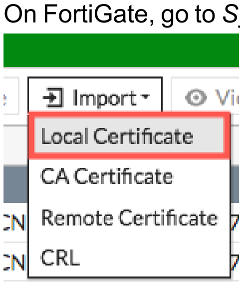
1. On FortiAuthenticator, go to *Certificate Management* > *Certificate Authorities* > *Local CAs* and select *Import*.
2. Set *Type* to *CSR to sign*, enter a *Certificate ID*, and specify the *example-cert.csr* file.
   Select the *Certificate authority* from the dropdown menu and set *Hash algorithm* to *SHA-256*.



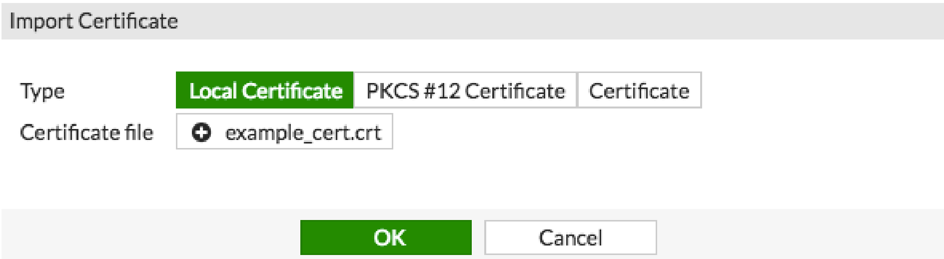
   When the certificate is imported, you see that *example_cert* has been signed by the FortiAuthenticator; *Status* shows *Active* and the *CA Type* shows *Intermediate (non-signing) CA*.
3. Select the certificate and select *Export Certificate*. This saves the *example-cert.crt* file to your local drive.

Importing the signed certificate to your FortiGate

1. On FortiGate, go to *System* > *Certificates* and select *Import* > *Local Certificate*.



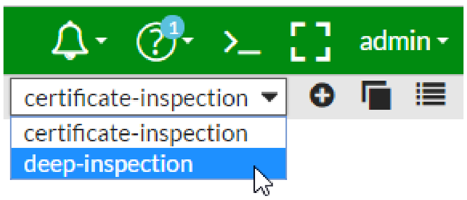
2. Browse to the certificate file and select *OK*.



The certificate has a *Status* of *OK*.

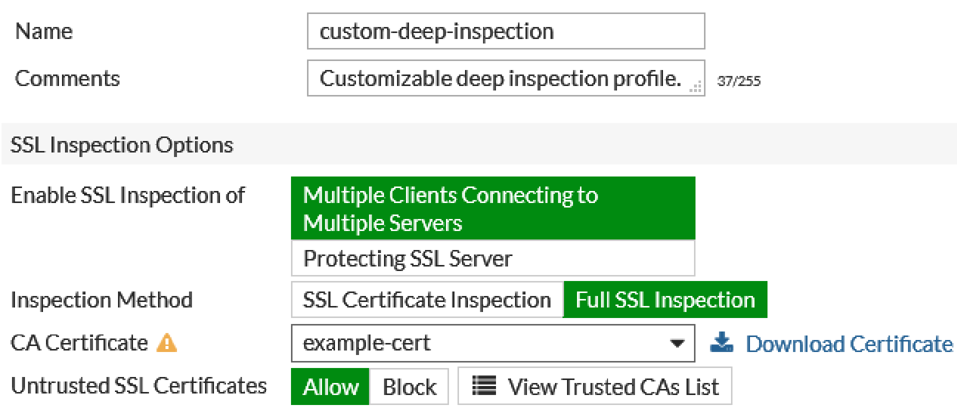
Editing the SSL inspection profile

1. To use your certificate in an SSL inspection profile, go to *Security Profiles > SSL/SSH Inspection*.
2. Use the dropdown menu in the top right to select *deep-inspection*.



The *deep-inspection* profile is read-only. To use the CA-signed certificate for SSL inspection, you must create a new *deep-inspection* profile.

3. Set *CA Certificate* to use the new certificate.



Importing the certificate into web browsers

When your certificate is signed by FortiAuthenticator, import the certificate into users' browsers.

If you have an environment such as the Windows Group Policy Management Console, you can push the certificate to users' browsers using the Windows Group Policy Editor. In this case, you do not have to import the certificate into users' browsers.

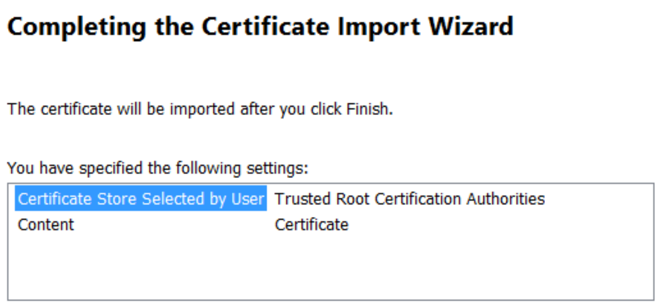
The method you use for importing the certificate depends on the type of browser.

Internet Explorer, Chrome, and Safari (on Windows and macOS)

Internet Explorer, Chrome, and Safari use the operating system's certificate store for Internet browsing. If users will be using these browsers, you must install the certificate into the certificate store for the OS.

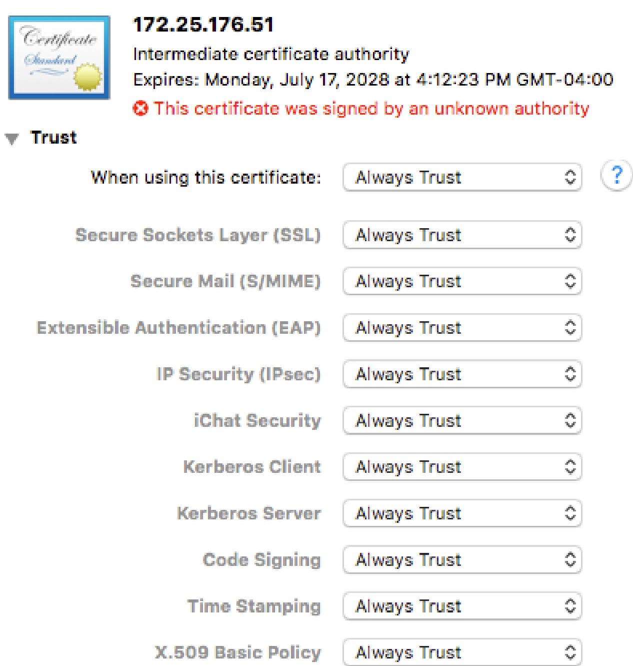
On Windows 7/8/10:

1. Double-click the certificate file and select *Open*.
2. Select *Install Certificate* to launch the *Certificate Import Wizard*.
3. Use the wizard to install the certificate into the *Trusted Root Certificate Authorities* store.
   If a security warning appears, select *Yes* to install the certificate.



On macOS:

1. Double-click the certificate file to launch *Keychain Access*.
2. Locate the certificate in the *Certificates* list and select it.
3. Expand *Trust* and select *Always Trust*.
   If necessary, enter the computer's administrative password.

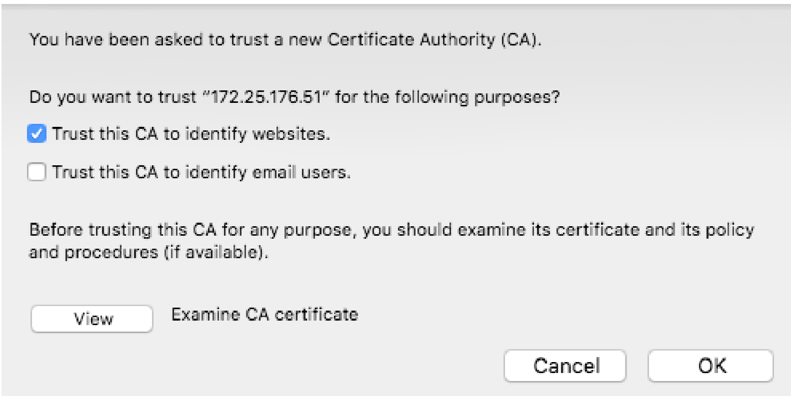


Firefox (on Windows and macOS)

Firefox has its own certificate store. To avoid errors in Firefox, the certificate must be installed in this store rather than in the OS.

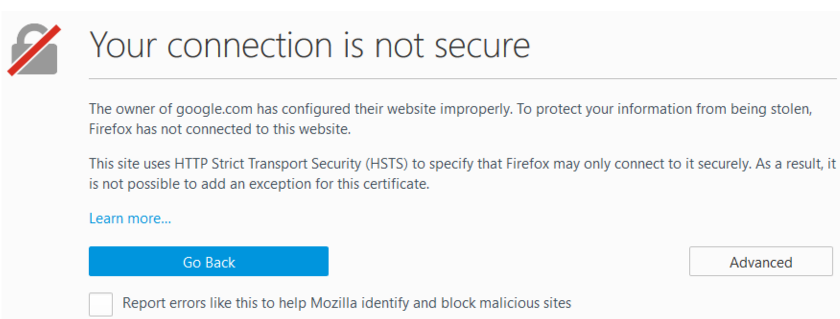
On Firefox, you must install the certificate on each device. It cannot be pushed onto all user devices.

1. In Firefox for Windows, go to *Options > Privacy & Security*.
   In Firefox for macOS, go to *Preferences > Privacy & Security*.
2. In the *Certificates* section, select *View Certificates* and select the *Authorities* list.
3. *Import* the certificate and set it to be trusted for website identification.



Results

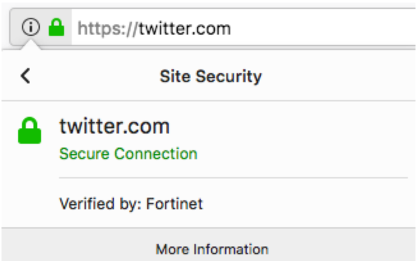
Before you install the certificate, when users access a site that uses HTTPS, an error message appears (this example shows an error message in Firefox).



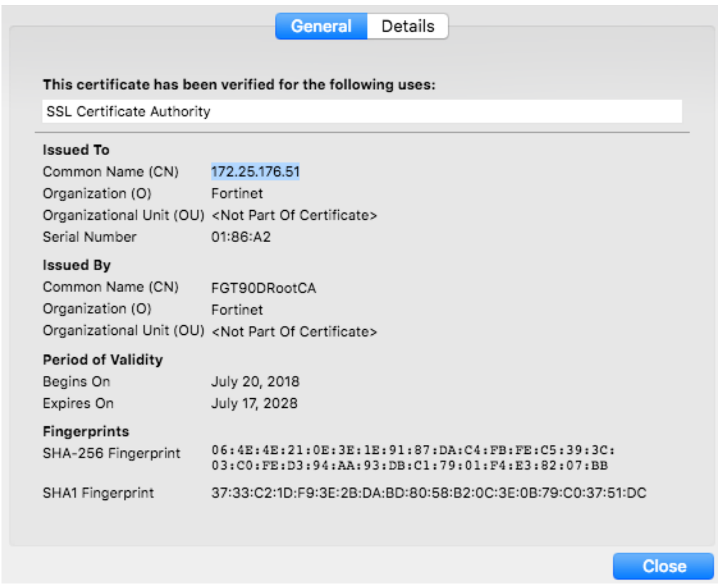
After you install the certificate, users do not have certificate security issues when they browse to sites that the FortiGate performs SSL content inspection on.

Users can view information about the connection and the certificate that's used.

When users view information about the connection, they'll see that it's verified by Fortinet.

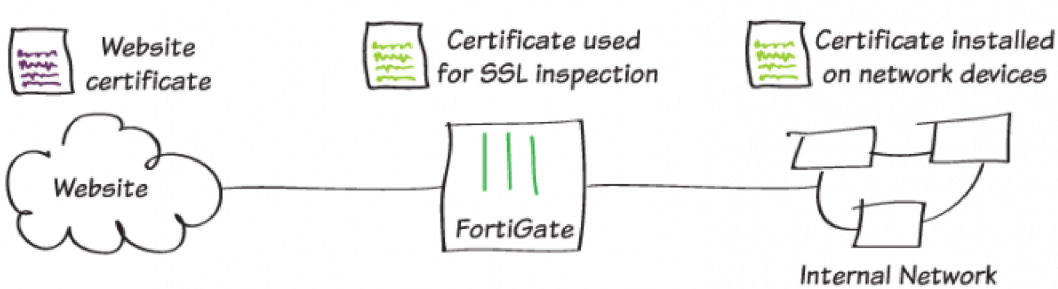


When users view the certificate in the browser, they see which certificate is used and information about that certificate.



Preventing certificate warnings (default certificate)

FORTIOS 5.6 VERSION



This example shows how to prevent users from receiving a security certificate warning when FortiGate performs full SSL inspection on incoming traffic. When you enable full SSL inspection, FortiGate impersonates the recipient of the originating SSL session and then decrypts and inspects the content. FortiGate then re-encrypts the content, creates a new SSL session between FortiGate and the recipient by impersonating the sender, and sends the content to the user. "Man-in-the-middle" attacks use a similar process which is why a user's device might show a security certificate warning.

When users receive security certificate warnings, they usually click *Continue* without understanding why the error occurs. To avoid encouraging this habit, you can prevent the warning from appearing in the first place.

For more information about SSL inspection, see Why you should use SSL inspection on page 215.

Using the default certificate

All FortiGate devices have a default certificate that is used for full SSL inspection. This certificate is also used in the default *deep-inspection* profile. To prevent users from seeing certificate warnings, you can install this certificate on users' devices.

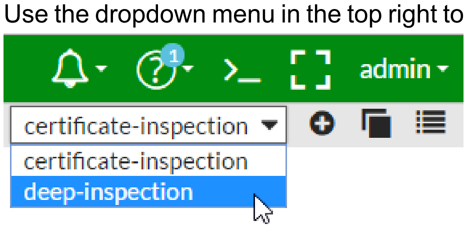
Generating a unique certificate

Run the following CLI command to generate an SSL certificate that's unique to your FortiGate:

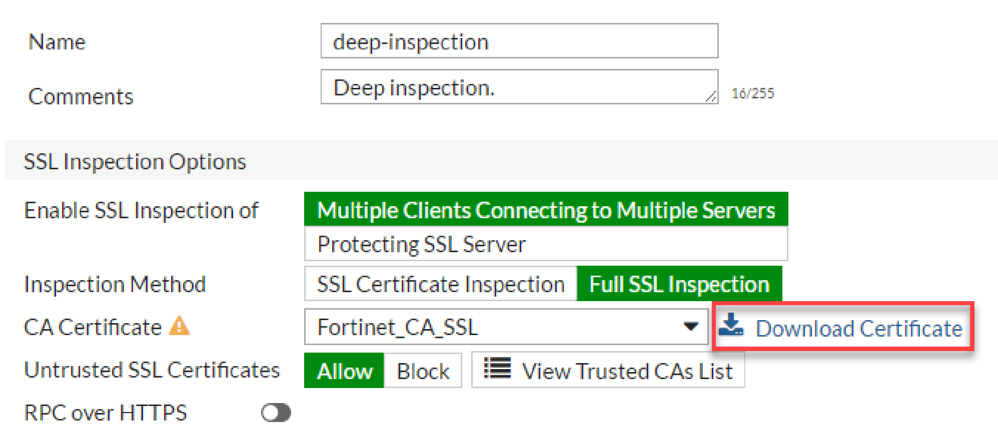
```
execute vpn certificate local generate default-ssl-ca
```

Downloading the certificate

1. Go to *Security Profiles > SSL/SSH Inspection*.
2. Use the dropdown menu in the top right to select *deep-inspection*.



3. The default FortiGate certificate is listed as the *CA Certificate*. Select *Download Certificate*.



Importing the certificate into web browsers

When you have your FortiGate device’s default certificate, import the certificate into users’ browsers.

If you have an environment such as the Windows Group Policy Management Console, you can push the certificate to users' browsers using the Windows Group Policy Editor. In this case, you do not have to import the certificate into users' browsers.

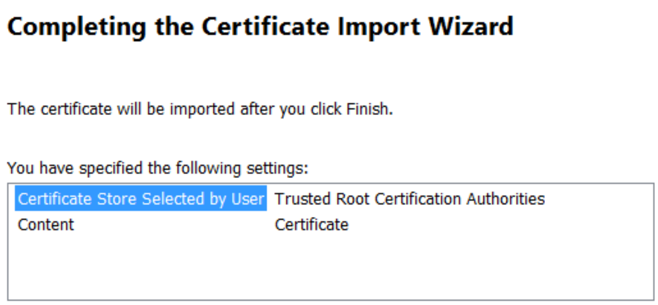
The method you use for importing the certificate depends on the type of browser.

Internet Explorer, Chrome, and Safari (on Windows and macOS)

Internet Explorer, Chrome, and Safari use the operating system's certificate store for Internet browsing. If users will be using these browsers, you must install the certificate into the certificate store for the OS.

On Windows 7/8/10:

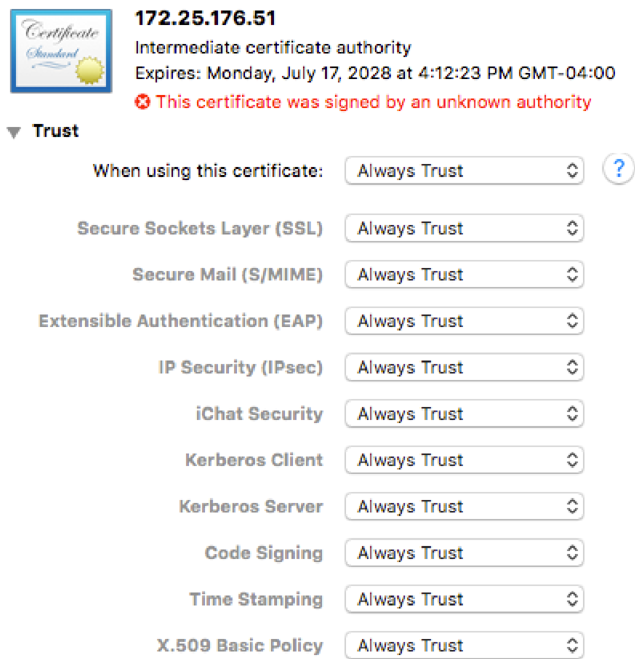
1. Double-click the certificate file and select *Open*.
2. Select *Install Certificate* to launch the *Certificate Import Wizard*.
3. Use the wizard to install the certificate into the *Trusted Root Certificate Authorities* store.
   If a security warning appears, select *Yes* to install the certificate.



On macOS:

1. Double-click the certificate file to launch *Keychain Access*.
2. Locate the certificate in the *Certificates* list and select it.

3. Expand *Trust* and select *Always Trust*.
   If necessary, enter the computer's administrative password.

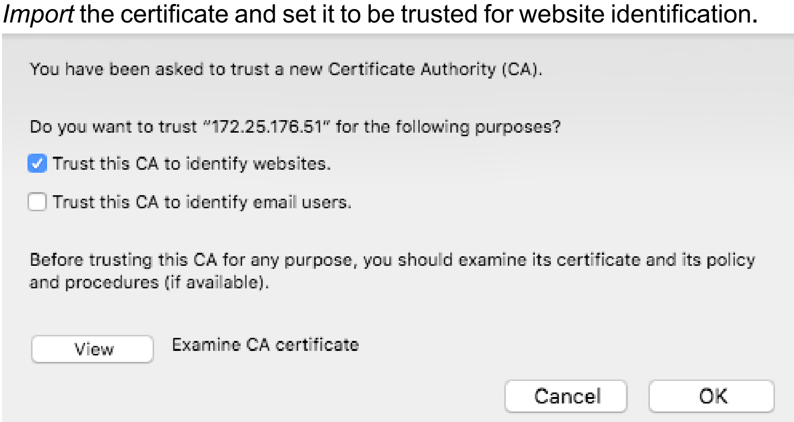


Firefox (on Windows and macOS)

Firefox has its own certificate store. To avoid errors in Firefox, the certificate must be installed in this store rather than in the OS.

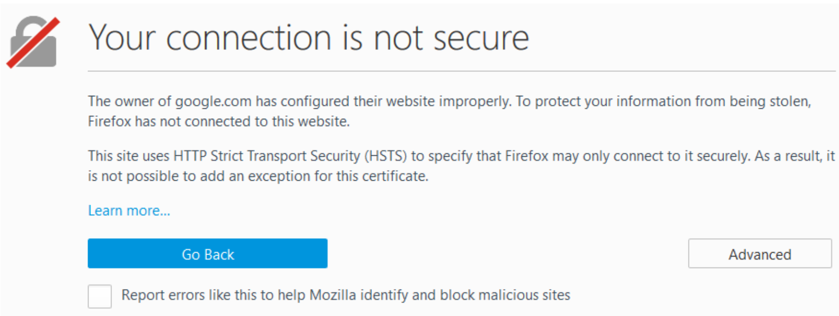
On Firefox, you must install the certificate on each device. It cannot be pushed onto all user devices.

1. In Firefox for Windows, go to *Options* > *Privacy & Security*.
   In Firefox for macOS, go to *Preferences* > *Privacy & Security*.
2. In the *Certificates* section, select *View Certificates* and select the *Authorities* list.
3. *Import* the certificate and set it to be trusted for website identification.



Results

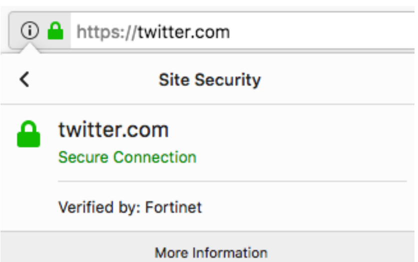
Before you install the certificate, when users access a site that uses HTTPS, an error message appears (this example shows an error message in Firefox).



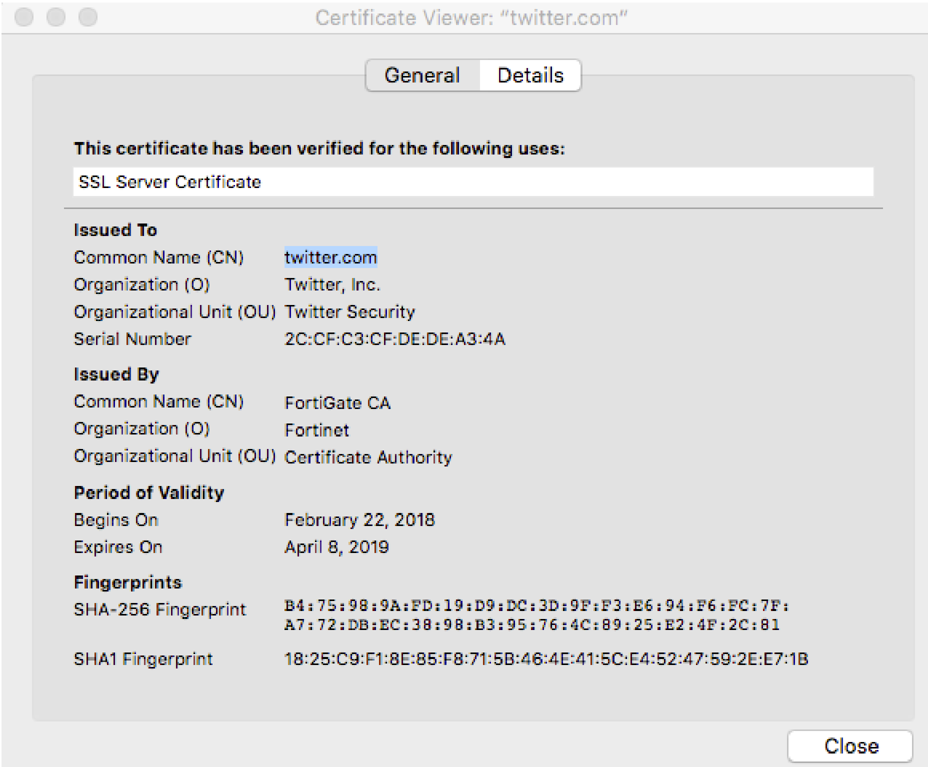
After you install the certificate, users do not have certificate security issues when they browse to sites that the FortiGate performs SSL content inspection on.

Users can view information about the connection and the certificate that's used.

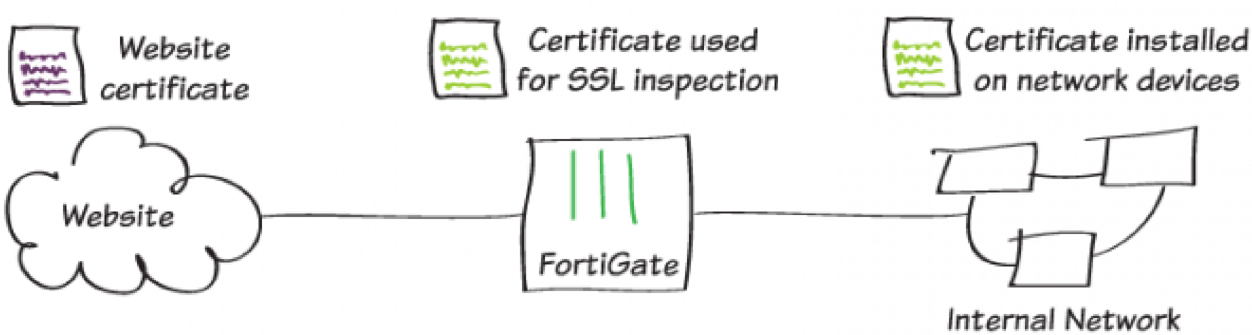
When users view information about the connection, they'll see that it's verified by Fortinet.



When users view the certificate in the browser, they see which certificate is used and information about that certificate.



Preventing certificate warnings (self-signed)



This example shows how to prevent users from receiving a security certificate warning when FortiGate performs full SSL inspection on incoming traffic. When you enable full SSL inspection, FortiGate impersonates the recipient of the originating SSL session and then decrypts and inspects the content. FortiGate then re-encrypts the content, creates a new SSL session between FortiGate and the recipient by impersonating the sender, and sends the content to the user. "Man-in-the-middle" attacks use a similar process which is why a user's device might show a security certificate warning.

When users receive security certificate warnings, they usually click *Continue* without understanding why the error occurs. To avoid encouraging this habit, you can prevent the warning from appearing in the first place.

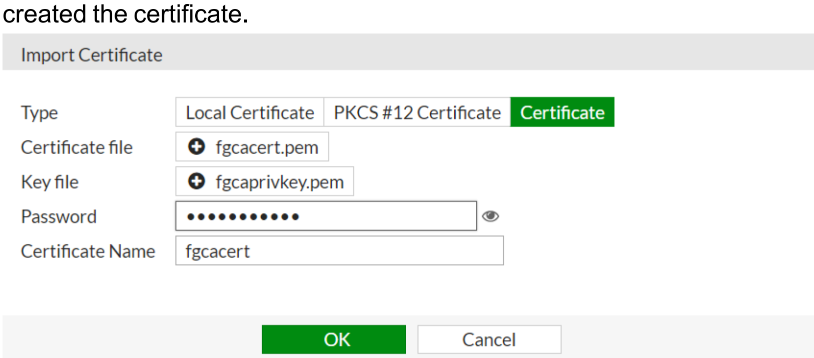
For more information about SSL inspection, see Why you should use SSL inspection on page 215.

Creating a certificate with OpenSSL

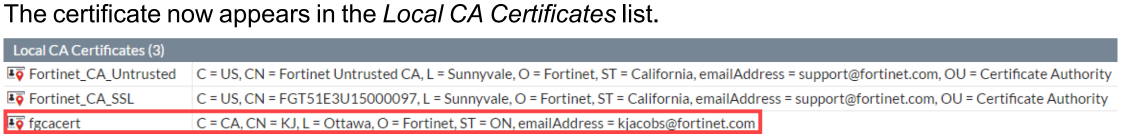
1. If necessary, download and install Open SSL and ensure hat the *openssl.cnf* file is located in the BIN folder for OpenSSL.
2. In the CLI, go to the BIN folder.
   In this example, the command is:
   ```
   cd c:\OpenSSL\bin
   ```
3. Generate an RSA key:
   ```
   openssl genrsa -aes256 -out fgcaprivkey.pem 2048 -config openssl cnf
   ```
   This RSA key uses AES-256 encryption and a 2048-bit key.
4. When prompted, enter a passphrase for encrypting the private key.
   Use the following command to launch OpenSSL, submit a new certificate request, and sign the request:
   ```
   openssl req -new -x509 -days 3650 -extensions v3_ca -key fgcaprivkey.pem -out
        fgcacert.pem -config openssl.cnf
   ```
   The result is a standard x509 binary certificate that’s valid for 3650 days (approximately 10 years).
5. When prompted, re-enter the passphrase for encryption, then enter the details for the certificate request such as location and organization name.
   Two files are created: a public certificate (*fgcacert.pem*) and a private key (*fgcaprivkey.pem*).

Importing the self-signed certificate

1. Go to *System* > *Certificates* and select *Import* > *Local Certificate*.
2. Set *Type* to *Certificate*, then select your *Certificate file* and *Key file*. Enter the *Password* that you set when you created the certificate.

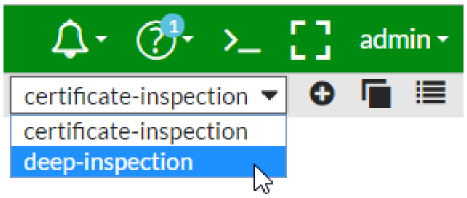


The certificate now appears in the *Local CA Certificates* list.



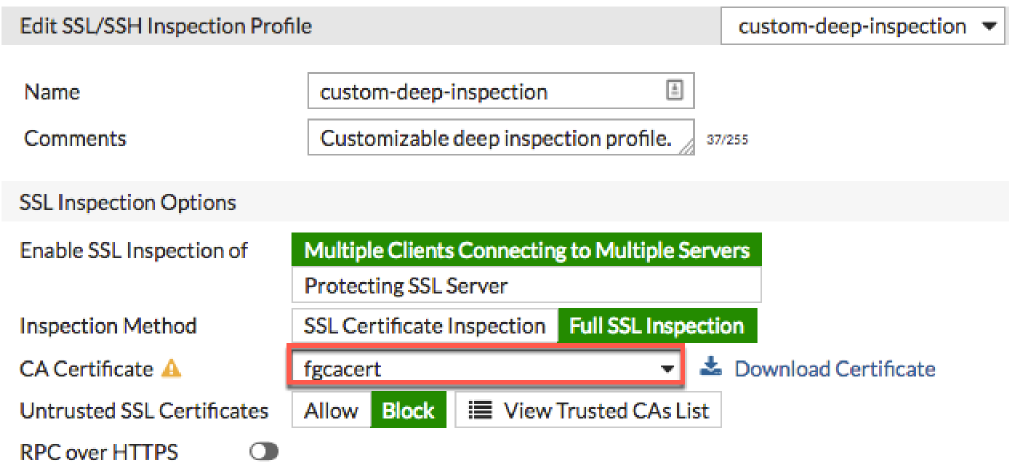
Editing the SSL inspection profile

1. To use your certificate in an SSL inspection profile go to *Security Profiles > SSL/SSH Inspection*.
2. Use the dropdown menu in the top right to select *deep-inspection*.



The *deep-inspection* profile is read-only. To use the CA-signed certificate for SSL inspection, you must create a new *deep-inspection* profile.

3. Select *Download Certificate* to download the certificate file and set *CA Certificate* to use the new certificate.



Importing the certificate into web browsers

When you have your self-signed certificate, import the certificate into users' browsers.

If you have an environment such as the Windows Group Policy Management Console, you can push the certificate to users' browsers using the Windows Group Policy Editor. In this case, you do not have to import the certificate into users' browsers.

The method you use for importing the certificate depends on the type of browser.

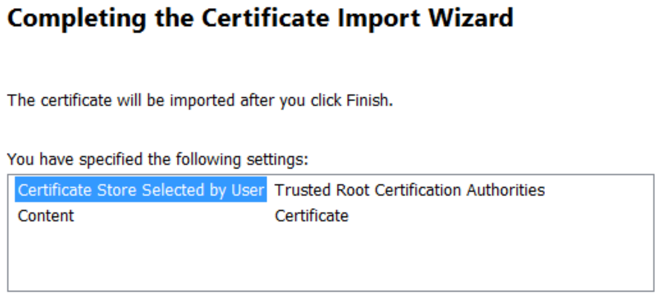
Internet Explorer, Chrome, and Safari (on Windows and macOS)

Internet Explorer, Chrome, and Safari use the operating system's certificate store for Internet browsing. If users will be using these browsers, you must install the certificate into the certificate store for the OS.

On Windows 7/8/10:

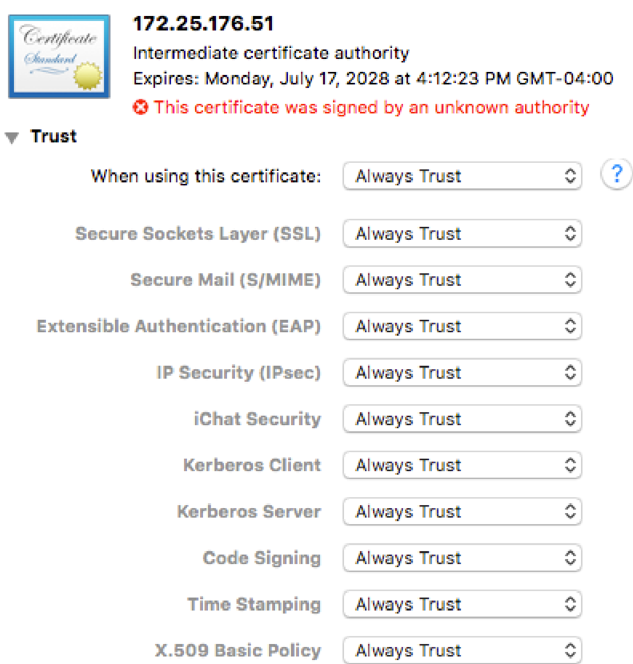
1. Double-click the certificate file and select *Open*.
2. Select *Install Certificate* to launch the *Certificate Import Wizard*.

3. Use the wizard to install the certificate into the *Trusted Root Certificate Authorities* store.
   If a security warning appears, select *Yes* to install the certificate.



On macOS:

1. Double-click the certificate file to launch *Keychain Access*.
2. Locate the certificate in the *Certificates* list and select it.
3. Expand *Trust* and select *Always Trust*.
   If necessary, enter the computer's administrative password.



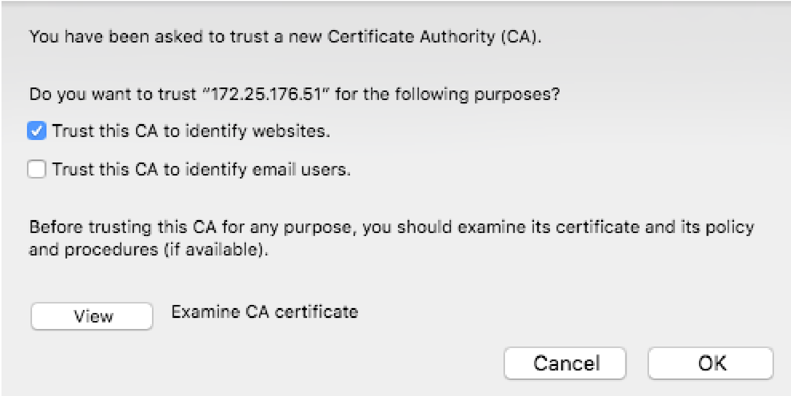
Firefox (on Windows and macOS)

Firefox has its own certificate store. To avoid errors in Firefox, the certificate must be installed in this store rather than in the OS.

On Firefox, you must install the certificate on each device. It cannot be pushed onto all user devices.

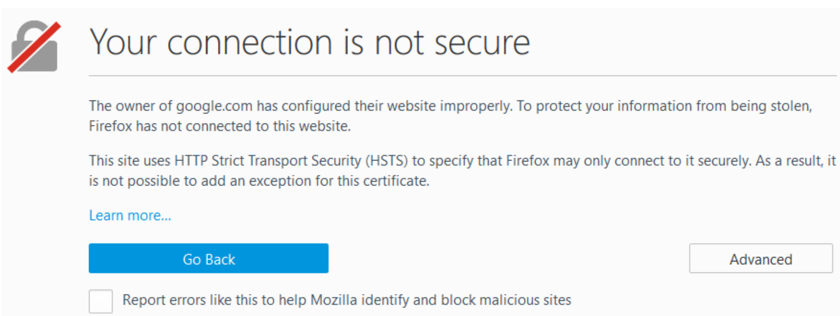
1. In Firefox for Windows, go to *Options* > *Privacy & Security*.
   In Firefox for macOS, go to *Preferences* > *Privacy & Security*.
2. In the *Certificates* section, select *View Certificates* and select the *Authorities* list.

3. *Import* the certificate and set it to be trusted for website identification.



Results

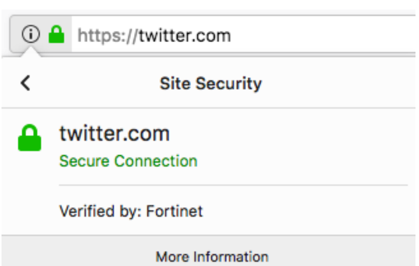
Before you install the certificate, when users access a site that uses HTTPS, an error message appears (this example shows an error message in Firefox).



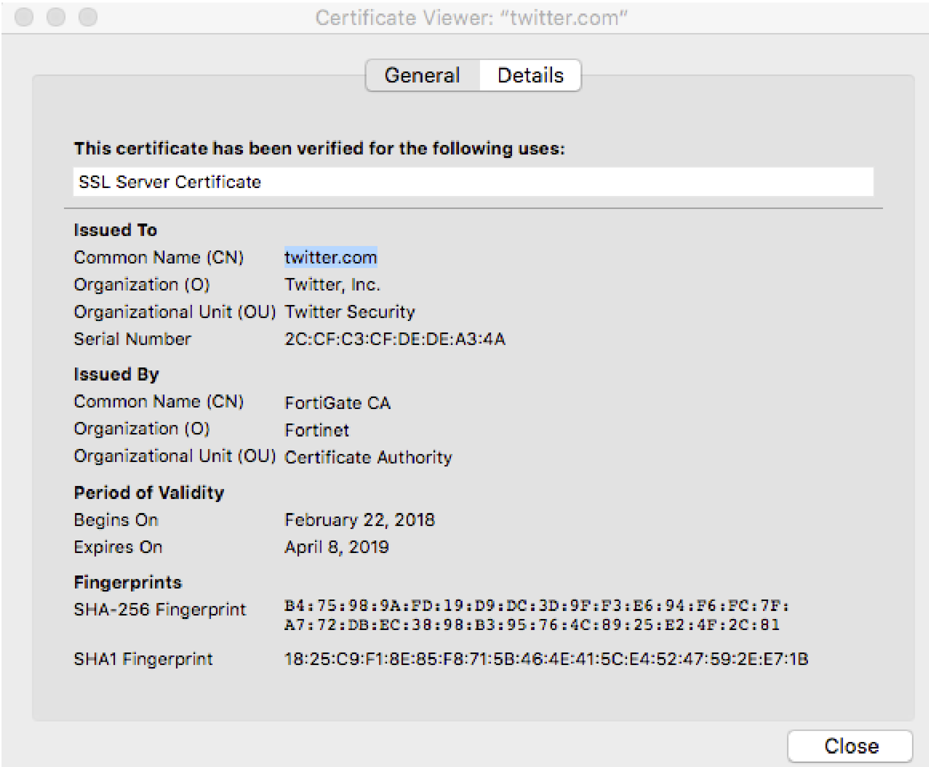
After you install the certificate, users do not have certificate security issues when they browse to sites that the FortiGate performs SSL content inspection on.

Users can view information about the connection and the certificate that's used.

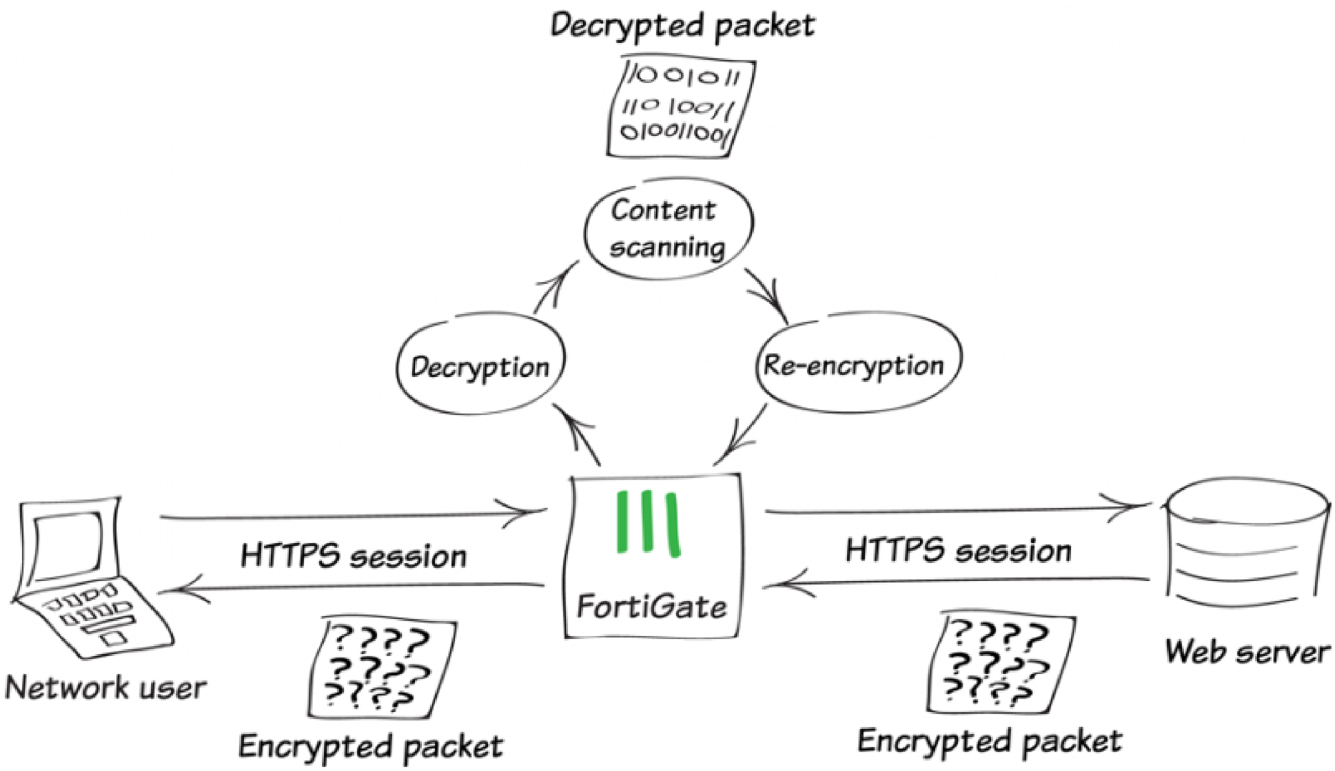
When users view information about the connection, they'll see that it's verified by Fortinet.



When users view the certificate in the browser, they see which certificate is used and information about that certificate.



Why you should use SSL inspection



HTTPS provides protection by applying SSL encryption to web traffic. However, the risk is that encrypted traffic can get around your normal Internet defences.

For example, in an e-commerce session, you might download a file containing a virus, or you might receive a phishing email containing a seemingly harmless file that, when launched, creates an encrypted session to a C&C server and downloads malware onto your computer. Because the sessions in these attacks are encrypted, they might get past your network's security measures.

To protect your network from these threats, SSL inspection is the key your FortiGate uses to unlock encrypted sessions, see into encrypted packets, find threats, and block them. SSL inspection not only protects you from attacks that use HTTPS, but also from other commonly used encrypted protocols such as SMTPS, POP3S, IMAPS, and FTPS.

Full SSL inspection

To ensure all encrypted content is inspected, you must use full SSL inspection (also known as deep inspection). With full SSL inspection, FortiGate impersonates the recipient of the originating SSL session, then decrypts and inspects the content. FortiGate then re-encrypts the content, creates a new SSL session between the FortiGate and the recipient by impersonating the sender, and sends the content to the sender.

When FortiGate re-encrypts the content, it uses a certificate stored on FortiGate. The client must trust this certificate to avoid certificate errors. Whether this trust exists depends on the client which can be the computer's OS, a browser, or another application, which likely maintains its own certificate repository.

There are two deployment methods for full SSL inspection:

1. Multiple Clients Connecting to Multiple Servers

- Uses a CA certificate which can be uploaded using the Certificates menu.
- Typically applies to outbound policies where destinations are unknown, that is, normal web traffic.
- Uses address and web category whitelists which can be configured to bypass SSL inspection.

2. Protecting SSL Server

- Uses a server certificate which can be uploaded using the Certificates menu to protect a single server.
- Typically applies to inbound policies to protect servers available externally through Virtual IPs.
- Since this is typically deployed “outside-in” (clients on the Internet accessing servers on the internal side of the FortiGate), server certificates using the public FQDN of the server are often purchased from a commercial Certificate Authority and uploaded to FortiGate. This avoids client applications generating SSL certificate errors due to certificate mismatch.

See details in the FortiOS Online Help and the Fortinet Knowledge Base for these technical notes:

- How to Enable SSL inspection from the CLI and Apply it to a Policy
- How to block web-based chat on Gmail webmail using App Sensor + SSL inspection

SSL certificate inspection

FortiGate supports a second type of SSL inspection called SSL certificate inspection. With certificate inspection, FortiGate inspects only the header information of packets. Certificate inspection verifies the identity of web servers and ensures HTTPS is not used as a workaround to access sites you have blocked using web filtering.

The only security feature that can be applied using SSL certificate inspection mode is web filtering. Since only the packet header is inspected, this method does not introduce certificate errors and can be a useful alternative to full SSL inspection when web filtering is used.

When using SSL certificate inspection, you might get certificate errors for blocked websites due to FortiGate trying to display a replacement message for that site using HTTPS. To prevent these errors, install the certificate that the FortiGate uses for encryption in your browser. By default, this is the same certificate for SSL inspection.

For more information, see:

- Preventing certificate warnings (CA-signed certificate) on page 198.
- Preventing certificate warnings (default certificate) on page 204.
- Preventing certificate warnings (self-signed) on page 209.

Troubleshooting

The most common problem with SSL inspection is users receiving SSL errors when the certificate is not trusted, because by default, FortiGate uses a certificate that is not trusted by the client. The way to fix this depends on whether you are using FortiGate’s default certificate, a self-signed certificate, or a CA-signed certificate.

Best practices

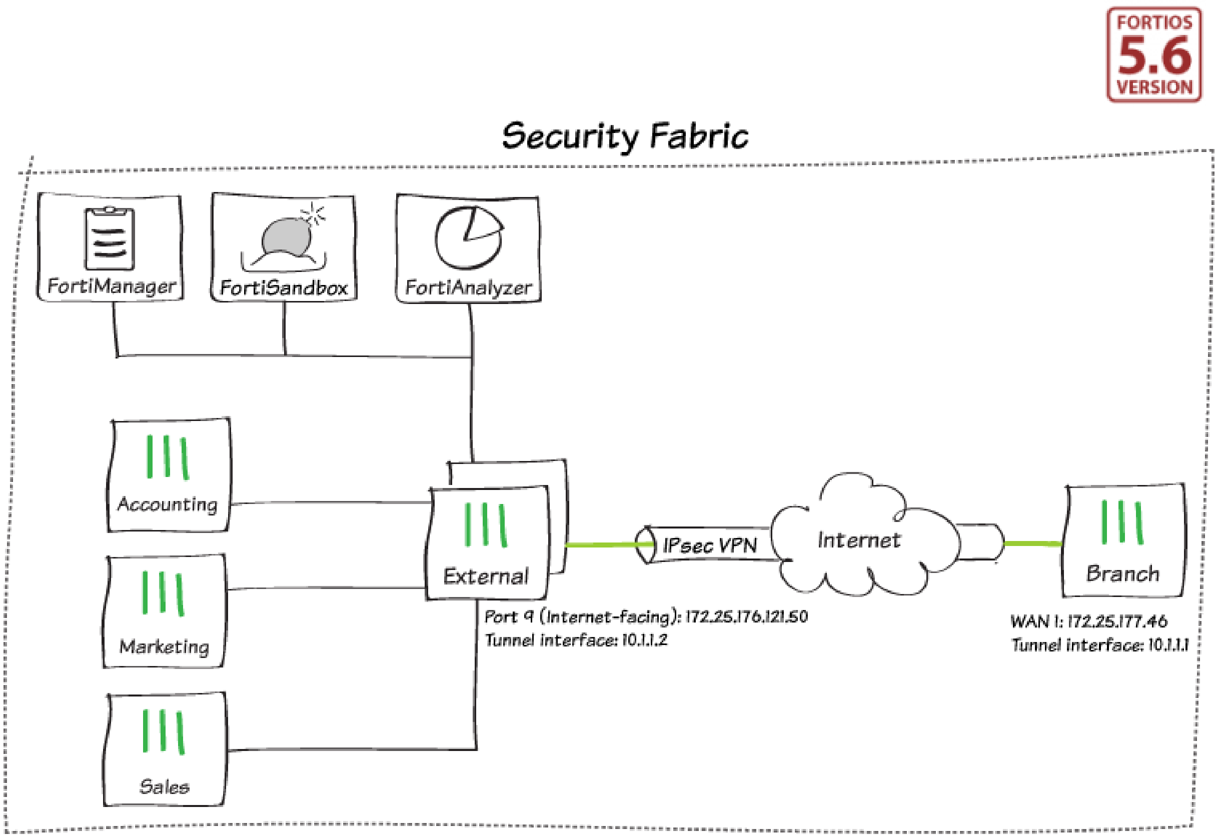
Because all traffic needs to be decrypted, inspected, and re-encrypted, using SSL inspection can reduce FortiGate's overall performance. To avoid using too many resources for SSL inspection, do the following:

- **Know your traffic** – Know how much traffic is expected and what percentage of the traffic is encrypted. You can also limit the number of policies that allow encrypted traffic.
- **Be selective** – Use whitelists or trim your policy to apply SSL inspection only where it is needed.
- **Use hardware acceleration** – FortiGate models with the CP6 or CPU processor have an SSL/TLS protocol processor for SSL content scanning and SSL acceleration. For more information, see the Hardware Acceleration handbook.
- **Test real-world SSL inspection performance yourself** – Use the flexibility of FortiGate's security policy to gradually deploy SSL inspection rather than enabling it all at once.

