# FortiOS - Cookbook

Version 6.0.0

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

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

**FORTINET BLOG**
https://blog.fortinet.com

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

**FORTINET TRAINING & CERTIFICATION PROGRAM**
https://www.fortinet.com/training-certification

**NSE 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

June 24, 2020
FortiOS 6.0.0 Cookbook
01-600-000000-20200624

# TABLE OF CONTENTS

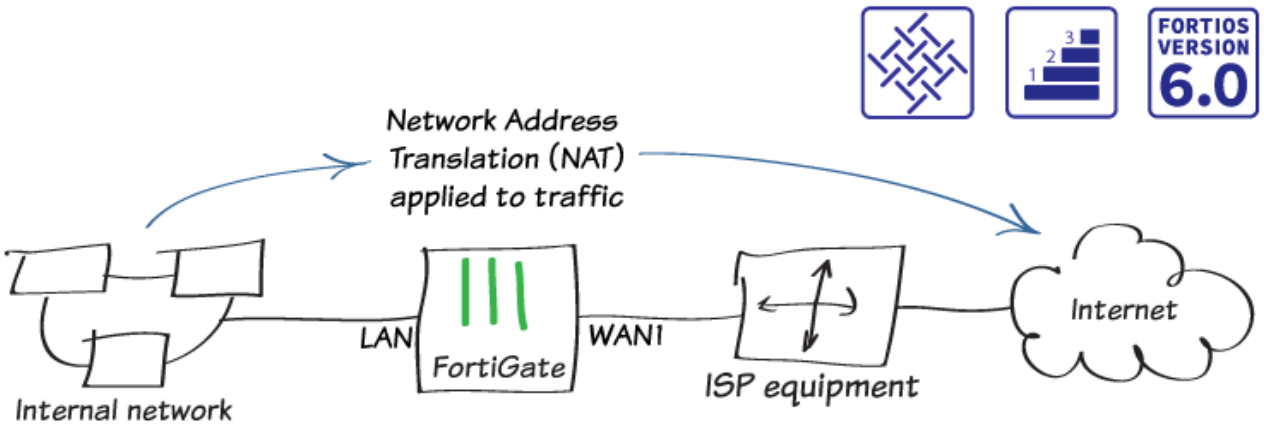
# Change log

| Date | Change Description |
|---|---|
| 2019-03-04 | Initial release. |
| 2019-05-09 | Added Blocking malicious domains using threat feeds on page 119. |
| 2019-05-22 | Added Replacing the Fortinet_Wifi certificate on page 348. |
| 2019-06-10 | Updated London FortiDNS server IP address in DNS Filtering on page 208 and related topics. |
| 2019-09-24 | Updated to remove outdated topic. |
| 2019-11-08 | Added video links. |
| 2020-03-24 | Added SSL VPN quick start on page 246 section. |
| 2020-06-24 | Added SSL VPN for remote users with MFA and user sensitivity on page 333. |

# Getting started

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

## Installing a FortiGate in NAT mode



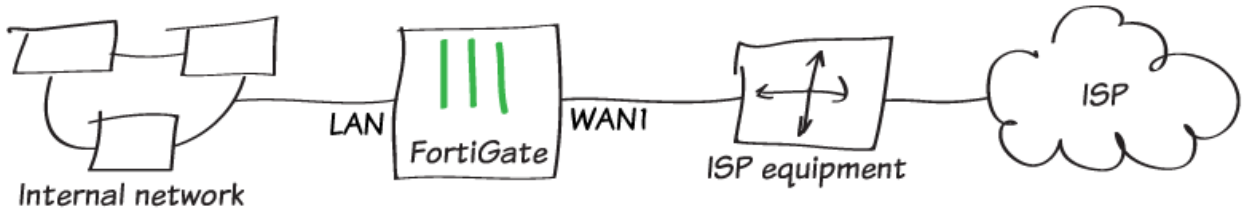

In this example, you connect and configure a new FortiGate in NAT mode, to securely connect a private network to the Internet.

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

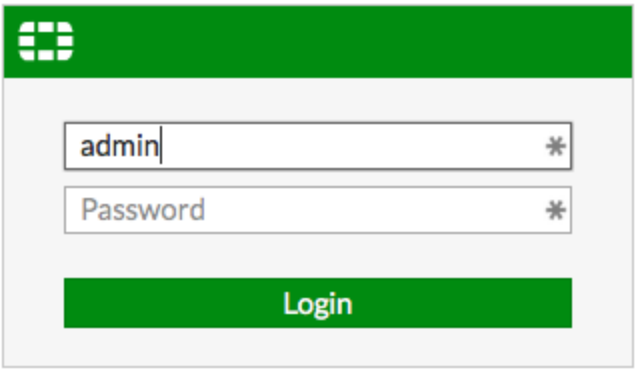
NAT mode is the most commonly used operating mode for a FortiGate.

### 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 the example, port 3).