VPNs

This section contains information about creating and using a virtual private network (VPN).

Fortinet Security Fabric over IPsec VPN



This example shows you how to add FortiTelemetry traffic to an existing IPsec VPN site-to-site tunnel between two FortiGate devices, so that you can add a remote FortiGate to the Security Fabric. This example also shows how to allow the remote FortiGate to access the FortiAnalyzer for logging.

If you have not set up a site-to-site VPN created, see Site-to-site IPsec VPN with two FortiGates.

In this example, an HA cluster called *External* is the root FortiGate in the Security Fabric and a FortiGate called *Branch* is the remote FortiGate.

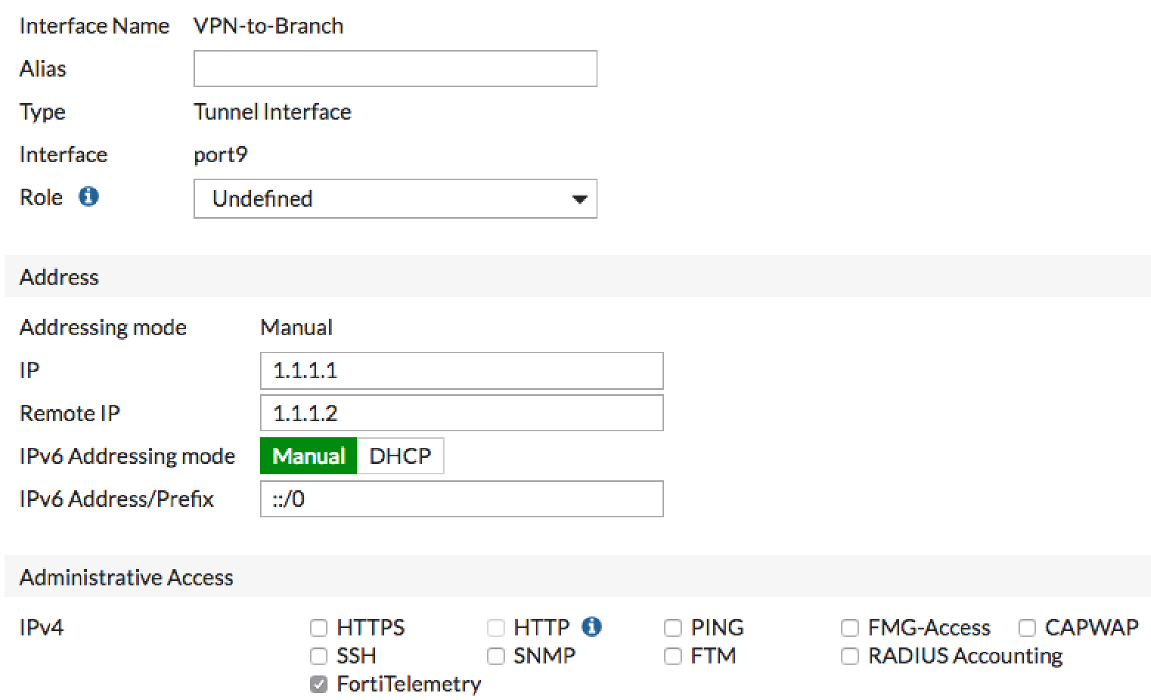
This recipe requires FortiOS 5.6.1 or higher.

Configuring the tunnel interfaces

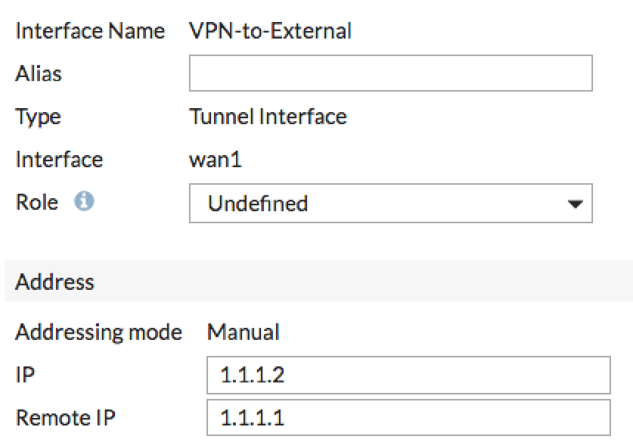
For FortiTelemetry traffic to flow securely through the IPsec VPN, FortiTelemetry traffic must travel between the tunnel interfaces with the interface on External listening for this traffic.

The tunnel interfaces require IP addresses. In this example, the External tunnel interface is assigned the IP address 1.1.1.1 and the Branch tunnel interface is assigned the IP address 1.1.1.2.

1. On External, go to *Network* > *Interfaces* and edit the tunnel interface.
   Set *IP* to the local IP address for this interface (*1.1.1.1*) and *Remote IP* to the local IP address for the Branch tunnel interface (*1.1.1.2*).
   Under *Administrative Access*, enable *FortiTelemetry*.

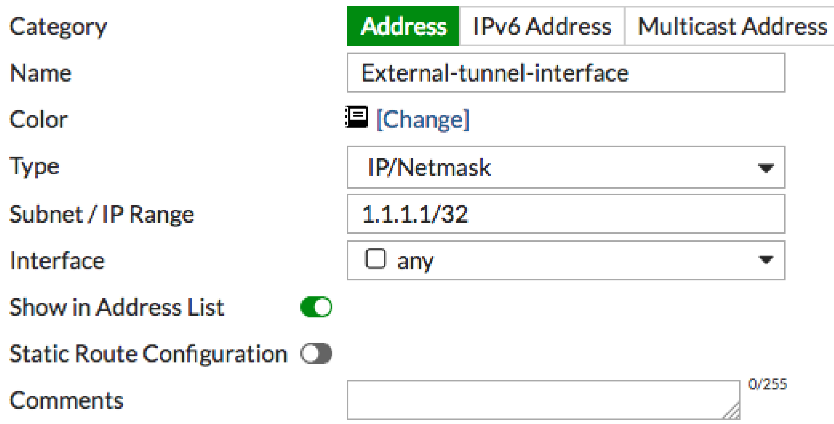


2. On Branch, go to *Network* > *Interfaces* and edit the tunnel interface.
   Set *IP* to the local IP address for this interface (*1.1.1.2*) and *Remote IP* to the local IP address for the External tunnel interface (*1.1.1.1*).

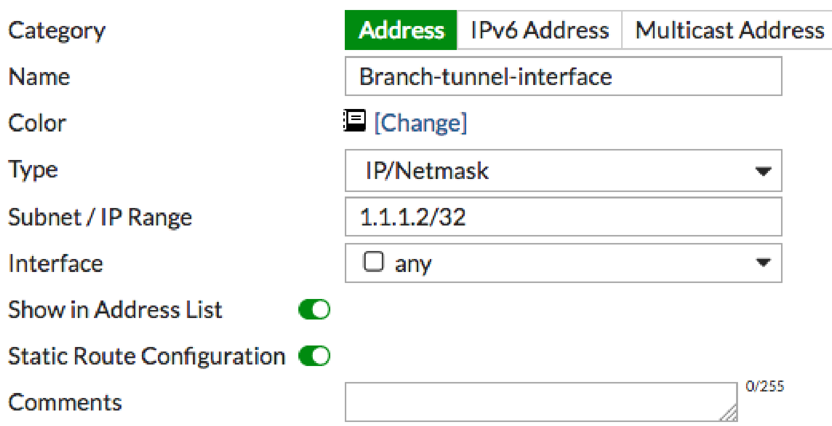


Adding the tunnel interfaces to the VPN

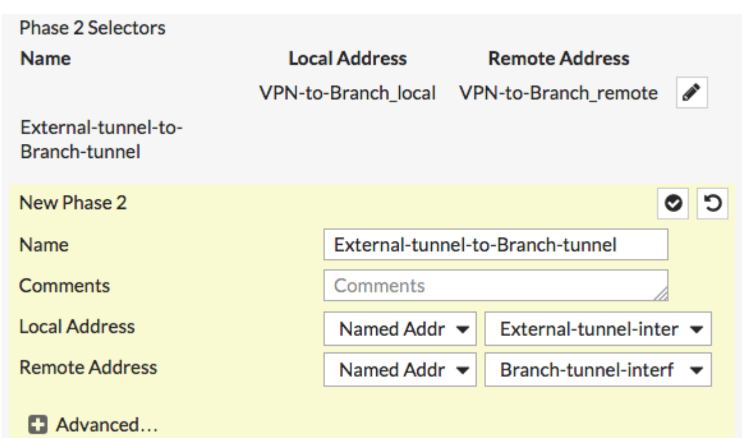
1. On External, go to *Policy & Objects > Addresses* and create an address for the External tunnel interface.



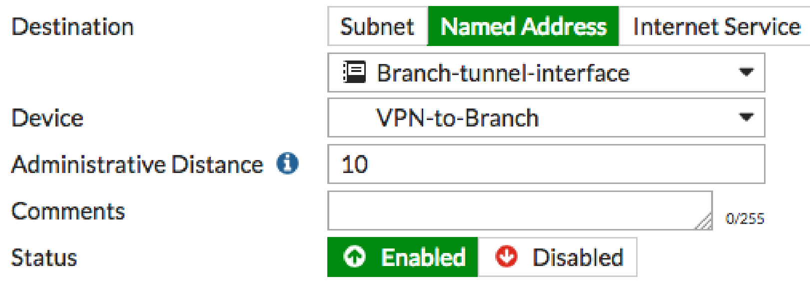
2. Create a second address for the Branch tunnel interface.
   For this address, enable *Static Route Configuration*.



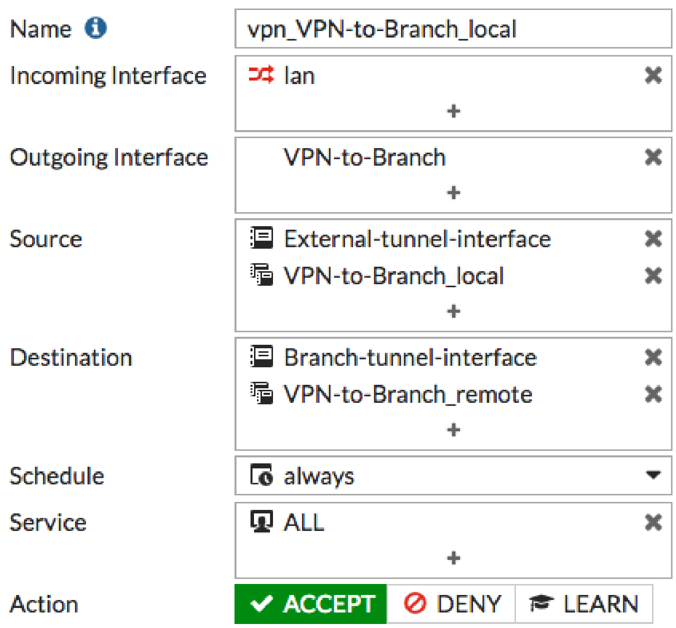
3. Go to *VPN > IPsec Tunnels* and edit the VPN tunnel.
   Select *Convert To Custom Tunnel*.
   Under *Phase 2 Selectors*, create a second Phase 2 allowing traffic between the External tunnel interface and the Branch tunnel interface.



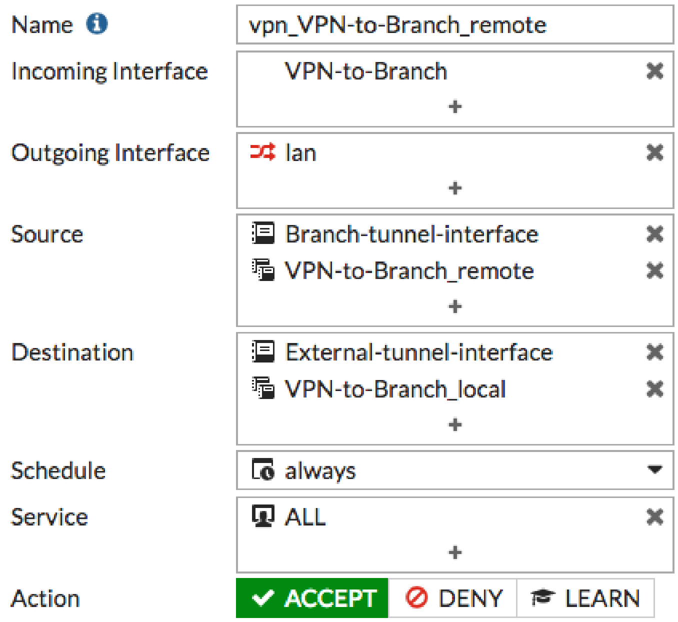
4. Go to *Network* > *Static Routes* and create a route to the Branch tunnel interface.
   Set *Destination* to *Named Address* and select the firewall address.
   Set *Device* to the tunnel interface.



5. Go to *Policy & Objects* > *IPv4 Policy* and edit the policy allowing local VPN traffic.
   Set *Source* to include the External tunnel interface.
   Set *Destination* to include the Branch tunnel interface.



6. Edit the policy allowing remote VPN traffic to include the tunnel interfaces.



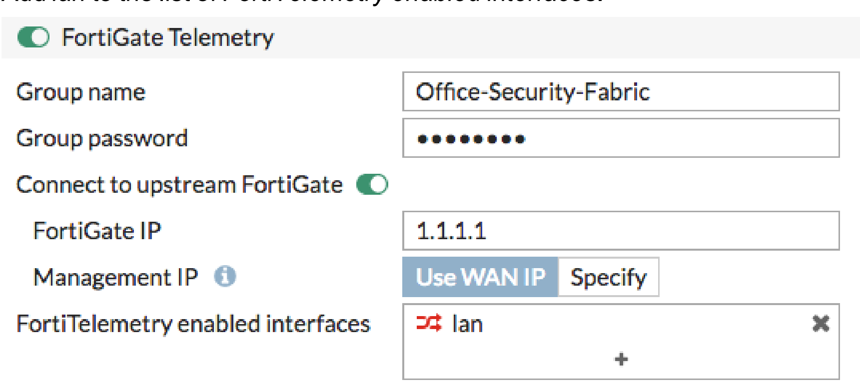
On Branch, repeat this procedure to include the following:

- Addresses for both tunnel interfaces. You must enable *Static Route Configuration* for the Branch tunnel interface.
- A Phase 2 allowing traffic between the Branch tunnel interface and the External tunnel interface.
- A static route to the External tunnel interface.
- Edited policies that allow traffic to flow between the tunnel interfaces.

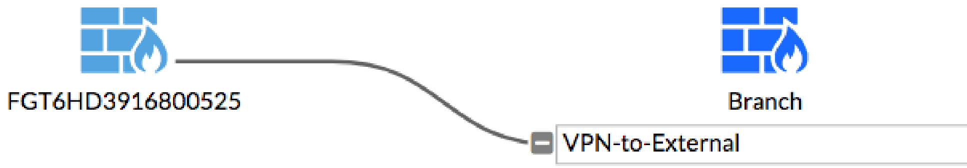
7. Go to *Monitor* > *IPsec Monitor* and restart the VPN tunnel to implement the new phase 2.

Adding Branch to the Security Fabric

1. On Branch, go to *Security Fabric* > *Settings* and enable *FortiGate Telemetry*.
Enter the *Group name* and *Group password* of the Security Fabric.
Enable *Connect to upstream FortiGate* and set *FortiGate IP* to the IP address of the External tunnel interface.
Add *lan* to the list of *FortiTelemetry enabled interfaces*.

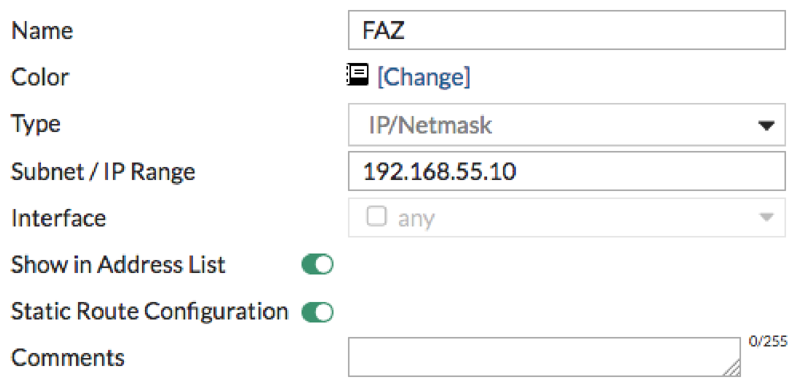


2. Go to *Security Fabric > Logical Topology*.
Branch connects to External (identified by serial number) over the IPsec VPN tunnel.

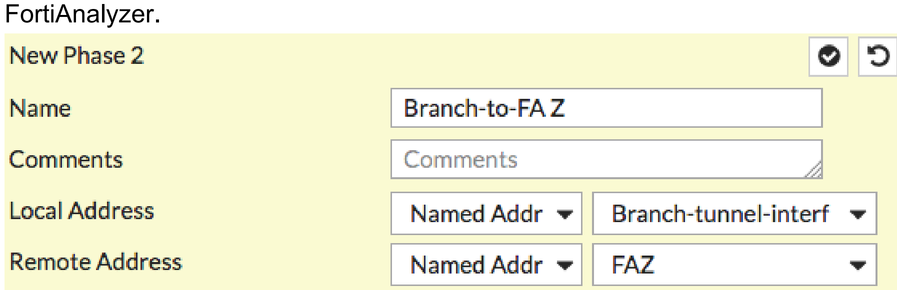


Allowing Branch to access the FortiAnalyzer

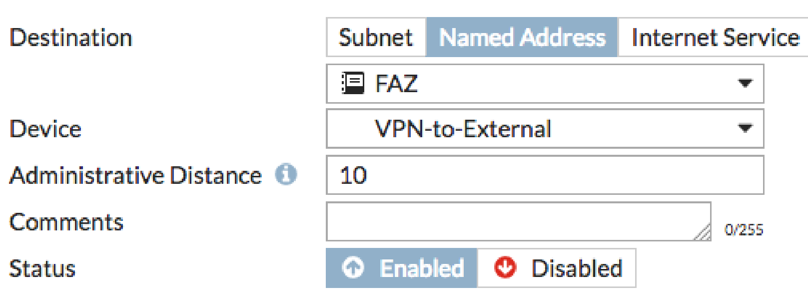
1. On Branch, go to *Policy & Objects > Addresses* and create an address for the FortiAnalyzer.
Enable *Static Route Configuration*.



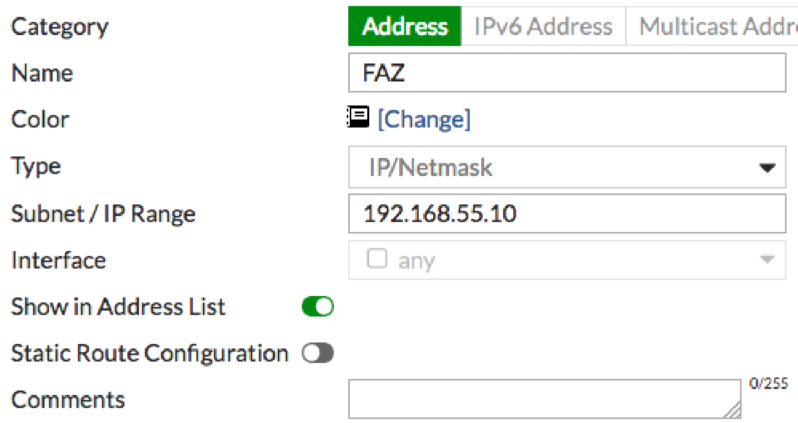
2. Go to *VPN > IPsec Tunnels* and create a Phase 2 to allow traffic between the Branch tunnel interface and the FortiAnalyzer.



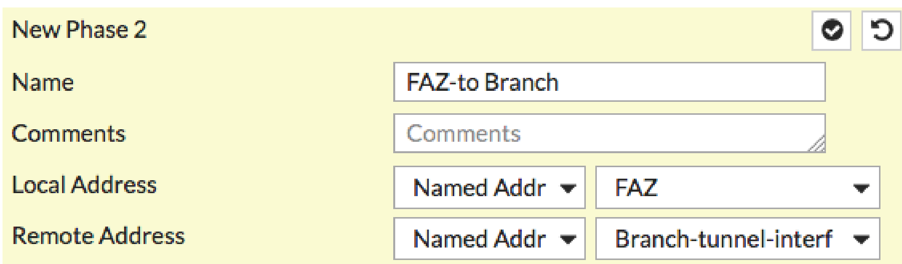
3. Go to *Network > Static Routes* and create a route to the FortiAnalyzer.



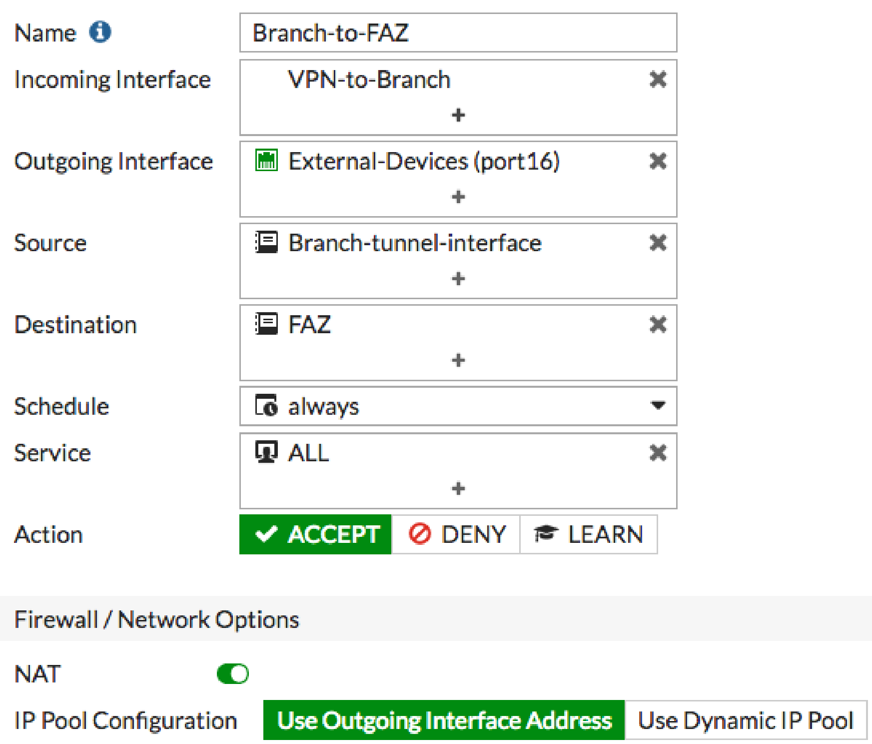
4. On External, go to *Policy & Objects > Addresses* and create an address for the FortiAnalyzer.



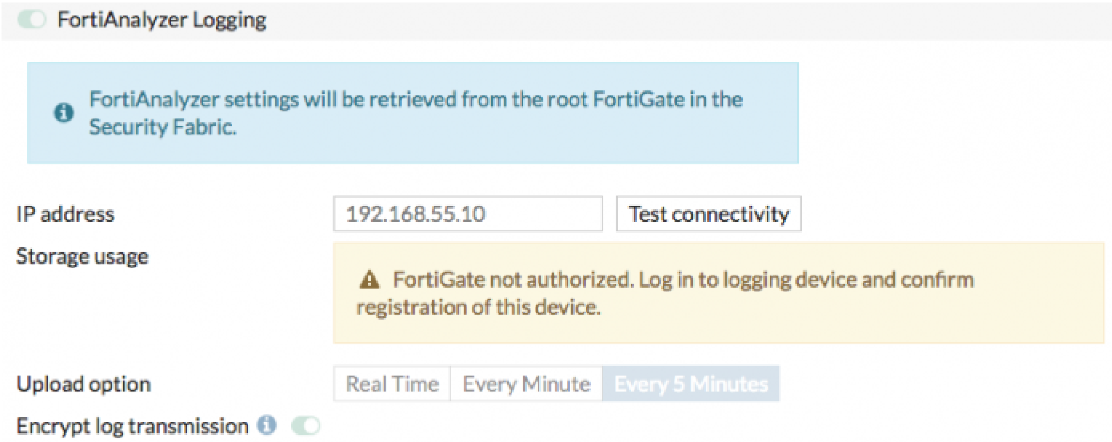
5. Go to *VPN > IPsec Tunnels* and create a Phase 2 to allow traffic between the FortiAnalyzer and the Branch tunnel interface.



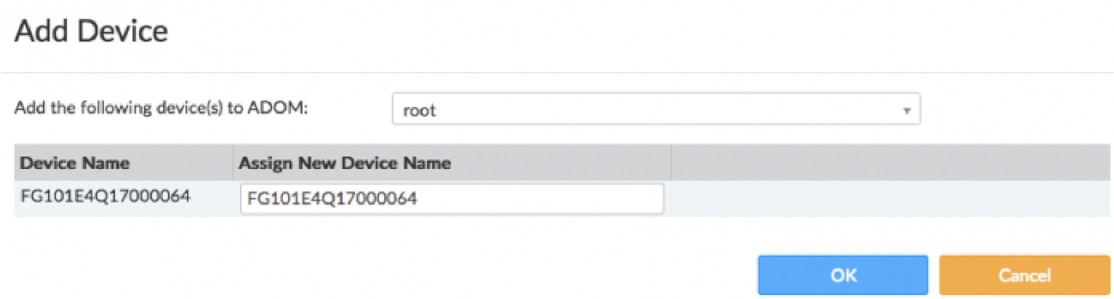
6. Go to *Policy & Objects > IPv4 Policy* and create a policy to allow traffic from the VPN tunnel to the FortiAnalyzer. Enable *NAT* for this policy.



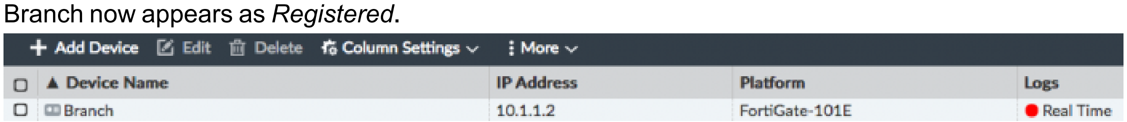
7. On Branch, go to *Security Fabric > Settings*.
In the *FortiAnalyzer Logging* section, an error appears because Branch is not yet authorized on the FortiAnalyzer.



8. On the FortiAnalyzer, go to *Device Manager > Unregistered*.
Select Branch and then select *+Add* to register Branch.

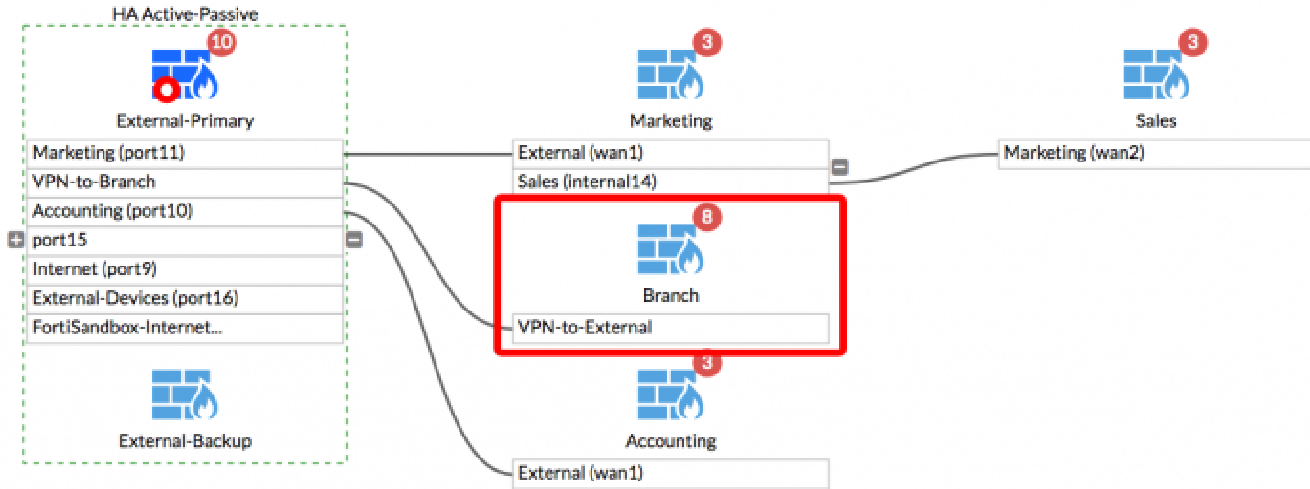


9. Branch now appears as *Registered*.



Results

On External, go to *Security Fabric > Logical Topology*. Branch is shown as part of the Security Fabric, connecting over the IPsec VPN tunnel.



(Optional) Using local logging for Branch

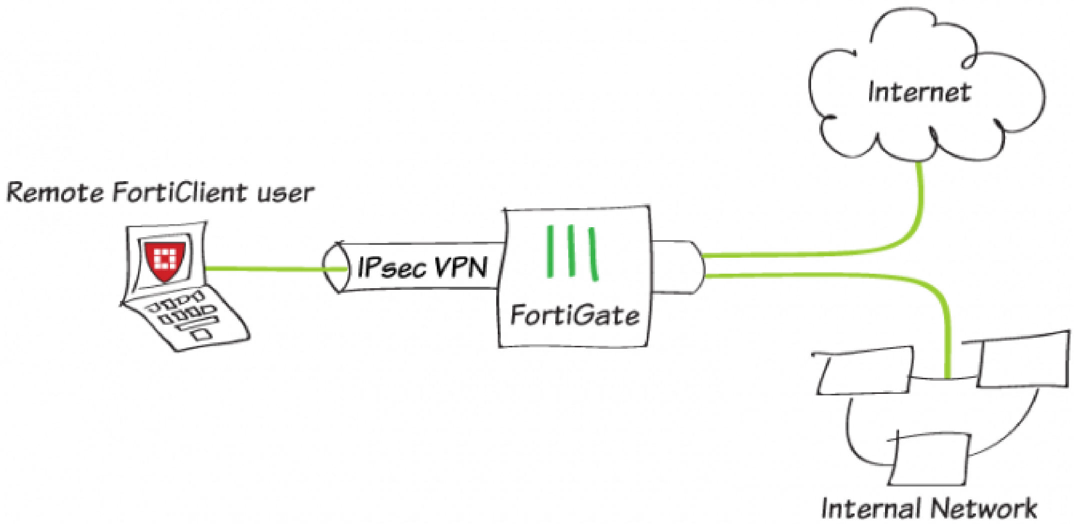
If you prefer to use local logging for Branch rather than sending logs to a remote FortiAnalyzer, you can do so using the following CLI commands:

```
config system csf
   set logging-mode local
end
```

Then go to *Log & Report > Log Settings* and configure local logging.

This option is available for all FortiGates in the Security Fabric except for the root FortiGate.

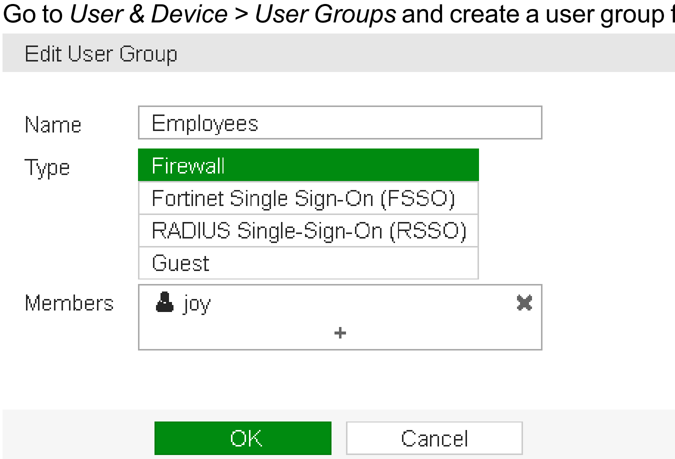
IPsec VPN with FortiClient



In this example, you allow remote users to access the corporate network using an IPsec VPN that they connect to using FortiClient. The remote user Internet traffic is also routed through the FortiGate (split tunneling is not enabled).

Creating a user group for remote users

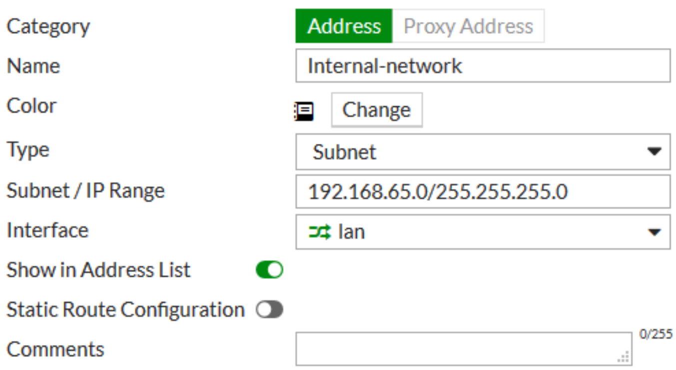
1. Go to *User & Device* > *User Definition* and create a local user account for an IPsec VPN user.
2. Go to *User & Device* > *User Groups* and create a user group for IPsec VPN users.



3. Add the new user account to the group.

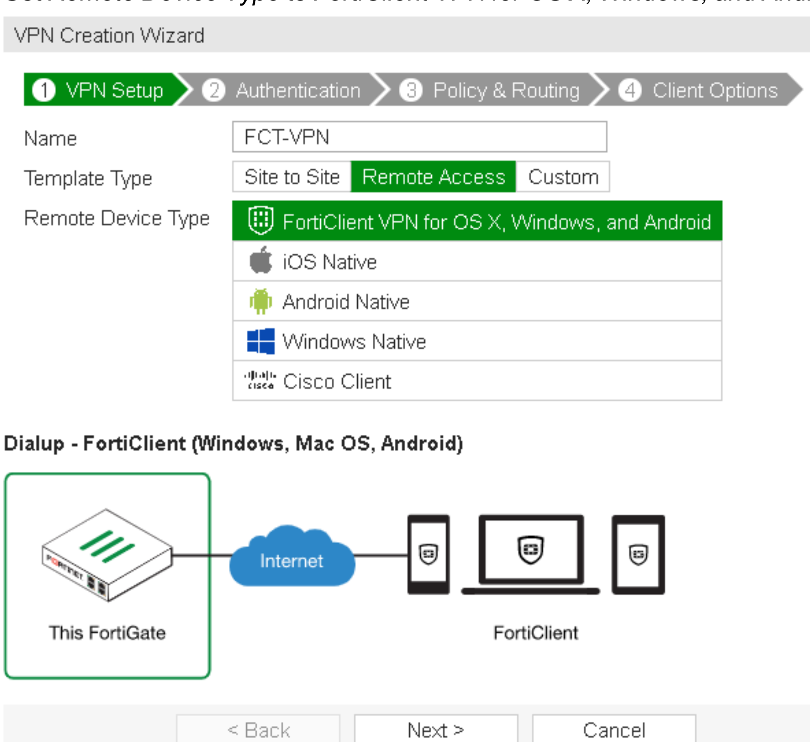
Adding a firewall address

1. Go to *Policy & Objects* > *Addresses* and create a new address.
2. Set *Category* to *Address* and enter a *Name*.
   Set *Type* to *Subnet*.
   Set *Subnet/IP Range* to the local subnet.
   Set *Interface* to *lan*.

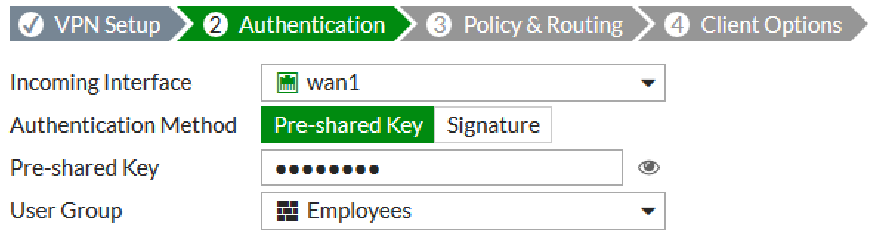


Configuring the IPsec VPN

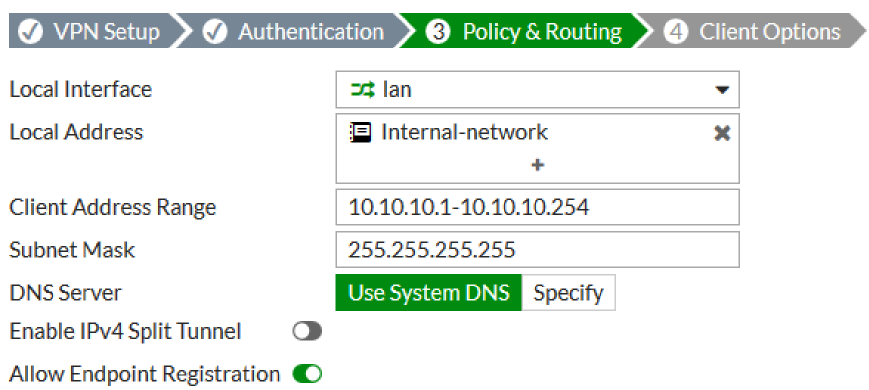
1. Go to *VPN* > *IPsec Wizard* and create a new tunnel.
2. Name the VPN. The tunnel name cannot include spaces or exceed 13 characters.
   Set *Template Type* to *Remote Access*.
   Set *Remote Device Type* to *FortiClient VPN for OS X, Windows, and Android*.



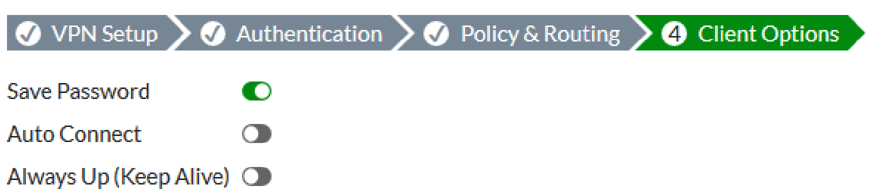
3. Set the *Incoming Interface* to *wan1*
Set *Authentication Method* to *Pre-shared Key*.
Enter a pre-shared key. This pre-shared key is a credential for the VPN and should differ from the user password.
For *User Group*, select *Employees*.



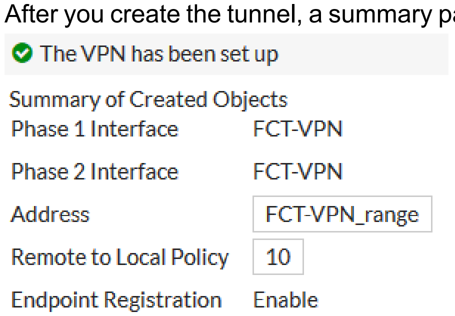
4. Set *Local Interface* to *lan*.
Set *Local Address* to the local network address.
Enter a *Client Address Range* for VPN users.
Ensure *Enable IPv4 Split Tunnel* is *not* enabled so that all Internet traffic goes through the FortiGate, otherwise traffic not intended for the corporate network will not flow through the FortiGate or be subject to the corporate security profiles.



5. Select *Client Options*.



6. After you create the tunnel, a summary page lists the objects that have been added to the FortiGate's configuration.



7. To view the VPN interface created by the wizard, go to *Network* > *Interfaces* and expand the *wan1* interface.

	Status	Name	Members	IP/Netmask	Type
		wan1		172.25.176.62 255.255.255.0	Physical Interface
		FCT-VPN		169.254.1.1 255.255.255.255	Tunnel Interface

8. To view the firewall address created by the wizard, go to *Policy & Objects* > *Addresses*.

Name	Type	Details
Address 16		
FCT-VPN_range	IP Range	10.10.10.1 - 10.10.10.254

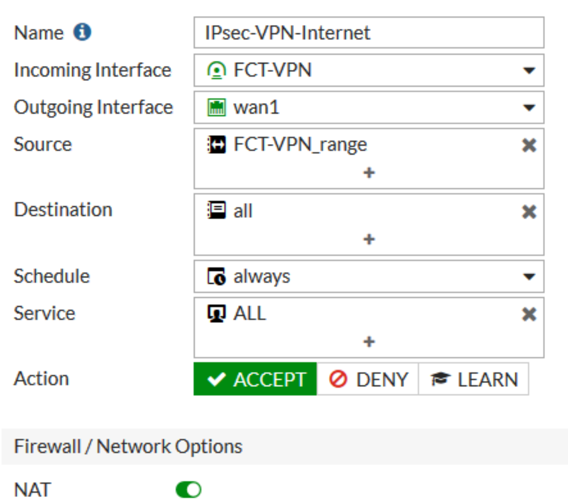
9. To view the security policy created by the wizard, go to *Policy & Objects* > *IPv4 Policy*.

ID	Name	Source	Destination	Schedule	Service	Action	NAT
FCT-VPN → lan 1							
10	vpn_FCT-V...	FCT-VPN	Internal-netw	always	ALL	ACCEPT	Enabled

Creating a security policy

The IPsec wizard automatically creates a security policy allowing IPsec VPN users to access the internal network. However, since split tunneling is disabled, you must create another policy to allow users to access the Internet through the FortiGate.

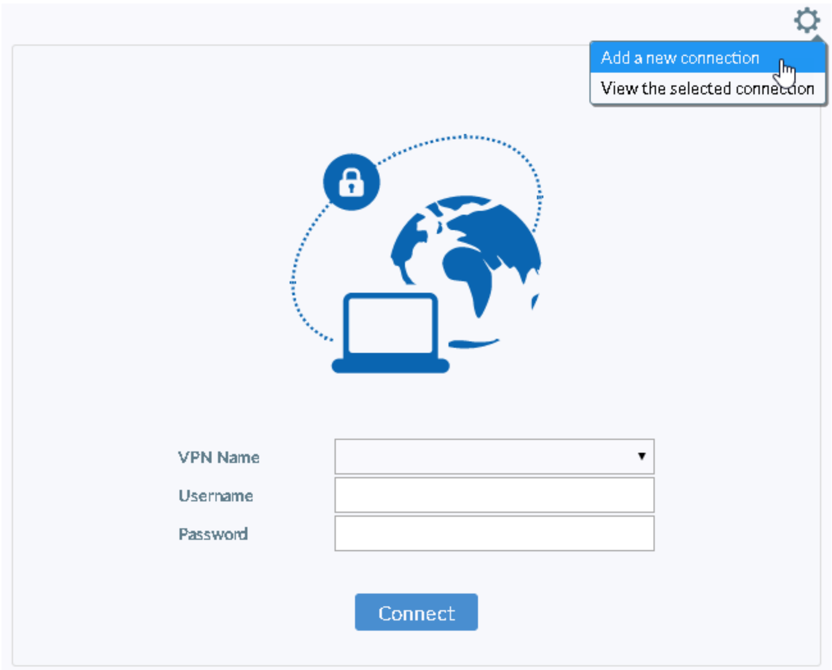
1. Go to *Policy & Objects* > *IPv4 Policy* and select *Create New*.
   Enter a policy *Name* (in this example, *IPsec-VPN-Internet*).
   Set *Incoming Interface* to the tunnel interface.
   Set *Outgoing Interface* to *wan1*.
   Set *Source* to the IPsec client address range.
   Set *Destination* to *all*.
   Set *Service* to *ALL*.
   Enable *NAT*.



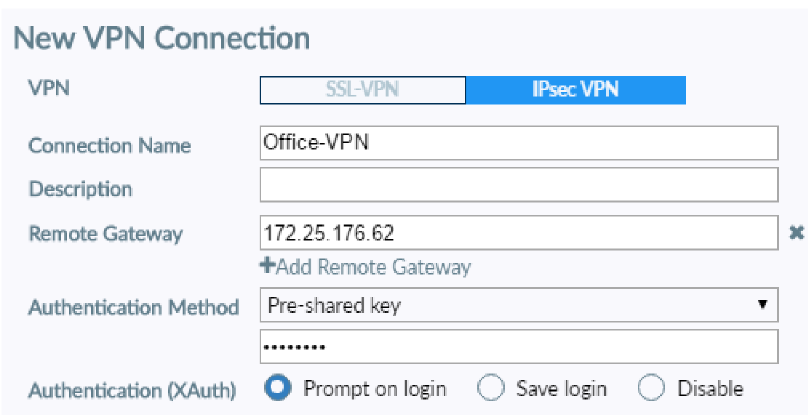
Configuring FortiClient

This example uses FortiClient 6.0.3.0155 for Windows to add the VPN connection.

1. In FortiClient, go to *Remote Access* and *Add a new connection*.



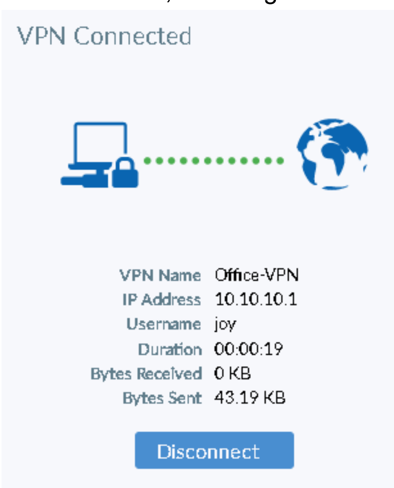
2. Set *VPN* to *IPsec VPN*.
   Enter a *Connection Name*.
   Set *Remote Gateway* to the FortiGate IP address.
   Set *Authentication Method* to *Pre-Shared Key* and enter the key.



Results

1. On FortiClient, select the VPN, enter the *Username* and *Password*, and select *Connect*.

2. When the connection is established, FortiGate assigns the user an IP address and FortiClient displays the status of the connection, including the IP address, connection duration, and bytes sent and received.



3. On FortiGate, go to *Monitor* > *IPsec Monitor*.
   Verify that the tunnel *Status* is *Up*.
   Remote Gateway shows the FortiClient user's assigned gateway IP address.

Name	Type	Remote Gateway	Status	Incoming Data
FCT-VPN_0	Dialup - FortiClient (Windows, Mac OS, Android)	172.25.177.102	Up	461.15 kB

4. Browse the Internet, then go to *FortiView* > *Policies* and select the *now* view.
   You can see traffic flowing through the *IPsec-VPN-Internet* policy.
   Right-click the policy to drill down to see more details.

Policy	Bytes (Sent/Received)	Sessions	Bandwidth	Packets (Sent/Received)
4 (IPsec-VPN-Internet)	54.37 kB	458	12 kbps	866

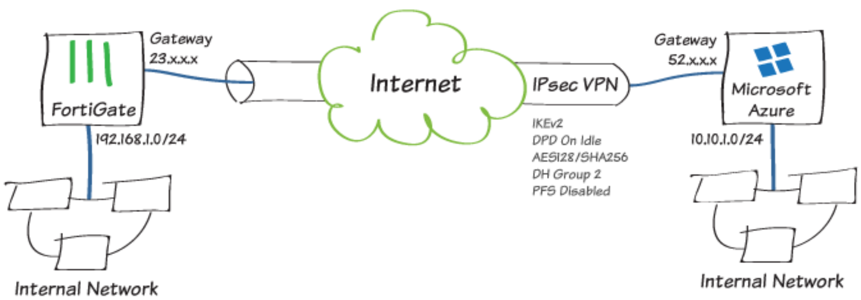
IPsec VPN to Azure

This example shows how to configure a site-to-site IPsec VPN tunnel to Microsoft Azure. This example shows how to configure a tunnel between each site, avoiding overlapping subnets, so that a secure tunnel can be established.

Prerequisites

- A FortiGate with an Internet-facing IP address.
- A valid Microsoft Azure account.

Sample topology



Sample configuration

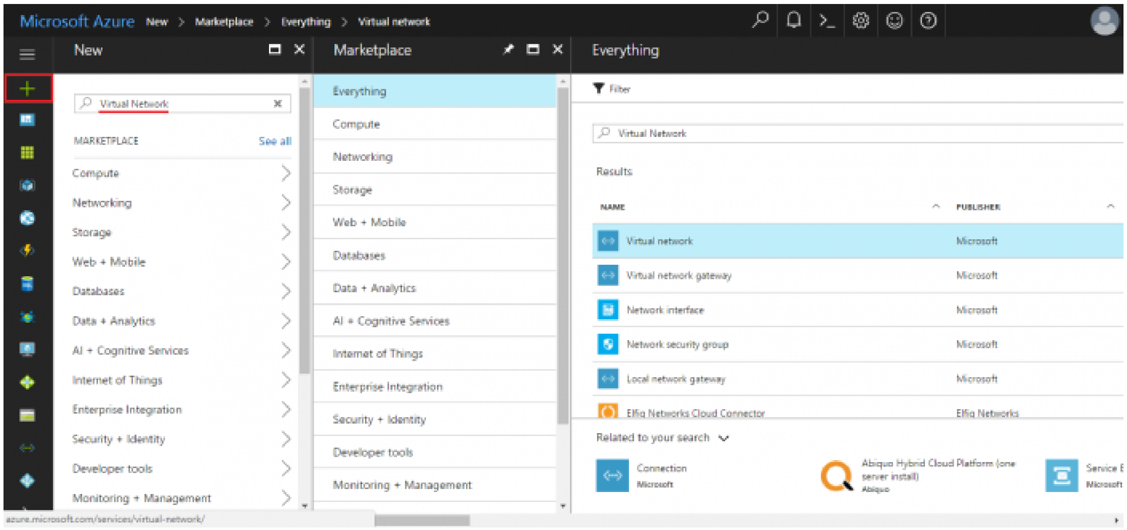
This sample configuration shows how to:

1. Configure an Azure virtual network.
2. Specify the Azure DNS server.
3. Configure the Azure virtual network gateway.
4. Configure the Azure local network gateway.
5. Configure the FortiGate tunnel.
6. Create the Azure firewall object.
7. Create the FortiGate firewall policies.
8. Create the FortiGate static route.
9. Create the Azure site-to-site VPN connection.
10. Check the results.

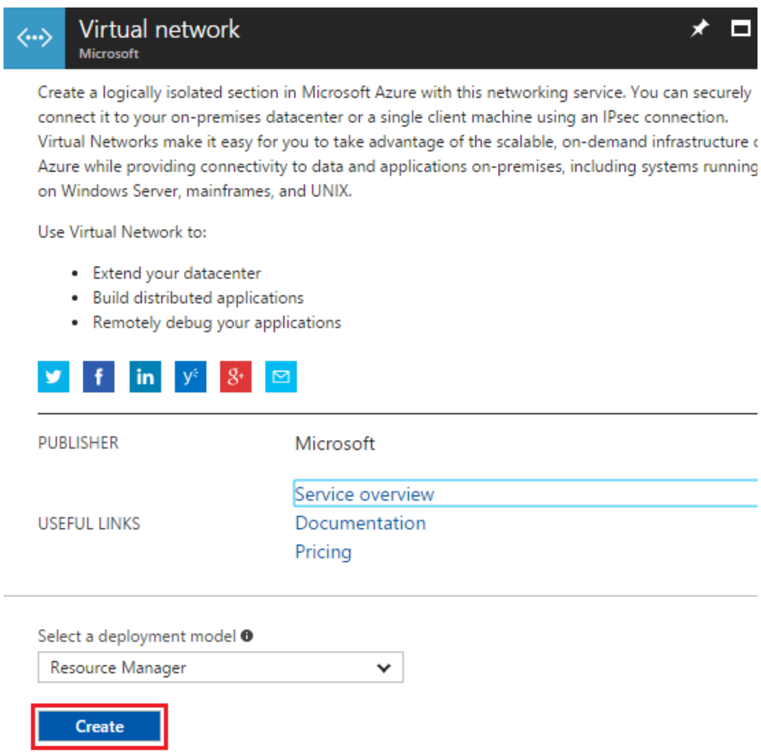
To configure an Azure virtual network:

1. Log into Azure and click *New*.
2. In *Search the Marketplace*, type *Virtual network*.

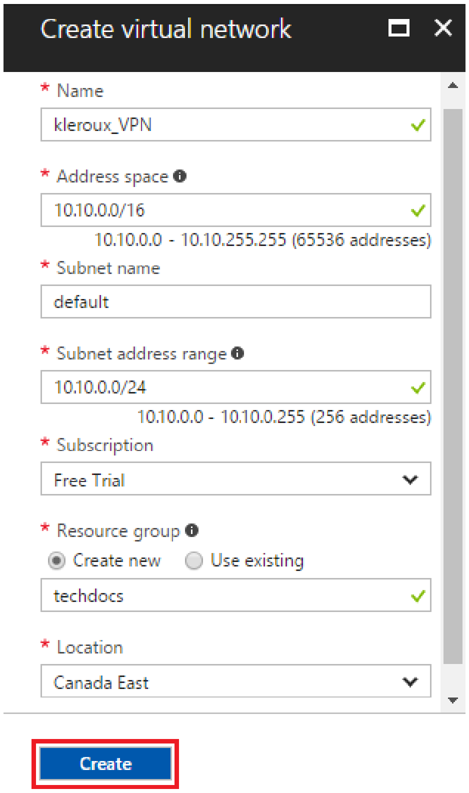
3. Click *Virtual network* to open the *Virtual network* pane.



4. At the bottom of the *Virtual network* pane, click the *Select a deployment model* dropdown list and select *Resource Manager*.
5. Click *Create*.

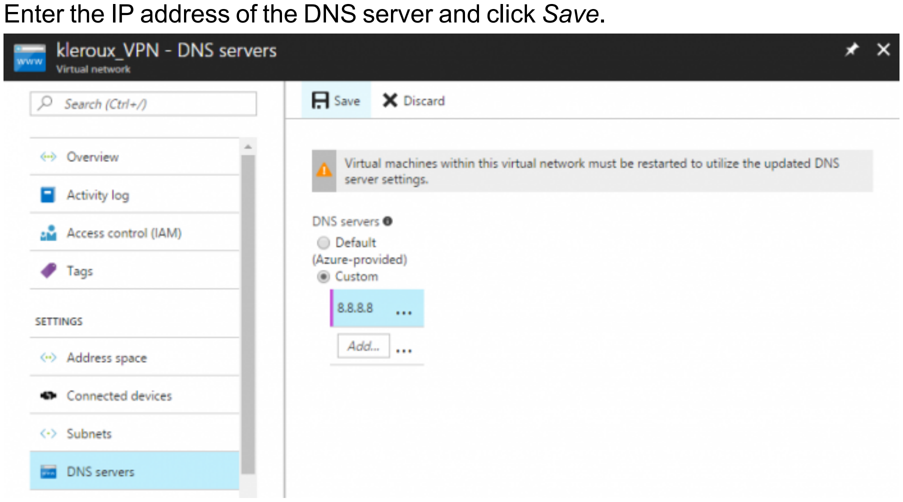


6. On the *Create virtual network* pane, enter you virtual network settings, and click *Create*.



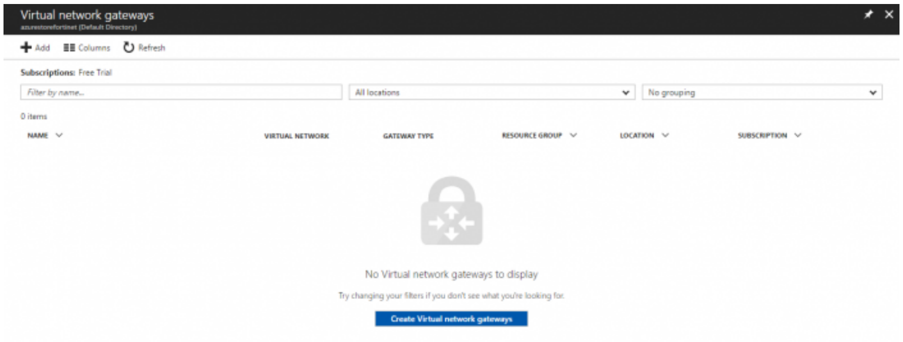
To specify the Azure DNS server:

1. Open the virtual network you just created.
2. Click *DNS servers* to open the *DNS servers* pane.
3. Enter the IP address of the DNS server and click *Save*.

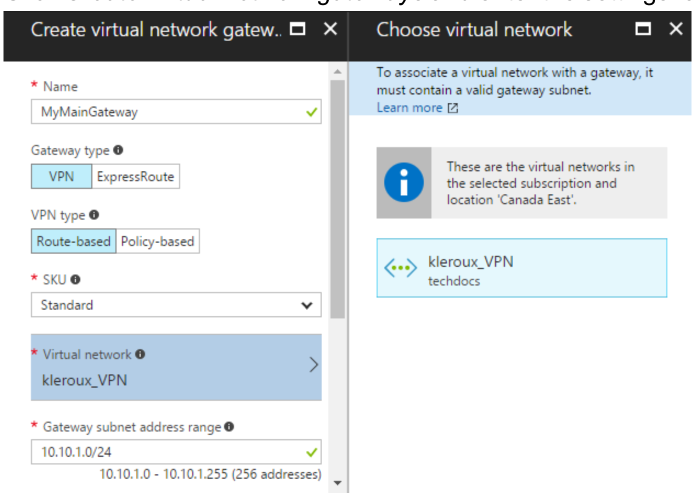


To configure the Azure virtual network gateway:

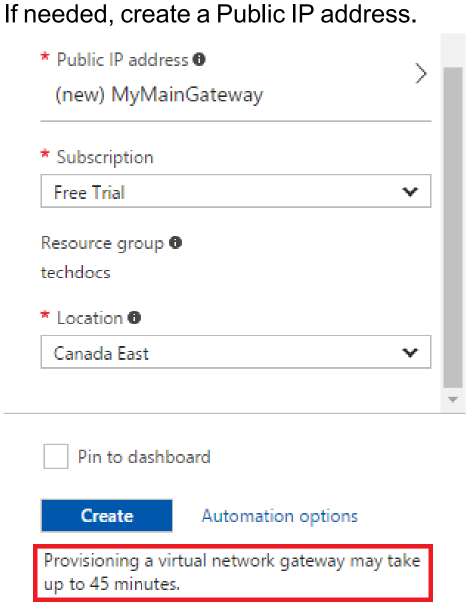
1. In the portal dashboard, go to *New*.
2. Search for *Virtual Network Gateway* and click it to open the *Virtual network gateway* pane.



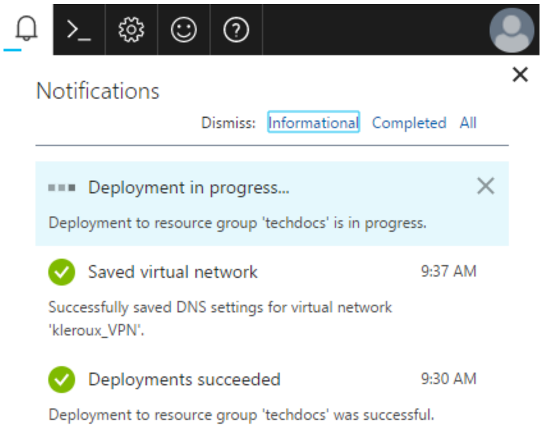
3. Click *Create Virtual network gateways* and enter the settings for your virtual network gateway.



4. If needed, create a Public IP address.

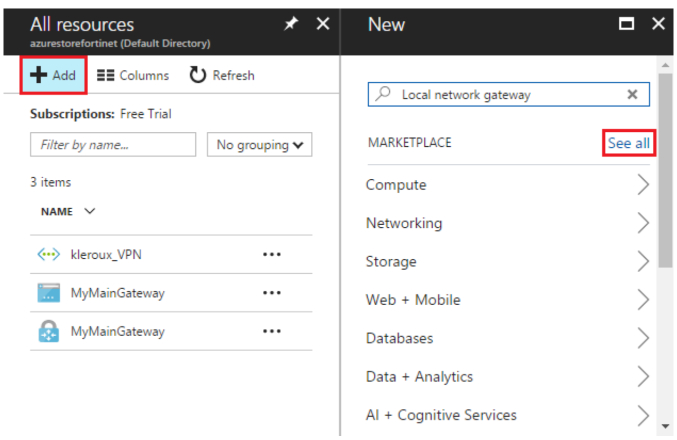


5. Click *Create*.
   Creating the virtual network gateway might take some time. When the provisioning is done, you'll receive a notification.

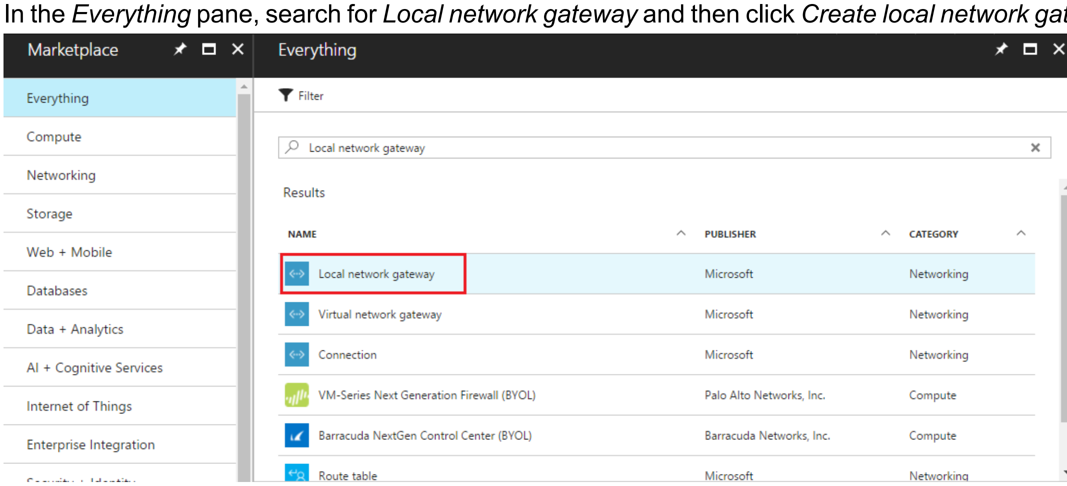


To configure the Azure local network gateway:

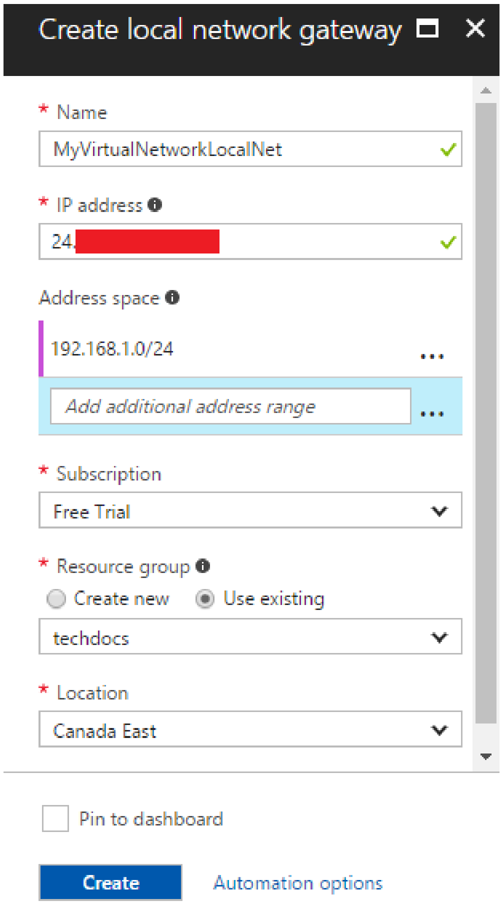
1. In the portal dashboard, click *All resources*.
2. Click *Add* and then click *See all*.



3. In the *Everything* pane, search for *Local network gateway* and then click *Create local network gateway*.



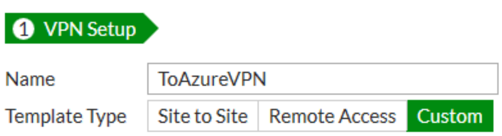
4. For the *IP address*, enter the local network gateway IP address, that is, the FortiGate's external IP address.



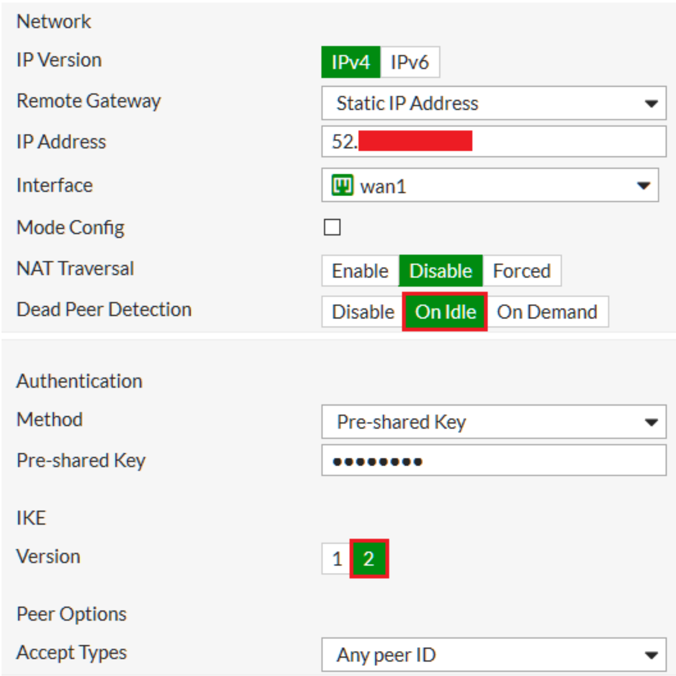
5. Set the remaining values for your local network gateway and click *Create*.

To configure the FortiGate tunnel:

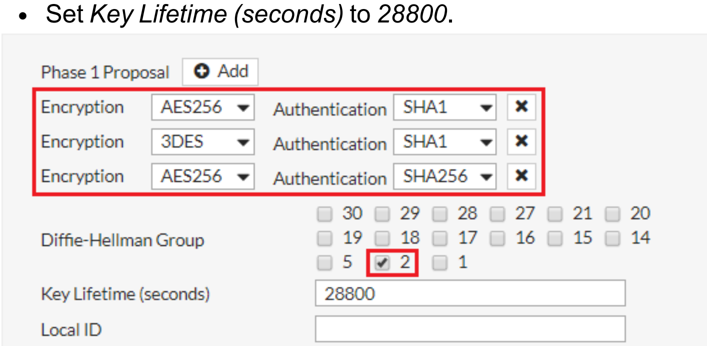
1. In the FortiGate, go to *VPN > IP Wizard*.
2. Enter a *Name* for the tunnel, click *Custom*, and then click *Next*.



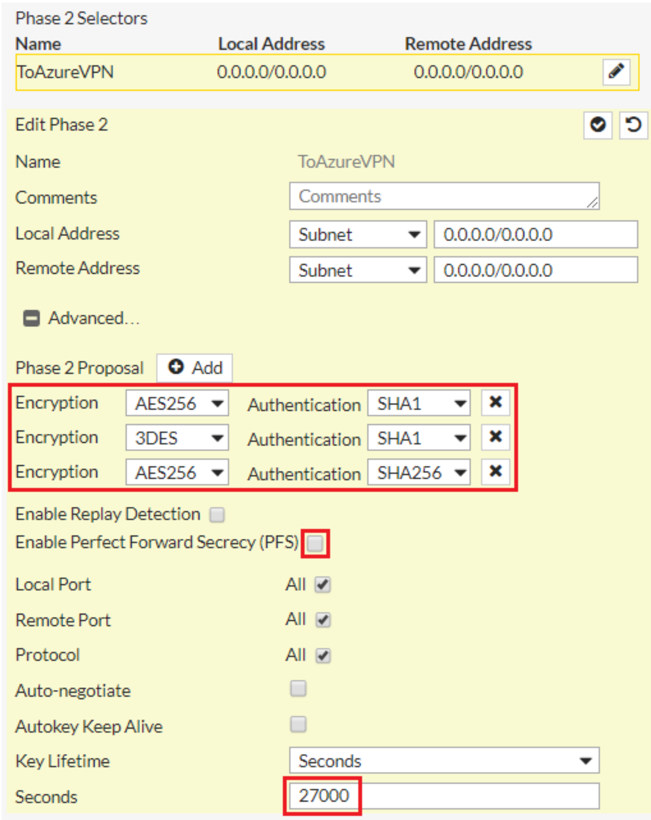
3. Configure the *Network* settings.
   - For *Remote Gateway*, select *Static IP Address* and enter the IP address provided by Azure.
   - For *Interface*, select *wan1*.
   - For *NAT Traversal*, select *Disable*,
   - For *Dead Peer Detection*, select *On Idle*.
   - In the Authentication section, select
4. Configure the *Authentication* settings.
   - For *Method*, select *Pre-shared Key* and enter the *Pre-shared Key*.
   - For *IKE*, select *2*.



5. Configure the *Phase 1 Proposal* settings.
   - Set the Encryption and Authentication combination to the three supported encryption algorithm combinations accepted by Azure.
     - AES256 and SHA1
     - 3DES and SHA1
     - AES256 and SHA256
   - For *Diffie-Hellman Groups*, select *2*.
   - Set *Key Lifetime (seconds)* to *28800*.



6. In *Phase 2 Selectors*, expand the *Advanced* section to configure the *Phase 2 Proposal* settings.
   - Set the Encryption and Authentication combinations.
     - AES256 and SHA1
     - 3DES and SHA1
     - AES256 and SHA256
   - Uncheck *Enable Perfect Forward Secrecy (PFS)*.
   - Set *Key Lifetime (seconds)* to *27000*.



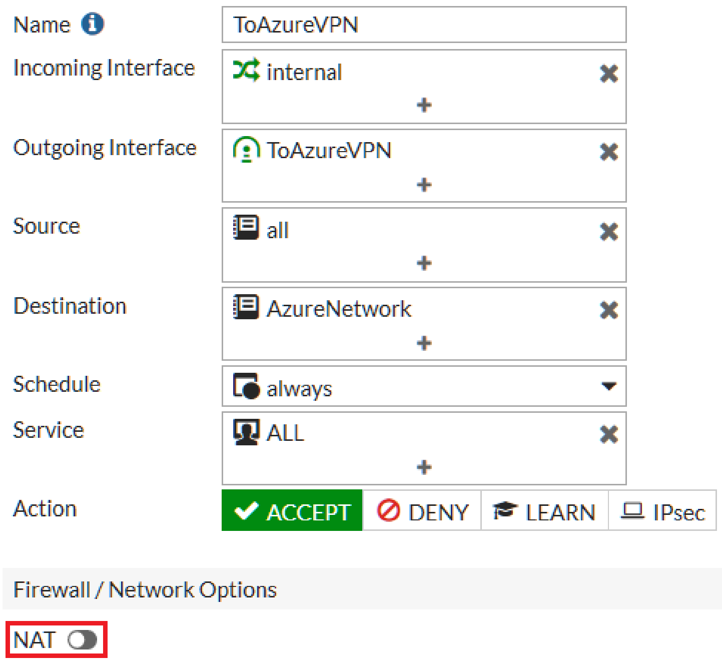
7. Click *OK*.

To create the Azure firewall object:

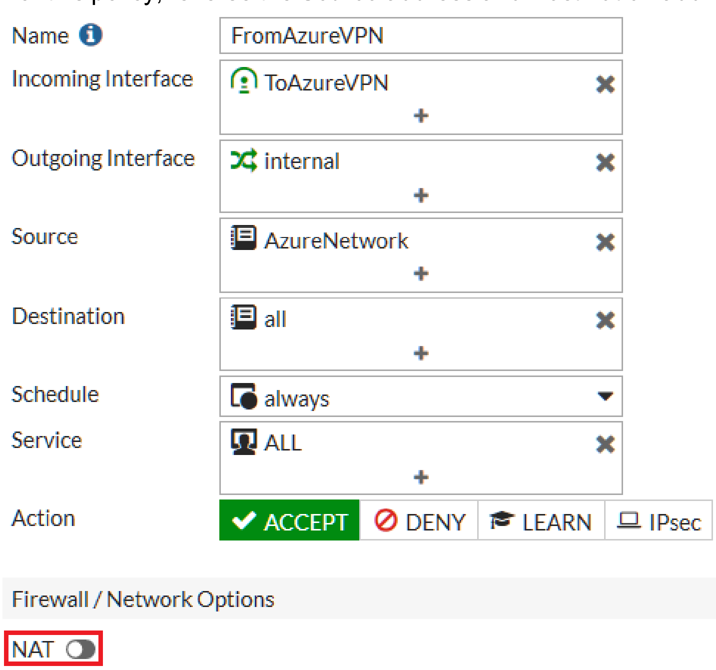
1. In the FortiGate, go to *Policy & Objects* > *Addresses*.
2. Create a firewall object for the Azure VPN tunnel.

To create the FortiGate firewall policies:

1. In the FortiGate, go to *Policy & Objects* > *IPv4 Policy*.
2. Create a policy for the site-to-site connection that allows outgoing traffic.
   - Set the *Source* address and *Destination* address using the firewall objects you just created.
   - Disable *NAT*.



3. Create another policy that allows incoming traffic.
   - For this policy, reverse the *Source* address and *Destination* address.



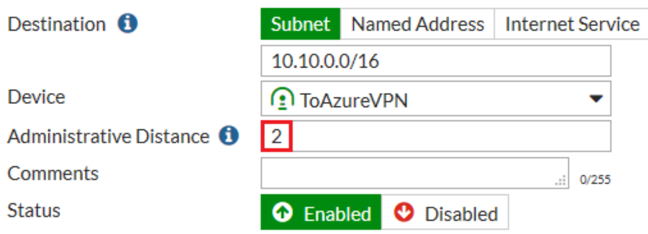
4. We recommend limiting the TCP maximum segment size (MSS) being sent and received so as to avoid packet drops and fragmentation.

To do this, use the following CLI commands on both policies.

```
config firewall policy
   edit <policy-id>
      set tcp-mss-sender 1350
      set tcp-mss-receiver 1350
   next
end
```

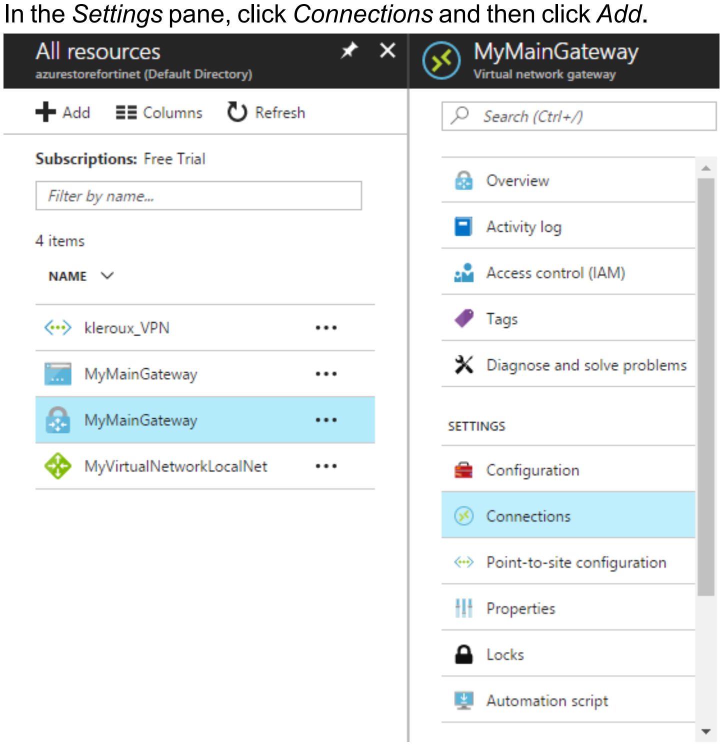
To create the FortiGate static route:

1. In the FortiGate, go to *Network > Static Routes*.
2. Create an IPv4 Static Route that forces outgoing traffic going to Azure to go through the route-based tunnel.
3. Set the *Administrative Distance* to a value lower than the existing default route value.



To create the Azure site-to-site VPN connection:

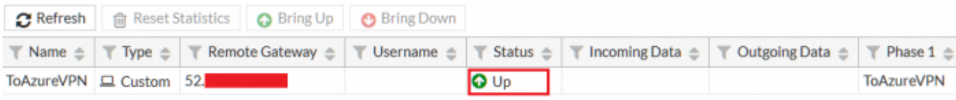
1. In the Azure portal, locate and select your virtual network gateway.
2. In the *Settings* pane, click *Connections* and then click *Add*.



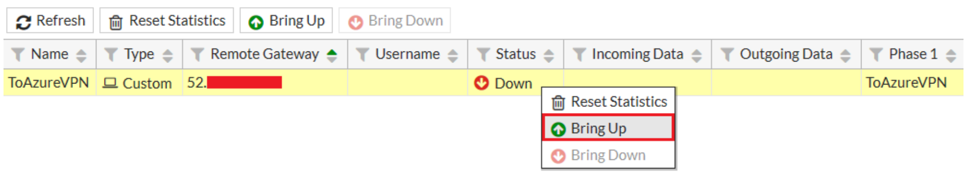
3. Enter the settings for your connection. Ensure the *Shared Key (PSK)* matches the *Pre-shared Key* for the FortiGate tunnel.

To check the results:

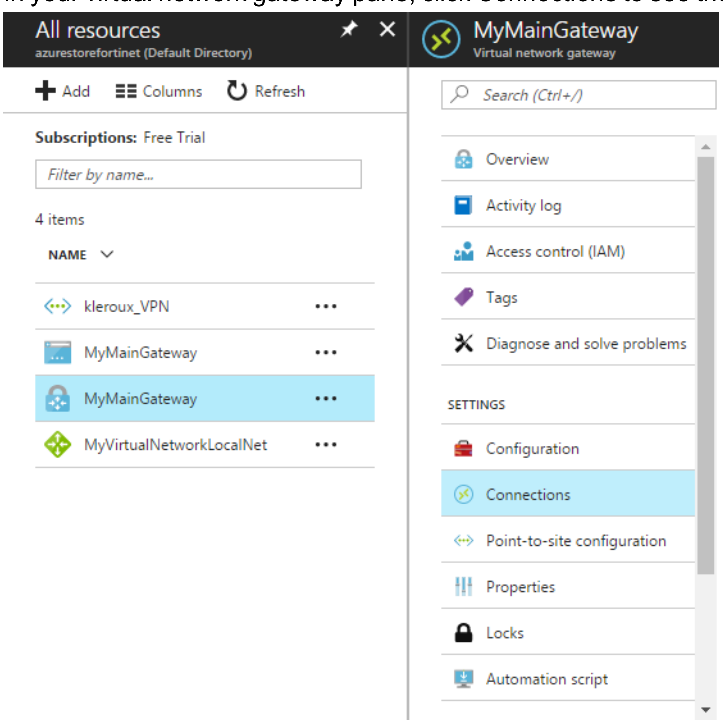
1. In the FortiGate, go to *Monitor* > *IPsec Monitor*.
   - Check that the tunnel is up.



   - If the tunnel is down, right-click the tunnel and select *Bring Up*.

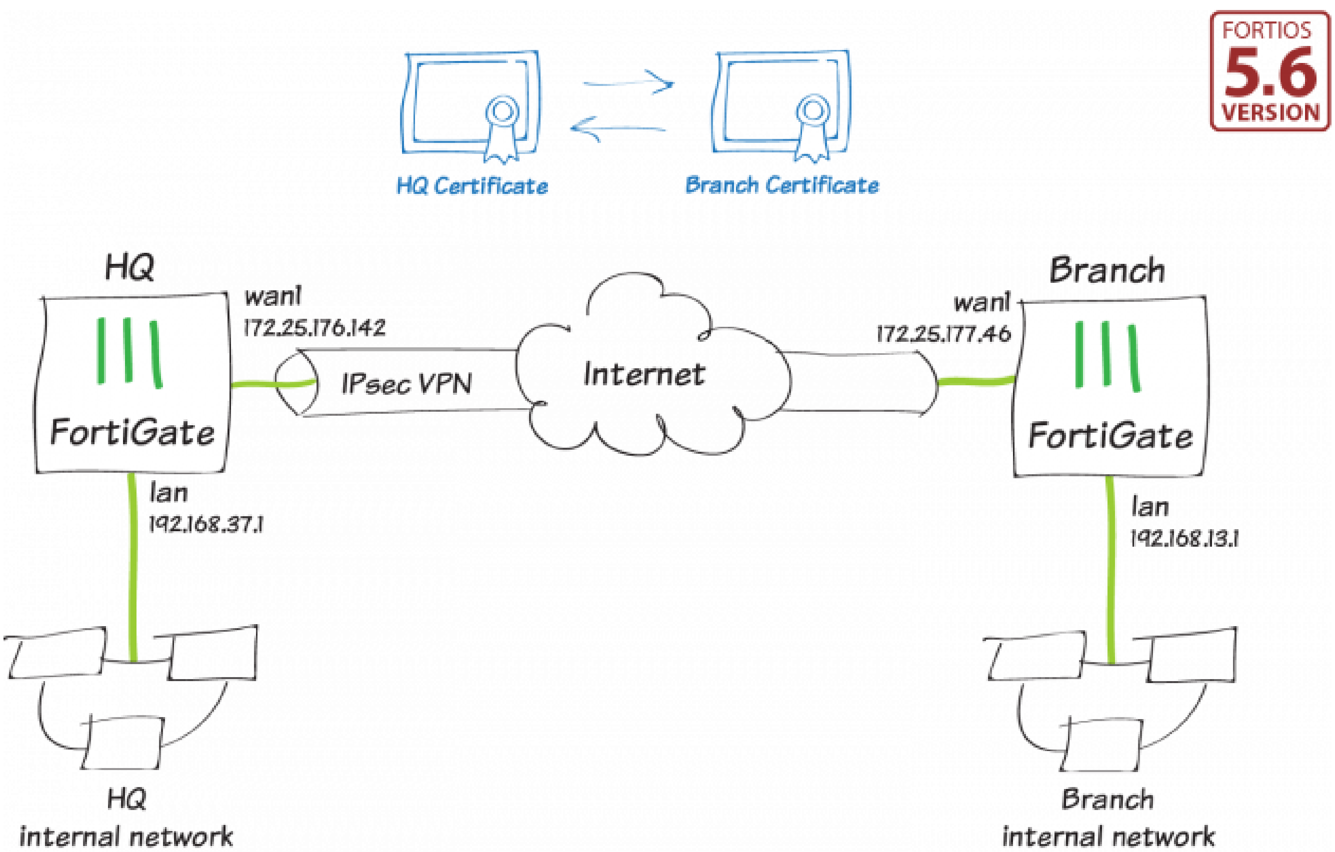


2. In the FortiGate, go to *Log & Report* > *Events*.
   - Select an event to view more information and verify the connection.
3. In the Azure portal dashboard, click *All resources* and locate your virtual network gateway.
   a. In your virtual network gateway pane, click *Connections* to see the status of each connection.



   b. Click a connection to open the *Essentials* pane to view more information about that connection.
      - If the connection is successful, the *Status* shows *Connected*.
      - See the *ingress* and *egress* bytes to confirm traffic flowing through the tunnel.

Site-to-site IPsec VPN with certificate authentication

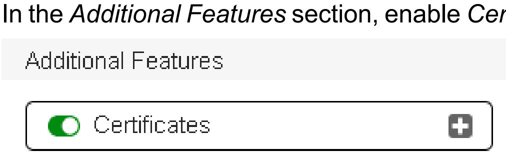


This example shows you how to create a route-based IPsec VPN tunnel to allow transparent communication between two networks that are located behind different FortiGates. The VPN is created on both FortiGates using the VPN Wizard's *Site to Site – FortiGate* template. For this example, instead of using a pre-shared key for authentication, the FortiGates use a certificate.

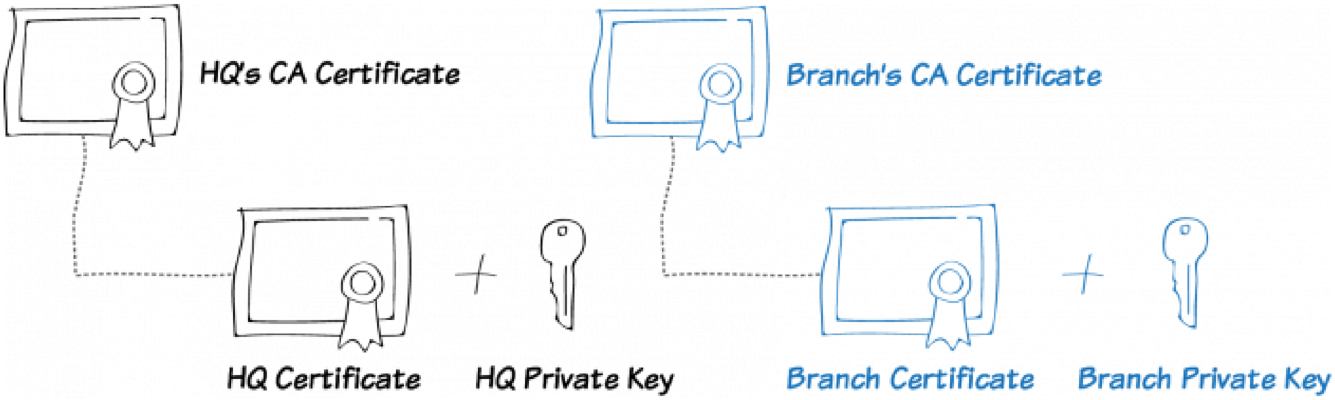
In this example, one FortiGate is called *HQ* and the other *Branch*.

Enabling certificate management

1. On both FortiGates, go to *System* > *Feature Visibility*
   In the *Additional Features* section, enable *Certificates*.



Obtaining the necessary certificates



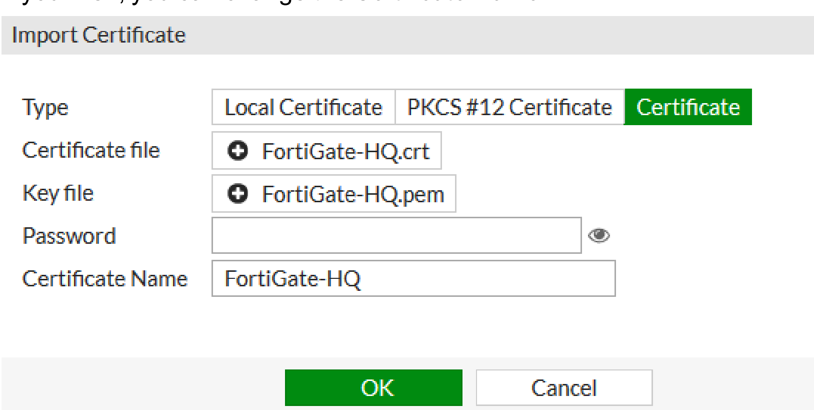
This example requires the following files:

- Client certificate for HQ and its matching private key.
- Client certificate for Branch and its matching private key.
- CA certificate that issued HQ's certificate.
- CA certificate that issued Branch's certificate.

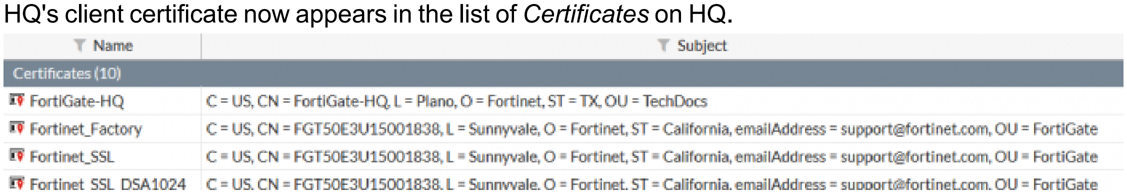
Installing the client certificates

The client certificate is used for authentication and represents the individual identity of each FortiGate.

1. On HQ, go to *System* > *Certificates* and select *Import* > *Local Certificate*.
   Set *Type* to *Certificate*.
   Select the *Certificate file* and the *Key file* for HQ.
   If you wish, you can change the *Certificate Name*.

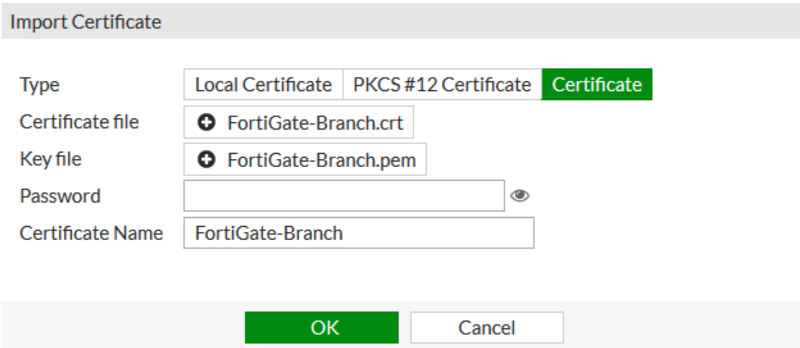


2. HQ's client certificate now appears in the list of *Certificates* on HQ.



Name	Subject
Certificates (10)	
FortiGate-HQ	C = US, CN = FortiGate-HQ, L = Plano, O = Fortinet, ST = TX, OU = TechDocs
Fortinet_Factory	C = US, CN = FGT50E3U15001838, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
Fortinet_SSL	C = US, CN = FGT50E3U15001838, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
Fortinet_SSL_DSA1024	C = US, CN = FGT50E3U15001838, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate

3. On Branch, go to *System* > *Certificates* and select *Import* > *Local Certificate*.
Set *Type* to *Certificate*.
Select the *Certificate file* and the *Key file* for Branch.
If you wish, you can change the *Certificate Name*.



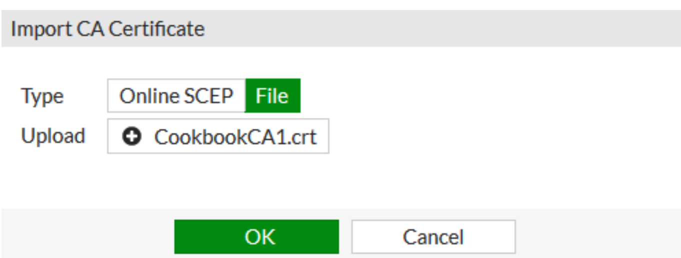
4. Branch's client certificate now appears in the list of *Certificates* on Branch.

Name	Subject
Certificates (10)	
FortiGate-Branch	C = US, CN = FortiGate-Branch, L = Sunnyvale, O = Fortinet, ST = CA, OU = TechDocs
Fortinet_Factory	C = US, CN = FGT50E3U15001552, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
Fortinet_SSL	C = US, CN = FGT50E3U15001552, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
Fortinet_SSL_DSA1024	C = US, CN = FGT50E3U15001552, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate

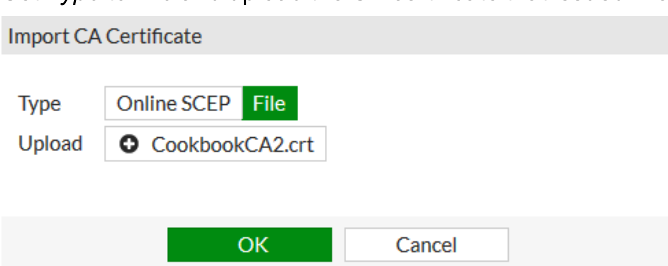
Installing the CA certificates

The CA certificate is used for verifying the identity of the remote FortiGate's client certificate imported earlier.

1. On HQ, go to *System* > *Certificates* and select *Import* > *CA Certificate*.
Set *Type* to *File* and upload the CA certificate that issued HQ's certificate.



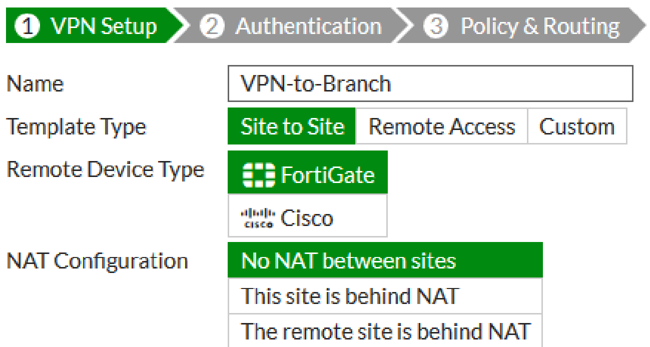
2. Go to *System* > *Certificates* and select *Import* > *CA Certificate*.
Set *Type* to *File* and upload the CA certificate that issued Branch's certificate.



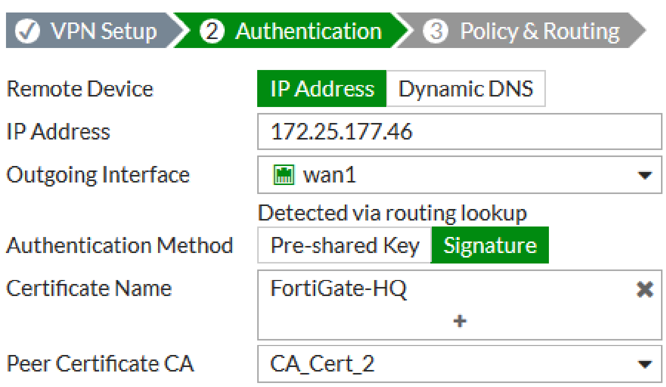
3. Both CA certificates now appear in HQ's list of *External CA Certificates*.
4. Repeat this procedure on Branch to import both CA certificates.

Configuring the IPsec VPN on HQ

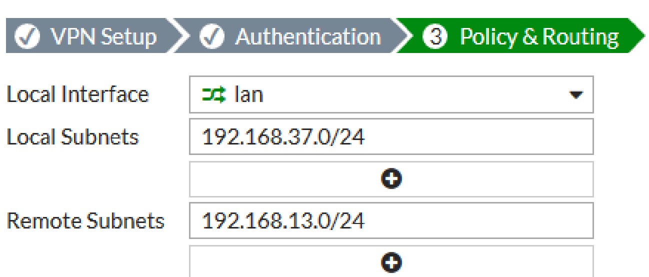
1. On HQ, go to *VPN* > *IPsec Wizard* and create a new tunnel.
   In the *VPN Setup* section, set *Template Type* to *Site to Site*.
   Set *Remote Device Type* to *FortiGate*.
   Set *NAT Configuration* to *No NAT between sites*.



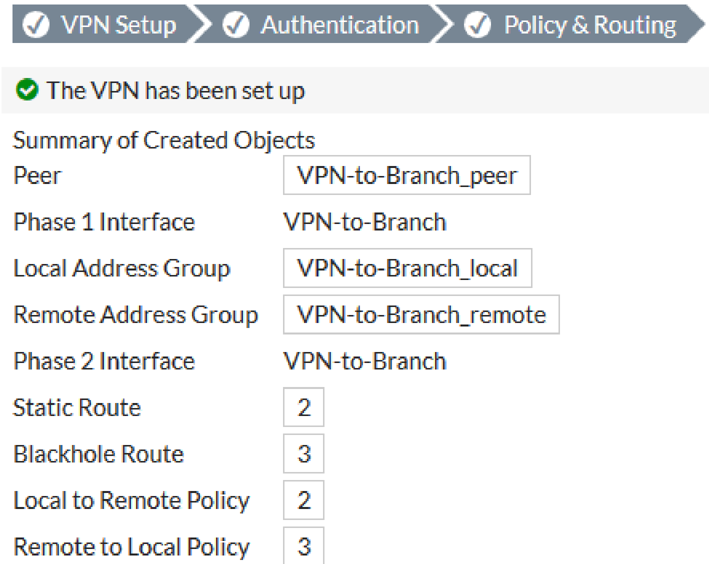
2. In the *Authentication* section, set *IP Address* to the public IP address of the Branch FortiGate (in this example, *172.25.177.46*).
   After you enter the IP address, an interface is assigned as the *Outgoing Interface*. If you want to use a different interface, select it from the dropdown menu.
   Set *Authentication Method* to *Signature*.
   For the *Certificate Name*, select the client certificate (in this example, *FortiGate-HQ*).
   For the *Peer Certificate CA*, select the CA certificate for Branch (in this example, *CA_Cert_2*).



3. In the *Policy & Routing* section, set *Local Interface* to *lan*. The local subnet is added automatically.
   Set *Remote Subnets* to Branch's local subnet (in this example, *192.168.13.0/24*).

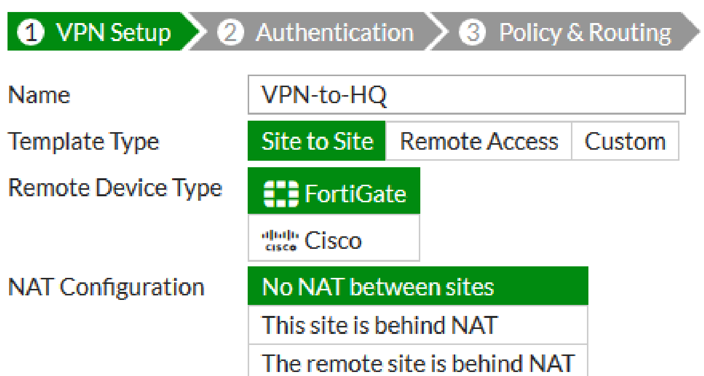


4. Review the configuration summary that shows the firewall addresses, static routes, and security policies.



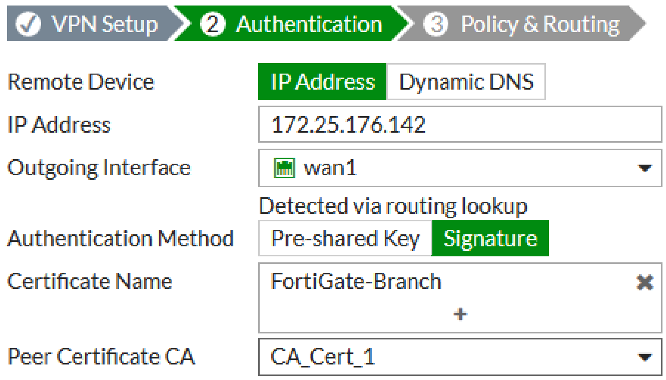
Configuring the IPsec VPN on Branch

1. On Branch, go to *VPN > IPsec Wizard* and create a new tunnel.
   In the *VPN Setup* section, set *Template Type* to *Site to Site*.
   Set *Remote Device Type* to *FortiGate*.

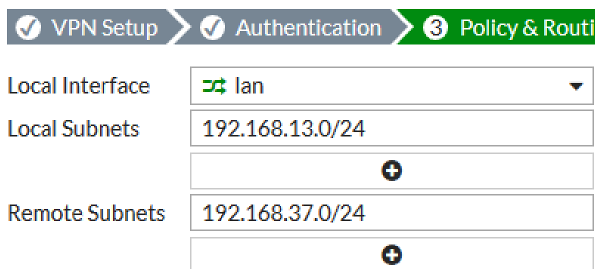


2. In the *Authentication* section, set *IP Address* to the public IP address of the HQ FortiGate (in this example, *172.25.176.142*).
   After you enter the IP address, an interface is assigned as the *Outgoing Interface*. If you want to use a different interface, select it from the dropdown menu.
   Set *Authentication Method* to *Signature*.
   For the *Certificate Name*, select the client certificate (in this example, *FortiGate-Branch*).

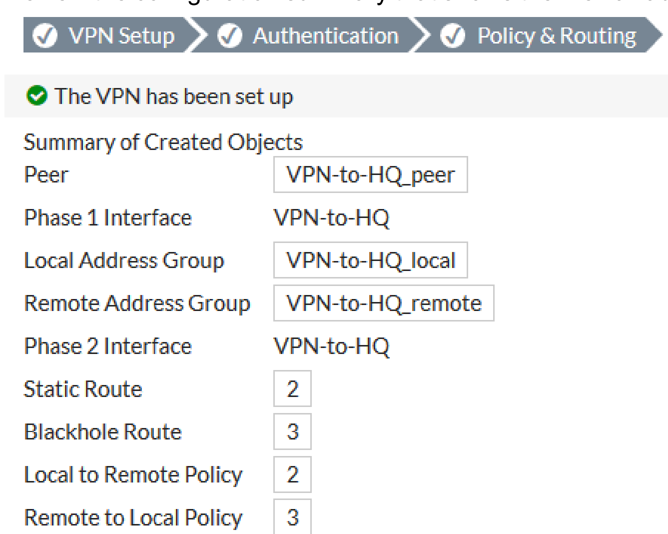
For the *Peer Certificate CA*, select the CA certificate for HQ (in this example, *CA_Cert_1*).



3. In the *Policy & Routing* section, set *Local Interface* to *LAN*. The local subnet is added automatically. Set *Remote Subnets* to HQ's local subnet (in this example, *192.168.37.0/24*).



4. Review the configuration summary that shows the firewall addresses, static routes, and security policies.



Results

On either FortiGate, go to *Monitor > IPsec Monitor* to verify the status of the VPN tunnel. If the tunnel *Status* is down, right-click its *Status* and select *Bring Up*.

Refresh | Reset Statistics | Bring Up | Bring Down

Name	Type	Remote Gateway	User Name	Status
VPN-to-Branch	Site to Site - FortiGate	172.25.177.46	C = US, ST = CA, L = Sunnyvale, O = Fortinet, OU = TechDocs, CN = FortiGate-Branch	Up

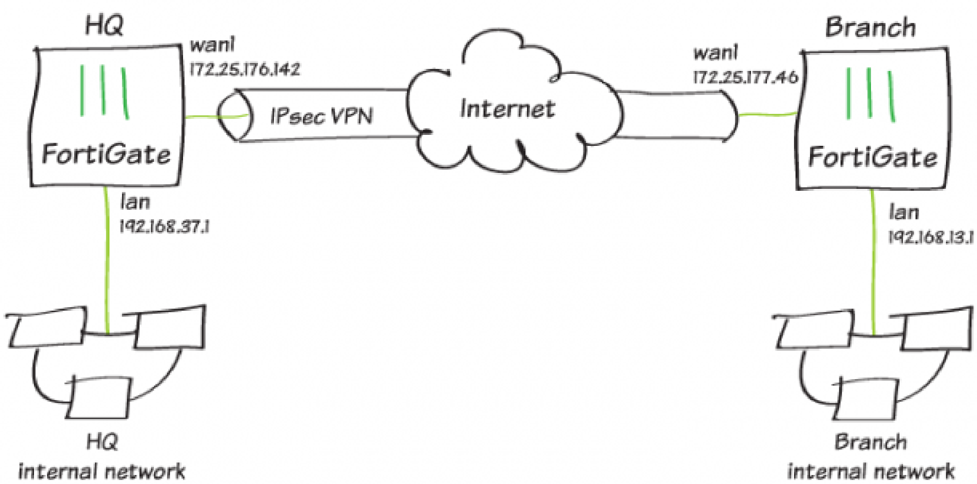
Refresh | Reset Statistics | Bring Up | Bring Down

Name	Type	Remote Gateway	User Name	Status
VPN-to-HQ	Site to Site - FortiGate	172.25.176.142	C = US, ST = TX, L = Plano, O = Fortinet, OU = TechDocs, CN = FortiGate-HQ	Up

A user on either office network can connect to any address on the other office network transparently.

To generate traffic to test the connection, ping Branch’s LAN interface from a device on HQ’s internal network.

Site-to-site IPsec VPN with two FortiGates



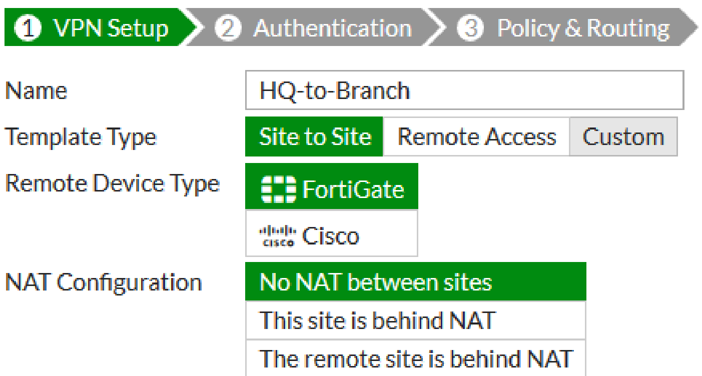
This example shows you how to create a site-to-site IPsec VPN tunnel to allow communication between two networks that are located behind different FortiGates. You use the VPN Wizard’s *Site to Site – FortiGate* template to create the VPN tunnel on both FortiGates.

In this example, one FortiGate is called HQ and the other is called Branch.

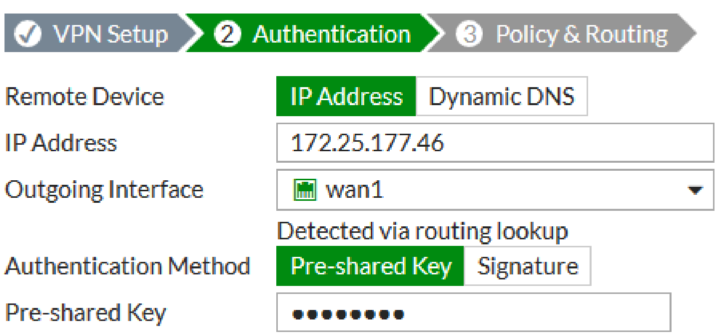
Site-to-Site IPsec VPN

Configuring IPsec VPN on HQ

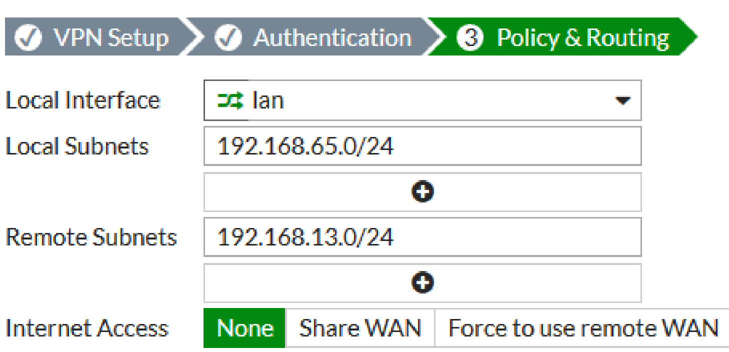
1. On HQ, go to *VPN > IPsec Wizard* and create a new tunnel.
   In the *VPN Setup* section, set *Template Type* to *Site to Site*.
   Set *Remote Device Type* to *FortiGate*.
   Set *NAT Configuration* to *No NAT between sites*.



2. In the *Authentication* section, set *IP Address* to the public IP address of the Branch FortiGate (in this example, *172.25.177.46*).
   After you enter the IP address, an interface is assigned as the *Outgoing Interface*. If you want to use a different interface, select it from the dropdown menu.
   Set a secure *Pre-shared Key*



3. In the *Policy & Routing* section, set *Local Interface* to *lan*. The local subnet is added automatically.
   Set *Remote Subnets* to the Branch network's subnet (in this example, *192.168.13.0/24*).
   Set *Internet Access* to *None*.



4. Review the configuration summary that shows the interfaces, firewall addresses, routes, and policies.

VPN Setup > Authentication > Policy & Routing

The VPN has been set up

Summary of Created Objects

Phase 1 Interface	HQ-to-Branch
Local Address Group	HQ-to-Branch_local
Remote Address Group	HQ-to-Branch_remote
Phase 2 Interface	HQ-to-Branch
Static Route	2
Blackhole Route	3
Local to Remote Policy	7
Remote to Local Policy	8

5. To view the VPN interface created by the wizard, go to *Network > Interfaces*.

Status	Name	IP/Netmask	Ref.
	wan1	172.25.176.62 255.255.255.0	10
	HQ-to-Branch	0.0.0.0 0.0.0.0	4

6. To view the firewall addresses created by the wizard, go to *Policy & Objects > Addresses*.

Name	Type	Details	Interface	Visibility	Ref.
Address 13					
FIREWALL_AUTH_...	Subnet	0.0.0.0/0		Hidden	0
HQ-to-Branch_local...	Subnet	192.168.65.0/24		Visible	1
HQ-to-Branch_rem...	Subnet	192.168.13.0/24		Visible	1

7. To view the routes created by the wizard, go to *Network > Static Routes*.

Destination	Gateway	Interface	Comment
0.0.0.0/0	172.25.176.1	wan1	
HQ-to-Branch_remote		HQ-to-Branch	VPN: HQ-to-Branch (Created by V...
HQ-to-Branch_remote		Blackhole	VPN: HQ-to-Branch (Created by V...

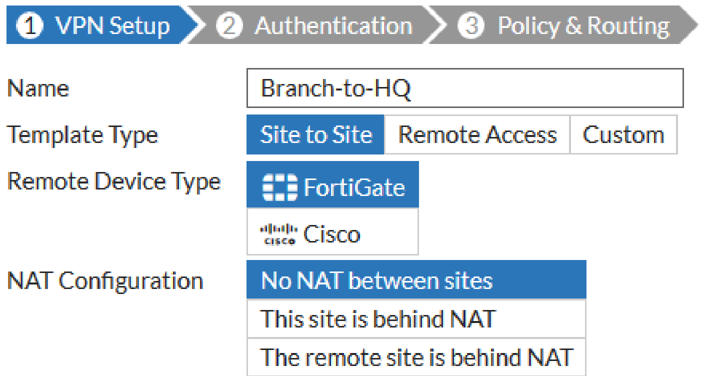
8. To view the policies created by the wizard, go to *Policy & Objects > IPv4 Policy*.

Name	From	To	Source	Destination
Internet	lan	wan1	all	all
vpn_HQ-to-Branch_local	lan	HQ-to-Branch	HQ-to-Branch_local	HQ-to-Branch_remote
vpn_HQ-to-Branch_remote	HQ-to-Branch	lan	HQ-to-Branch_remote	HQ-to-Branch_local

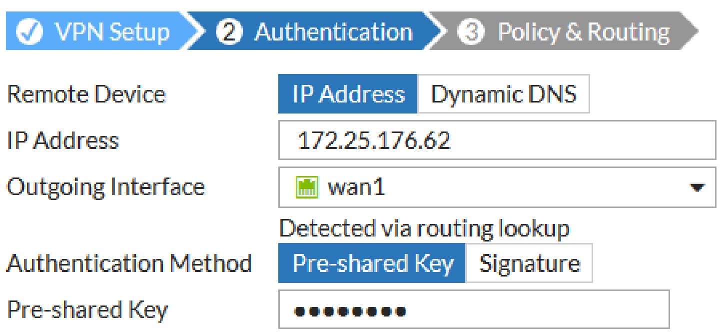
Configuring IPsec VPN on Branch

1. On Branch, go to *VPN > IPsec Wizard*, and create a new tunnel.
   In the *VPN Setup* section, set *Template Type* to *Site to Site*.
   Set *Remote Device Type* to *FortiGate*.

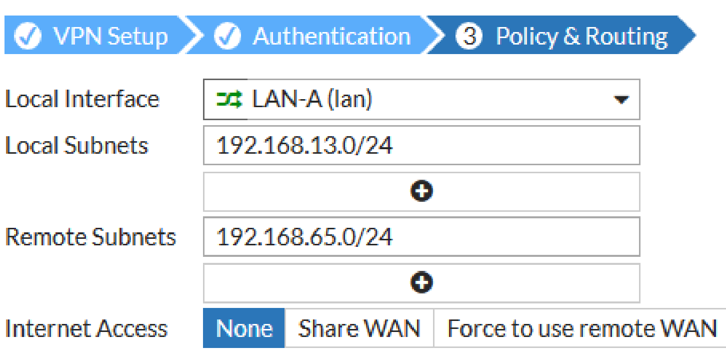
Set *NAT Configuration* to *No NAT between sites*.



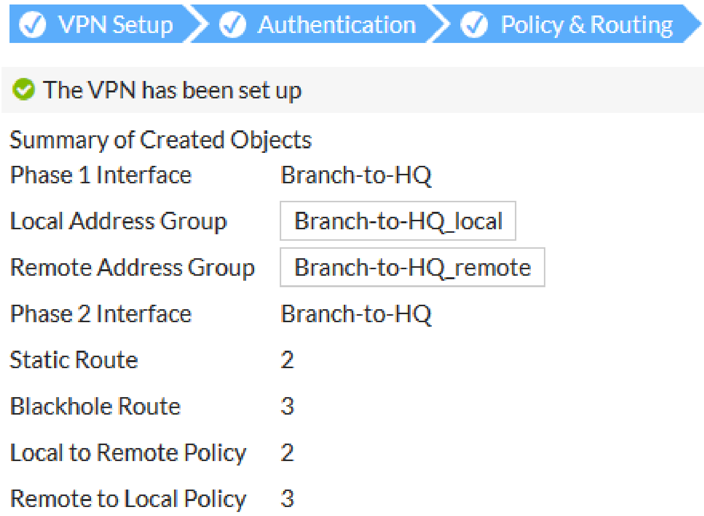
2. In the *Authentication* section, set *IP Address* to the public IP address of the HQ FortiGate (in this example, *172.25.176.62*).
   After you enter the IP address, an interface is assigned as the *Outgoing Interface*. If you want to use a different interface, select it from the dropdown menu.
   Set the secure *Pre-shared Key* that was used for the VPN on HQ.



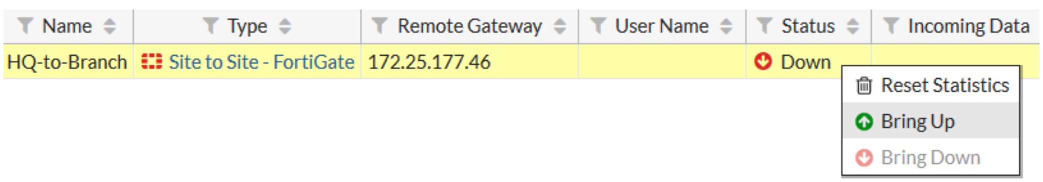
3. In the *Policy & Routing* section, set *Local Interface* to *lan*. The local subnet is added automatically.
   Set *Remote Subnets* to the HQ network's subnet (in this example, *192.168.65.0/24*).
   Set *Internet Access* to *None*.



4. Review the configuration summary that shows the interfaces, firewall addresses, routes, and policies.



5. To bring up the VPN tunnel, go to *Monitor > IPsec Monitor*. Right-click the *Status* and select *Bring Up*. You might need to refresh the page before the *Status* shows *Up*.



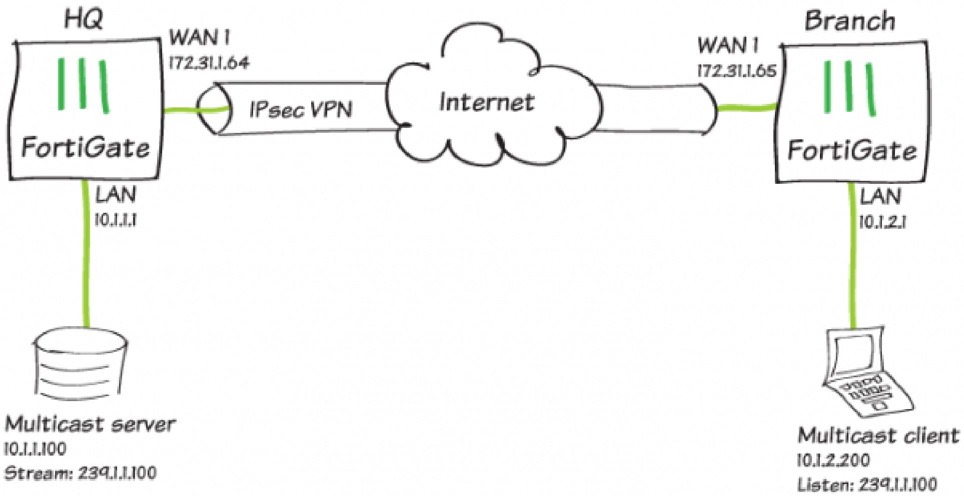
Results

Users on the HQ internal network can access resources on the Branch internal network and vice versa.

To test the connection, ping HQ's LAN interface from a device on the Branch internal network.

```
Pinging 192.168.65.1 with 32 bytes of data:
Reply from 192.168.65.1: bytes=32 time=1ms TTL=254
Reply from 192.168.65.1: bytes=32 time=1ms TTL=254
Reply from 192.168.65.1: bytes=32 time<1ms TTL=254
Reply from 192.168.65.1: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.65.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

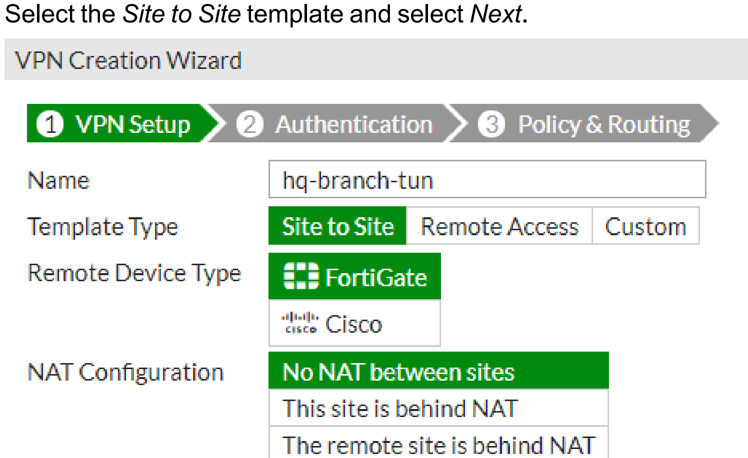
Multicast IPsec VPN without PIM



This is an example of allowing transparent multicast communication between two networks located behind FortiGates connected via IPsec VPN. Multicast is configured to send traffic across the IPsec tunnel without the use of protocol-independent multicast (PIM) or other multicast routing protocols. Two hosts are used to send and receive a multicast stream between the two sites. In this example, the FortiGate with the multicast streaming server is *HQ* while the FortiGate with the multicast client is *Branch*.

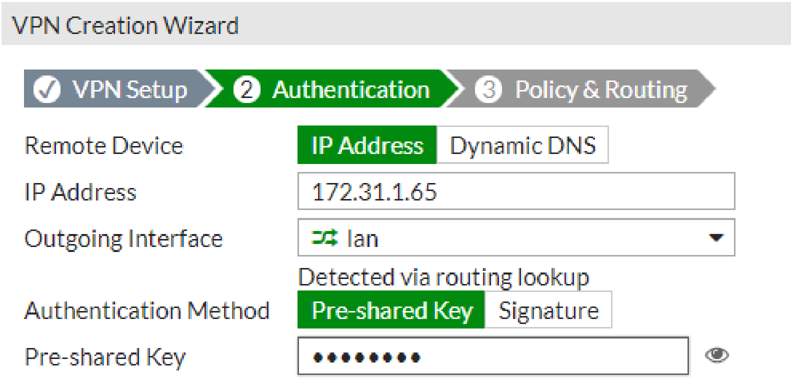
Configuring the HQ IPsec VPN

1. On HQ, go to *VPN > IPsec Wizard*.
   Select the *Site to Site* template and select *Next*.

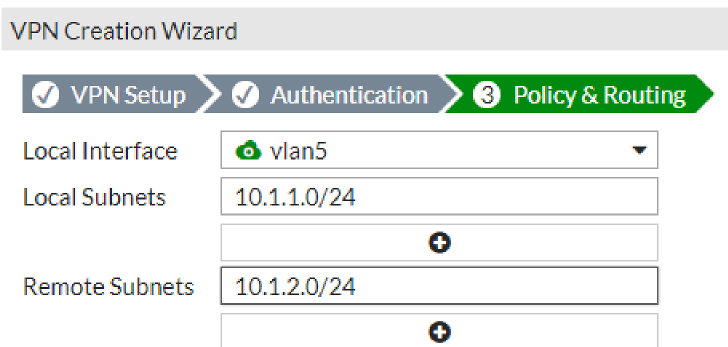


2. In the *Authentication* section, set *IP Address* to Branch's Internet-facing IP (in this example, *172.31.1.65*).
   After you enter the gateway, an interface is assigned as the *Outgoing Interface*.

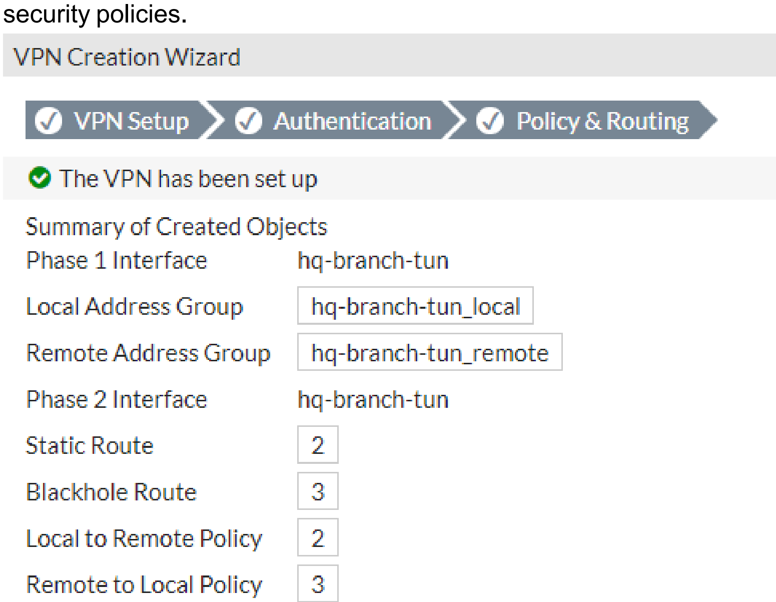
Set a secure *Pre-shared Key*.



3. In the *Policy & Routing* section, set the *Local Interface*. The *Local Subnets* are added automatically. Set *Remote Subnets* to Branch's local subnet (in this example, *10.1.2.0/24*).

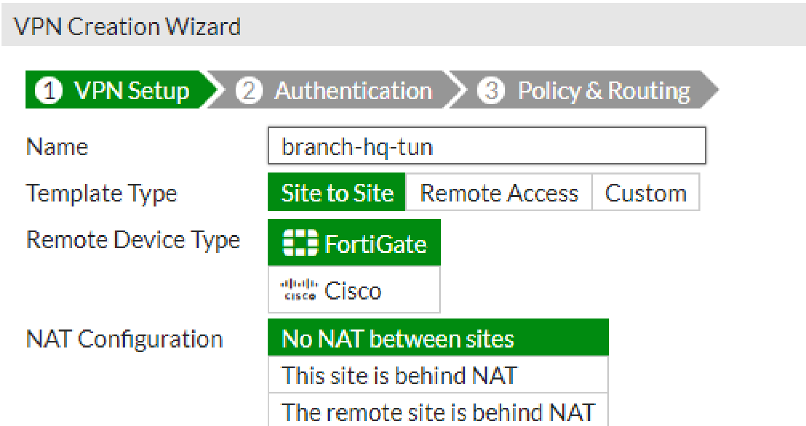


4. Review the configuration summary that shows the firewall addresses, firewall address groups, a static route, and security policies.

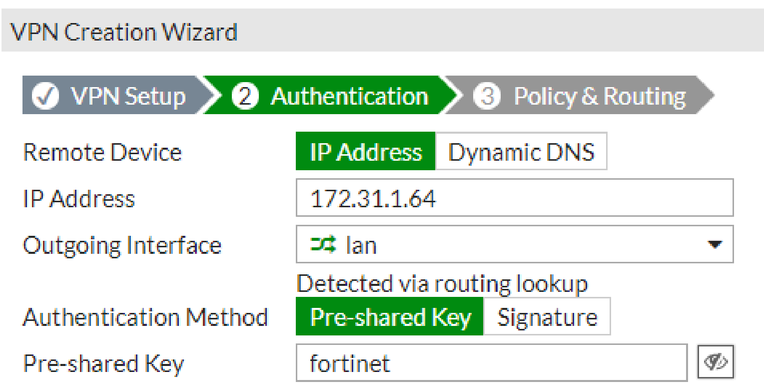


Configuring the Branch IPsec VPN

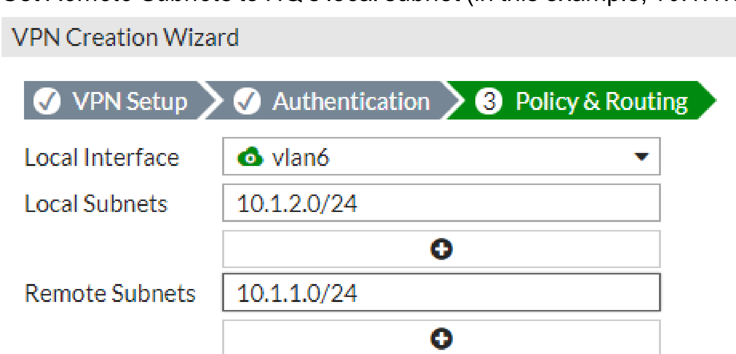
1. On Branch, go to *VPN > IPsec Wizard*.
   Select the *Site to Site* template and select *Next*.



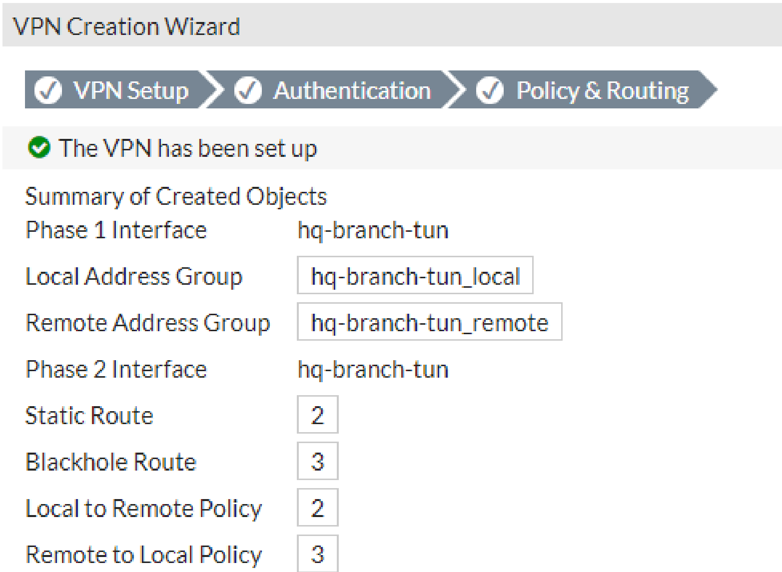
2. In the *Authentication* section, set *IP Address* to HQ's Internet-facing IP (in this example, *172.31.1.64*).
   After you enter the gateway, an interface is assigned as the *Outgoing Interface*.
   Set the same *Pre-shared Key* that was used for HQ's VPN.



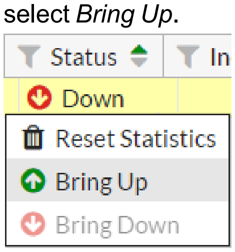
3. In the *Policy & Routing* section, set the *Local Interface*. The *Local Subnets* is added automatically.
   Set *Remote Subnets* to HQ's local subnet (in this example, *10.1.1.0/24*).



4. Review the configuration summary.



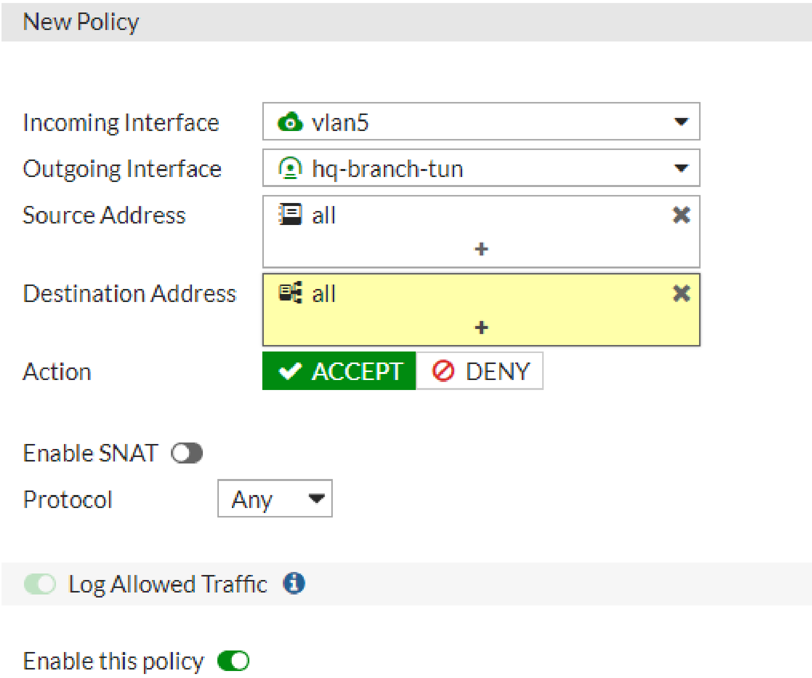
5. On either FortiGate, go to *Monitor > IPsec Monitor* to verify the status of the VPN tunnel. Right-click its *Status* and select *Bring Up*.



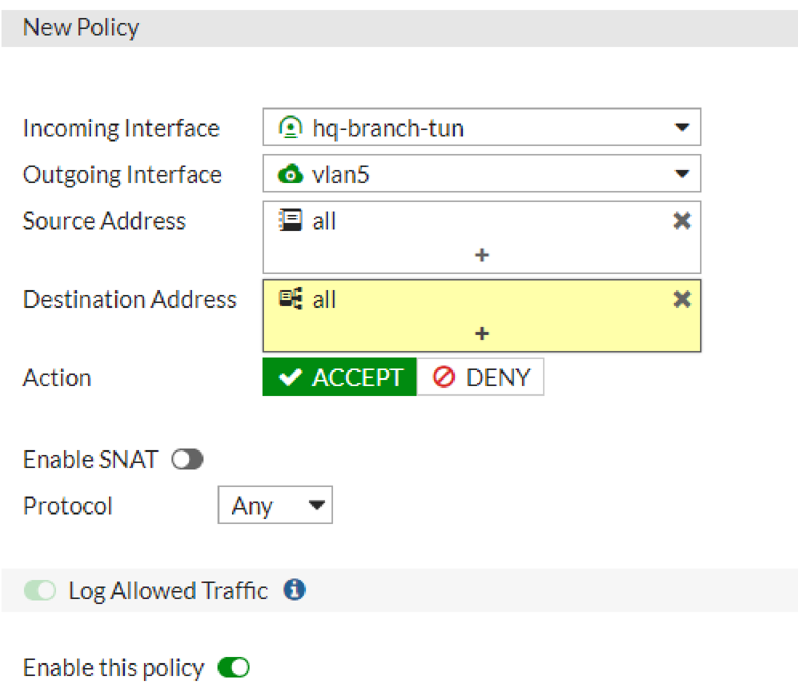
Check that the multicast server behind HQ can ping the client at Branch. To generate traffic to test the connection, ping Branch's internal interface from HQ’s internal network.

Configuring the HQ multicast policy and phase 2 settings

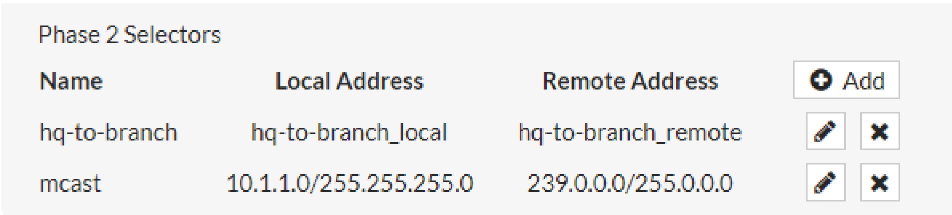
1. On HQ, go to *Policy & Objects* > *Multicast Policy*.
   Create a new policy and allow the multicast traffic from the source interface to the tunnel.



2. Create another multicast policy that allows multicast traffic from the tunnel to the LAN interface of the multicast server.



3. Go to *VPN > IPsec Tunnels* and edit the VPN tunnel.
Select *Convert To Custom Tunnel* and add a *Phase 2 Selector* with 10.1.1.0/24 as the local address and 239.0.0.0/8 as the remote address.

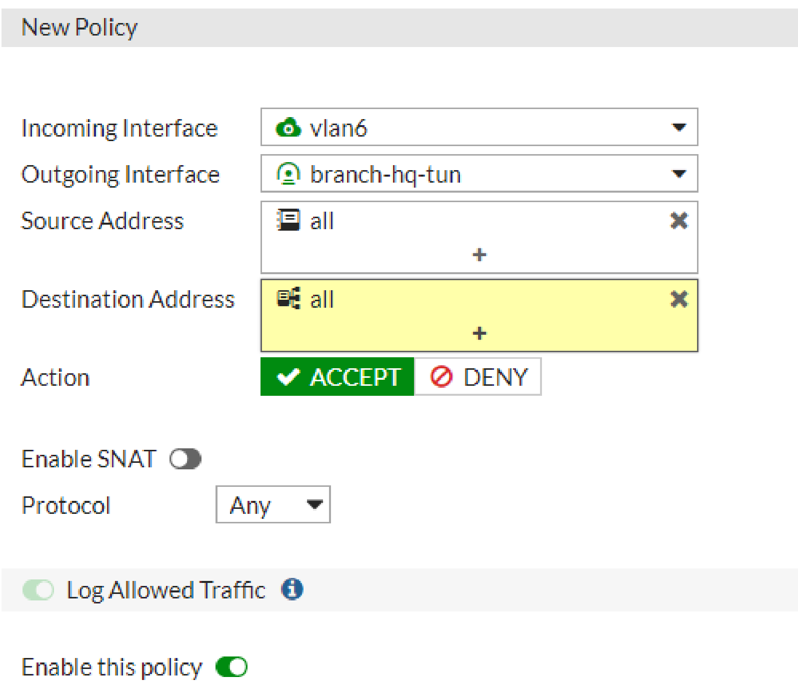


4. Enter the following CLI command to enable multicast forwarding.

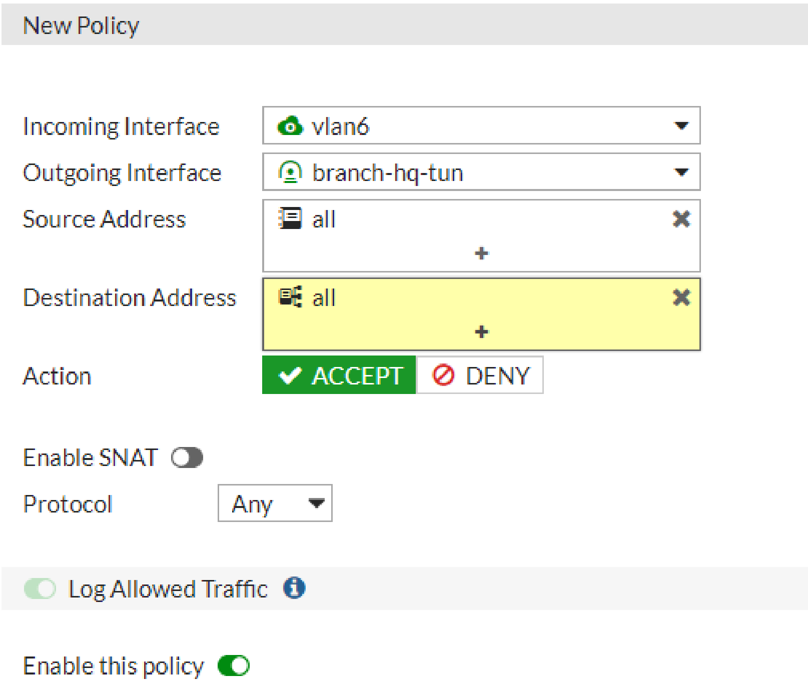
```
config system settings
   set multicast-forward enable
end
```

Configuring the Branch multicast policy and phase 2 settings

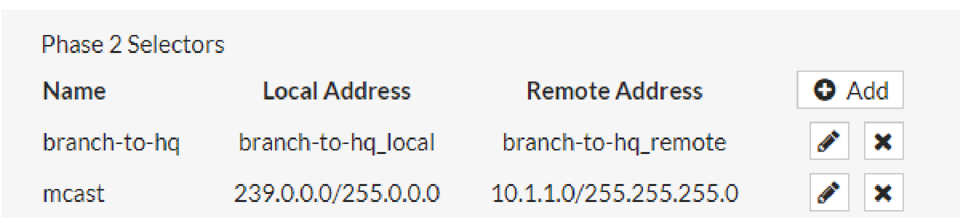
1. On Branch, go to *Policy & Objects > Multicast Policy*.
Create a new policy and allow the multicast traffic from the source interface to the tunnel.



2. Create another multicast policy that allows multicast traffic from the tunnel to the LAN interface of the multicast server.



3. Go to *VPN > IPsec Tunnels* and edit the VPN tunnel.
   Select *Convert To Custom Tunnel* and add a *Phase 2 Selector* with 239.0.0.0/8 as the local address and 10.1.1.0/24 as the remote address.


Phase 2 Selectors

Name	Local Address	Remote Address	Add
branch-to-hq	branch-to-hq_local	branch-to-hq_remote	
mcast	239.0.0.0/255.0.0.0	10.1.1.0/255.255.255.0	

4. Enter the following command to enable multicast forwarding.

```
config system settings
   set multicast-forward enable
end
```

Results

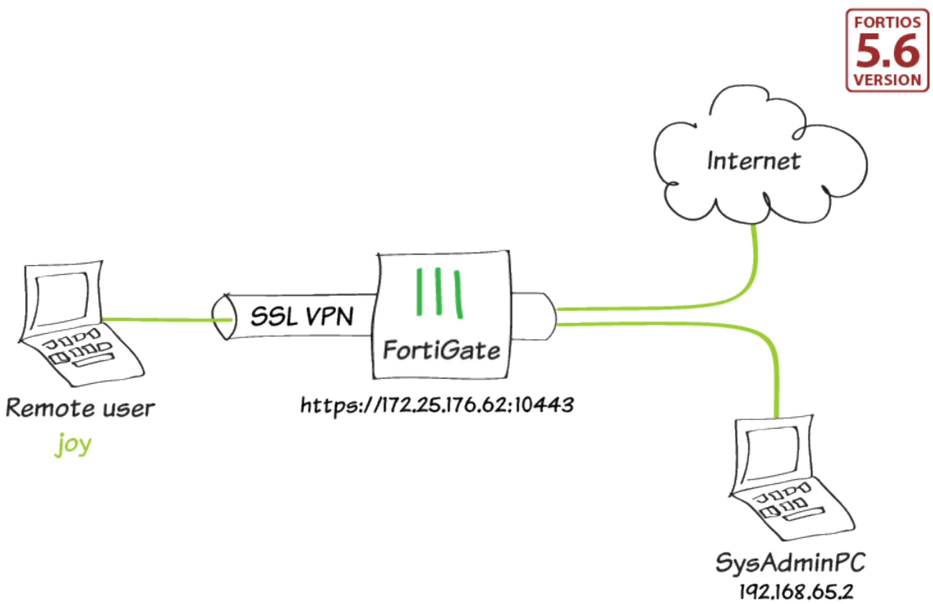
Multicast traffic now flows from the multicast server to the client. Start the multicast stream and make note of the address. In this configuration, all multicast traffic that matches 239.0.0.0/8 flows from HQ to Branch.

Multicast traffic flow can be verified by the `diagnose sys mcast-session list` command on Branch.

In this example, the multicast group from the HQ server is transmitting on multicast group address 239.1.1.100:1234. The multicast receiver application on the Branch host can now receive this multicast traffic.

```
lab-fgt-81e-02 # diag sys mcast-session list

session info: id=1378025 vf=0 proto=2 10.1.2.100.0->224.0.0.22.0
used=2 path=1 duration=3326 expire=153 indev=39 pkts=113 bytes=6240
state=00000088:offloadable ofld-check-fail
session-npu-info: ipid/vlifid=0/0 vlanid/vtag_in=0/0 in_npuid=0 tae_index=0 qid=0 fwd_map=0x00000000
path: log policy=1, outdev=42

session info: id=1378969 vf=0 proto=17 10.1.2.100.63735->224.0.0.253.3544
used=2 path=1 duration=160 expire=19 indev=39 pkts=1 bytes=68
state=00000008:offloadable
session-npu-info: ipid/vlifid=0/0 vlanid/vtag_in=0/0 in_npuid=0 tae_index=0 qid=0 fwd_map=0x00000000
path: log policy=1, outdev=42

session info: id=1378994 vf=0 proto=17 10.1.1.100.54391->239.1.1.100.1234
used=2 path=1 duration=39 expire=178 indev=42 pkts=1 bytes=1344
state=00000018:offloadable npu-info
session-npu-info: ipid/vlifid=249/249 vlanid/vtag_in=6/6 in_npuid=1 tae_index=3188 qid=1 fwd_map=0x00000000
path: log offloaded policy=2, outdev=39
act-npu-info:  ipid/vlifid=249/249 vlanid/vtag_in=6/6 in_npu_id=1, out_npuid=1 epid=82 fwd=0
Total 3 sessions
```

SSL VPN using web and tunnel mode



In this example, you allow remote users to access the corporate network using an SSL VPN, connecting either by web mode using a web browser or tunnel mode using FortiClient.

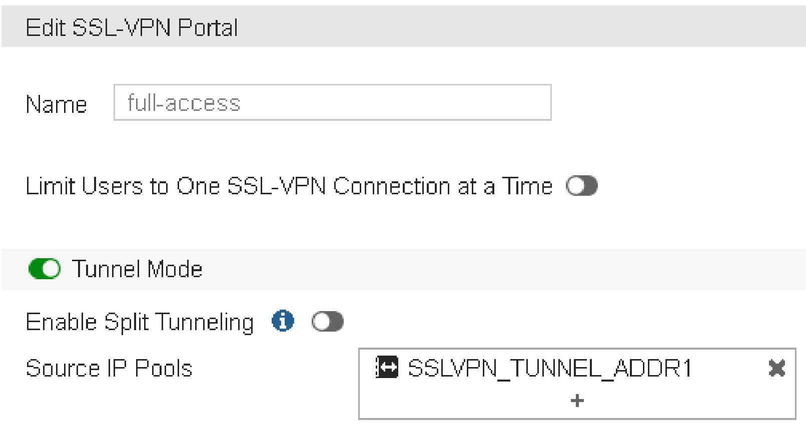
Web mode allows users to access network resources, such as the AdminPC used in this example.

For users connecting via tunnel mode, traffic to the Internet also flows through the FortiGate to apply security scanning to this traffic. In the connecting phase, the FortiGate also verifies that the remote user’s antivirus software is installed and up-to-date.

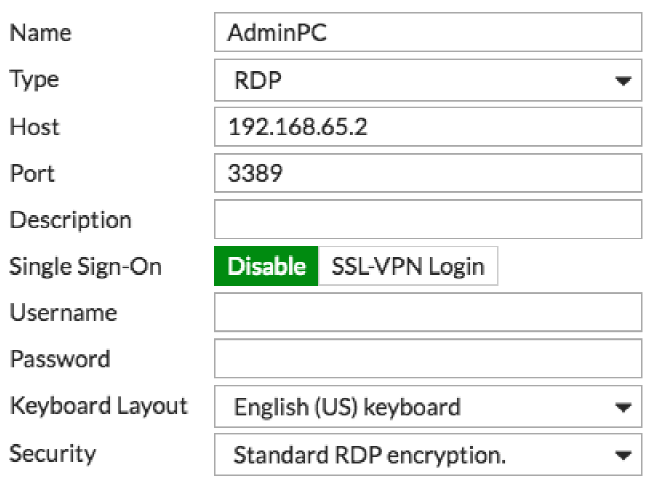
This example allows access for members of the *Employees* user group.

Editing the SSL VPN portal

1. Go to *VPN > SSL-VPN Portals* and edit the *full-access* SSL VPN portal that allows the use of tunnel mode and web mode.
2. Under *Tunnel Mode*, disable *Enable Split Tunneling* for both IPv4 and IPv6 traffic so that all Internet traffic goes through the FortiGate.
3. Set *Source IP Pools* to use the default IP range *SSLVPN_TUNNEL_ADDR1*.



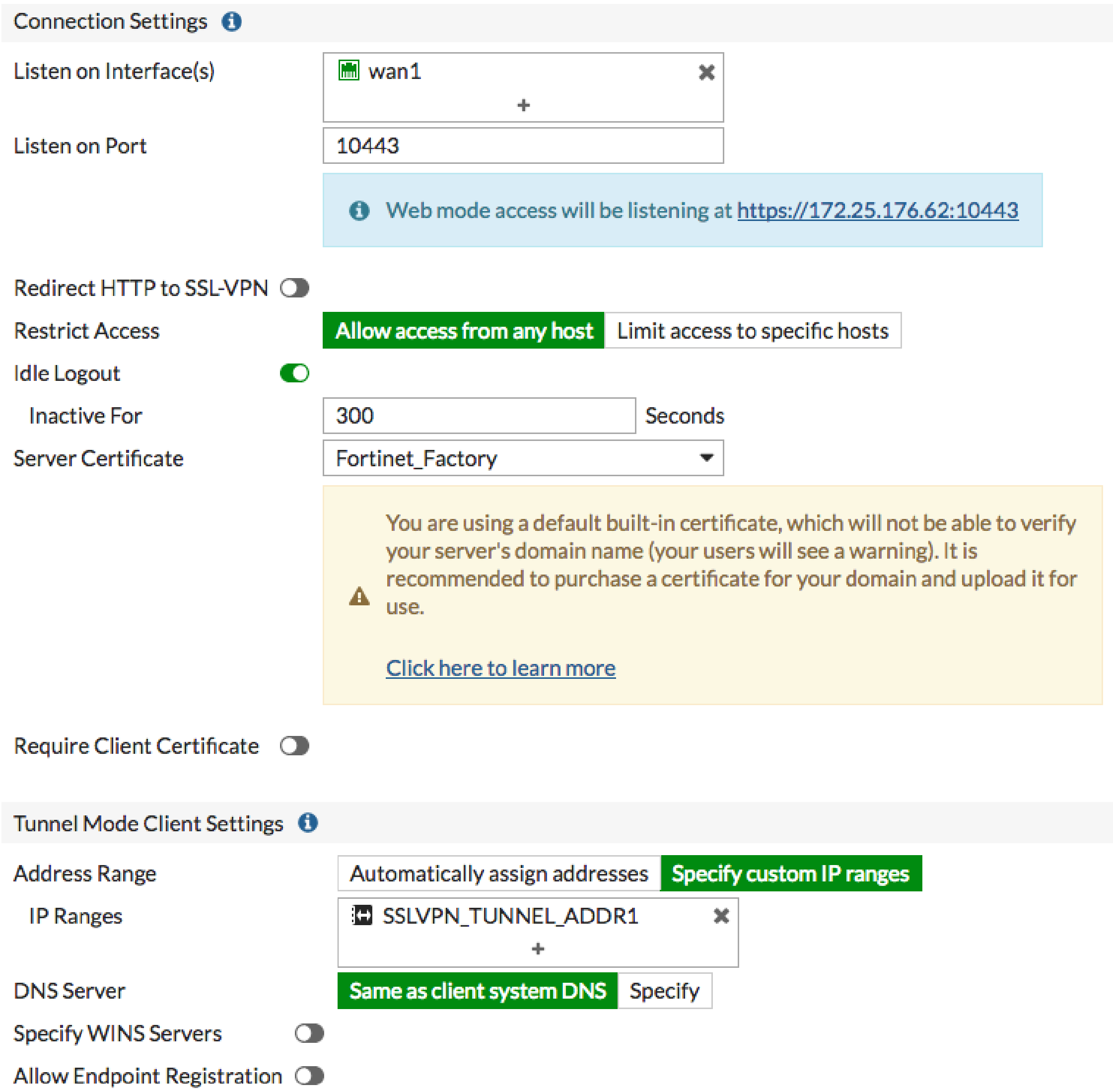
4. Under *Enable Web Mode*, create *Predefined Bookmarks* for any internal resources that SSL VPN users need to access.
   In this example, the bookmark allows the remote user RDP access to a computer on the internal network.



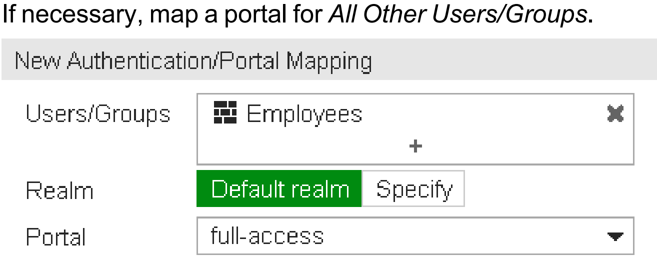
Configuring the SSL VPN tunnel

1. Go to *VPN > SSL-VPN Settings*.
2. Set *Listen on Interface(s)* to *wan1*.
   Set *Listen on Port* to *10443* to avoid port conflicts.
   Set *Restrict Access* to *Allow access from any host*.
   In this example, *Server Certificate* uses the *Fortinet_Factory* certificate. To ensure that traffic is secure, use your own CA-signed certificate. .

Under *Tunnel Mode Client Settings*, set *IP Ranges* to use the default IP range *SSLVPN_TUNNEL_ADDR1*.

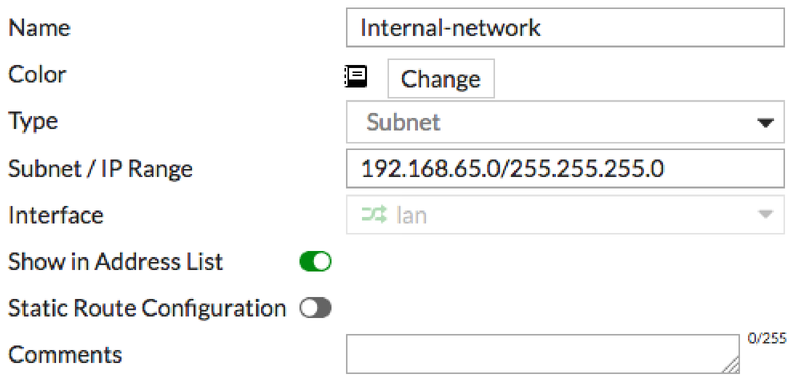


3. Under *Authentication/Portal Mapping*, select *Create New*.
   Add the *Employees* user group and map it to the *full-access Portal*.
   If necessary, map a portal for *All Other Users/Groups*.

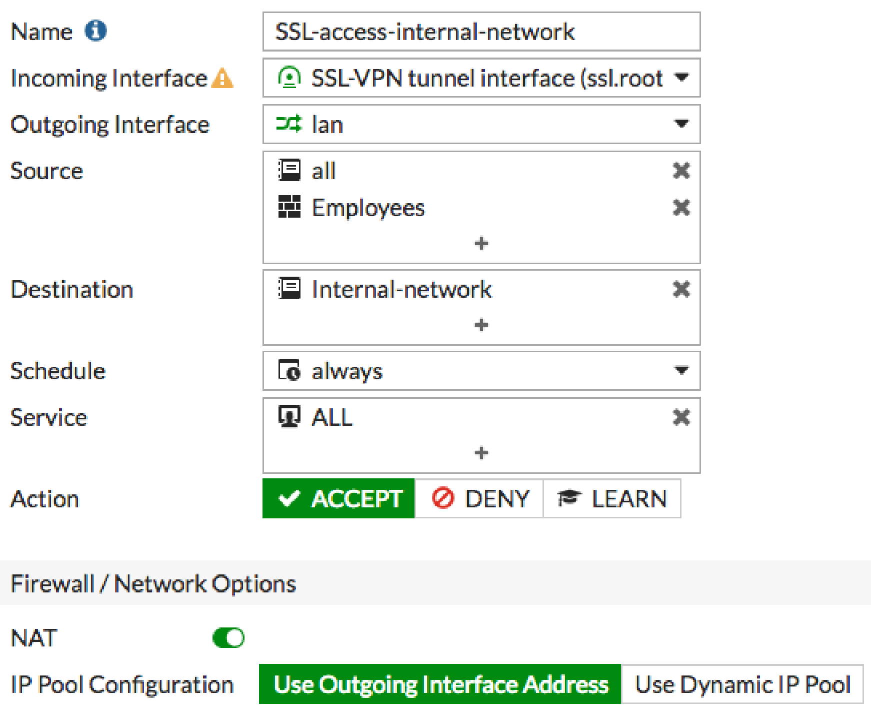


Adding security policies

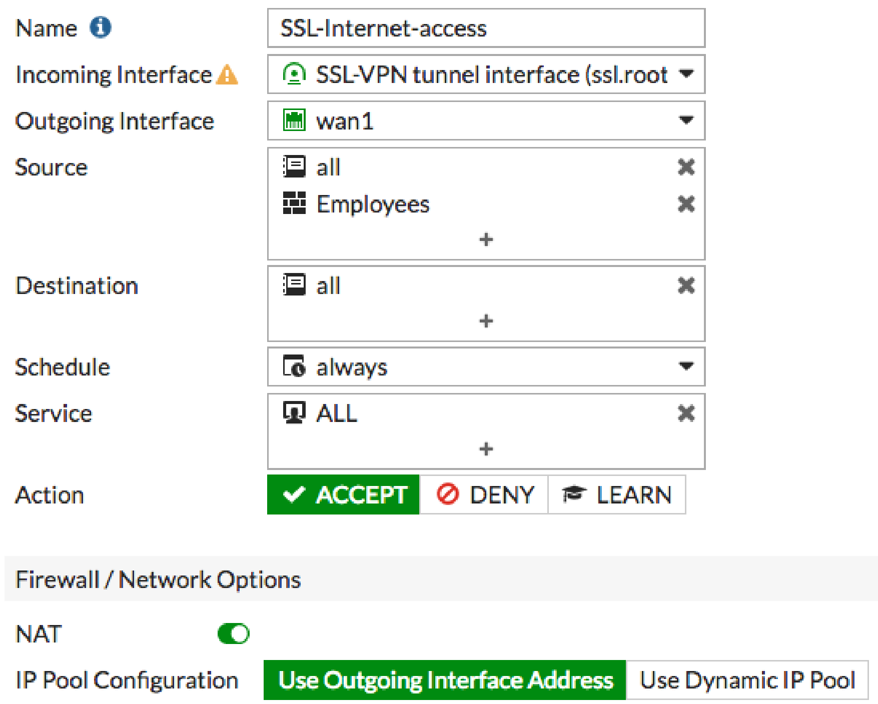
1. Go to *Policy & Objects* > *Addresses* and create a new address for the local network.
2. Set *Type* to *Subnet*.
   Set *Subnet/IP Range* to the local subnet.
   Set *Interface* to *lan*.



3. Go to *Policy & Objects* > *IPv4 Policy* to create a security policy to allowing access to the internal network through the VPN tunnel interface.
   Set *Incoming Interface* to *ssl.root*.
   Set *Outgoing Interface* to *lan*.
   Set *Source* to *all* and to the *Employees* user group.
   Set *Destination* to the local network address.
   Set *Service* to *ALL*.
   Enable *NAT*.



4. Add a second security policy allowing SSL VPN access to the Internet.
   If you allow split tunneling, this policy is not required.
5. For this policy, set *Incoming Interface* to *ssl.root*.
   Set *Outgoing Interface* to *wan1*.
   Set *Source* to *all* and to the *Employees* user group.



Verifying remote user OS and software

To verify that remote users are using up-to-date devices to connect to your network, you can configure a host check for Windows operating systems and software.

Only FortiOS 6.0 supports OS host checking for both Mac OS and Windows.

You can configure an OS host check for specific OS versions, including the following options: allow the device to connect, block the device, or check that the OS is up-to-date. The default action for all OS versions is *allow*.

The software host can verify whether the device has AntiVirus software recognized by Windows Security Center, firewall software recognized by Windows Security Center, both, or a custom setting.

Configure both checks using the CLI:

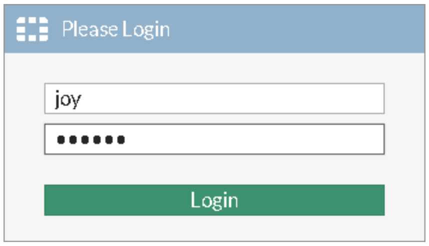
```
config vpn ssl web portal
   edit full-access
      set os-check enable
         config os-check-list {windows-7 | windows-8 | windows-8.1 | windows-10 | windows-
               2000 | windows-vista | windows-xp}
            set action {deny | allow | check-up-to-date}
         end
      set host-check {none | av | fw | av-fw | custom}
   end
```

Results

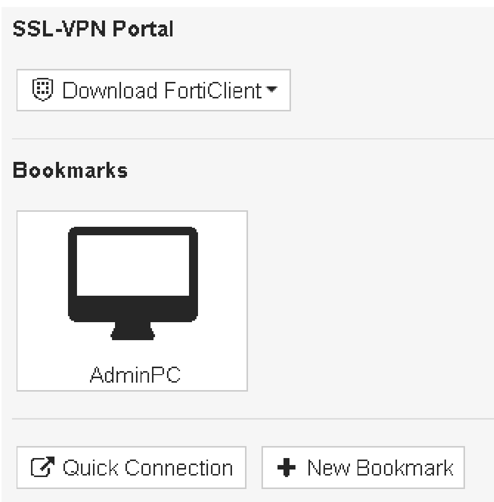
The steps for connecting to the SSL VPN are different depending on whether you use a web browser or FortiClient.

Web browsers

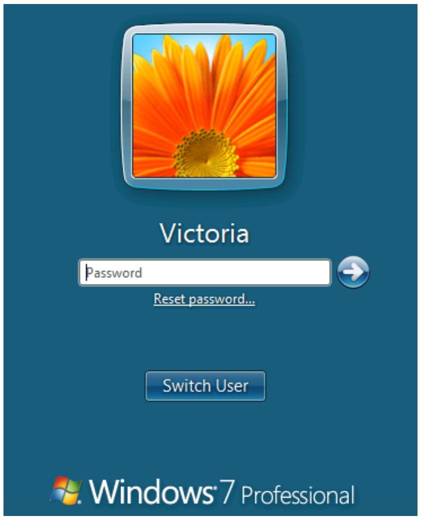
1. Use a supported Internet browser to connect to the SSL VPN web portal using the remote gateway configured in the SSL VPN settings (in this example, *https://172.25.176.62:10443*).
2. Log in to the SSL VPN.



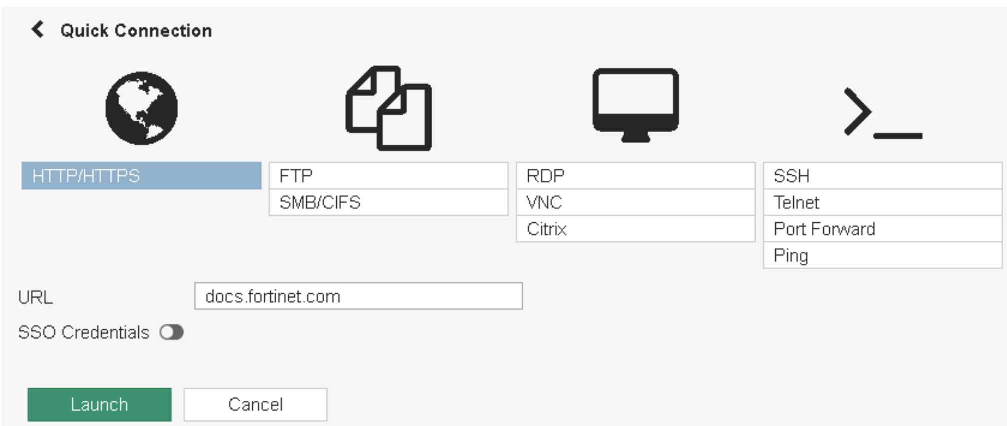
3. After authenticating, you can access the *SSL-VPN Portal*. From this portal, you can launch or download FortiClient, access *Bookmarks*, or connect to other resources using the *Quick Connection* tool.



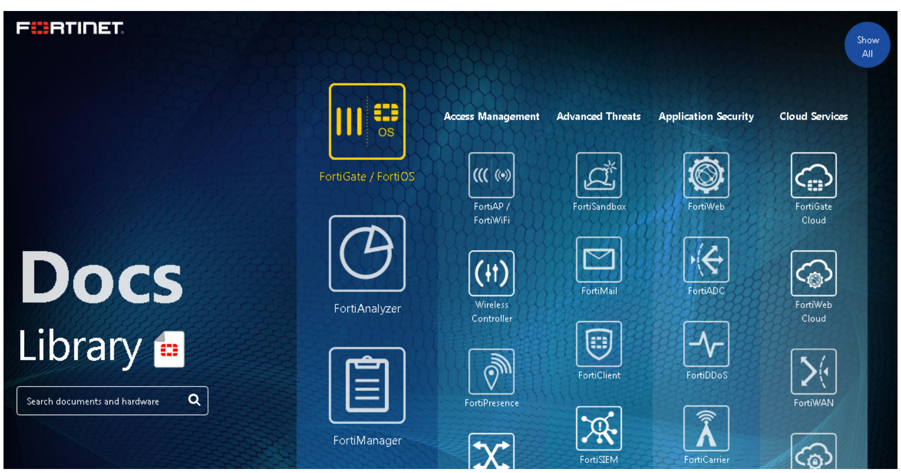
In this example, select the bookmark to connect to the AdminPC.



4. To connect to the Internet, select *Quick Connection*, select *HTTP/HTTPS*, then enter the *URL* and select *Launch*.



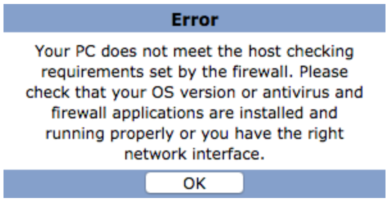
The website loads.



5. To view the list of users currently connected to the SSL VPN, go to *Monitor* > *SSL-VPN Monitor*.
The user is connected to the VPN.

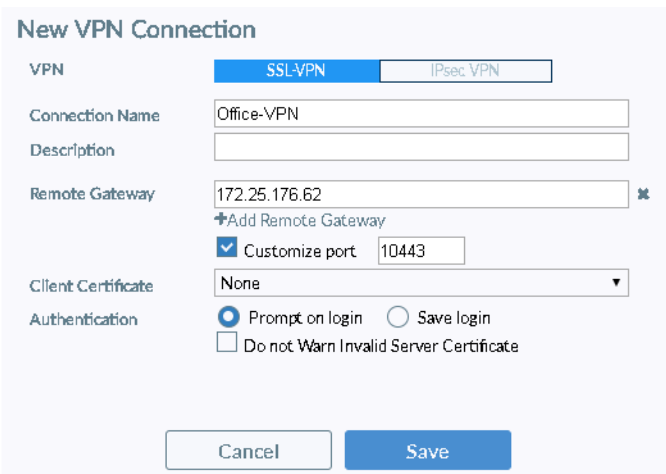
Username	Last Login	Remote Host	Active Connections
joy	Tue May 28 10:36:40 2019	172.25.181.138	

6. If a remote device fails the OS or host check, a warning message appears after authentication instead of the portal.



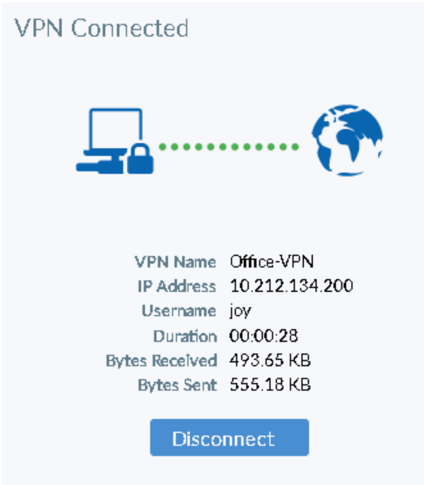
FortiClient

1. If you have not already done so, download FortiClient from www.forticlient.com.
2. Open the FortiClient console and go to *Remote Access*. Add a new connection.
   Set *VPN* to *SSL VPN*.
   Set *Remote Gateway* to the IP of the listening FortiGate interface (in this example, *172.25.176.62*).
   Select *Customize Port* and set it to *10443*.
   Select *Save*.



3. Log in to the SSL VPN.

You can connect to the VPN tunnel.



4. To view the list of users currently connected to the SSL VPN, go to *Monitor > SSL-VPN Monitor*. The user is connected to the VPN.

Username	Last Login	Remote Host	Active Connections
joy	Tue May 28 10:46:29 2019	172.25.181.138	Tunnel: 10.212.134.200

Configuring ADVPN

Auto Discovery VPN (ADVPN) is an IPsec technology based on an IETF RFC draft (Auto Discovery VPN Protocol). ADVPN allows a traditional hub and spoke VPN's spokes to establish dynamic, on-demand direct tunnels between each other. This avoids routing through the topology's hub device. ADVPN requires using dynamic routing. FortiOS 5.6 supports both BGP and RIP. This example focuses on using BGP and its route-reflector mechanism as the dynamic routing solution to use with ADVPN.

ADVPN's main advantage is that it provides the full meshing capabilities to a standard hub and spoke topology. This reduces the provisioning effort required for full spoke-to-spoke, low-delay reachability, and addressing the scalability issues associated with large, fully meshed VPN networks.

BGP (and specifically iBGP) is a good fit for ADVPN as its route reflector mechanism resides on the VPN hub device and mirrors routing information from each spoke peer to each other. Furthermore, dynamic group peers result in near zero-touch hub provisioning when a new spoke is introduced in the topology.

While the static configuration involves both spoke FortiGate units to connect to the hub FortiGate, Spoke A can establish a dynamic on-demand shortcut IPsec tunnel to Spoke B (and vice versa) if a host behind either spoke attempts to reach a host behind the other spoke. After configuration, the verification step shows reachability from 192.168.2.1 (Spoke A) to 192.168.3.1 (Spoke B) over the dynamically created shortcut link.

This example uses CLI since BGP and ADVPN are best done using CLI. This example requires that basic IP and default routing has been completed on the devices.

Configuring the Hub FortiGate

1. Using the CLI, configure phase 1 parameters.
   The auto-discovery commands enable sending and receiving shortcut messages to spokes. The hub is responsible for letting the spokes know that they should establish those tunnels.

   Aggressive mode is not supported for ADVPN in 5.6. It is supported in 6.0.1 and higher.

```
config vpn ipsec phase1-interface
   edit "ADVPN"
      set type dynamic
      set interface "wan1"
      set proposal des-sha1
      set add-route disable
      set net-device enable
      set dhgrp 2
      set auto-discovery-sender enable
      set psksecret fortinet
   next
end
```

2. Configure the phase 2 parameters using a standard phase 2 configuration.

```
config vpn ipsec phase2-interface
   edit "ADVPN-P2"
      set phase1name "ADVPN"
      set proposal des-sha1
   next
end
```

3. Configure the tunnel interface IP.
   ADVPN requires that tunnel IPs be configured on each connecting device. The IP addresses must be unique for each peer. The hub needs to define a bogus remote-IP address (in this example, *10.10.10.254*). This address should not be used in the topology and it is not considered part of the configuration for the hub.

```
config system interface
   edit "ADVPN"
      set vdom "root"
      set ip 10.10.10.1 255.255.255.255
      set type tunnel
      set remote-ip 10.10.10.254
      set interface "wan1"
   next
end
```

4. Configure iBGP and route-reflection.
   iBGP is the overlay protocol for enabling ADVPN communications. We are using an arbitrary private AS number (in this example, `65000`), and configuring a dynamic client group to reduce provisioning requirements.

   This example advertises our LAN network directly (the `config network` command). Another option is to use route redistribution.

```
config router bgp
   set as 65000
   set router-id 10.10.10.1
   config neighbor-group
      edit "ADVPN-PEERS"
```

```
        set remote-as 65000
        set route-reflector-client enable
        set next-hop-self enable
      next
    end
    config neighbor-range
      edit 0
        set prefix 10.10.10.0 255.255.255.0
        set neighbor-group "ADVPN-PEERS"
      next
    end
    config network
      edit 0
        set prefix 192.168.1.0 255.255.255.0
      next
    end
  end
```

5. Configure basic policies to allow traffic to flow between the local network and the ADVPN VPN topology. To allow traffic between spokes in an ADVPN setup, create a policy allowing spoke-to-spoke communications.

```
config firewall policy
  edit 0
    set name "OUT ADVPN"
    set srcintf "lan"
    set dstintf "ADVPN"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set status enable
  next
  edit 0
    set name "IN ADVPN"
    set srcintf "ADVPN"
    set dstintf "lan"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set status enable
  next
  edit 0
    set name "ADVPNtoADVPN"
    set srcintf "ADVPN"
    set dstintf "ADVPN"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set status enable
  next
end
```

Configuring the Spoke FortiGates

This example shows the configuration for only one of the spokes. The parameters that need to change for each spoke are in **red**.

1. Configure phase 1 parameters.
```
config vpn ipsec phase1-interface
   edit "ADVPN"
      set interface "wan1"
      set proposal des-sha1
      set add-route disable
      set dhgrp 2
      set auto-discovery-receiver enable
      set remote-gw 192.0.2.11
      set psksecret fortinet
   next
end
```
2. Configure phase 2 parameters.
```
config vpn ipsec phase2-interface
   edit "ADVPN-P2"
      set phase1name "ADVPN"
      set proposal des-sha1
      set auto-negotiate enable
   next
end
```
3. Configure the tunnel interface IP.
   On the spokes, the remote IP is actually used and points to the IP defined on the hub.
```
config system interface
   edit "ADVPN"
      set vdom "root"
      set ip 10.10.10.2 255.255.255.255
      set allowaccess ping
      set type tunnel
      set remote-ip 10.10.10.1
      set interface "wan1"
   next
end
```
4. Configure iBGP.
   This is a static standard configuration. You can use redistribution instead of explicit route advertisement.
```
config router bgp
   set as 65000
   set router-id 10.10.10.2
   config neighbor
      edit "10.10.10.1"
         set soft-reconfiguration enable
         set remote-as 65000
         set next-hop-self enable
      next
   end
   config network
      edit 0
         set prefix 192.168.2.0 255.255.255.0
      next
   end
end
```

5. Configure a static route for the tunnel IP subnet.
This step is important for the spokes as they need a summary route that identifies all tunnel IP addresses used in the topology to point to the ADVPN interface. This example uses 10.10.10.0/24 (for networks that expect fewer than 255 sites). Plan this IP range carefully as it is hardcoded in the spokes.
```
config router static
   edit 0
      set dst 10.10.10.0 255.255.255.0
      set device "ADVPN"
   next
end
```
6. Configure the following policies.
```
config firewall policy
   edit 0
      set name "OUT ADVPN"
      set srcintf "lan"
      set dstintf "ADVPN"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set status enable
   next
   edit 0
      set name "IN ADVPN"
      set srcintf "ADVPN"
      set dstintf "lan"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
      set status enable
   next
end
```

Results

Check the behavior of the configuration using CLI commands from Spoke A.

`get router info routing-table bgp` displays the learned routes from the topology. The recursive routing is a result of the spoke's required static route. In this case, there has not been any traffic between our local subnet (*192.168.2.0/24*) and the other spoke's subnet as the routes are both going through the hub.

```
B 192.168.1.0/24 [200/0] via 10.0.0.1, ADVPN, 22:30:21
B 192.168.3.0/24 [200/0] via 10.0.0.3 (recursive via 10.0.0.1), 22:30:21
```

When you initiate a ping between both spokes, you see a different display of routing information – routing now goes through a newly established dynamic tunnel directly through the remote spoke rather than through the hub. The ping hiccup is the tunnel rerouting through a newly negotiated tunnel to the other spoke.

The routing information now displays the remote subnet as being available through the spoke directly, through interface ADVPN_0, a dynamically instantiated interface going to that spoke.

```
FG # execute ping-options source 192.168.2.1
```

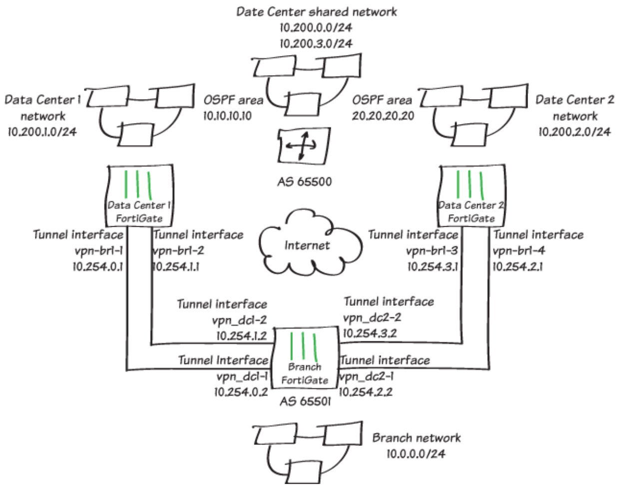
```
FG # execute ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1): 56 data bytes
64 bytes from 192.168.3.1: icmp_seq=0 ttl=254 time=38.3 ms
64 bytes from 192.168.3.1: icmp_seq=1 ttl=254 time=32.6 ms
Warning: Got ICMP 3 (Destination Unreachable)
64 bytes from 192.168.3.1: icmp_seq=2 ttl=255 time=43.0 ms
64 bytes from 192.168.3.1: icmp_seq=3 ttl=255 time=31.7 ms
64 bytes from 192.168.3.1: icmp_seq=4 ttl=255 time=31.2 ms

--- 192.168.3.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 31.2/35.3/43.0 ms

FG # get router info routing-table bgp

B 192.168.1.0/24 [200/0] via 10.0.0.1, ADVPN, 22:34:13
B 192.168.3.0/24 [200/0] via 10.0.0.3, ADVPN_0, 00:02:28
```

The `diagnose vpn tunnel list` command gives more information. This example highlights aspects in the output which convey data specific to ADVPN, in this case, the auto-discovery flag and the child-parent relationship of new instantiated dynamic tunnel interfaces.

```
FG # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=ADVPN_0 ver=1 serial=a 10.1.1.2:0->10.1.1.3:0
bound_if=6 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/0
parent=ADVPN index=0
proxyid_num=1 child_num=0 refcnt=19 ilast=3 olast=604 auto-discovery=2
stat: rxp=7 txp=7 rxb=1064 txb=588
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=ADVPN-P2 proto=0 sa=1 ref=2 serial=1 auto-negotiate adr
   src: 0:0.0.0.0/0.0.0.0:0
   dst: 0:0.0.0.0/0.0.0.0:0
   SA: ref=3 options=2f type=00 soft=0 mtu=1438 expire=42680/0B replaywin=2048 seqno=8 esn=0
   life: type=01 bytes=0/0 timeout=43152/43200
   dec: spi=9a487db3 esp=aes key=16 55e53d9fbc8dbeaa6df1032fbc80c4f6
      ah=sha1 key=20 a1470452c6a444f26a070add087f0d970c18e3a7
   enc: spi=3c37fea7 esp=aes key=16 8fd62a6745a9ba4fda062d4504b76851
      ah=sha1 key=20 44c606f1ef1bf5739ba62f6572031aa956974d0a
   dec:pkts/bytes=7/588, enc:pkts/bytes=7/1064
------------------------------------------------------
name=ADVPN ver=1 serial=9 10.1.1.2:0->10.1.1.1:0
bound_if=6 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=1 refcnt=22 ilast=8 olast=8 auto-discovery=2
stat: rxp=3120 txp=3120 rxb=399536 txb=191970
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=12
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=ADVPN-P2 proto=0 sa=1 ref=2 serial=1 auto-negotiate adr
   src: 0:0.0.0.0/0.0.0.0:0
   dst: 0:0.0.0.0/0.0.0.0:0
   SA: ref=3 options=2f type=00 soft=0 mtu=1438 expire=4833/0B replaywin=2048 seqno=5ba
        esn=0
   life: type=01 bytes=0/0 timeout=43148/43200
   dec: spi=9a487db2 esp=aes key=16 4f70d27edad656cfcacbae61b23d4b11
      ah=sha1 key=20 b19ea87c90dd92d1cab58cbf24ae8fe12ee927cb
   enc: spi=b3dde355 esp=aes key=16 efbb4440df75018610b4ba8f5756167d
```

```
      ah=sha1 key=20 81cc9cee3bee1c2dba0eb1e7ac66e9d34b67bde9
   dec:pkts/bytes=1465/90152, enc:pkts/bytes=1465/187560
------------------------------------------------------------
```

Client-Side SD-WAN with IPsec VPN Deployment Scenario (Expert)



This advanced deployment scenario provides a high-level picture of how to combine SD-WAN, IPsec VPN, and BGP routing to provide a branch office with redundant connections to two remote data centers and the networks behind them. Using this deployment scenario allows you to replace private or MPLS connections to data centers with lower-cost encrypted SD-WAN connections over the Internet.

This scenario is intended for network engineers who are familiar with the FortiGate platform and are looking for an example FortiOS 5.6 SD-WAN configuration. It does not include all of the required configuration steps but the intention is to provide the information you need to implement SD-WAN technology.

Configuring the data center FortiGates

The configuration described here must be set up on Data Center 1 FortiGate and Data Center 2 FortiGate. The following steps show how to configure Data Center 1 FortiGate (as shown in the diagram). You can repeat this configuration for Data Center 2 FortiGate, substituting the proper IP addresses and interface names.

This configuration has the following objectives:

- Zero touch IPsec VPN provisioning of new branches
- Point-to-multipoint IPsec VPN
- Central management of data center access from each data center firewall
- Dynamic peering to share routing information between each branch and the data center

Each data center configuration includes dynamic (or dial-up) IPsec VPN, BGP, firewall policies to control access, and a blackhole route for each branch office.

Creating the data center side of the IPsec VPN

To facilitate zero touch provisioning of new spokes to establish VPNs on each data center FortiGate, this example uses dial-up VPNs with auto-discovery-sender enabled in the ADVPN configuration.

Also, add-route is disabled to support multiple dynamic tunnels to the same host advertising the same network. This dynamic discovery of the network is facilitated by the BGP configuration.

Wildcard security associations are used for phase 2 since BGP routes determine whether traffic is sent over the IPSec VPN tunnel. In this example, IPsec VPN is added to each FortiGate interface connected to the Internet.

The Phase 1 configuration includes:

- A dynamic VPN tunnel name that is 11 characters or less.
- Setting `type` to `dynamic`
- Setting `interface` to the Internet connected interface
- Setting `peertype` to `any`
- Setting `add-route` to `disable`
- Setting `auto-discovery-sender` to `enable`

```
config vpn ipsec phase1-interface
   edit "vpn-brl-1"
      set type dynamic
      set interface "vlan-3510"
      set peertype any
      set proposal aes256-sha256
      set add-route disable
      set dhgrp 5
      set auto-discover-sender enable
      set psksecret <password>
   next
   edit "vpn-brl-2"
      set type dynamic
      set interface "vlan-3511"
      set peertype any
      set proposal aes256-sha256
      set dhgrp 5
      set auto-discovery-sender enable
      set psksecret <password>
   end
```

The Phase 2 configuration includes:

- Setting `phase1name` to the name of the phase 1 configuration
- Disabling `pfs` and `replay`

```
   config vpn ipsec phase2-interface
      edit "vpn-brl-1_ps"
         set phase1name "vpn-isp-a"
         set proposal aes256-sha256
         set pfs disable
         set replay disable
      next
      edit "vpn-br1-2_p2"
         set phase1name "vpn-isp-b"
         set proposal aes256-sha256
```

```
      set pfs disable
      set replay disable
   end
```

Adding addresses to the tunnel interfaces

The BGP configuration requires IP addresses assigned to the IPsec VPN tunnel interfaces that BGP peers over. The ADVPN feature enabled by set auto-discovery-sender enable allows FortiOS to establish a point-to-multipoint connection to each FortiGate.

The IPsec VPN tunnel interface `ip` is set to the IP address that the tunnels will connect to, and `remote-ip` is set to the highest unused IP address that is part of your tunnel network. This adds two host-based routes to the FortiGate's routing table that point directly back to the branch FortiGate.

The IPsec VPN interface configuration includes:

- Setting the `ip` to `<vpn interface ip> 255.255.255.255`
- Setting `type` to `tunnel`
- Setting `remote-ip` to the highest unused IP address in the VPN subnet
- Setting `allowaccess` to `ping` to allow for confirmation that a point-to-point tunnel has been established between the data center FortiGate and the branch FortiGate.

```
config system interface
   edit "vpn-br1-1"
      set vdom "root"
      set ip 10.254.0.1 255.255.255.255
      set allowaccess ping
      set type tunnel
      set remote-ip 10.254.0.254/24
      set interface "port1"
   next
   edit "vpn-br1-2"
      set vdom
      "root"
      set ip 10.254.1.1. 255.255.255.255.255
      set allowaccess ping
      set type tunnel
      set remote-ip 10.254.1.254/24
      set interface "port2"
   end
```

Implementing route discovery with BGP

Network route discovery is facilitated by BGP and EBGP, which prevent the redistribution of routes learned that are contained in the same autonomous system number as the host. Also, EBGP influences route selection on the branches because of AS-Path prepending.

Enable `ebgp-multipath` to allow the FortiGate to dynamically discover multiple paths for networks advertised at branches.

Configure `neighbor-range` and `neighbor-group` to allow peering relationships to be established without defining each individual peer. The branch IPsec VPN tunnel interface addresses must be in the BGP peer range.

The BGP configuration includes:

- Enabling `ebgp-multipath`
- Enabling `soft-reconfiguration`, `link-down-failover`, and `ebgp-enforce-multihop` for each BGP peer in the neighbor group
- Adding the branch `remote-as` (which is 65501) to each peer configuration
- Setting the `prefix` for the neighbor range to the network matching the BGP peers
- Configuring a `network` with the prefix of the network advertised into BGP

To facilitate the fastest route failovers, the following timers are set to their lowest values:

- `scan-time`
- `advertisement-interval`
- `keep-alive timer`
- `holdtime-timer`

```
config router bgp
   set as 65500
   set router-id 10.10.0.1
   set ebgp-multipath enable
   set scan-time 5
   set graceful-restart enable
   config neighbor-group
      edit "branch-peeers-1"
         set advertisement-interval 1
         set link-down-failover enable
         set soft-reconfiguritation enable
         set remote-as 65501
         set keep-alive-timer 1
         set holdtime-timer 3
         set ebgp-enforce-multihop enable
      next
      edit "branch-peers-2"
         set advertisment-inteval 1
         set link-downfailover enable
         set remote-as 65501
         set keep-alive-timer 1
         set holdtime-timer 3
         set ebgp-enforce-multihop enable
      next
   end
   config neighbor-range
      edit 1
         set prefix 10.254.0.0 255.255.255.0
         set neighbor-group "branch-peers-1"
      next
      edit 2
         set prefix 10.254.1.0 255.255.255.0
         set neighbor-group "branch-peers-2"
      next
   end
   config network
      edit 1
         set prefix 10.200.1.0 255.255.255.0
      next
      edit 2
         set prefix 10.200.0.0 255.255.255.0
```

```
        next
        edit 3
            set prefix 10.200.3.0 255.255.255.0
        next
    end
end
```

Controlling access to data center networks

Create firewall policies to allow users on the branch office networks to access the data center networks (behind the FortiGate). Security profiles can be added to these firewall policies to inspect of layer 7 traffic.

Include a policy on the data center FortiGate to allow a branch FortiGate to check the health of the data center FortiGate by allowing the branch FortiGate to ping the data center FortiGate IPsec VPN interface:

- **Source interface**: IPsec VPN interface
- **Destination interface**: Internal interface
- **Source Address**: Tunnel IP addresses of branch
- **Destination Address**: Data Center 1 FortiGate Internal interface
- **Action**: Accept
- **Schedule**: Always
- **Service**: ICMP

Policies to allow traffic from branch networks to reach data center networks should have the following firewall settings:

- **Source interface**: IPsec VPN interface
- **Destination interface**: Internal interface
- **Source Address**: Branch networks
- **Destination Address**: Date center networks
- **Action**: Accept
- **Schedule**: Always (or define a more restrictive schedule)
- **Service**: Allowed Service(s)

Pointing to branch offices with black hole routes

It is a best practice to create black hole routes with destinations set to each branch network. If the FortiGate temporarily loses connectivity with a branch network, traffic destined to that network is sent to the black hole until connectivity has been restored.

Each Black hole route includes:

- Setting `dst` to the branch network IP address
- Setting the `distance` to 254

```
config router static
    edit 1
        set dst 10.0.0.0/14
        set distance 254
        set blackhole enable
    next
end
```

Configuring Branch FortiGate

The following steps describe how to use the SD-WAN feature to set up the branch FortiGate with redundant connections to the two data centers. This configuration includes the following:

- Client-side SD-WAN (intelligent load balancing based on link quality)
- A configuration template for quick deployment of branch FortiGates
- Split tunneling for Internet access from the branch office networks

The branch FortiGate configuration includes IPsec VPN, BGP, SD-WAN load balancing, and firewall policies to control access.

Creating the branch side of the IPsec VPN

The IPsec VPN configuration is similar to a normal site-to-site VPN configuration. Wildcard security associations are used for phase 2 since BGP routes determine whether traffic is sent over the IPSec VPN tunnel.

1. Create two **Phase 1** configurations, one for each data center. These configurations include:
   - Setting `peertype` to `any`
   - Setting `remote-gw` to the IP address of the data center.

```
config vpn ipsec phase1-interface
  edit "vpn_dc1-1"
    set interface "vlan-3000"
    set peertype any
    set proposal aes256-sha256
    set dhgrp 5
    set remote-gw 172.20.10.10
    set psksecret <password>
  next
  edit "vpn_dc1-2"
    set interface "vlan-3001"
    set peertype any
    set proposal aes256-sha256
    set dhgrp 5
    set remote-gw 172.20.11.10
    set psksecret <password>
  next
end
```

2. Create two **Phase 2** configurations, one for each data center. These configurations include:
   - Disabling `pfs` and `replay`
   - Enabling `auto-negotiate` to ensure VPN establishment

```
config vpn ipsec phase2-interface
  edit "vpn_dc1-1_p2"
    set phase1name "vpn_dc1-1"
    set proposal aes256-sha256
    set pfs disable
    set replay disable
    set auto-negotiate enable
  next
  edit "vpn_dc1-2_p2"
    set phase1name "vpn_dc1-2"
    set proposal aes256-sha256
    set pfs disable
    set replay disable
```

```
        set auto-negotiate enable
      next
    end
```

Adding IP addresses to the tunnel interfaces

To establish the point-to-multipoint IPsec VPN between the branch and the data center, the tunnel interfaces must include the following IP addresses.

The **IPsec VPN Interface** configuration includes:

- Setting `ip` to the local IP address of the VPN interface
- Setting `remote-ip` to the data center FortiGate's IPsec VPN interface IP address

```
config system interface
  edit "vpn_dc1-1"
    set vdom "root"
    set ip 10.254.0.2 255.255.255.255
    set allowaccess ping
    set type tunnel
    set remote-ip 10.254.0.1
    set interface "wan1"
  next
  edit "vpn_dc1-2"
    set vdom "root"
    set ip 10.254.1.2 255.255.255.255
    set allowaccess ping
    set type tunnel
    set remote-ip 10.254.1.1
    set interface "wan2"
  next
end
```

Implementing route discovery with BGP

BGP allows the branch and data center FortiGates to dynamically discover routes from each other. To make this happen add the data center FortiGate IPsec VPN tunnel interface IP addresses to the branch BGP configuration as BGP peers.

Routes that have the same network mask, administrative distance, and priority are automatically considered for SD-WAN when the interfaces where those routes are learned are added to the SD-WAN interface group.

Begin by adding a route-map to set the extended tag to 10.

```
config router route-map
  edit "add-tag"
    config rule
      edit 1
        set set-extended_tag 10
      end
```

The branch BGP configuration includes:

- Enabling `ebgp-multipath`
- Enabling `soft-reconfiguration`, `link-down-failover`, and `ebgp-enforce-multihop` for each BGP peer

- Adding the data center `remote-as` (which is 65500) to each peer configuration
- Setting the `prefix` for the neighbor range to the network matching the BGP peers
- Set `route-map-in` to the configured `route-map` tag (`add-tag`) for each BGP peer.

To facilitate the fastest route failovers, the following timers are set to their lowest values:

- `scan-time`
- `advertisement-interval`
- `keep-alive timer`
- `holdtime-timer`

```
config router bgp
   set as 65501
   set router-id 10.254.0.2
   set keepalive-timer 1
   set holdtime-timer 3
   set ebgp-multipath enable
   set scan-time 5
   set distance-external 1
   config neighbor
      edit "10.254.0.1"
         set advertisement-interval 1
         set link-down-failover enable
         set soft-reconfiguration enable
         set remote-as 65500
         set route-map-in add-tag
         set ebgp-enforce-multihop enable
      next
      edit "10.254.1.1"
         set advertisement-interval 1
         set link-down-failover enable
         set soft-reconfiguration enable
         set remote-as 65500
         set route-map-in add-tag
         set ebgp-enforce-multihop enable
      next
   end
end
```

Setting up the load balancing SD-WAN configuration

The SD-WAN configuration sets up load balancing based on link quality. Link quality is determined by health checking; which measures jitter, packet loss, and latency on each link. FortiOS dynamically creates policy routes that send traffic over the link with the highest quality.

1. Create **an SD-WAN Interface** (also called a virtual WAN link) and add the IPsec VPN tunnel interfaces to it. These members are also the BGP neighbors that are tied to specific interfaces.

```
config system virtual-wan-link
   set status enable
   config members
      edit 1
         set interface "vpn_dc1-1"
      next
      edit 2
         set interface "vpn_dc1-2"
      next
```

```
      end
   end
```

2. Create SD-WAN **Health-Checks** for each data center network. Set server to the IP address of a server on the data center network.

```
config system virtual-wan-link
   config health-check
      edit "datacenter1-net"
         set server "10.200.1.1"
         set interval 1
         set failtime 1
         set recoverytime 3
      next
      edit "datacenter2-net"
         set server "10.200.2.1"
         set interval 1
         set failtime 1
         set recoverytime 3
      end
   end
```

3. Add SD-WAN Service Rules to define the criteria for the policy routes. Criteria include:
   - Protocol
   - Destination Address
   - Source Address
   - Identity Based Group
   - Internet Service Definition
   - Source Port
   - Destination Port
   - Destination Tag

```
config system virtual-wan-link
   config service
      edit 1
         set mode priority
         set dst-tag 10
         set health-check "datacenter1-net"
         set priority-members 1 2
      next
      edit 2
         set mode priority
         set dst-tag 10
         set health-check "datacenter2-net"
         set priority-members 1 2
      next
   end
end
```

To dynamically determine the networks the policy routes point to, the routes learned from a BGP neighbor are matched against a route map and matching routes are tagged. The service rules determine the routes to use based on these tags.

Controlling access from branch networks

Create firewall policies to allow users on the branch office networks to access the data center networks. Security profiles can be enabled on these firewall policies to inspect layer 7 traffic.

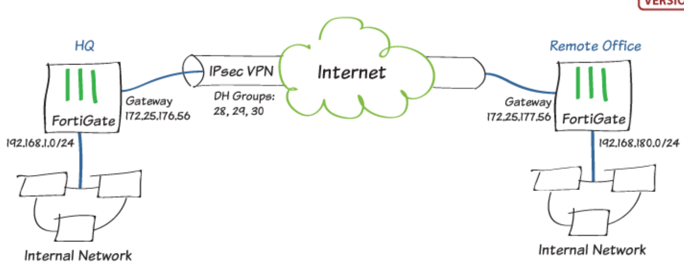
Policies to allow traffic from the branch office to the data center networks:

- **Source interface**: Internal interface
- **Destination interface**: SD-WAN interface
- **Source Address**: Branch networks
- **Destination Address**: Data center networks
- **Action**: Accept
- **Schedule**: Always (or define a more restrictive schedule)
- **Service**: Allowed services

Policies to allow traffic from the data center to the branch networks:

- **Source interface**: SD-WAN interface
- **Destination interface**: Internal interface
- **Source Address**: Data center networks
- **Destination Address**: Branch networks
- **Action**: Accept
- **Schedule**: Always (or define a more restrictive schedule)
- **Service**: Allowed Services

Brainpool curves in IKEv2 IPsec VPN



This recipe demonstrates how to establish a more secure IPsec VPN tunnel using high-level “Brainpool curves” for greater encryption, as specified in RFC 6954.

Such high-level cryptography improves the confidentiality, authenticity, and integrity of an IKEv2 IPsec VPN tunnel, which is typically limited by the weakest cryptographic primitive applied to the tunnel.

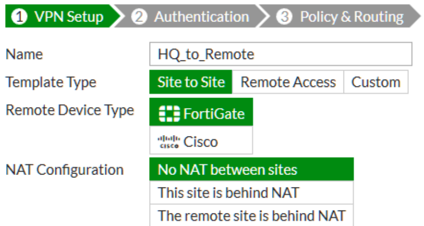
This recipe assumes that a VPN user group already exists. The example is demonstrated with a site-to-site IPsec VPN tunnel between an ‘HQ’ FortiGate and a ‘Remote Office’ FortiGate.

Creating the HQ tunnel

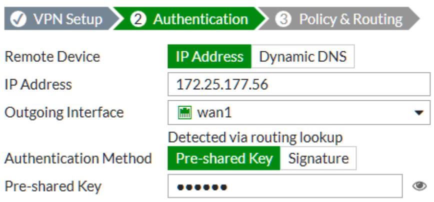
Create a site-to-site IPsec VPN tunnel using the VPN Creation Wizard. You will later convert it to a custom tunnel.

1. Go to *VPN* > *IPsec Wizard*.
   a. In the *Name* field, give the tunnel a name.
   b. Select the *Site to Site* template and set the *Remote DeviceType* to *Fortigate*.

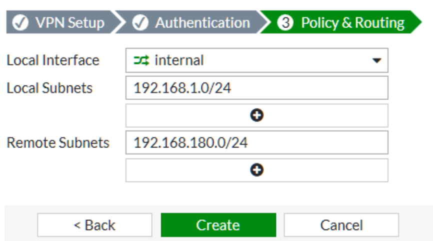
c. Click *Next*.



2. In the *Authentication* tab:
   a. Set *IP address* to the remote gateway interface. The *Outgoing Interface* should populate automatically.
   b. Enter a *Pre-shared Key*.
   c. Click *Next*.

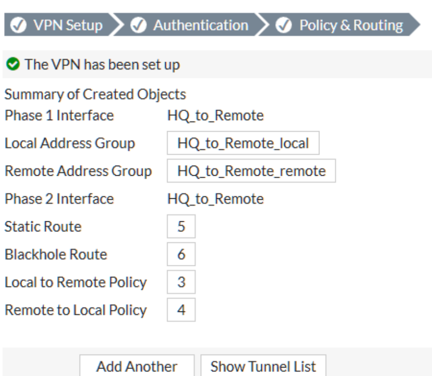


3. In the *Policy & Routing* tab:
   a. Select the *Local Interface* and set the *Local Subnets* and *Remote Subnets*. Ensure that the subnets do not overlap.
   b. Click *Create*.



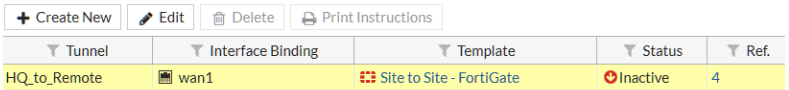
The VPN Creation Wizard provides a summary of the VPN configuration.

Click *Show Tunnel List*.

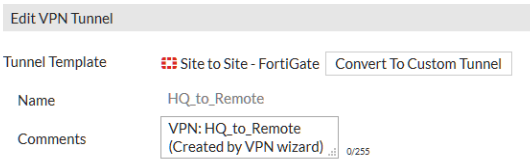


Customizing the HQ tunnel

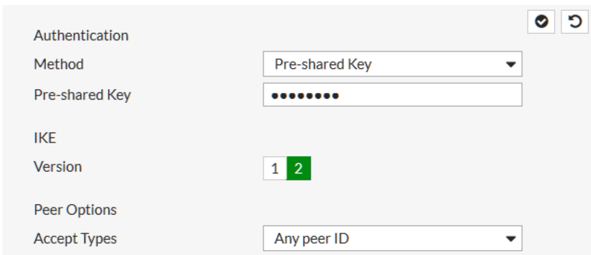
1. In the IPsec Tunnels list, highlight the new tunnel and select *Edit*.



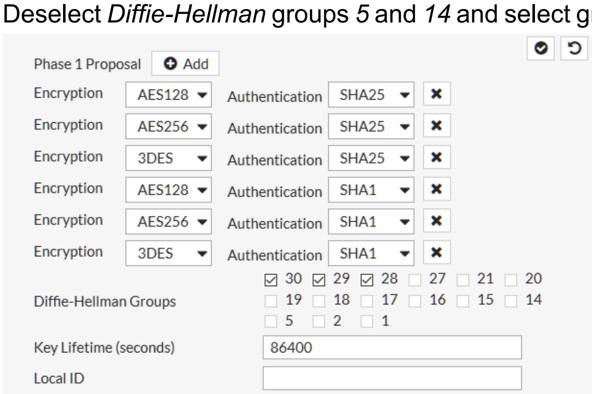
2. In the Edit VPN Tunnel dialog, click *Convert to Custom Tunnel*.



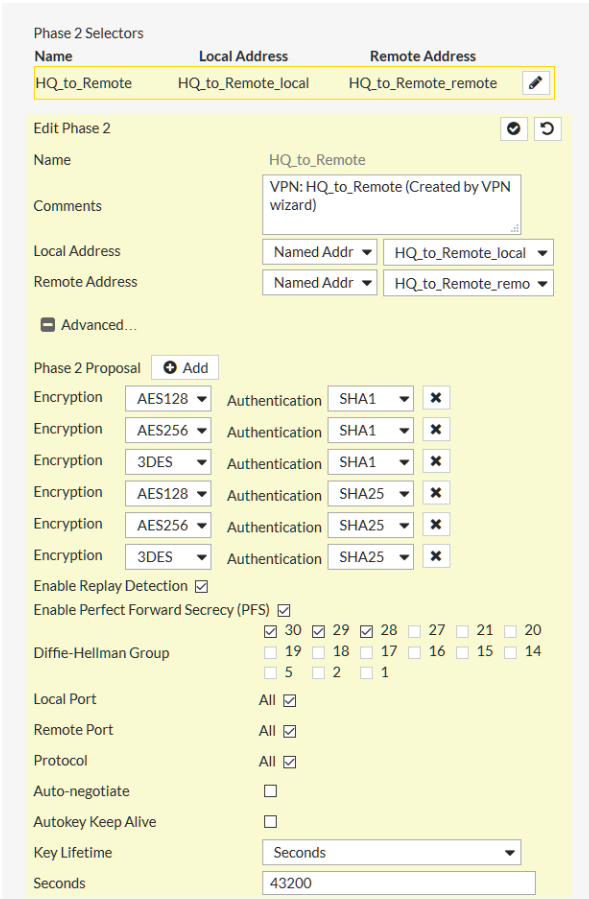
3. Edit the *Authentication* section and enable *IKE Version 2*.



4. Edit the *Phase 1 Proposal* section.
   a. Deselect *Diffie-Hellman* groups *5* and *14* and select groups *28*, *29*, and *30*.



5. Edit the *Phase 2 Selectors* section (don't click the Add Button) and click *Advanced…*.
   a. Deselect *Diffie-Hellman* groups *5* and *14* and select groups *28*, *29*, and *30*.
   b. Click *OK*.



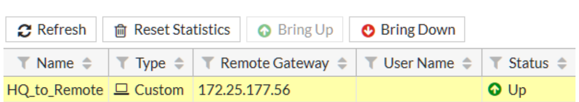
Creating and customizing the Remote Office tunnel

Repeat Creating the HQ tunnel on page 285 and Customizing the HQ tunnel on page 287 on the Remote Office FortiGate, alternating names and IP addresses appropriately.

Ensure that the same Phase 1 and Phase 2 selectors are applied and that there are no overlapping subnets.

Results

On either FortiGate, navigate to *Monitor* > *IPsec Monitor* and verify that the tunnel status is *Up*. If it us not up, highlight the tunnel and select *Bring up*.



You can confirm the use of Brainpool curves by performing diagnostics on the tunnel:

1. Go to *Monitor* > *IPsec Monitor*, highlight the tunnel and select *Bring Down*.
2. Open the CLI Console (>_) and enter the following command:
```
diagnose debug application ike 63
diagnose debug enable
```

`63` will remove encryption hash from the debug output, making it easier to read.

Return to *Monitor* > *IPsec Monitor* and bring the tunnel up again, then view the CLI Console.

While the SA proposal negotiates the tunnel, the output of the diagnose command should be similar to the following. The relevant parts appear as **bold** font:

```
FGT_1 # ike 0: comes 172.25.177.56:500->172.25.176.56:500,ifindex=5....
ike 0: IKEv2 exchange=INFORMATIONAL id=262e65aad12e5e8e/598faf8398c7acbe:00000001 len=80
ike 0:HQ_to_Remote:7: received informational request
ike 0:HQ_to_Remote:7: processing delete request (proto 3)
ike 0:HQ_to_Remote: deleting IPsec SA with SPI 00f82773
ike 0:HQ_to_Remote:HQ_to_Remote: deleted IPsec SA with SPI 00f82773, SA count: 0
ike 0:HQ_to_Remote: sending SNMP tunnel DOWN trap for HQ_to_Remote
ike 0:HQ_to_Remote:7: sending delete ack
ike 0:HQ_to_Remote:7: sent IKE msg (INFORMATIONAL_RESPONSE): 172.25.176.56:500-
     >172.25.177.56:500, len=80, id=262e65aad12e5e8e/598faf8398c7acbe:00000001
ike 0: comes 172.25.177.56:500->172.25.176.56:500,ifindex=5....
ike 0: IKEv2 exchange=CREATE_CHILD id=262e65aad12e5e8e/598faf8398c7acbe:00000002 len=656
ike 0:HQ_to_Remote:7: received create-child request
ike 0:HQ_to_Remote:7: responder received CREATE_CHILD exchange
ike 0:HQ_to_Remote:7: responder creating new child
ike 0:HQ_to_Remote:7:1: peer proposal:
ike 0:HQ_to_Remote:7:1: TSi_0 0:192.168.180.0-192.168.180.255:0
ike 0:HQ_to_Remote:7:1: TSr_0 0:192.168.1.0-192.168.1.255:0
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: trying
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: matched phase2
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: accepted proposal:
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: TSi_0 0:192.168.180.0-192.168.180.255:0
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: TSr_0 0:192.168.1.0-192.168.1.255:0
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: autokey
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: incoming child SA proposal:
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: proposal id = 1:
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: protocol = ESP:
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: encapsulation = TUNNEL
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: type=ENCR, val=AES_CBC (key_len = 128)
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: type=INTEGR, val=SHA
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: type=DH_GROUP, val=ECP512BP
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: type=DH_GROUP, val=ECP384BP
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: type=DH_GROUP, val=ECP256BP
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: type=ESN, val=NO
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: matched proposal id 1
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: proposal id = 1:
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: protocol = ESP:
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: encapsulation = TUNNEL
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: type=ENCR, val=AES_CBC (key_len = 128)
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: type=INTEGR, val=SHA
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: type=DH_GROUP, val=ECP512BP
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: type=ESN, val=NO
```

```
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: lifetime=43200
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: PFS enabled, group=30
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: replay protection enabled
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: set sa life soft seconds=42929.
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: set sa life hard seconds=43200.
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: IPsec SA selectors #src=1 #dst=1
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: src 0 7 0:192.168.1.0-192.168.1.255:0
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: dst 0 7 0:192.168.180.0-192.168.180.255:0
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: add IPsec SA: SPIs=2bf96e39/00f82774
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: added IPsec SA: SPIs=2bf96e39/00f82774
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: sending SNMP tunnel UP trap
ike 0:HQ_to_Remote:7:HQ_to_Remote:1: responder preparing CREATE_CHILD message
ike 0:HQ_to_Remote:7: sent IKE msg (CREATE_CHILD_RESPONSE): 172.25.176.56:500-
     >172.25.177.56:500, len=336, id=262e65aad12e5e8e/598faf8398c7acbe:00000002
```

Note how the SA proposal finds the first matching encryption type, in this case `ECP512BP` (DH Group 30), which represents ‘**E**lliptic **C**urve **P**arameter **512**-bit **B**rainpool **P**rimitive’.

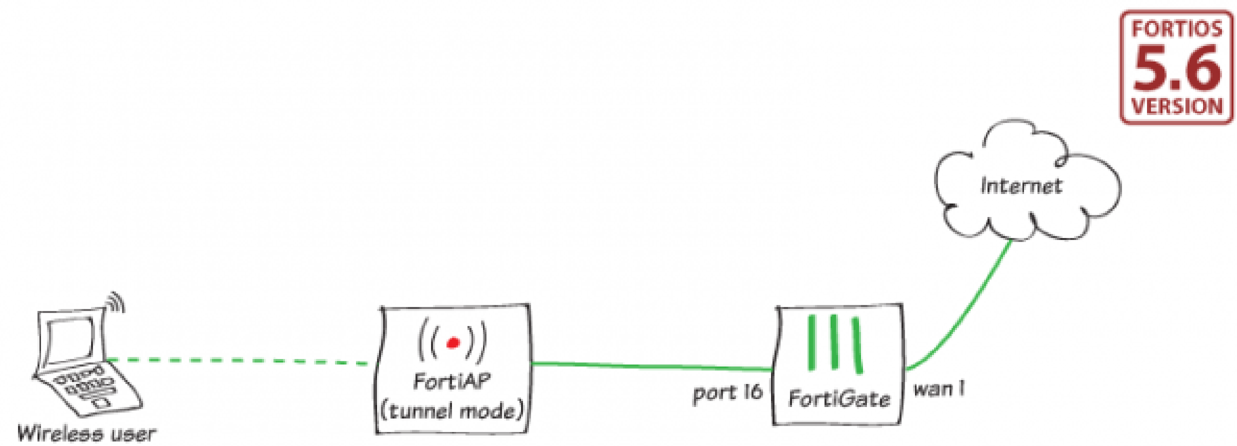
The diagnostic debug will run for 30 minutes, but you can stop it with these commands:

```
diagnose debug disable
diagnose debug reset
```

WiFi

This section contains examples about creating and configuring WiFi networks.

Setting up WiFi with a FortiAP



This examples shows how to set up a WiFi network with a FortiGate managing a FortiAP in Tunnel mode.

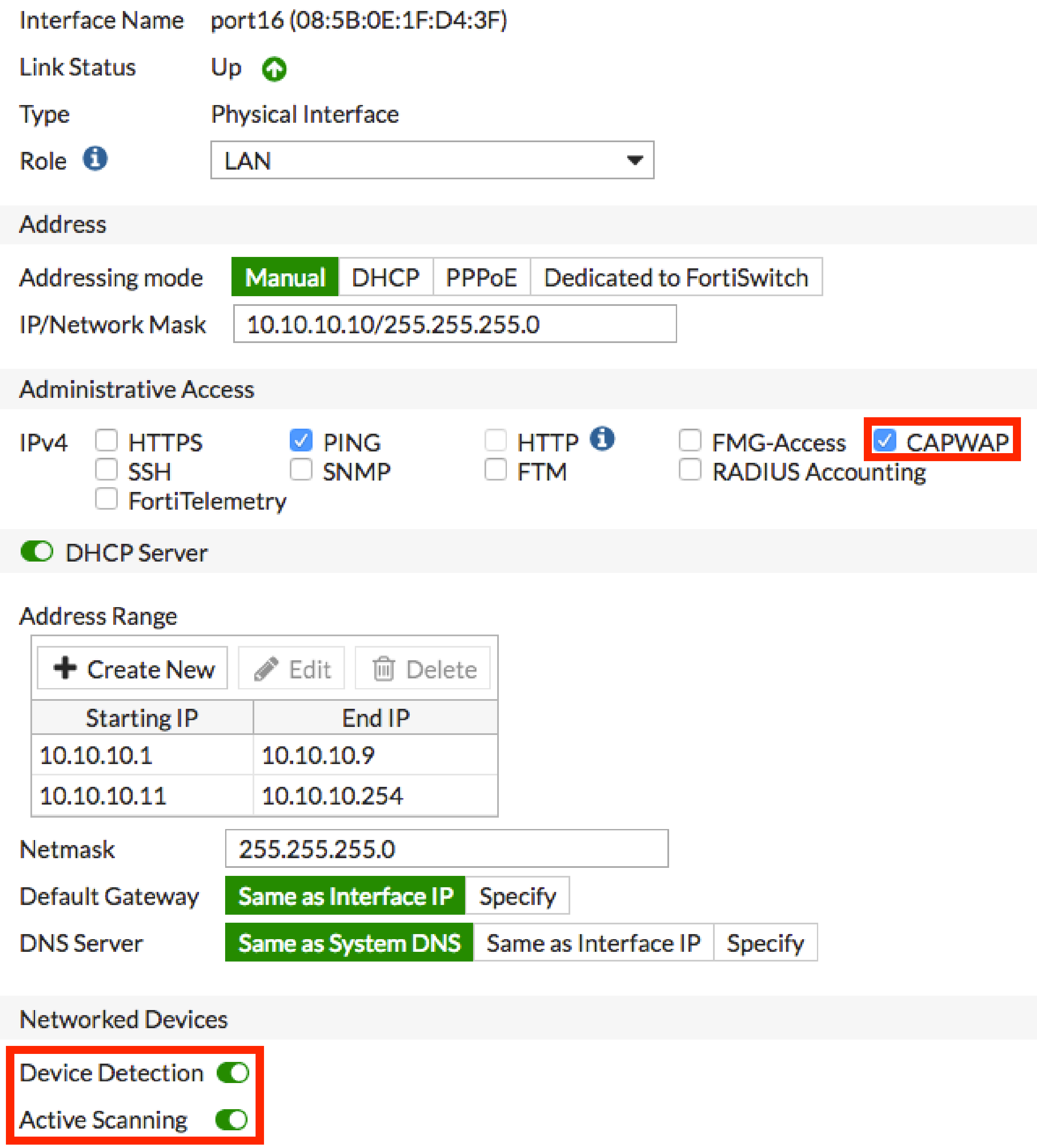
You can configure a FortiAP unit in either Tunnel mode (default) or Bridge mode. FortiAP in Tunnel mode uses a wireless-only subnet for wireless traffic. In Bridge mode, the Ethernet and WiFi interfaces are connected (or bridged) allowing wired and wireless networks to be on the same subnet.

For information on using a FortiAP in Bridge mode, see Setting up a WiFi Bridge with a FortiAP on page 298.

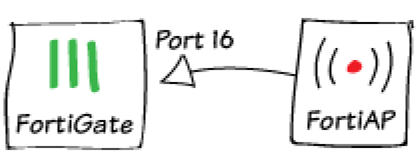
Connecting and authorizing the FortiAP unit

1. Go to *Network* > *Interfaces* and edit the interface that connects to the FortiAP (in this example, port 16).
   Set *Addressing mode* to *Manual* and set an *IP/Network Mask*.
   Under *Administrative Access*, enable *CAPWAP* and optionally enable *PING* to test your connection.

Under *Networked Devices*, enable both *Device Detection* and *Active Scanning*.

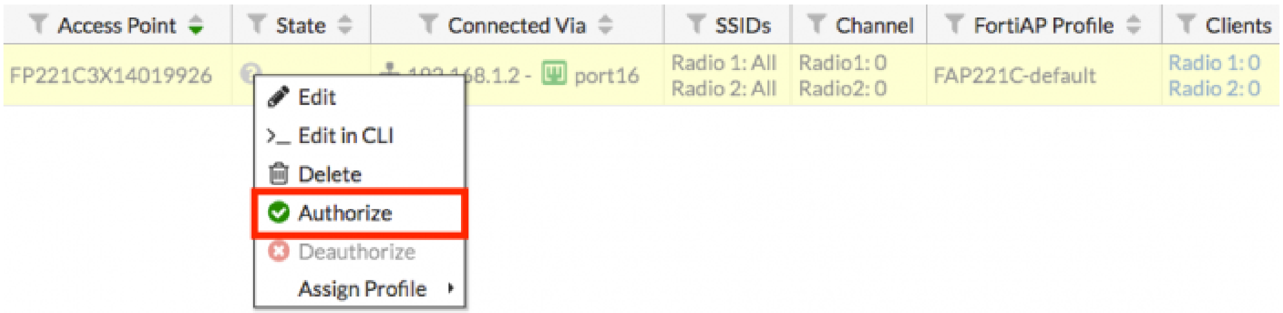


2. Connect the FortiAP unit to the interface.

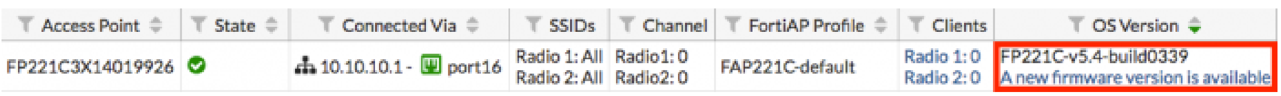


3. Go to *WiFi & Switch Controller > Managed FortiAPs*.
   The FortiAP is listed as not authorized as indicated by the in the *State* column.
   By default, FortiGate adds newly discovered FortiAPs to the *Managed FortiAPs* list but does not authorize them.

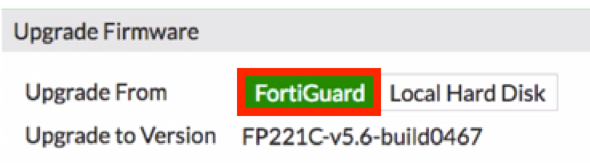
4. Right-click the FortiAP, and select *Authorize*.



5. Wait a few minutes after the device interface goes down, then select *Refresh* and the icon confirms that the device is authorized.
   Ensure your FortiAP is on the latest firmware. If the *OS Version* column shows *A new firmware version is available*, check the release notes for your product.



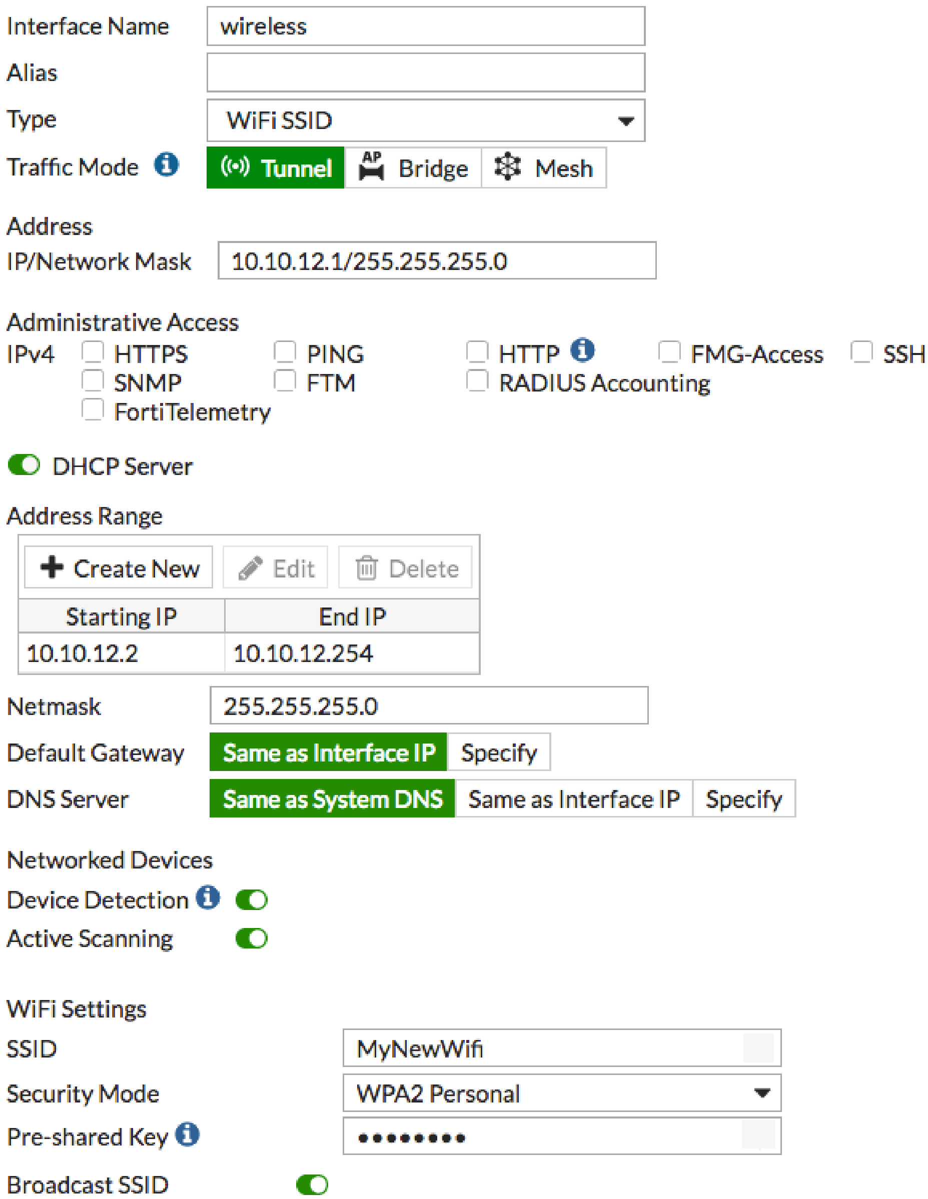
6. You can download the firmware images from the support site to your *Local Hard Disk*, or you can select *A new firmware version is available* and download the latest version directly from *FortiGuard*.



Creating an SSID

1. Go to *WiFi & Switch Controller > SSID* and create a new SSID.
   Set *Traffic Mode* to *Tunnel*.
   Set an *IP/Network Mask* for the wireless interface.
   Enable *DHCP Server*.
   Enable *Device Detection*.
   Enable *Active Scanning*.
   Name the *SSID* (in this example, *MyNewWiFi*).
   Set the *Security Mode* and enter a secure *Pre-shared Key*.

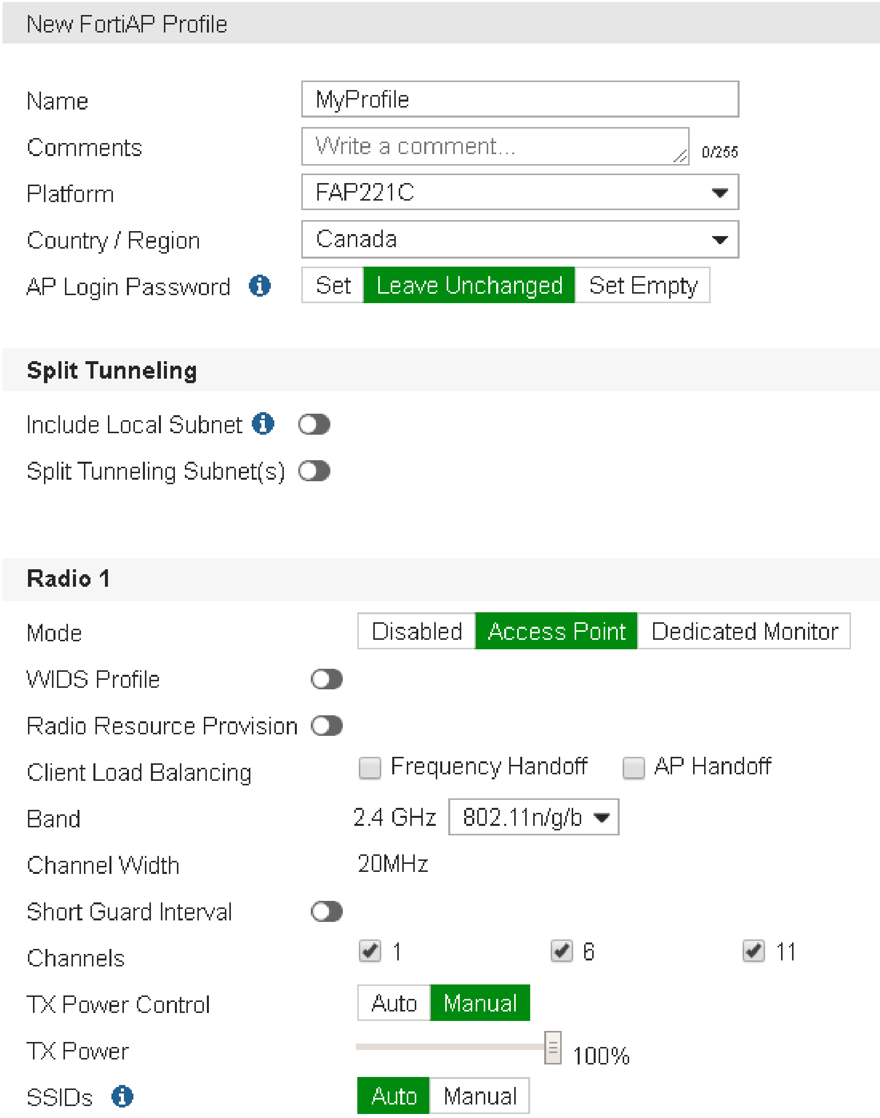
Enable *Broadcast SSID*.



Creating a custom FAP profile

1. Go to *WiFi & Switch Controller > FortiAP Profiles* and create a new profile.
   Set *Platform* to the FortiAP model you are using (in this example, *FAP221C*).
   Set the *Country/Region*.
   Set the *AP Login Password*.
   Under *Radio 1*, set *Mode* to *Access Point*.

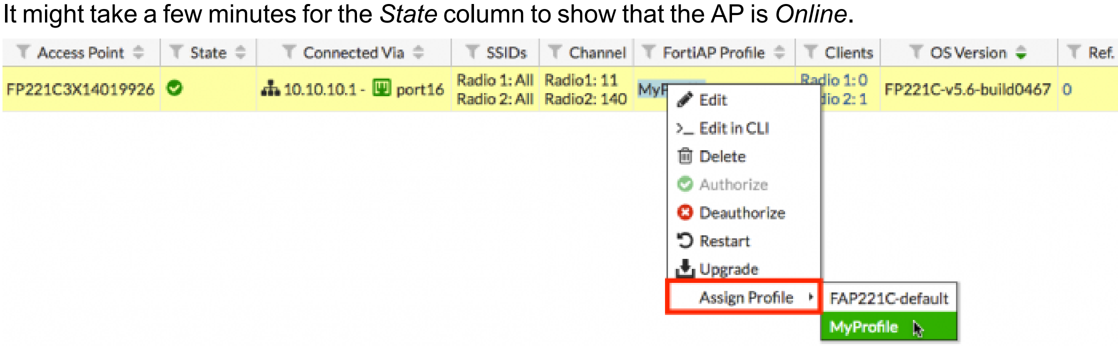
Leave *SSIDs* as *Auto*.



2. Go to *WiFi & Switch Controller > Managed FortiAPs* and right-click the FortiAP you added earlier. Select *Assign Profile* and set the FortiAP to use the new SSID profile (in this example, *MyProfile*).

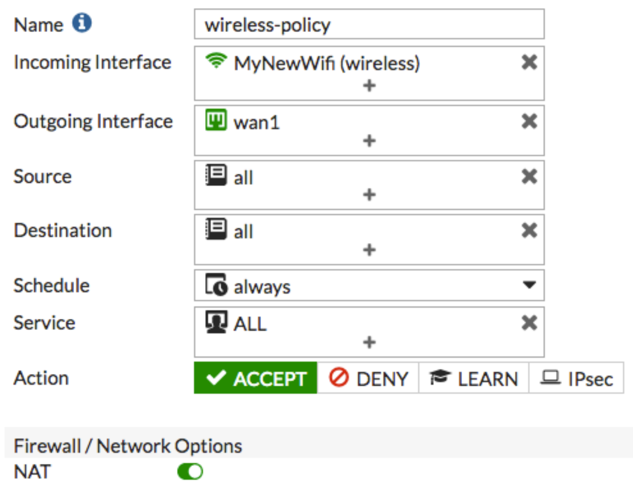
   By default, the FortiGate assigns all SSIDs to this profile.

   It might take a few minutes for the *State* column to show that the AP is *Online*.



Allowing wireless access to the Internet

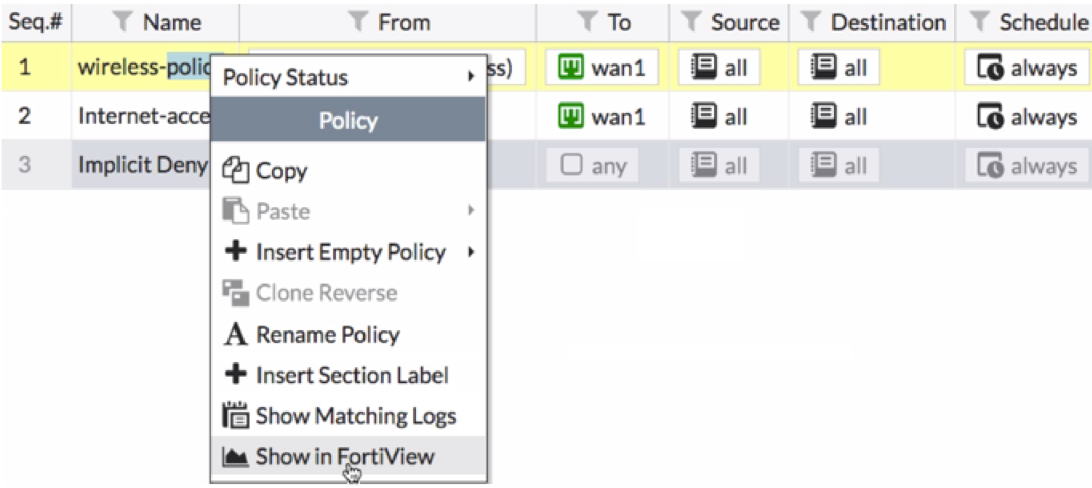
1. Go to *Policy & Objects* > *IPv4 Policy* and create a new policy.
   Set *Incoming Interface* to the SSID.
   Set *Outgoing Interface* to your Internet-facing interface.
   Ensure *NAT* is enabled.



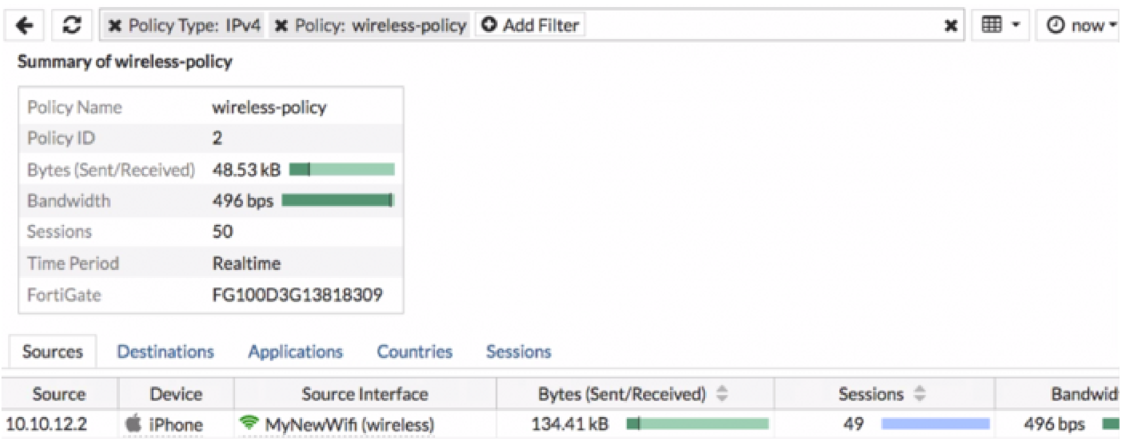
Results

1. Connect to the SSID with a wireless device. After a connection is established, browse the Internet to generate traffic.

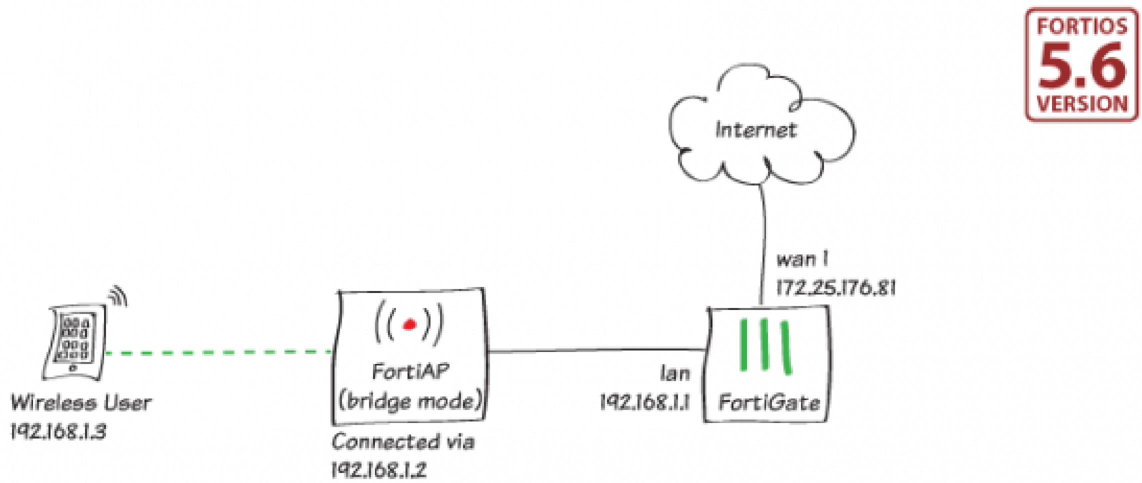
2. From the policy list page, right-click your wireless policy and select *Show in FortiView* or go directly to *FortiView > All Sessions*.



3. You can view more details by selecting the tabs (*Sources*, *Destinations*, *Applications*, *Countries*, *Sessions*).



Setting up a WiFi Bridge with a FortiAP



In this example, you set up a WiFi network with a FortiGate managing a FortiAP in Bridge mode.

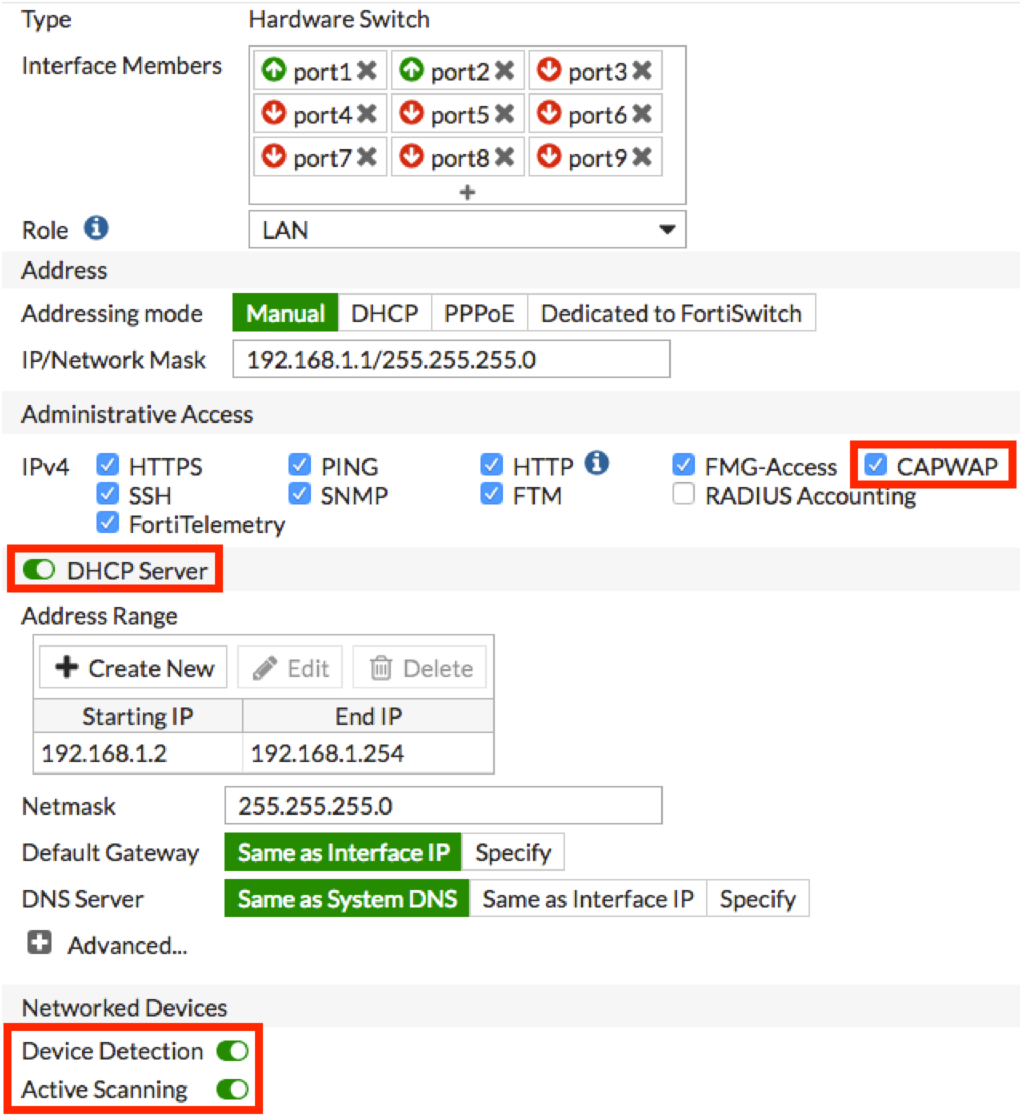
You can configure a FortiAP unit in either Tunnel (default) or Bridge mode. In Bridge mode, the Ethernet and WiFi interfaces are connected (or bridged) to allow wired and wireless networks to be on the same subnet. Tunnel mode uses a wireless-only subnet for wireless traffic.

For information about using a FortiAP in Tunnel mode, see Setting up WiFi with a FortiAP on page 291.

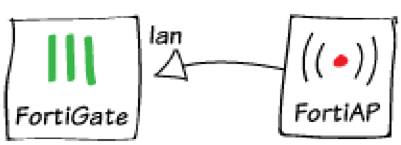
Connecting and authorizing the FortiAP unit

1. Go to *Network* > *Interfaces* and edit the *lan* interface.
   Set *Addressing Mode* to *Manual* and set an *IP/Network Mask*.
   Under *Administrative Access*, enable *CAPWAP* and optionally enable *PING* to test your connection.
   Enable the *DHCP Server*.

Under *Networked Devices*, enable both *Device Detection* and *Active Scanning*.



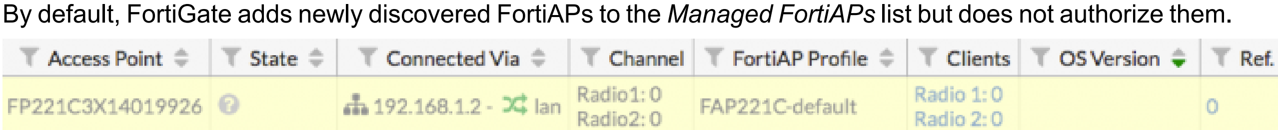
2. Connect the FortiAP to the *lan* interface.



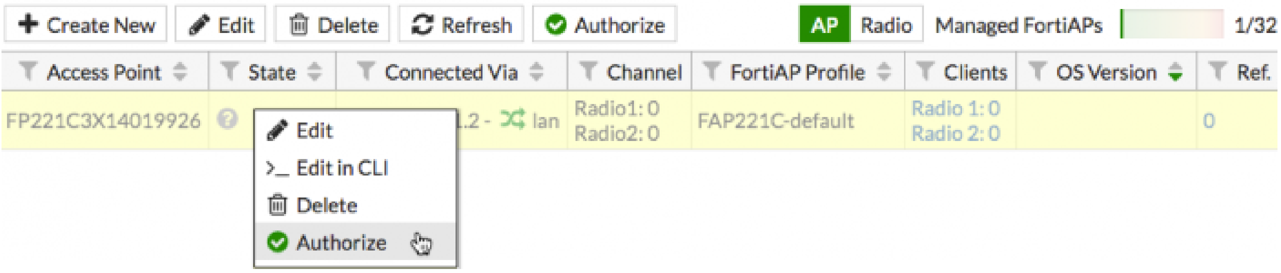
3. Go to *WiFi & Switch Controller > Managed FortiAPs*.

The FortiAP is listed as not authorized as indicated by the ? in the *State* column.

By default, FortiGate adds newly discovered FortiAPs to the *Managed FortiAPs* list but does not authorize them.

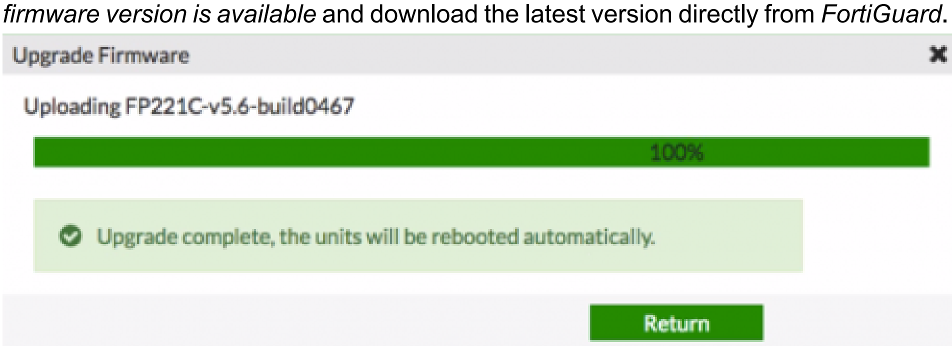


4. Right-click the FortiAP and select *Authorize*.



5. Wait a few minutes after the device interface goes down, then select *Refresh* and the icon confirms that the device is authorized.
Ensure your FortiAP is on the latest firmware. If the OS Version shows that a newer firmware version is available, check the release notes for your product.

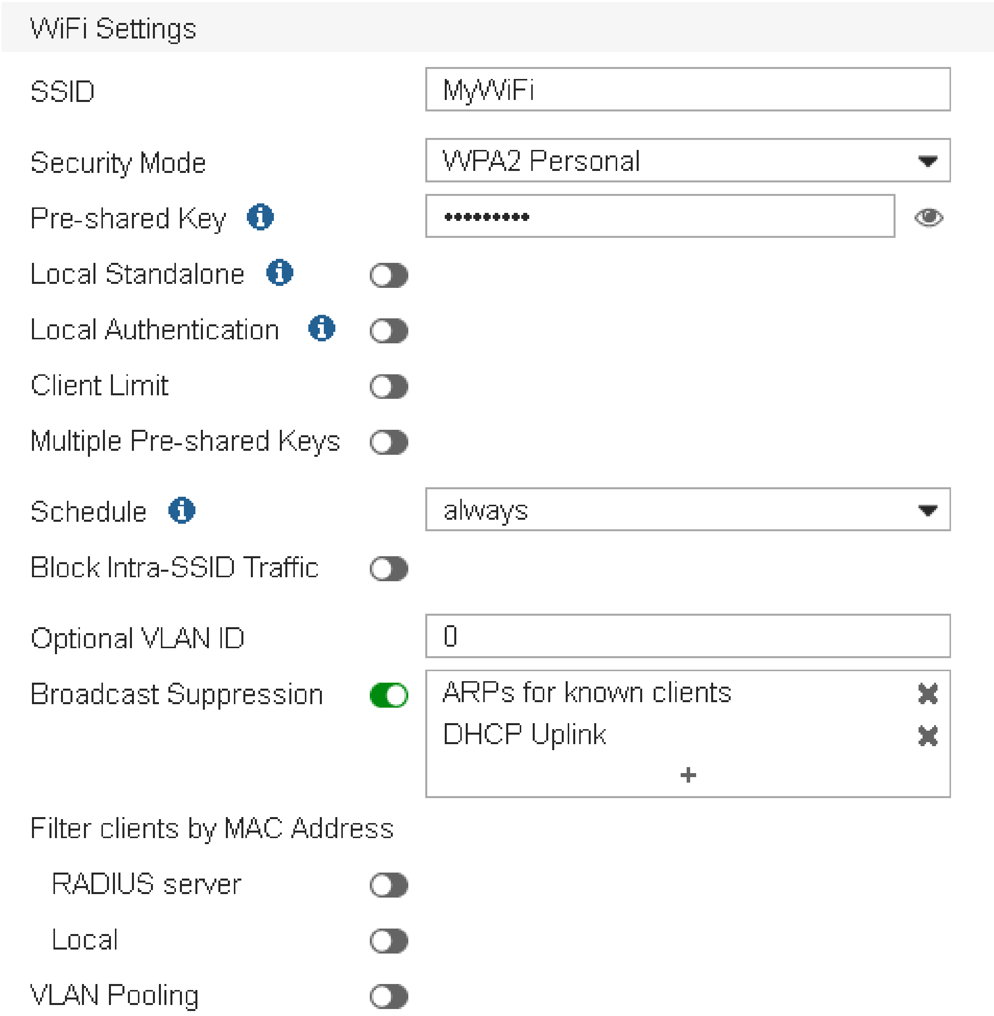
6. You can download the firmware images from the support site to your *Local Hard Disk*, or you can select *A new firmware version is available* and download the latest version directly from *FortiGuard*.



Creating an SSID

1. Go to *WiFi & Switch Controller > SSID* and create a new SSID.
Set *Traffic Mode* to *Bridge*.

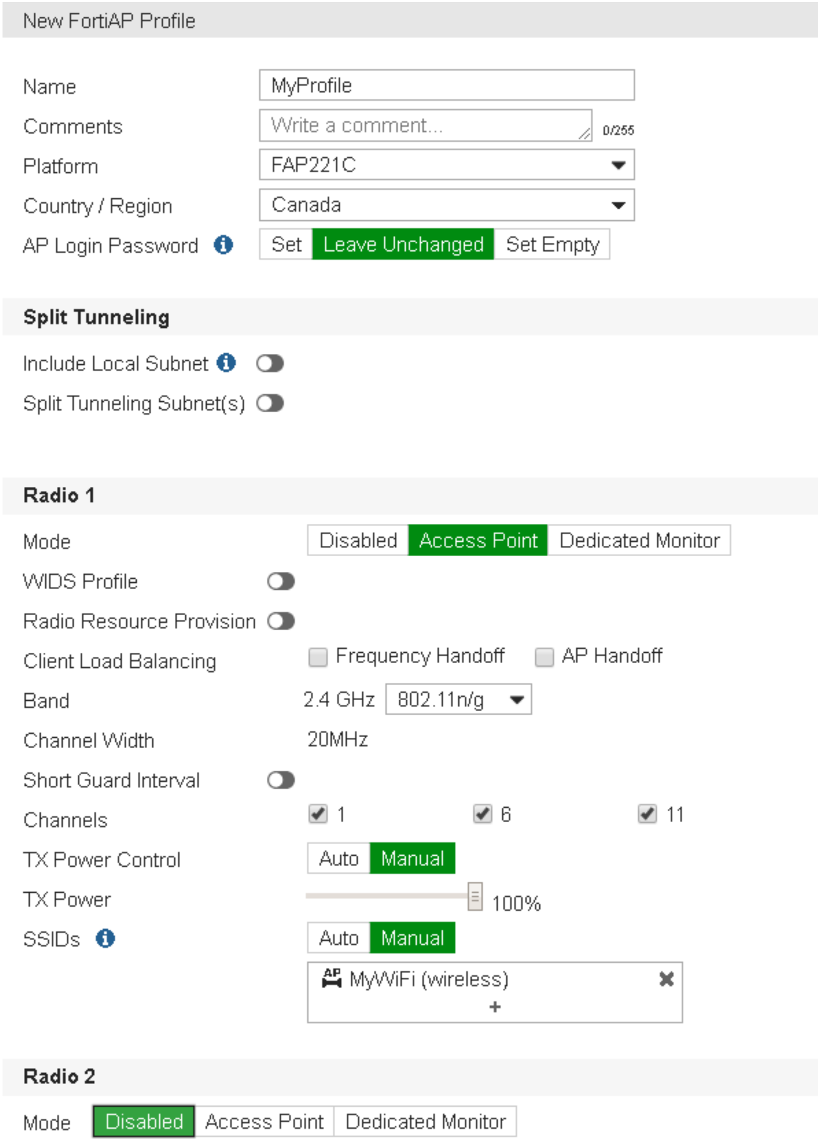
Configure the *WiFi Settings* as you would for a regular wireless network and set a secure *Pre-shared Key*.



Creating a custom FortiAP profile

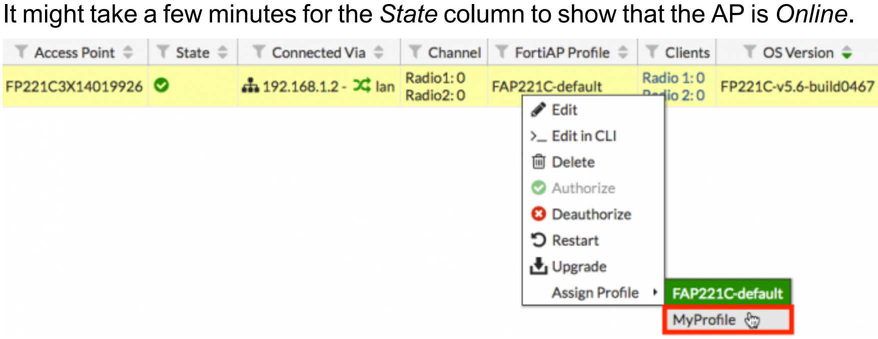
1. Go to *WiFi & Switch Controller* > *FortiAP Profiles* and create a new profile.
   Set *Platform* to the FortiAP model you are using (in this example, *FAP221C*).
   Select the *Country/Region*.
   Set the *AP Login Password*.
   Under *Radio 1*, set *Mode* to *Access Point*.
   Set *SSID* to use the new SSID profile (in this example, *MyWiFi*).

Set *Radio 2* to *Disabled*.



2. Go to *WiFi & Switch Controller* > *Managed FortiAPs* and right-click the FortiAP. Select *Assign Profile* and set the FortiAP to use the new SSID profile (in this example, *MyProfile*).

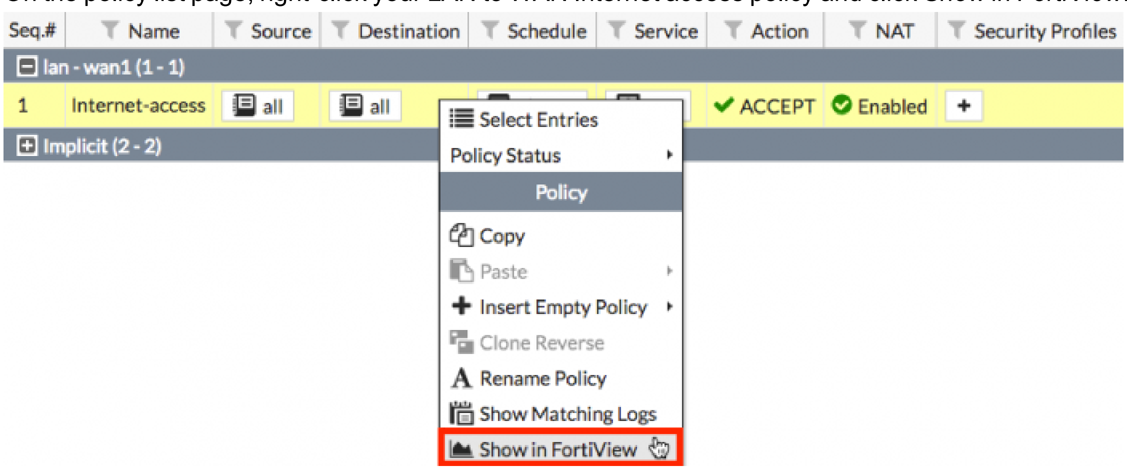
   It might take a few minutes for the *State* column to show that the AP is *Online*.



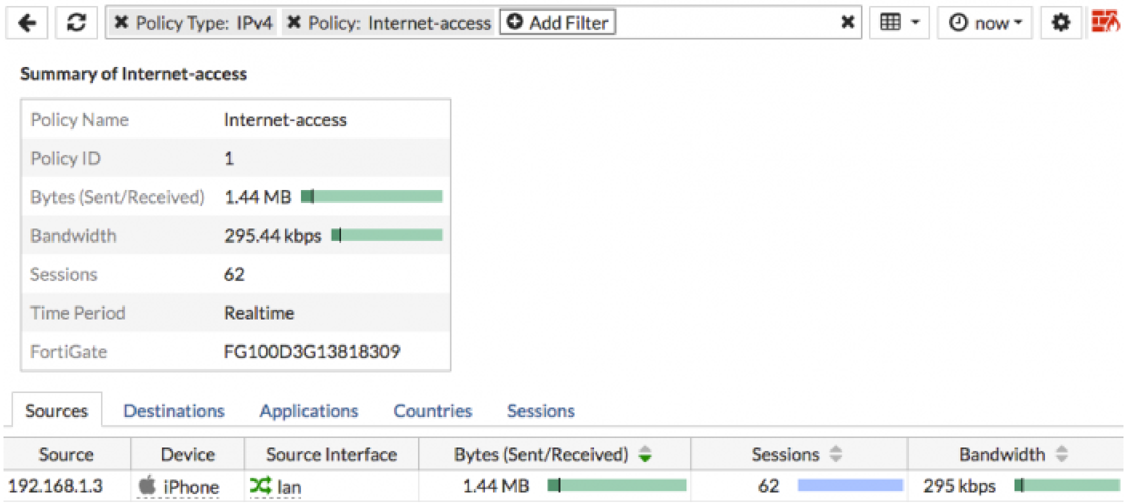
Results

1. Connect to the SSID with a wireless device. After a connection is established, browse the Internet using the wireless network configured in this recipe.

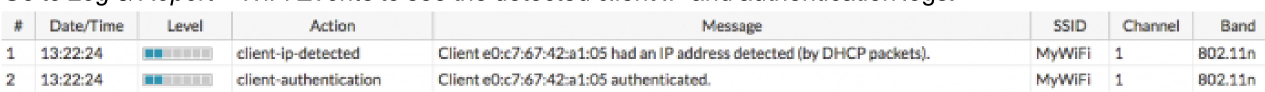
2. On the policy list page, right-click your LAN to WAN Internet access policy and click *Show in FortiView*.



3. You can view more details by selecting the tabs (*Sources*, *Destinations*, *Applications*, *Countries*, *Sessions*).

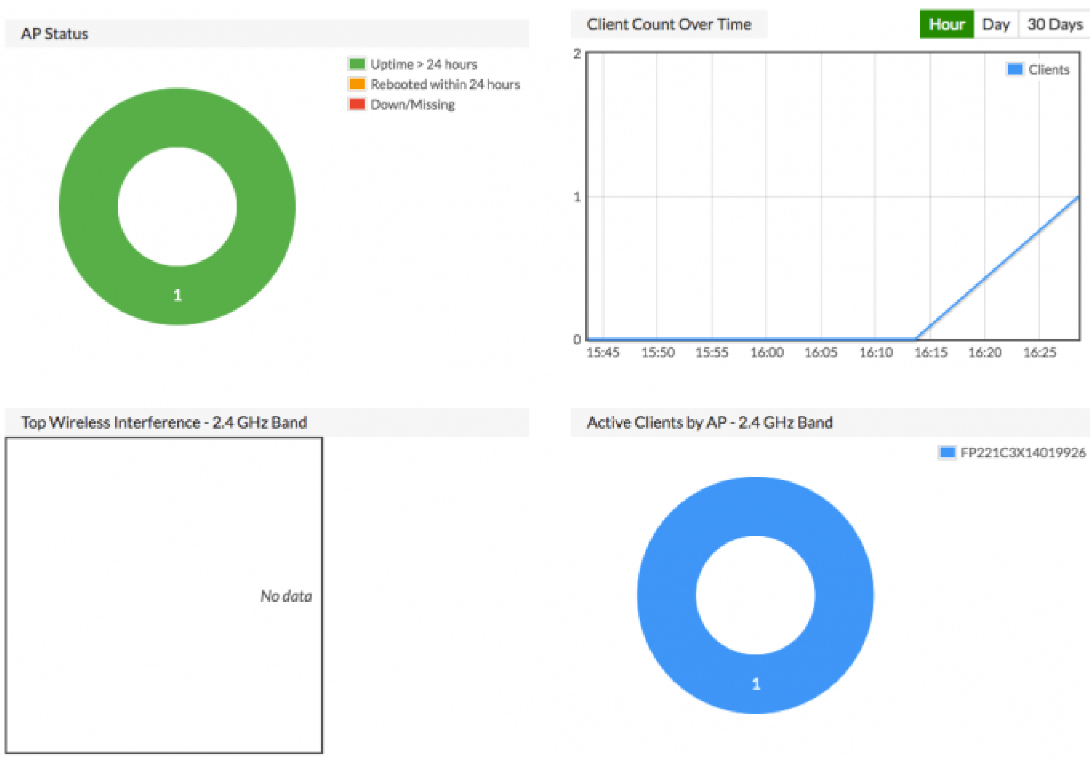


4. Go to *Log & Report* > *WiFi Events* to see the detected client IP and authentication logs.

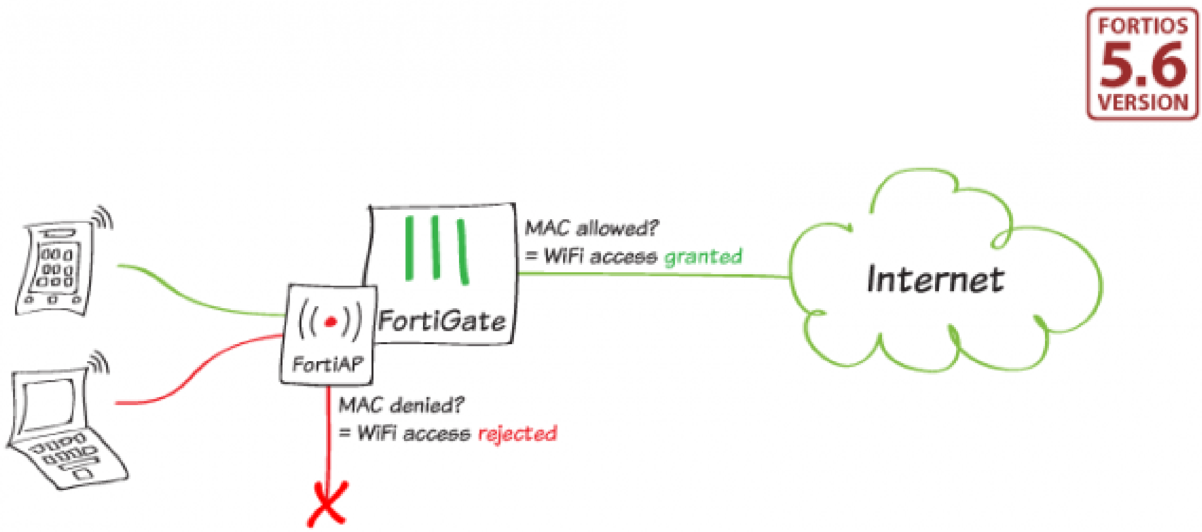


#	Date/Time	Level	Action	Message	SSID	Channel	Band
1	13:22:24		client-ip-detected	Client e0:c7:67:42:a1:05 had an IP address detected (by DHCP packets).	MyWiFi	1	802.11n
2	13:22:24		client-authentication	Client e0:c7:67:42:a1:05 authenticated.	MyWiFi	1	802.11n

5. Go to *Monitor* > *WiFi Client Monitor* for user details and *Monitor* > *WiFi Health Monitor* for the *AP Status*.



Filtering WiFi clients by MAC address



In this example, you configure a managed FortiAP to filter client devices based on MAC address. Only authorized devices have access to the wireless network.

Acquiring the MAC address

This list does not include all device types. Instructions are accurate when this was published. Older or newer operating systems might have different instructions.

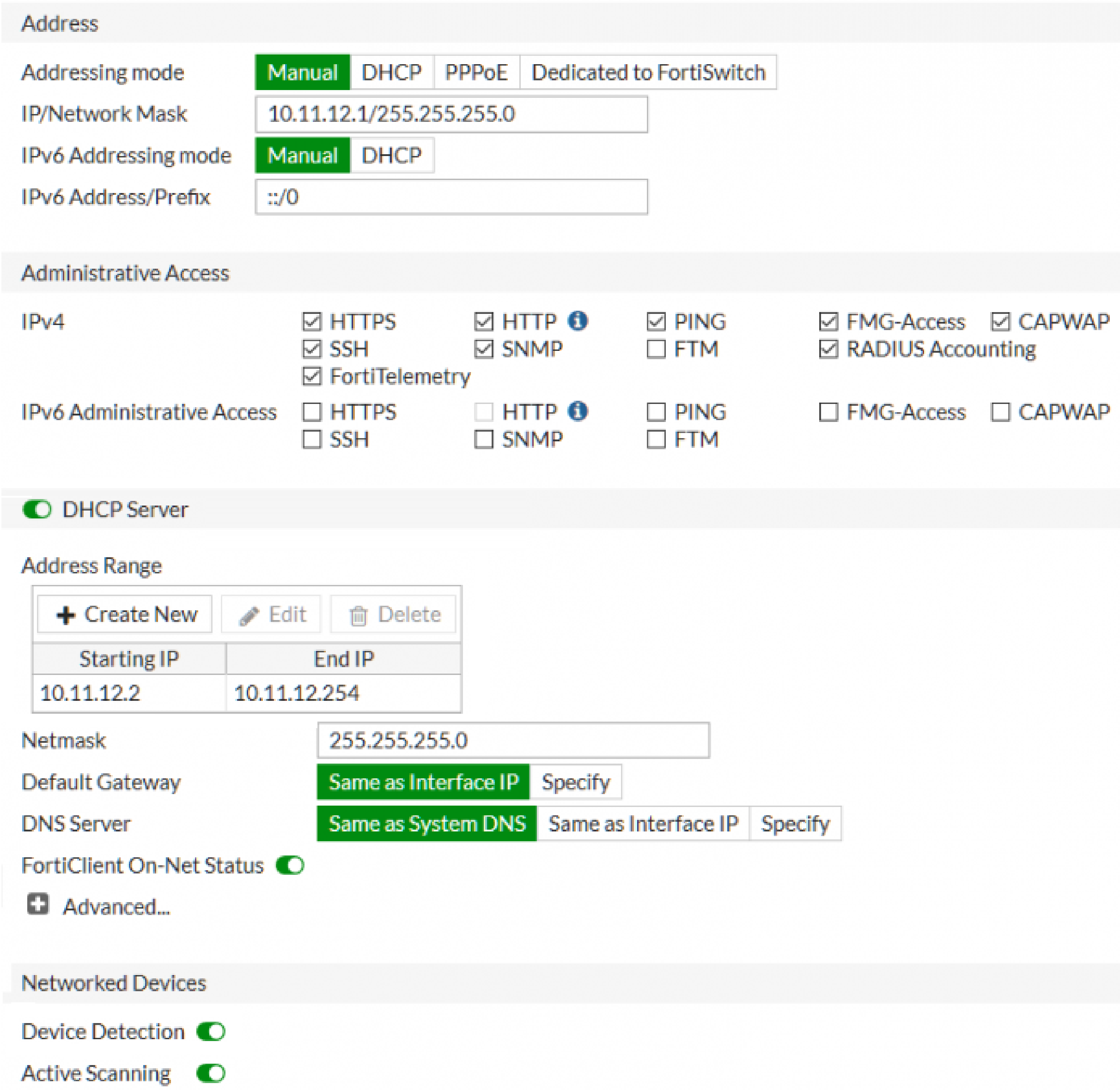
To acquire the MAC address of a device:

- Windows: Open the command prompt and type `ipconfig /all`.
  The MAC address of your Windows device is the *Physical Address*, under information about the wireless adapter.
- Mac OS X: Open Terminal and type `ifconfig en1 | grep ether`.
  The MAC address displays.
- iOS: Go to *Settings* > *General* > *About*.
  The *Wi-Fi Address* is your iOS device's MAC address.
- Android: Go to *Settings* > *About Device* > *Status*.
  The *Wi-Fi MAC address* is your Android device's MAC address.

Creating the FortiAP interfaces

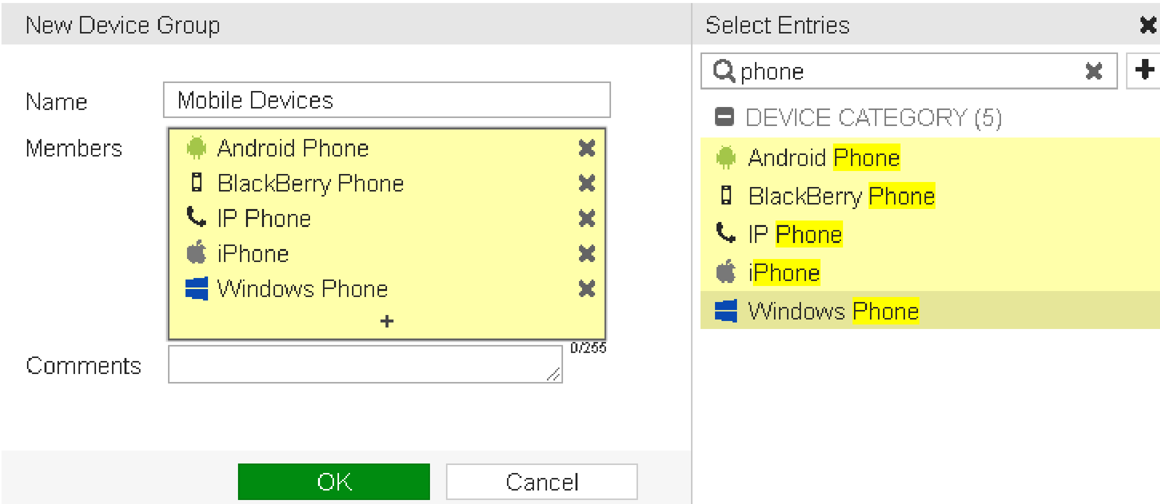
1. Go to *Network* > *Interfaces* and create an internal FortiAP interface.
   Set *Addressing mode* to *Manual* and set an *IP/Network Mask*.
   Under *Administrative Access*, enable *CAPWAP*.
   Enable *DHCP Server*. The *Starting IP* and *End IP* address range should automatically populate.

Enable *Device Detection* and select *OK*.

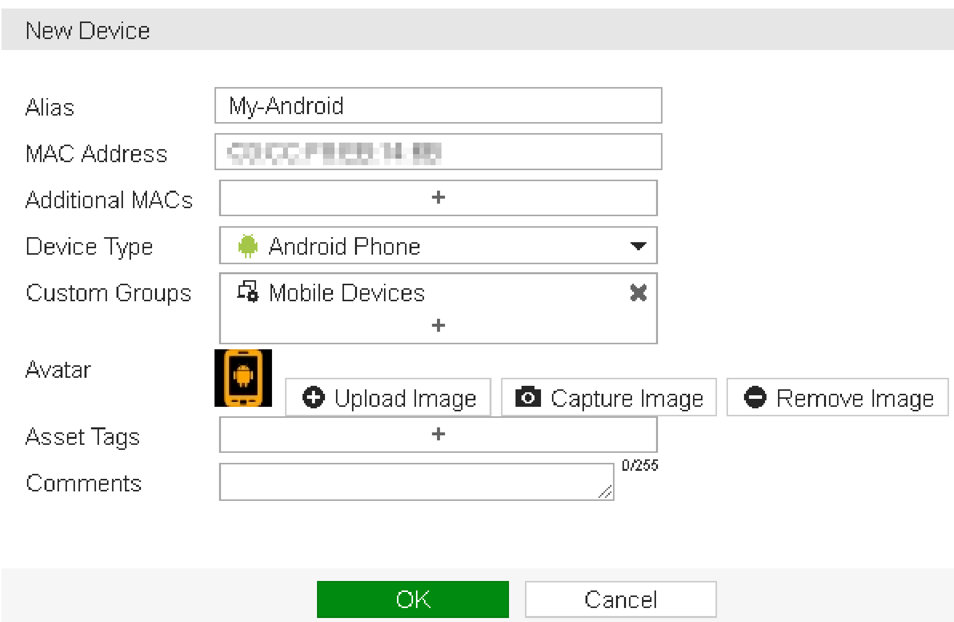


Defining a device using its MAC address

1. Go to *User & Device* > *Custom Devices & Groups* and create a new device group.
   In this example, a broad *Mobile Devices* group is created for all mobile phones.



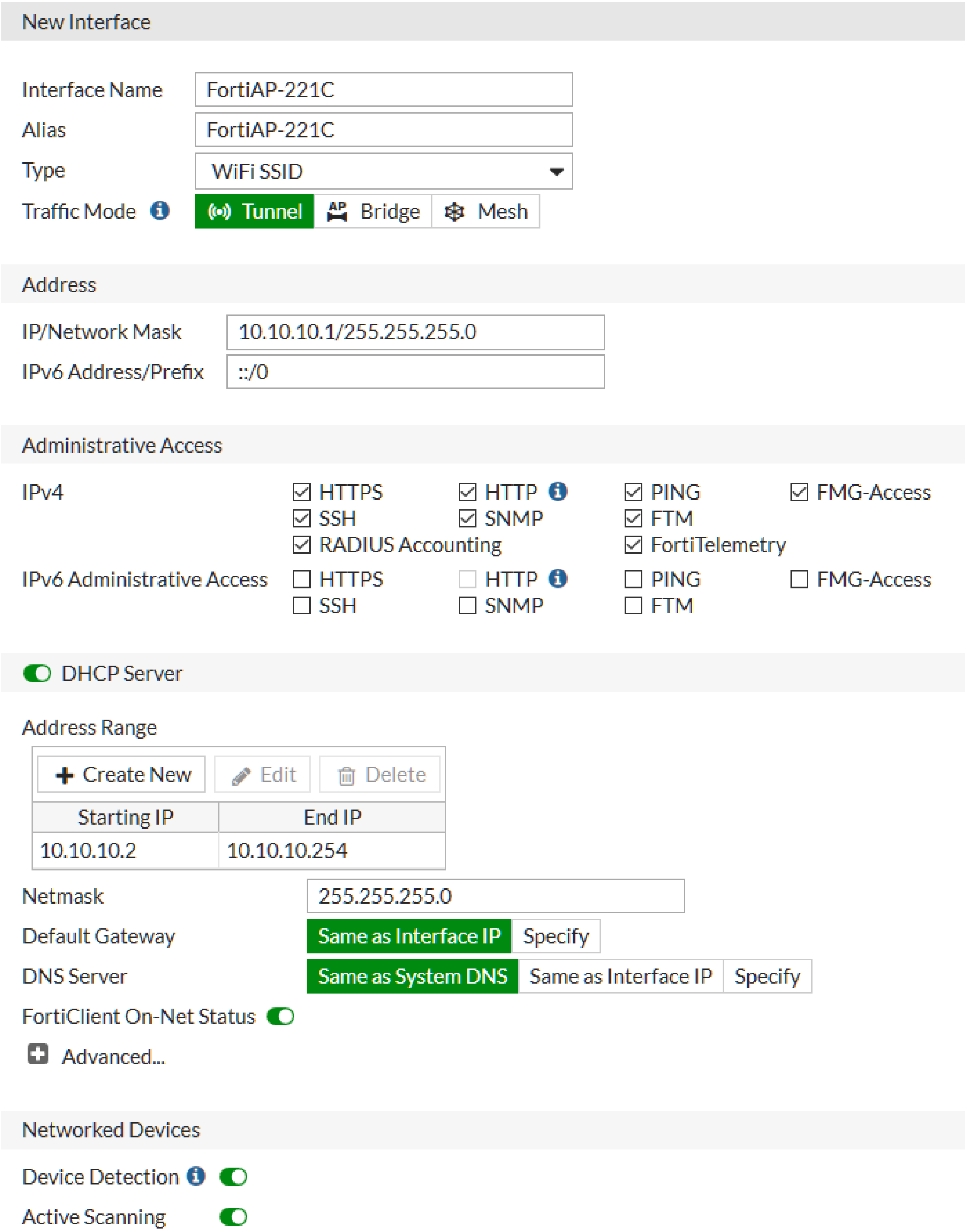
2. Create a new device definition.
   Set the *MAC Address* to the device's address.
   For *Device Type*, select *Mobile Devices*.



Creating the new SSID

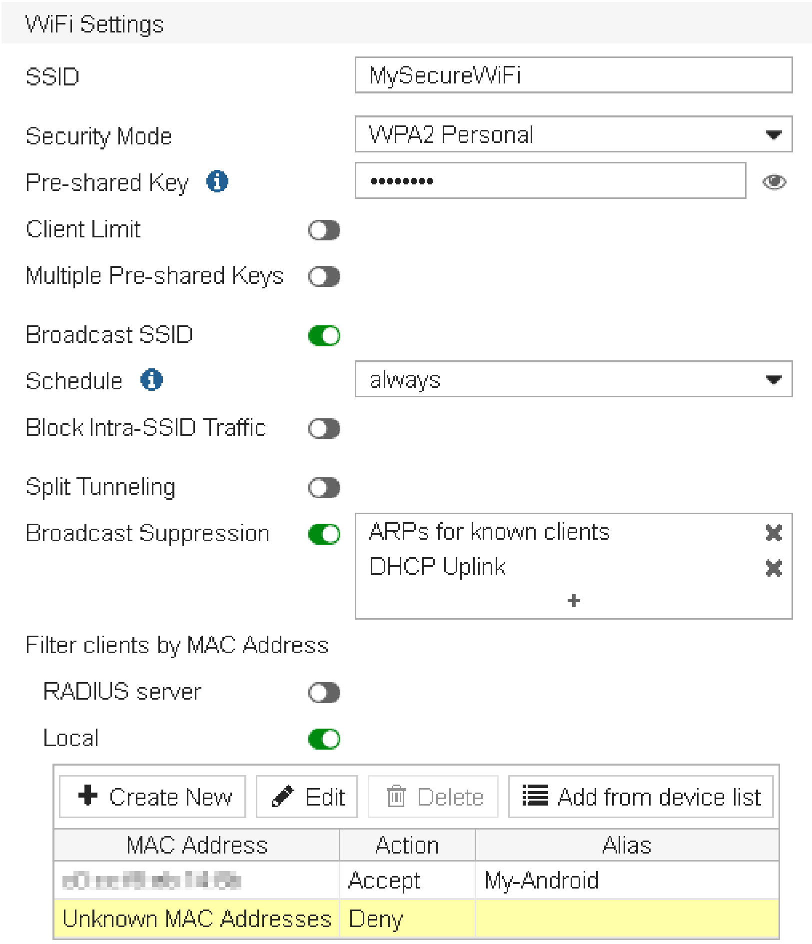
1. Go to *WiFi & Switch Controller* > *SSID* and create a new SSID.
   Set *Traffic Mode* to *Tunnel*.
   Select an *IP/Network Mask* for the wireless interface.

Enable *DHCP Server* and *Device Detection*.



2. Under *WiFi Settings*, name the *SSID* (in this example, *MySecureWiFi*).
Select a *Security Mode* and enter a secure *Pre-shared Key*.
Enable *Broadcast SSID*.
Under *Filter clients by MAC Address*, enable *Local* and select *Add from device list*.
Add the device you configured earlier and set its *Action* to *Accept*.

Set the *Action* for *Unknown MAC Addresses* to *Deny*.

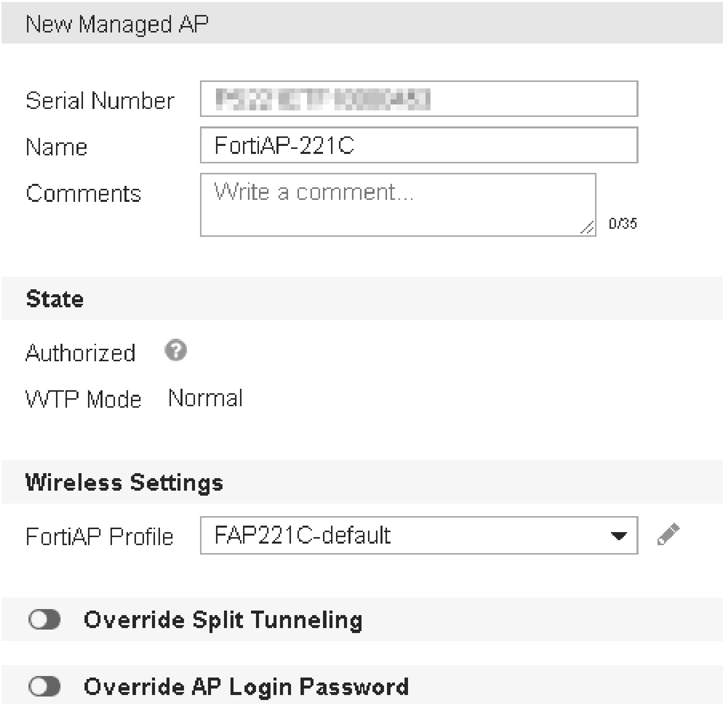


3. Connect the FortiAP unit to the interface configured earlier.

Managing the FortiAP

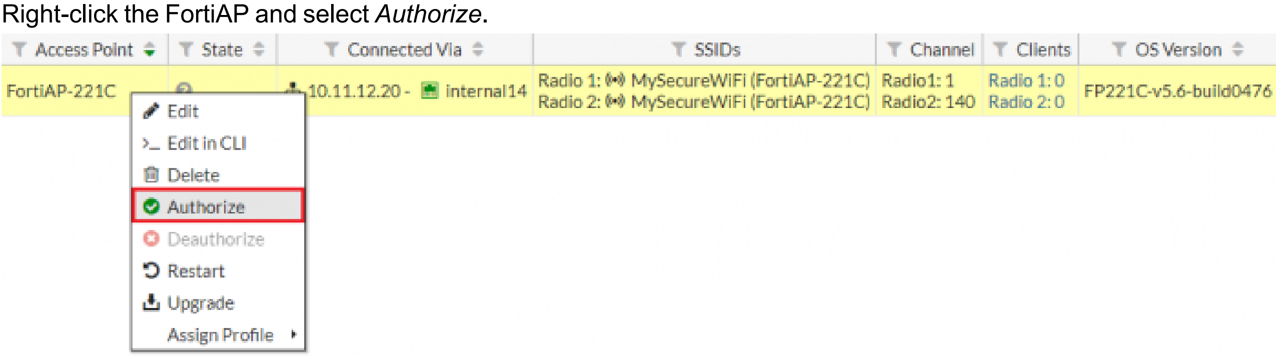
1. Go to *WiFi & Switch Controller > Managed FortiAPs*.
   If the FortiAP is not listed, wait a few minutes. If the device still does not appear, select *Create New > Managed AP*.

When you enter the *Serial Number*, the default *FortiAP Profile* for that model is applied.



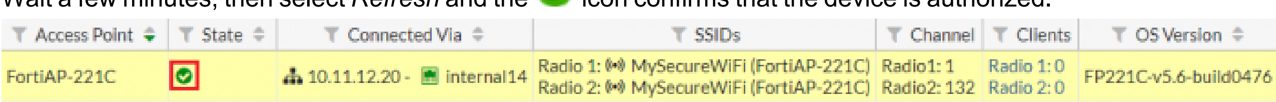
Authorizing the managed FortiAP

1. Right-click the FortiAP and select *Authorize*.



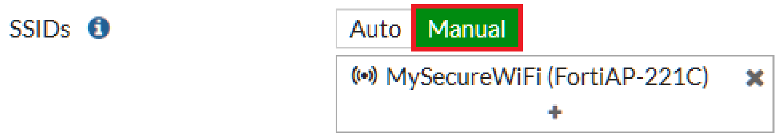
The device interface is initially down.

2. Wait a few minutes, then select *Refresh* and the icon confirms that the device is authorized.



Editing the default FortiAP profile

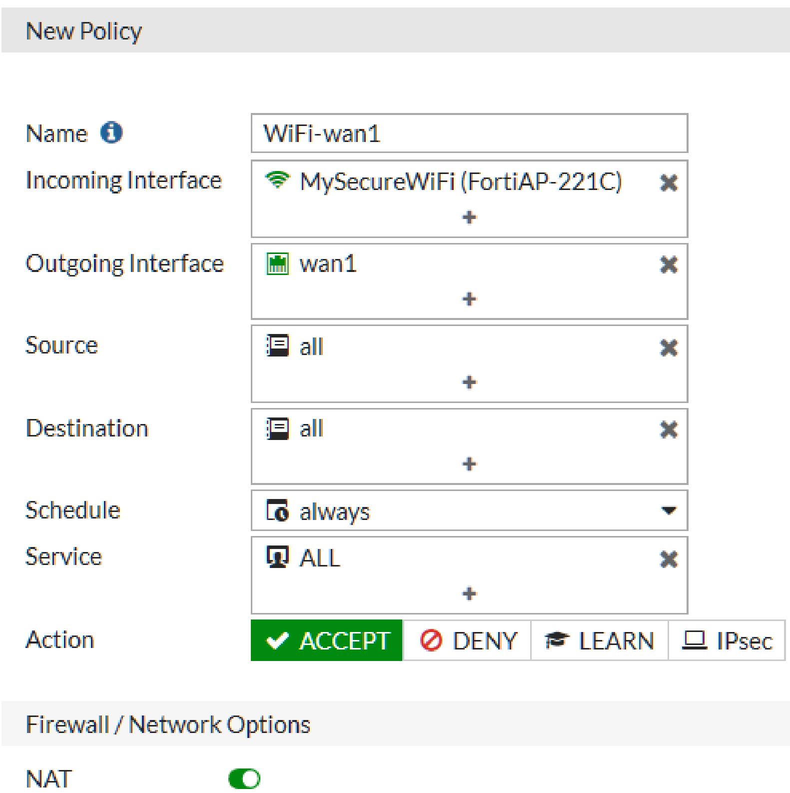
1. Go to *WiFi & Switch Controller* > *FortiAP Profiles* and *Edit* the default profile for your FortiAP model.



For all radios you want to use, set the SSID to *Manual* and select the SSID created earlier.

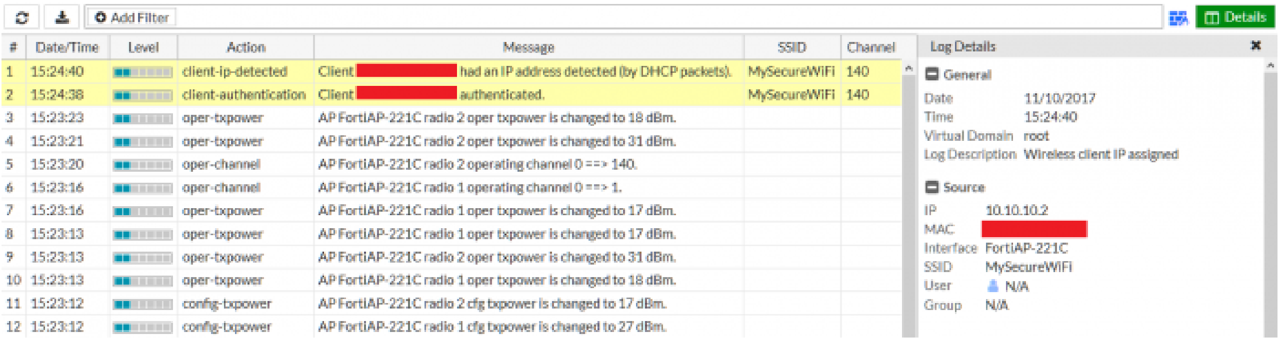
Allowing wireless access to the Internet

1. Go to *Policy & Objects* > *IPv4 Policy* and create a new policy.
Set *Incoming Interface* to the SSID.
Set *Outgoing Interface* to your Internet-facing interface.
Enable *NAT*.

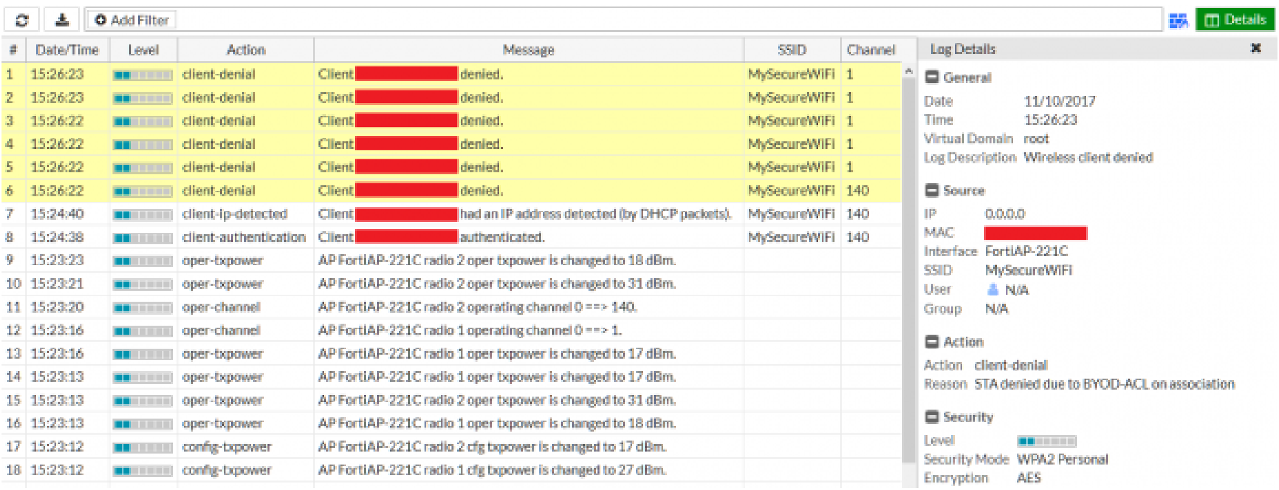


Results

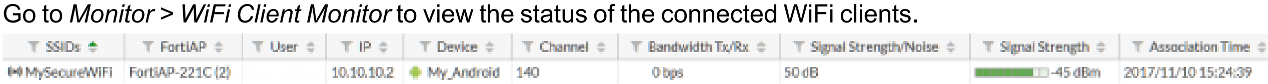
1. Use the authorized device to connect to the broadcast SSID (in this example, *MySecureWifi*).
2. Go to *Log & Report* > *WiFi Events* and verify the authorized connection.



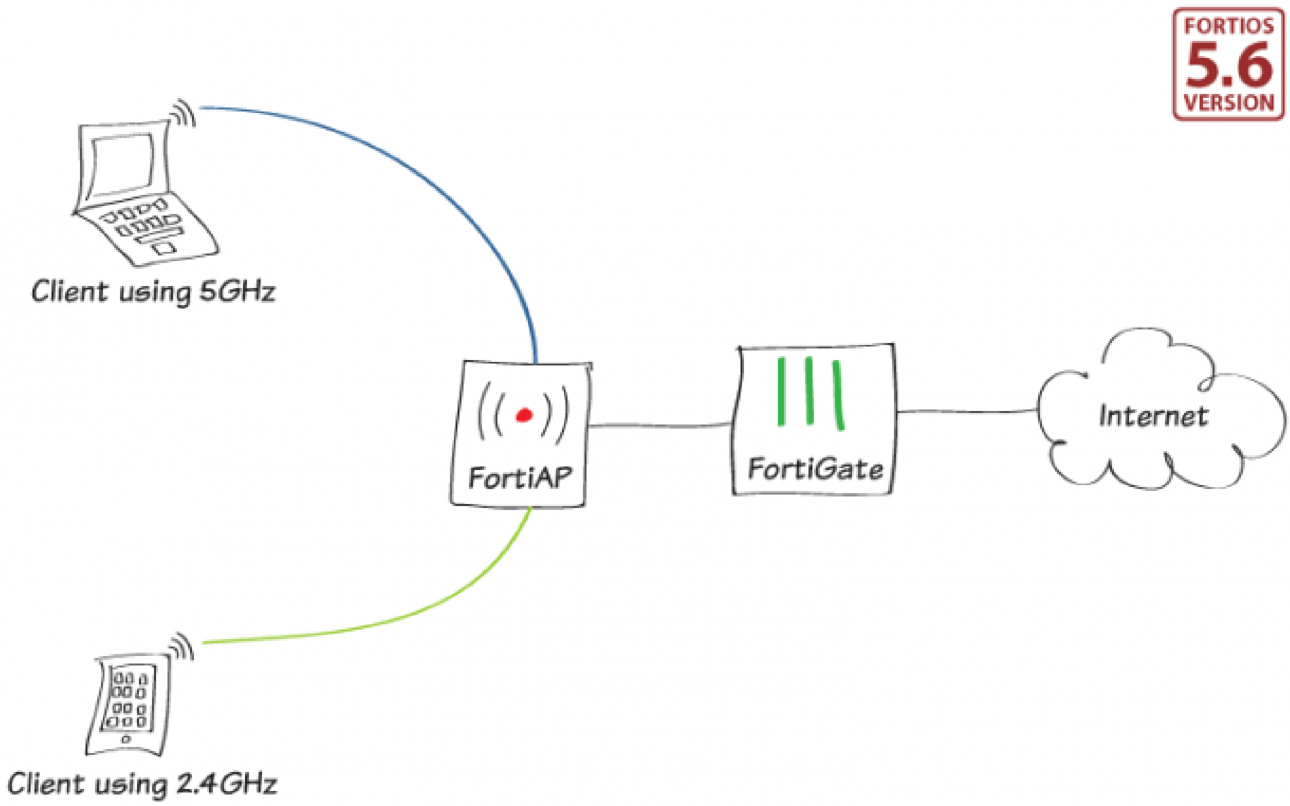
3. Try to connect using an unauthorized device and verify that the connection is rejected.



4. Go to *Monitor* > *WiFi Client Monitor* to view the status of the connected WiFi clients.



Dual-band SSID with optional client load balancing



This example shows you how to configure your FortiAP to broadcast the same SSID on both WiFi bands: 2.4GHz and 5GHz. This example includes information about using client load balancing.

This example uses a FortiAP model with two radios that is configured in your network with an SSID (*MyWiFi*).

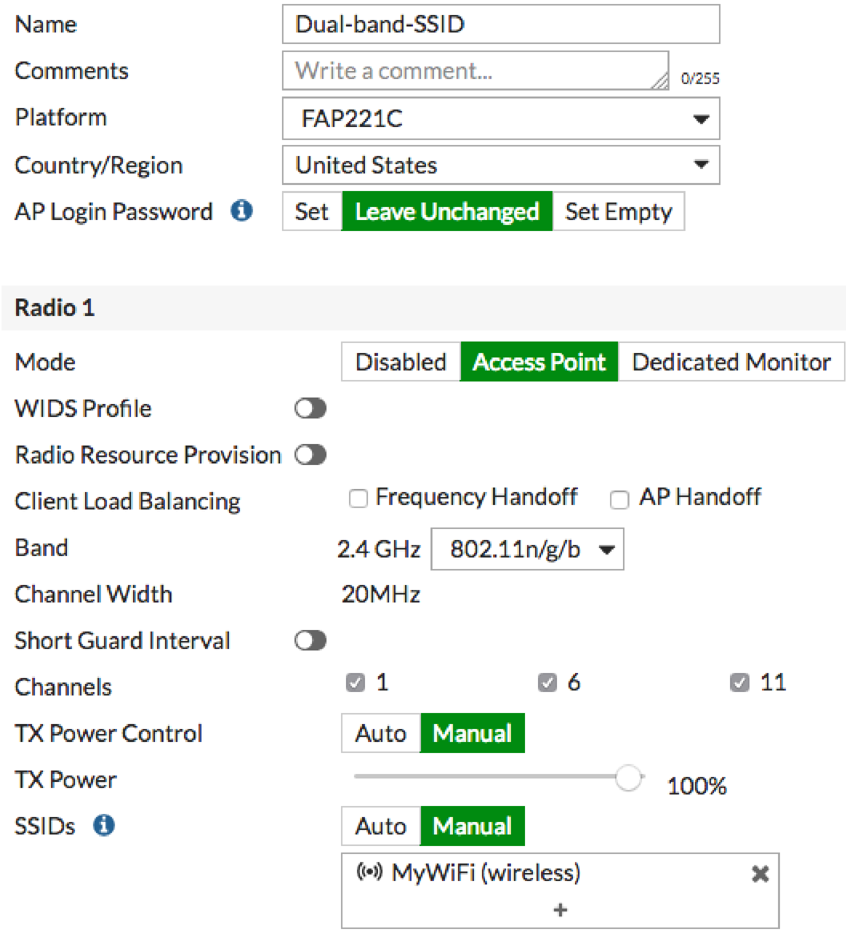
For more information, see Setting up WiFi with a FortiAP (tunnel mode) or Setting up a WiFi Bridge with a FortiAP (bridge mode).

Configuring the dual-band SSID

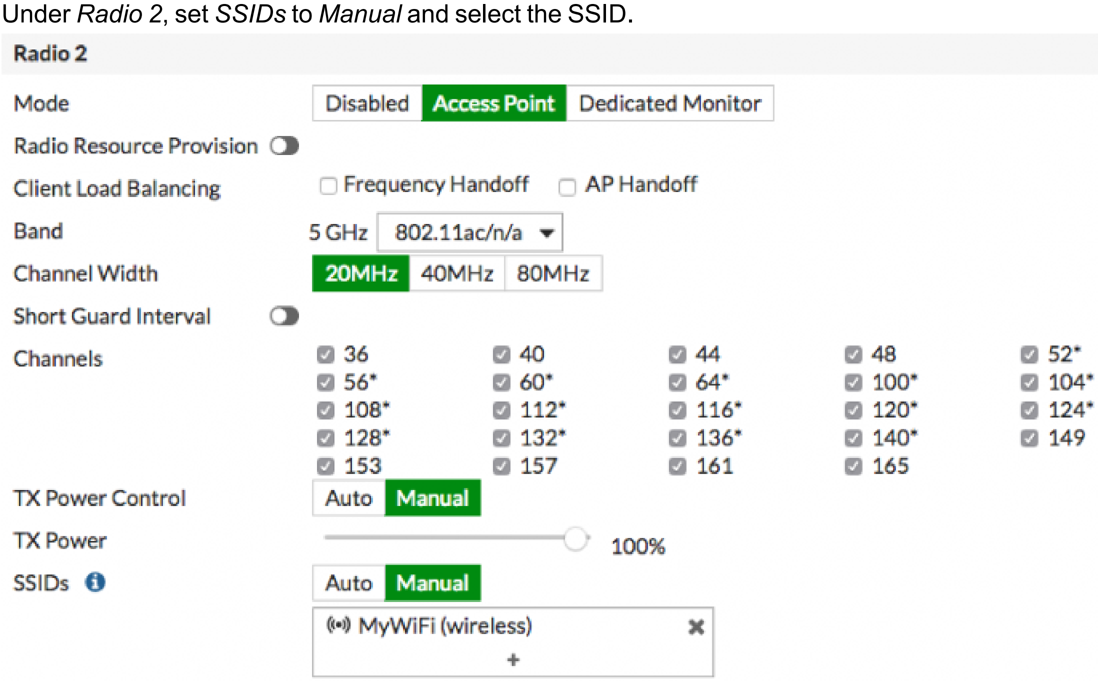
This example uses a FortiAP 221C to broadcast the dual-band SSID with *Radio 1* broadcasting using the 2.4GHz band and *Radio 2* using the 5GHz band.

1. Go to *WiFi & Switch Controller* > *FortiAP Profiles* and create a FortiAP profile.
   Set *Platform* to the model of your FortiAP.
   Set the *Country/Region*.

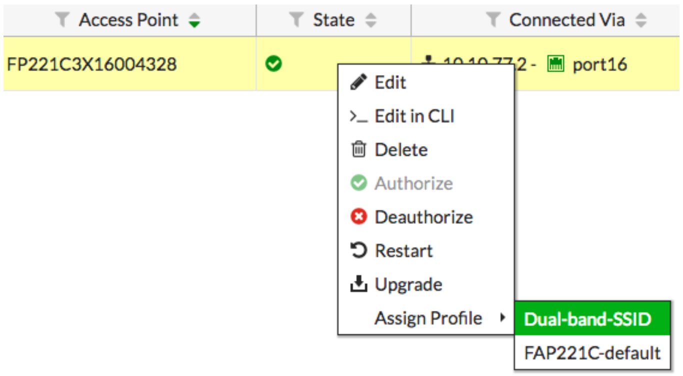
Under *Radio 1*, set *SSIDs* to *Manual* and select the SSID.



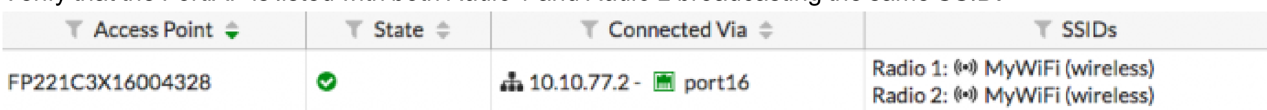
2. Under *Radio 2*, set *SSIDs* to *Manual* and select the SSID.



3. Go to *WiFi & Switch Controller* > *Managed FortiAPs*.
   Right-click the FortiAP, select *Assign Profile*, and set the FortiAP to use your new profile.
   Wait for the *State* column to update and show that the AP is *Online*.

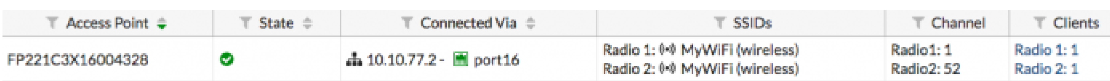


4. Verify that the FortiAP is listed with both *Radio 1* and *Radio 2* broadcasting the same SSID.

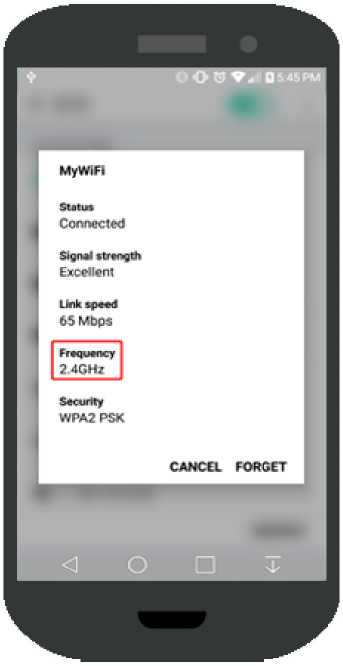


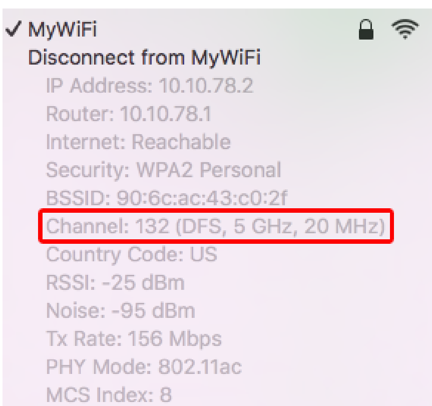
Results

1. Connect to the SSID from different devices.
2. Go to *WiFi & Switch Controller* > *Managed FortiAPs*.
   Clients are shown connecting to the same SSID on both WiFi bands.



3. Check on the devices that the same SSID is used on both bands (in this example, an Android device and Mac OS X computer).





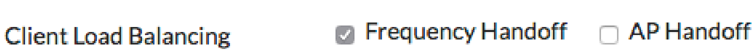
(Optional) Adding client load balancing

In a dual-band SSID configuration, it is best to have most clients using the 5GHz band and leave the 2.4GHz band for clients that do not support 5GHz. Because modern WiFi clients automatically choose the 5GHz band, client load balancing might not be necessary.

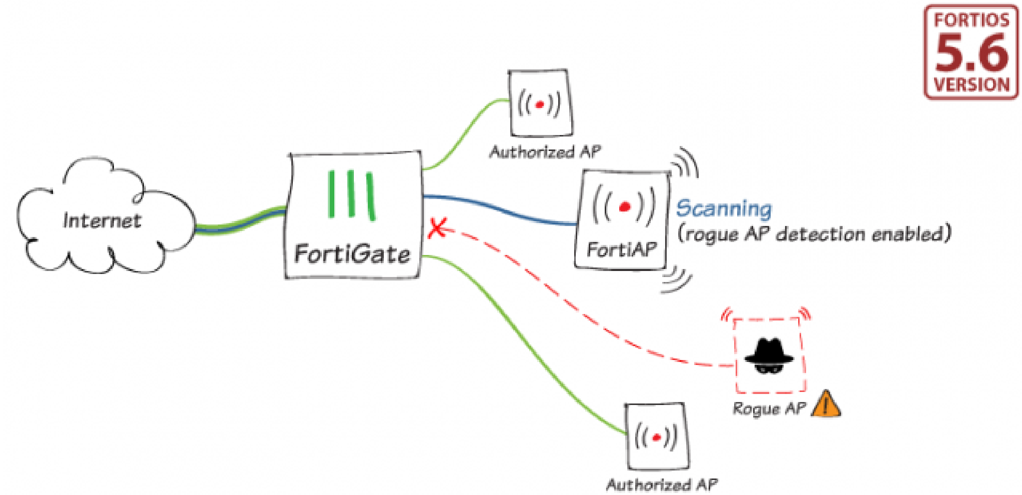
If you see that most clients use the 2.4GHz band, you can use the client load balancing's *Frequency Handoff* method (also known as band-steering). This method helps clients use the 5GHz band if possible.

It is also recommended to use FortiOS 5.6.2 or later because it supports 802.11 k/v/r that newer clients use to select the AP and band.

1. Go to *WiFi & Switch Controller > FortiAP Profiles* and edit the FortiAP profile.
2. Set *Client Load Balancing* to *Frequency Handoff* for both *Radio 1* and *Radio 2*.



Monitoring and suppressing rogue APs



In this example, you learn how to monitor and suppress rogue access points (APs). A rogue AP is an unauthorized AP connected to your wired network ("on-wire").

Before suppressing any AP, confirm that rogue suppression is compliant with the applicable laws and regulations of your region.

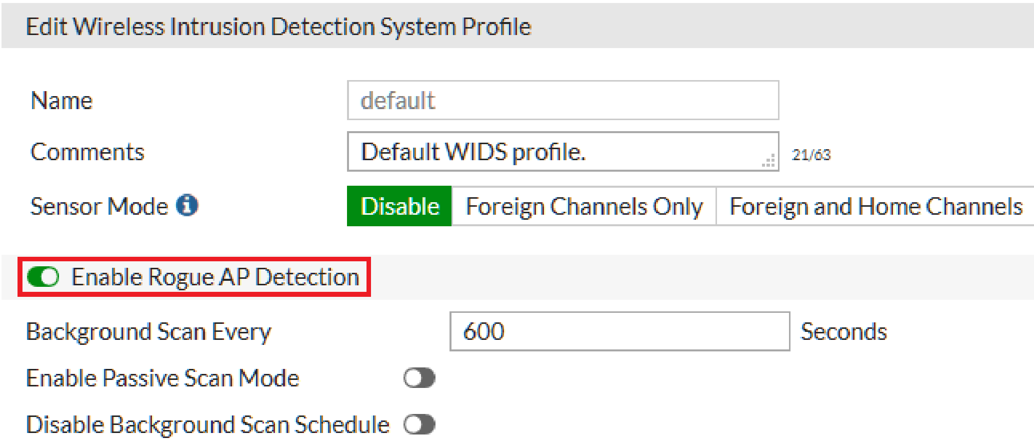
Monitor > Rogue AP Monitor lists discovered access points. You can mark them as *Accepted* or *Rogue APs*. These designations help you track APs. They do not stop anyone from using these APs.

Other APs that are available in the same area might not be rogue. A neighboring AP that has no connection to your network might cause interference but it is not a security threat. In general, only mark unauthorized APs that are on-wire as rogue.

For more information, see FortiWiFi and FortiAP Configuration Guide.

Configuring rogue scanning

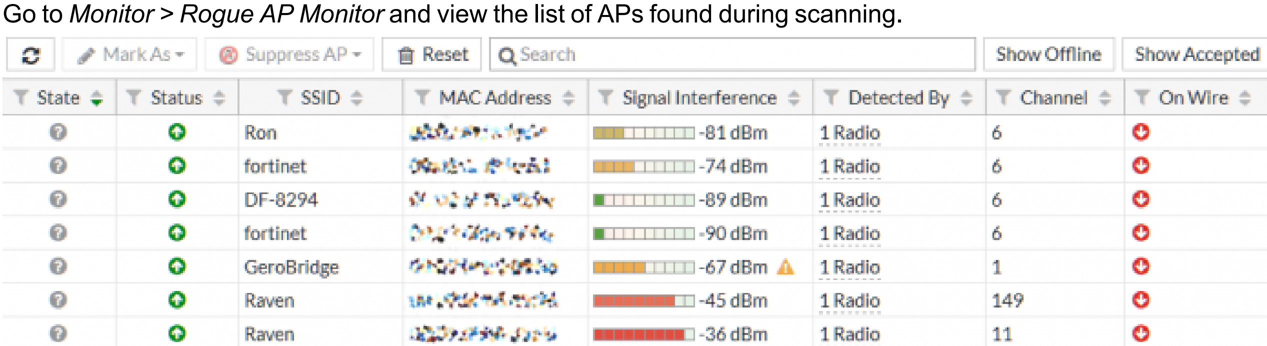
1. On the FortiGate, go to *WiFi & Switch Controller* > *WIDS Profiles* and edit the default profile. Select *Enable Rogue AP Detection*.



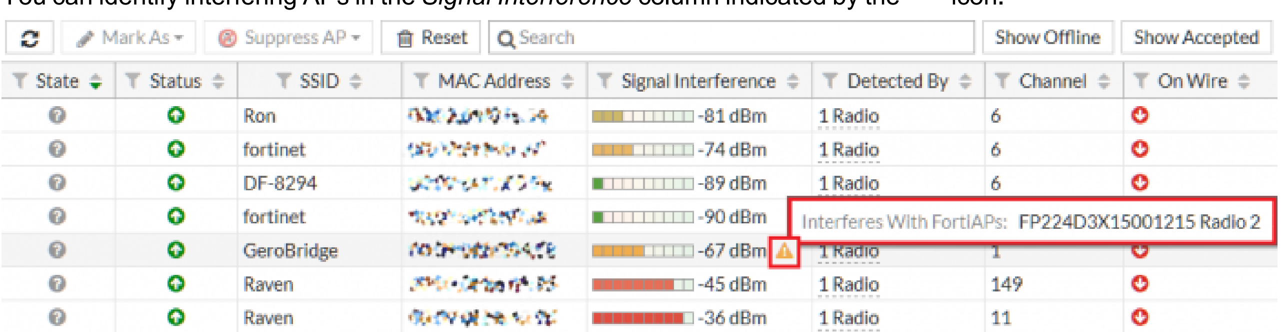
2. Go to *WiFi & Switch Controller* > *FortiAP Profiles* and edit your FortiAP profile. Under *Radio 1*, enable *WIDS Profile* and apply the *default* WIDS profile.

Monitoring rogue APs

1. Go to *Monitor* > *Rogue AP Monitor* and view the list of APs found during scanning.



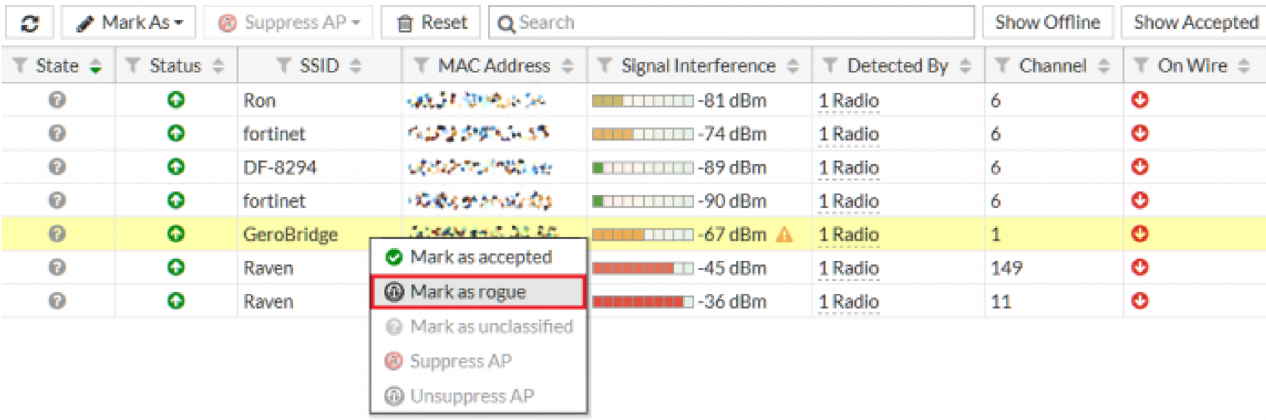
2. You can identify interfering APs in the *Signal Interference* column indicated by the icon.



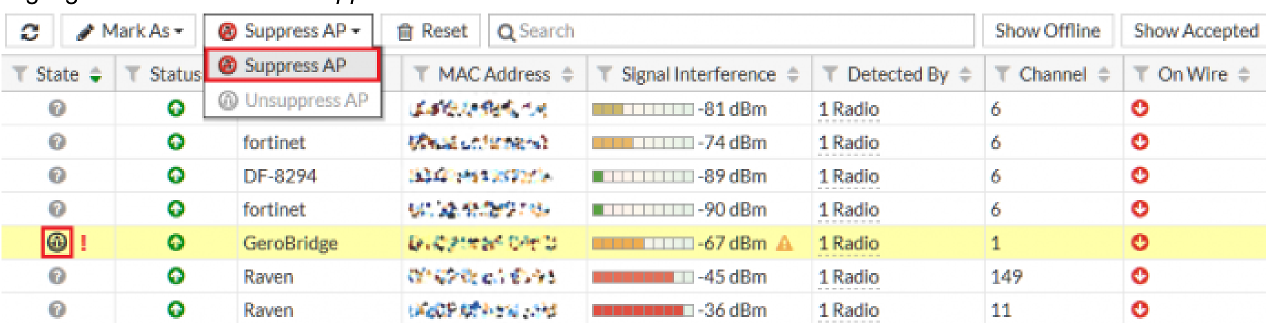
Suppressing rogue APs

To suppress a rogue AP, you must first mark the AP as rogue.

1. Right-click the AP and select *Mark as rogue*.

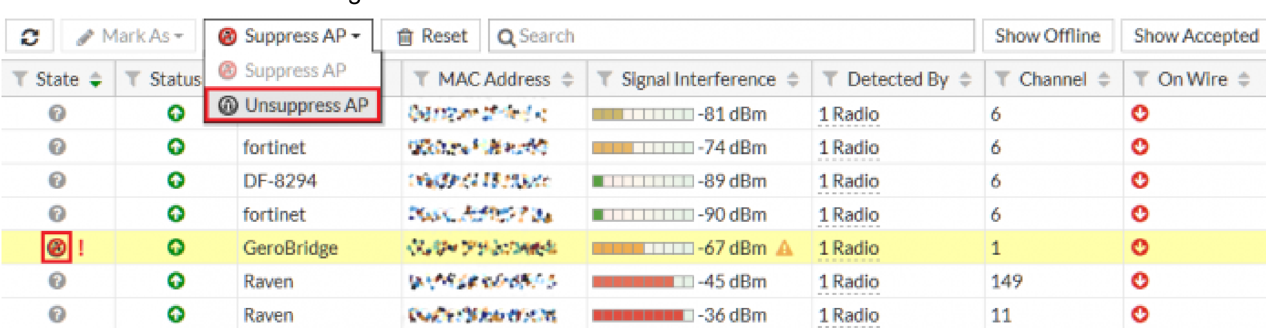


2. Highlight the AP and select *Suppress AP*.

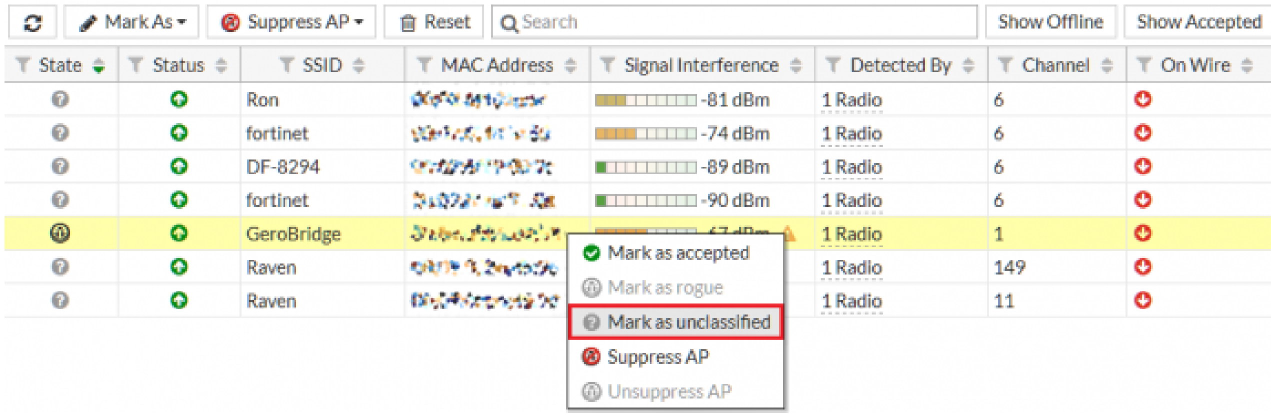


Reverting a suppressed AP

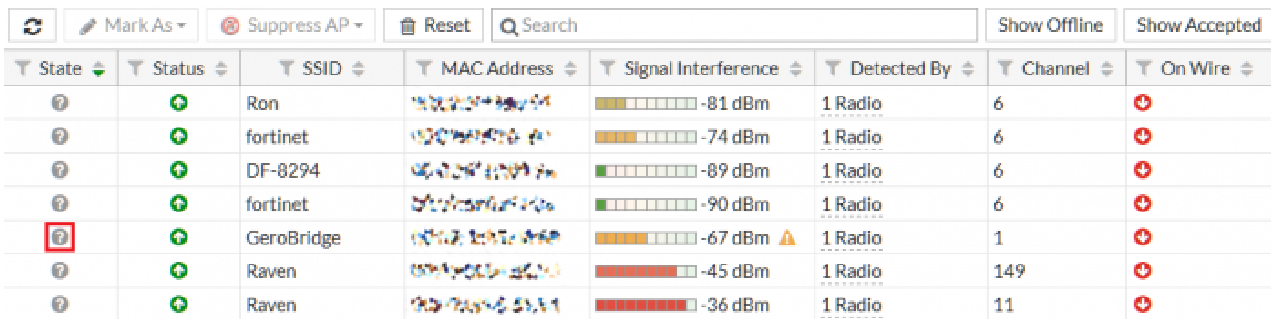
1. Highlight the AP and select *Unsuppress AP*.
   The AP remains identified as rogue.



2. To revert the rogue designation, right-click the AP and select *Mark as unclassified*.

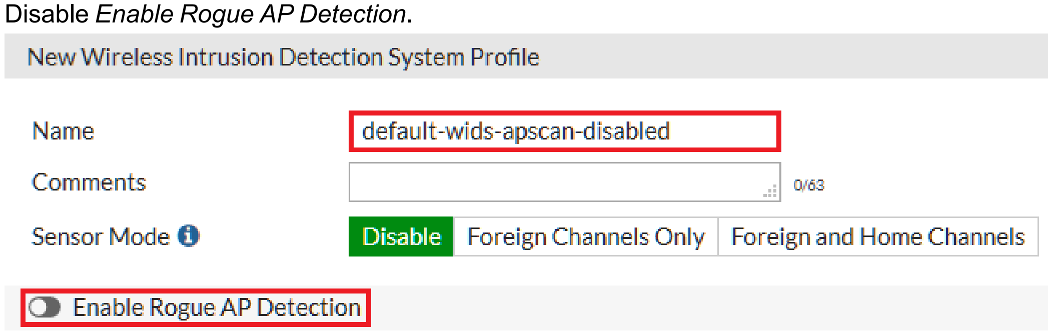


3. An unclassified AP appears with a ? icon in the *State* column.

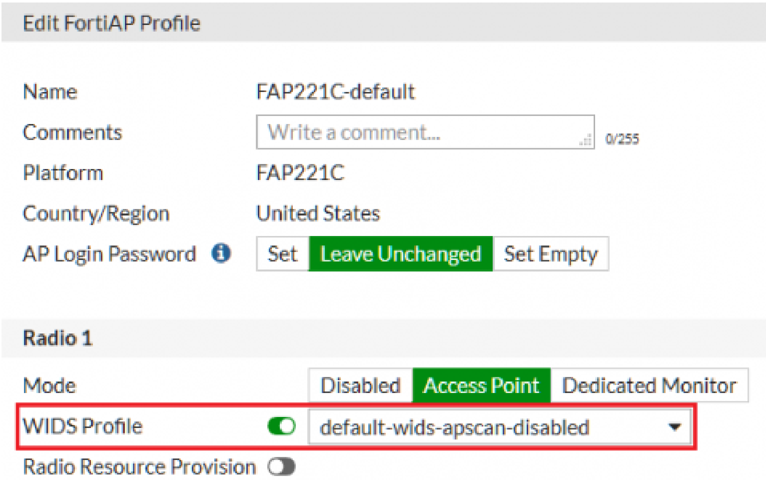


Exempting an AP from rogue scanning

1. Go to *WiFi & Switch Controller > WIDS Profiles* and create a new WIDS profile.
2. Disable *Enable Rogue AP Detection*.



3. Go to *WiFi & Switch Controller > FortiAP Profiles* and select the FortiAP profile. Enable *WIDS Profile* and select that profile.

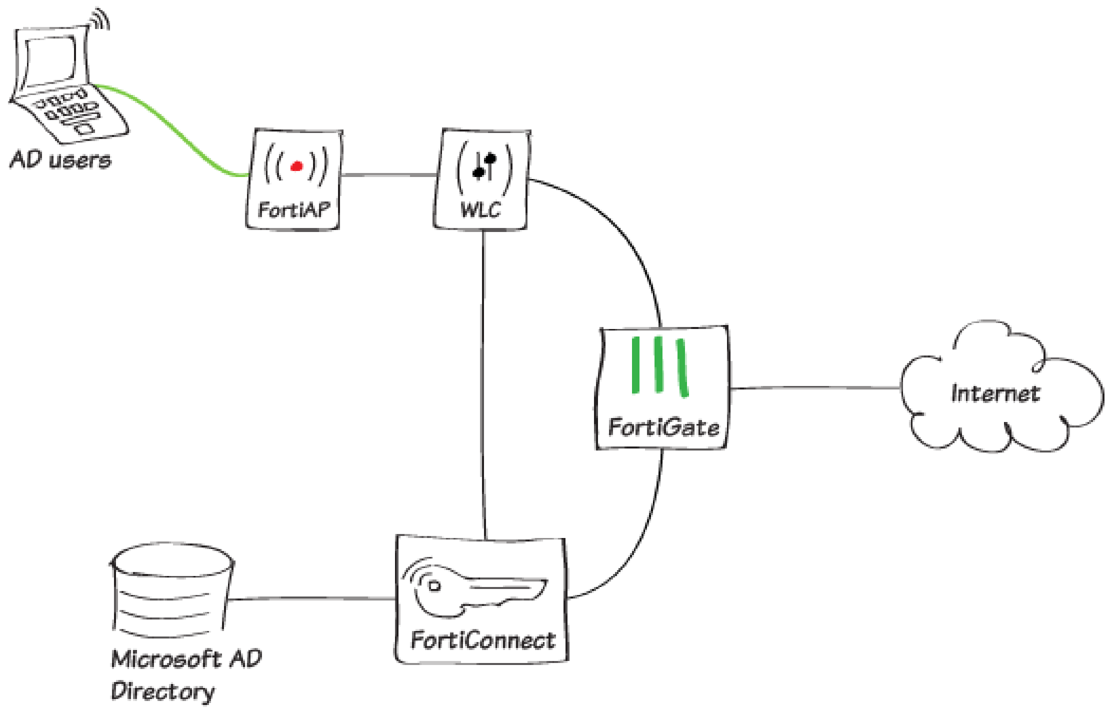


Rogue AP Monitor icons

The *Rogue AP Monitor* page uses the following icons:

Column	Icon + Description
State	AP is detected but not yet classified. AP is accepted. AP is marked as rogue, but unsuppressed. AP is marked as rogue, but suppressed.
Status	AP is online and active. AP is inactive.
Signal Interference	AP signal interferes with a managed AP. AP signal interference ranges from low (green) to high (red), measured in dBm.
On Wire	AP is suspected rogue. AP is not a suspected rogue.

FortiConnect guest on-boarding using RSSO



This example shows using RADIUS Single Sign-On (RSSO), FortiGate, FortiConnect (for guest portal and RADIUS authentication), and FortiWLC (for providing wireless access). Captive portal users are mapped to user groups on the FortiGate and security policies are applied based on these user groups.

Authentication flow:

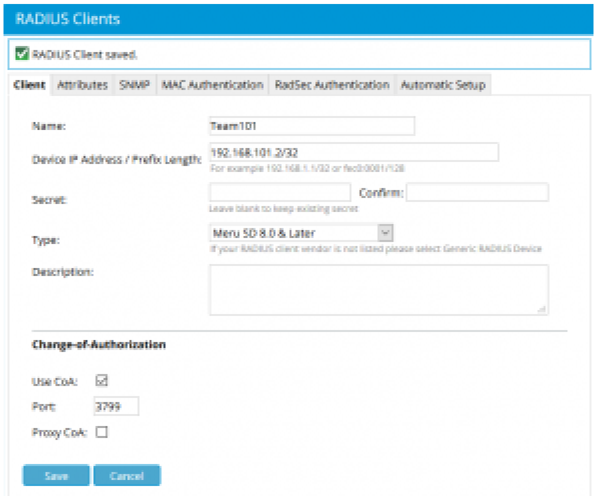
1. User authenticates to WLC via a security profile where a RADIUS authentication is established (802.1x / captive portal).
2. WLC validates user credentials at RADIUS server.
3. RADIUS servers authenticate user for access and sends access-accept back to WLC to allow connection (including class attribute).
4. WLC allows device/user to establish wireless connection.
5. WLC sends accounting packets to RADIUS server.
6. RADIUS server proxies those accounting packets and forwards them to FortiGate.
7. FortiGate registers user and maps the user to an RSSO-user group.

Registering the WLC as a RADIUS client on the FortiConnect

1. On FortiConnect, go to *Devices* > *RADIUS clients* and add your WLC as a RADIUS client.
   Enter a *Name* for the WLC and enter its *Device IP Address*.

Enter a *Secret* that will be shared between FortiConnect and WLC.

Set *Type* to *Meru SD 8.0 & Later*.

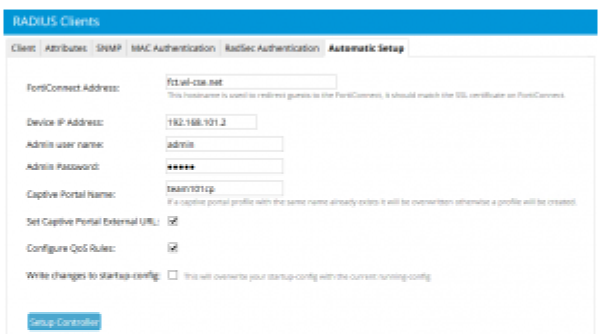


2. Go to the *Automatic Setup* tab and enter the information for the FortiConnect to perform WLC configuration.
   Enter the *Device IP Address* of the WLC.

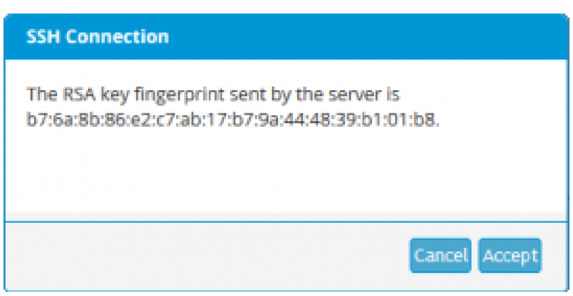
   Enter an Admin user name and password.

   Enter a *Captive Portal Name* that will be used to create/name the *Captive Portal Profile* at WLC.

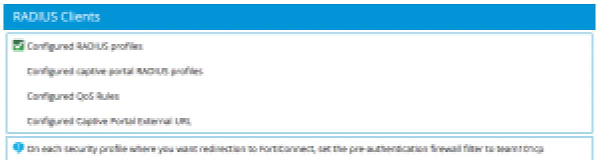
   This creates a RADIUS profile, a captive portal profile, and a Quality of Service (QoS) rule to allow access to the guest portal on the WLC. The QoS rule is similar to a firewall rule that allows the wireless device to be redirected to FortiConnect captive portal before the user or device is authenticated.



3. Click *Setup Controller*.
   FortiConnect establishes an SSH connection to the WLC. Wait for the configuration to finish.

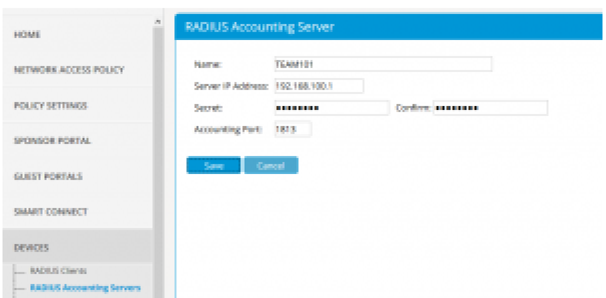


4. When the configuration is done, a message similar to this appears.



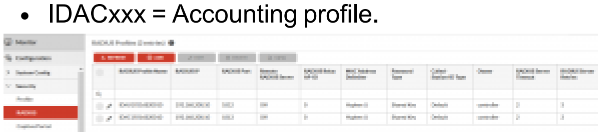
Registering the FortiGate as a RADIUS accounting server on the FortiConnect

1. On FortiConnect, go to *Devices > RADIUS Accounting Servers* and add your FortiGate a RADIUS accounting server.
   Enter a *Name* and the *Server IP Address* of the FortiGate that matches the interface that listens to the RADIUS accounting messages.
   Enter a *Secret* that will be shared between FortiConnect and the FortiGate.
   Set *Accounting Port* to the RADIUS accounting port *1813*.

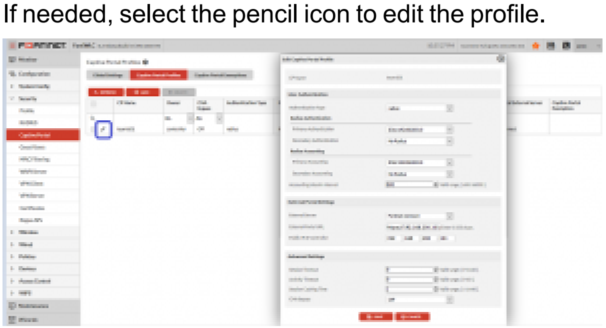


Validating the WLC configuration created from FortiConnect

1. On the WLC, go to *Configuration > Security > RADIUS* and validate that FortiConnect has created the two RADIUS profiles.
   Verify that the automatic setup process on FortiConnect has created the two RADIUS profiles.
   - IDAUxxx = Authentication profile.
   - IDACxxx = Accounting profile.

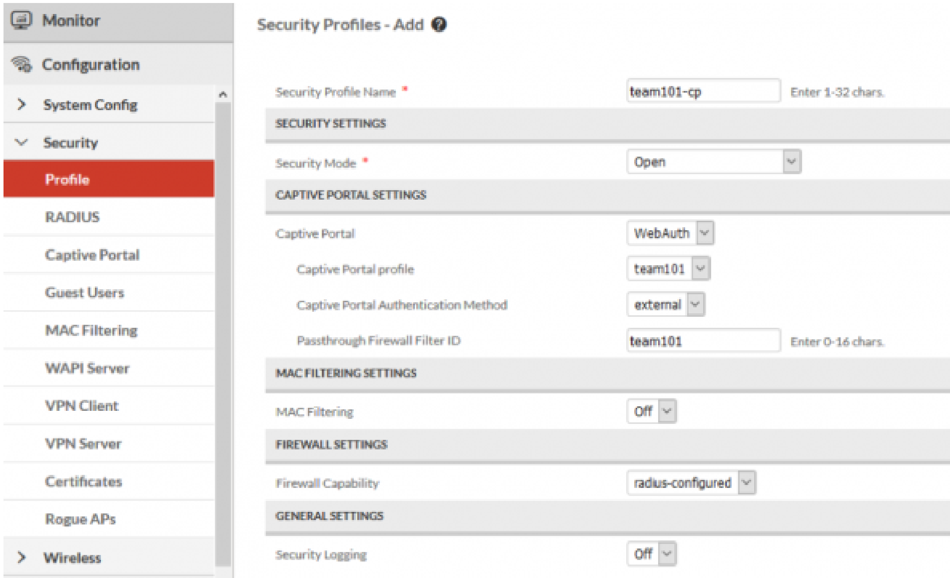


2. Go to *Configuration > Security > Captive Portal* and select the *Captive Portal Profiles* tab.
   Verify that the *Captive Portal* profile is created.
   If needed, select the pencil icon to edit the profile.



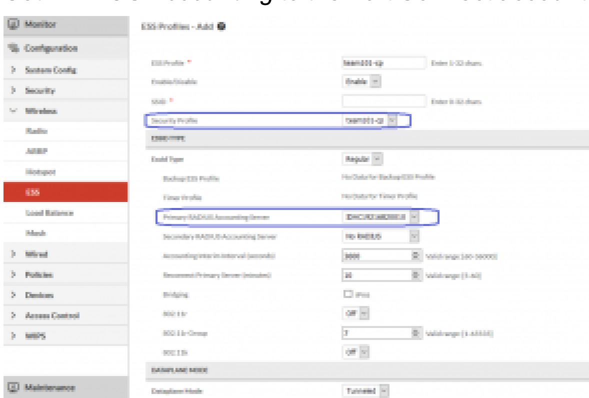
Creating a security profile on the WLC

1. On the WLC, go to *Configuration* > *Security* > *Profile* and click *ADD* to create a new security profile.
   Enter the following information shown in this example.



Creating the wireless ESS profile on the WLC

1. On the WLC, go to *Configuration* > *Wireless* > *ESS* and select *ADD* to create a new ESS profile.
   Enter a name for the *ESS Profile* and *SSID*.
   Set *Security Profile* to the newly created security profile.
   Set *RADIUS Accounting* to the FortiConnect accounting profile (IDACxxxx).

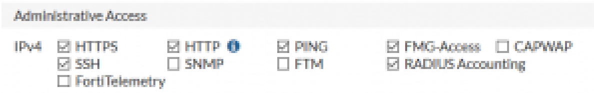


2. Select *SAVE* and accept the message that this is only for Virtual Cell AP's (the default option in WLC).

Enabling RADIUS accounting listening on the FortiGate

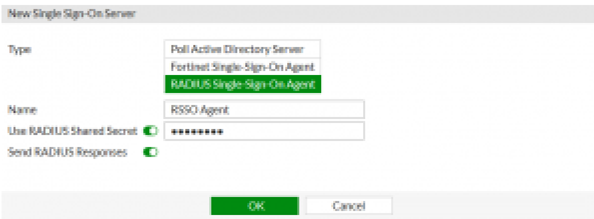
1. On the FortiGate, go to *Network* > *Interfaces* and edit the interface that matches the IP address added as RADIUS Accounting Server in FortiConnect.

2. Enable *RADIUS Accounting*.



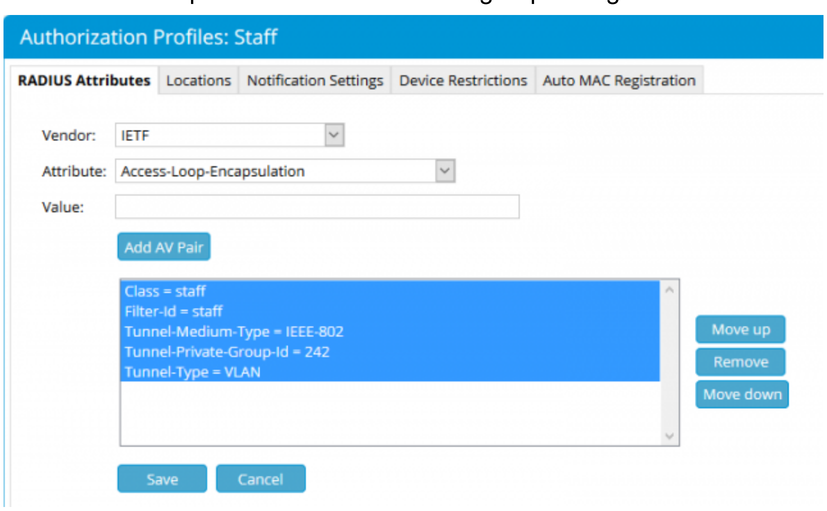
Configuring the RSSO Agent on the FortiGate

1. On the FortiGate, go to *User & Device* > *Single Sign-On* and create a new agent.
   Set *Type* to *RADIUS Single-Sign-On Agent*.
   Enable *Use RADIUS Shared Secret* and enter a shared secret.
   Enable *Send RADIUS Responses*.



2. Go to *User & Device* > *User Groups* and create a new user group.
   Set *Type* to *RADIUS Single Sign-On (RSSO)* and enter a *RADIUS Attribute Value* (case-sensitive) that matches the FortiConnect attribute. This example uses *staff* to identify a staff user.

3. On FortiConnect, set the same RADIUS attribute for the *Authorization Profile*.
   Set the *Attribute Value* to use *Class*.
   FortiConnect maps the user to the account group during the backend authentication to Microsoft AD.



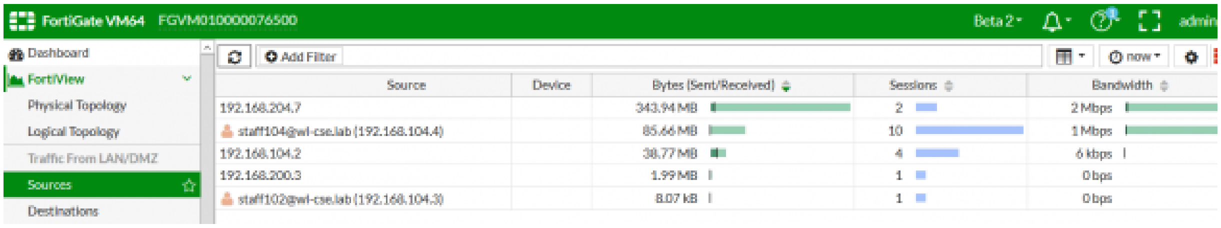
4. On FortiGate, open the *CLI Console* and enter the following commands:

```
config user radius
```

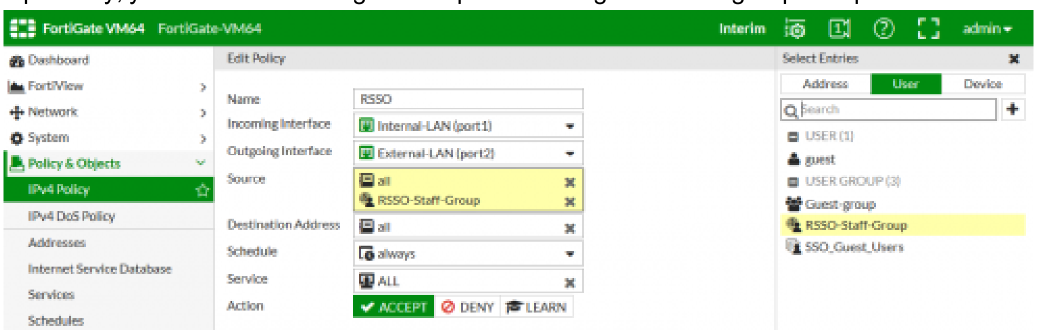
```
    edit "RSSO Agent"
        set rsso-endpoint-attribute "User-Name"
    next
end
```

Results

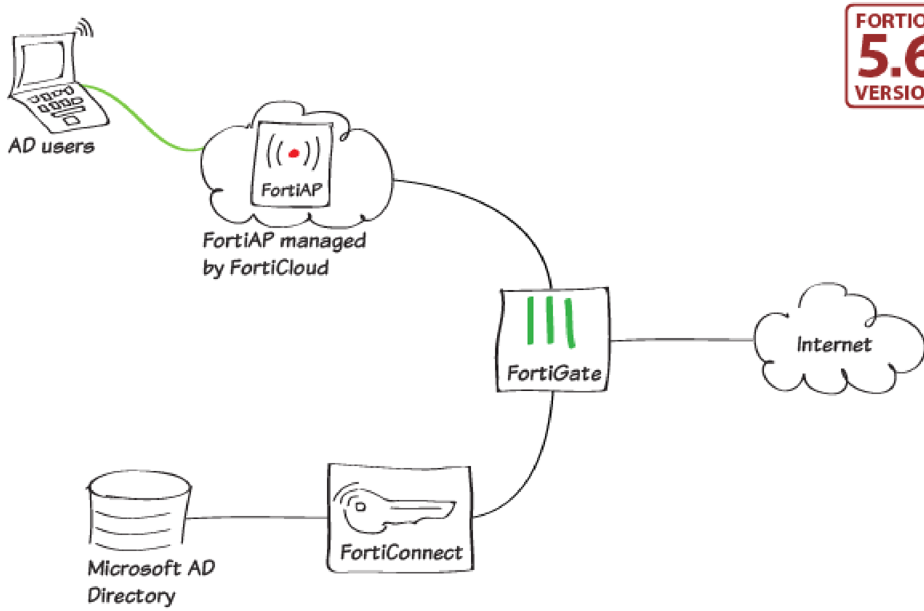
1. On FortiGate, go to *FortiView* > *Traffic From LAN/DMZ* > *Sources* to view users from the staff member group who have logged in using the captive portal.



2. Optionally, you can start creating firewall policies using the RSSO group as a parameter.



FortiConnect as a RADIUS server in FortiCloud

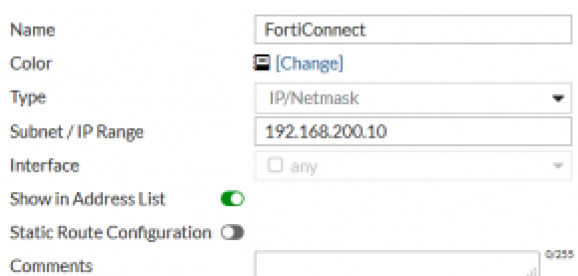


This example uses a local on-premise FortiConnect as a RADIUS server for a FortiCloud-based captive portal network. A FortiGate is used to allow access from FortiCloud to FortiConnect.

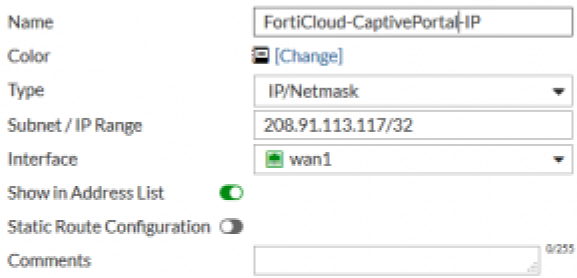
This example requires FortiAP to be already in your FortiCloud inventory and at least one configured AP network.

Configuring FortiCloud to access FortiConnect

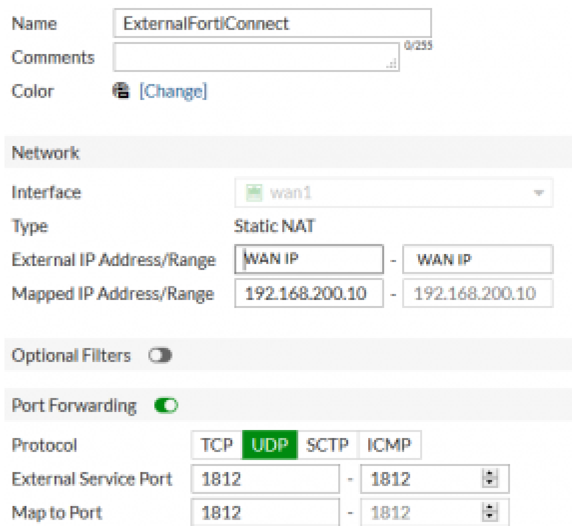
1. On the FortiGate go to *Policy & Objects* > *Addresses* and create a new address for FortiConnect.



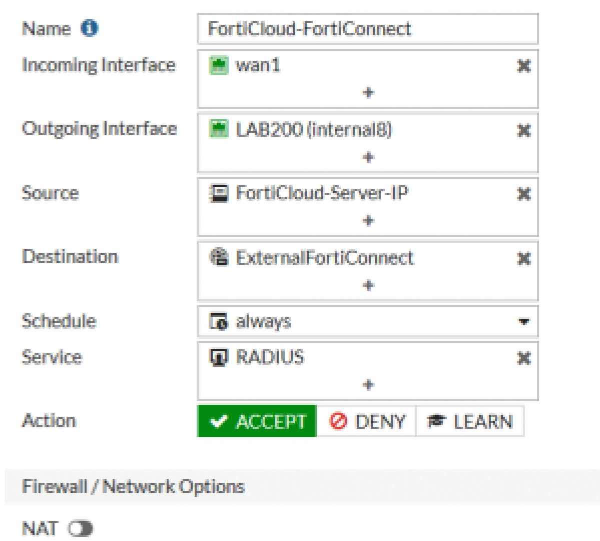
2. Create another address for FortiCloud used by the captive portal.
   In this example, *208.91.113.117/32* is used by *apau.forticloud.com*.



3. Go to *Policy & Objects* > *Virtual IPs* and create a virtual IP pointing from your WAN to the local FortiConnect.

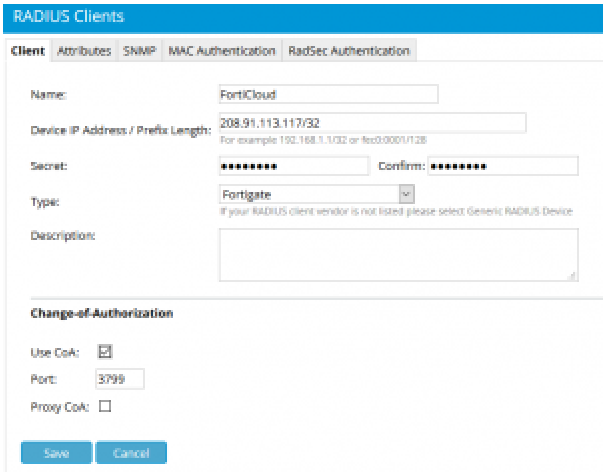


4. Go to *Policy & Objects* > *IPv4 Policy* and create a policy to allow RADIUS requests from FortiCloud to FortiConnect.



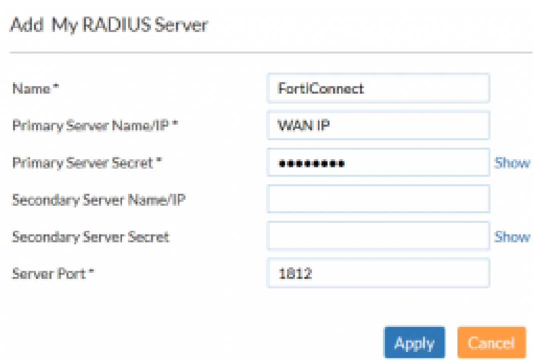
Configuring FortiCloud as a RADIUS client on FortiConnect

1. On FortiConnect, go to *Devices* > *RADIUS Clients* and select *Add RADIUS Client*.
   Enter a *Name*.
   Set *Device IP Address/Prefix Length* to *208.91.113.117/32* that is used by *apau.forticloud.com*.
   Enter a shared *Secret* to be used between FortiCloud and FortiConnect.



Configuring FortiConnect as a RADIUS server on FortiCloud

1. In FortiCloud, go to *AP Network* > *"your AP network"* > *Configure* > *My RADIUS Server* and select *Add My RADIUS Server*.
   Enter a *Name*.
   Set *Primary Server Name/IP* to the WAN IP address.
   Enter the same shared secret as entered on FortiConnect.

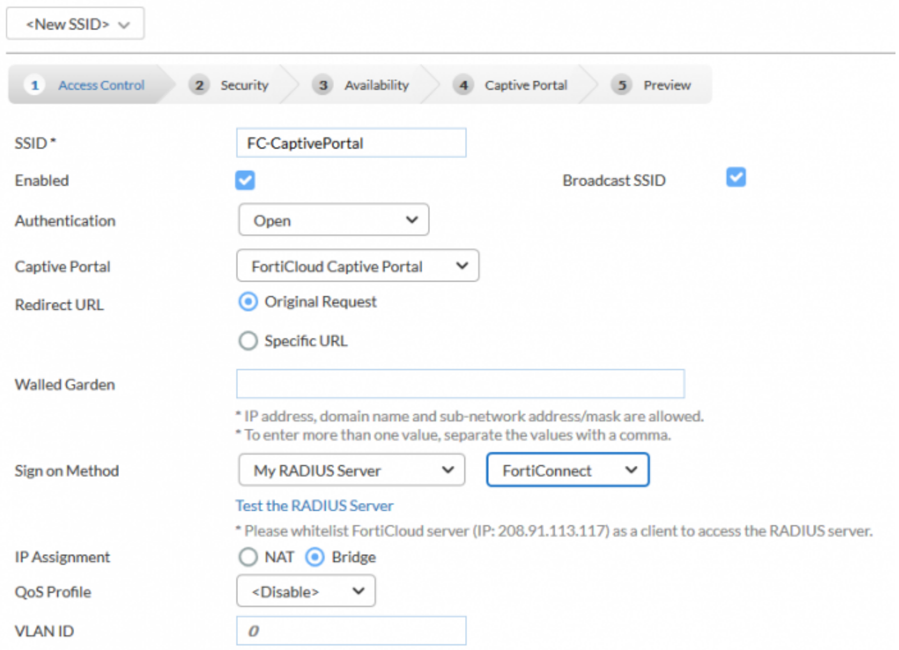


Creating a new SSID on FortiCloud

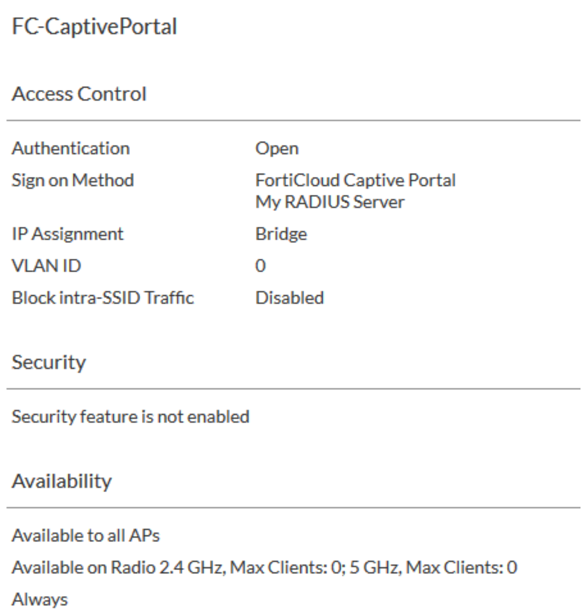
1. On FortiCloud, go to *SSIDs* and select *Add SSID*.
   Enter the name and enable the SSID.
   Set *Captive Portal* to *FortiCloud Captive Portal*.
   Set *Sign on Method* to use *FortiConnect* as the RADIUS server.

Note the IP address to use for FortiCloud access.

If necessary, configure the settings in the other tabs: *Security*, *Availability*, and *Captive Portal*.

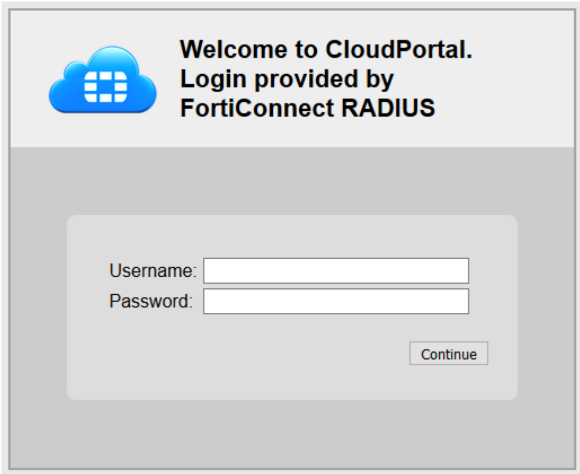


2. In the *Preview* tab, select *Apply*.

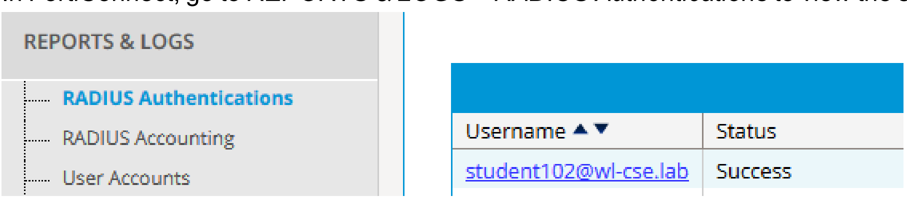


Results

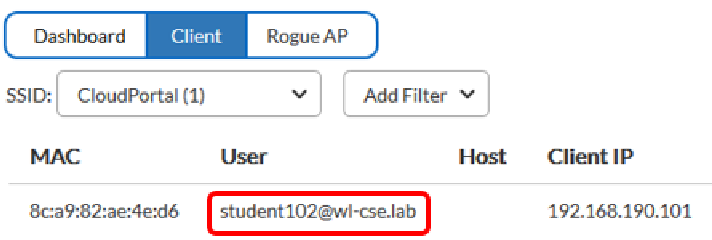
1. Use the Portal to log in to the FortiCloud Portal.



2. In FortiConnect, go to *REPORTS & LOGS > RADIUS Authentications* to view the successful authentication.



3. In FortiCloud, go to *AP Network > "your AP network" > Monitor > Client* to view the client and verify that the user is shown.



Replacing the Fortinet_Wifi certificate

These instruction apply to FortiWiFi devices using internal WiFi radios and FortiGate/FortiWiFi devices configured as WiFi Controllers that manage FortiAP devices, and have WiFi clients that are connected to WPA2-Enterprise SSID and authenticated with local user groups.

On FortiOS, the built-in *Fortinet_Wifi* certificate is a publicly signed certificate that is only used in WPA2-Enterprise SSIDs with local user-group authentication. The default WiFi certificate configuration is:

```
config system global
   set wifi-ca-certificate "Fortinet_Wifi_CA"
   set wifi-certificate "Fortinet_Wifi"
```

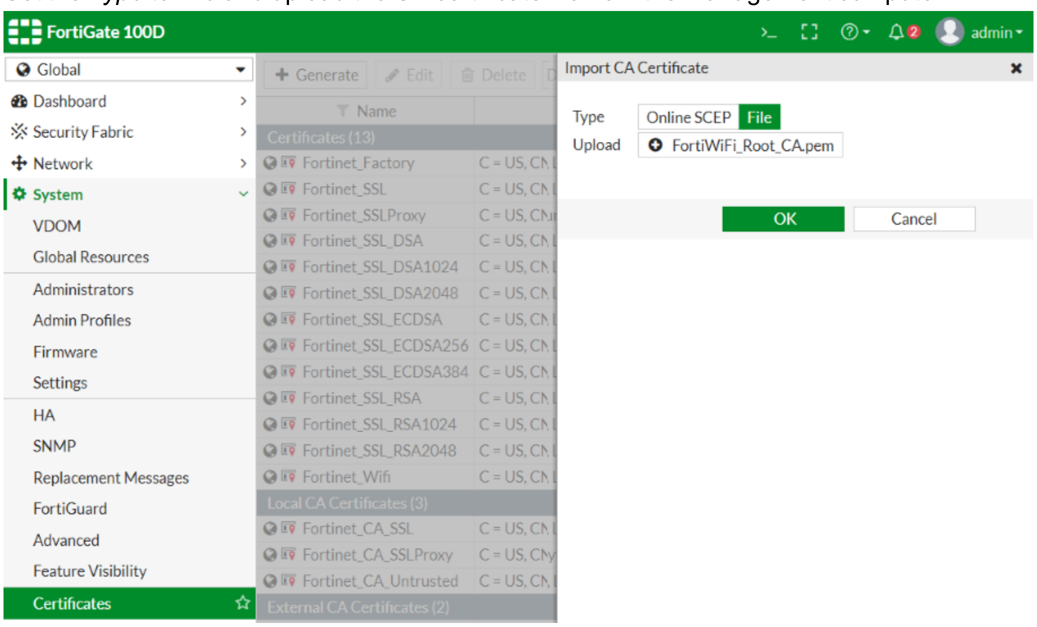
```
end
```

WiFi administrators must consider the following factors:

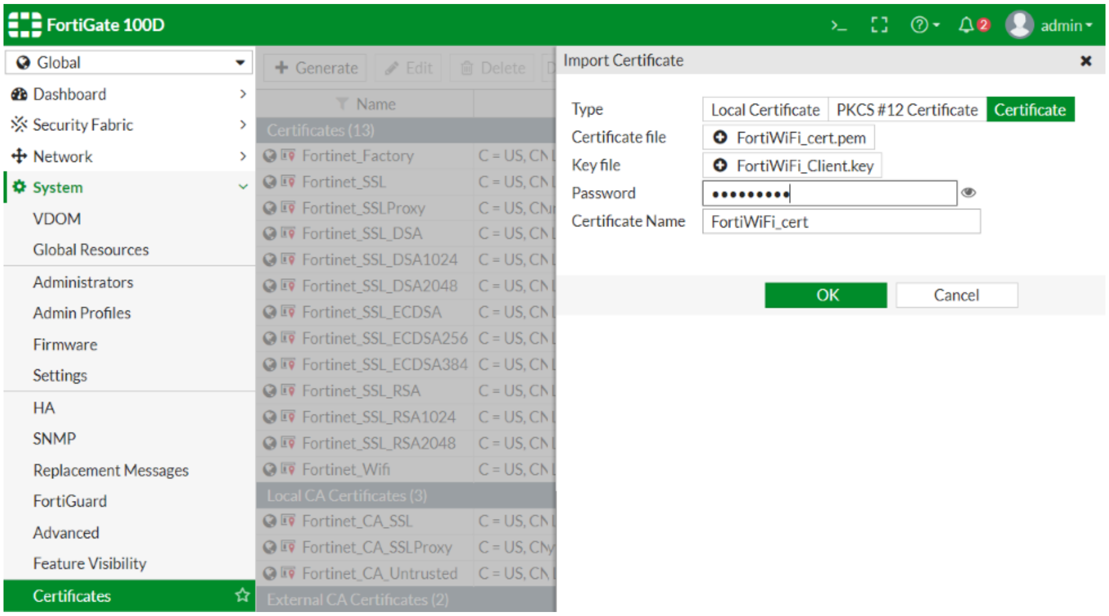
- The *Fortinet_Wifi* certificate is issued to *Fortinet Inc.* with the common name (CN) *auth-cert.fortinet.com*. If an organization requires its own CN in their WiFi deployment, they must replace it with their own certificate.
- The *Fortinet_Wifi* certificate has an expiry date. When it is expires, renew or replace it with a new certificate.

To replace the Fortinet_Wifi certificate:

1. Get new certificate files, including a root CA certificate, a certificate signed by the CA, and the corresponding private key file.
   You can purchase a publicly signed certificate from a commercial certificate service provider or generate a self-signed certificate.
2. Import the new certificate files into FortiOS:
   a. On the FortiGate, go to *System* > *Certificates*.
      If VDOMs are enable, got to *Global* > *System* > *Certificates*.
   b. Click *Import* > *CA Certificate*.
   c. Set the *Type* to *File* and upload the CA certificate file from the management computer.



   d. Click *OK*.
      The imported CA certificate name is *CA_Cert_N* (or *G_CA_Cert_N* if VDOMs are enabled), where *N* starts at *1* and increments for each imported certificate, and *G* stands for global range.
   e. Click *Import* > *Local Certificate*.
   f. Set *Type* to *Certificate*, upload the *Certificate file* and *Key file*, enter the *Password* and enter the *Certificate Name*.



g. Click *OK*.
The *Certificates* page lists the imported certificates.

3. Change the WiFi certificate settings:

```
config system global
    set wifi-ca-certificate <name of the imported CA certificate>
    set wifi-certificate <name of the imported certificate signed by the CA>
end
```

If necessary, use the factory default certificates to replace the certificates:

```
config system global
    set wifi-ca-certificate "Fortinet_CA"
    set wifi-certificate "Fortinet_Factory"
end
```

As the factory default certificates are self-signed, WiFi clients need to accept it at the connection prompt or import the *Fortinet_CA* certificate to validate it.

If the built-in *Fortinet_Wifi* certificate has expired and not been renewed or replaced, WiFi clients can still connect to the WPA2-Enterprise SSID with local user-group authentication by ignoring warning messages or bypassing *Validate server certificate* (or similar) options.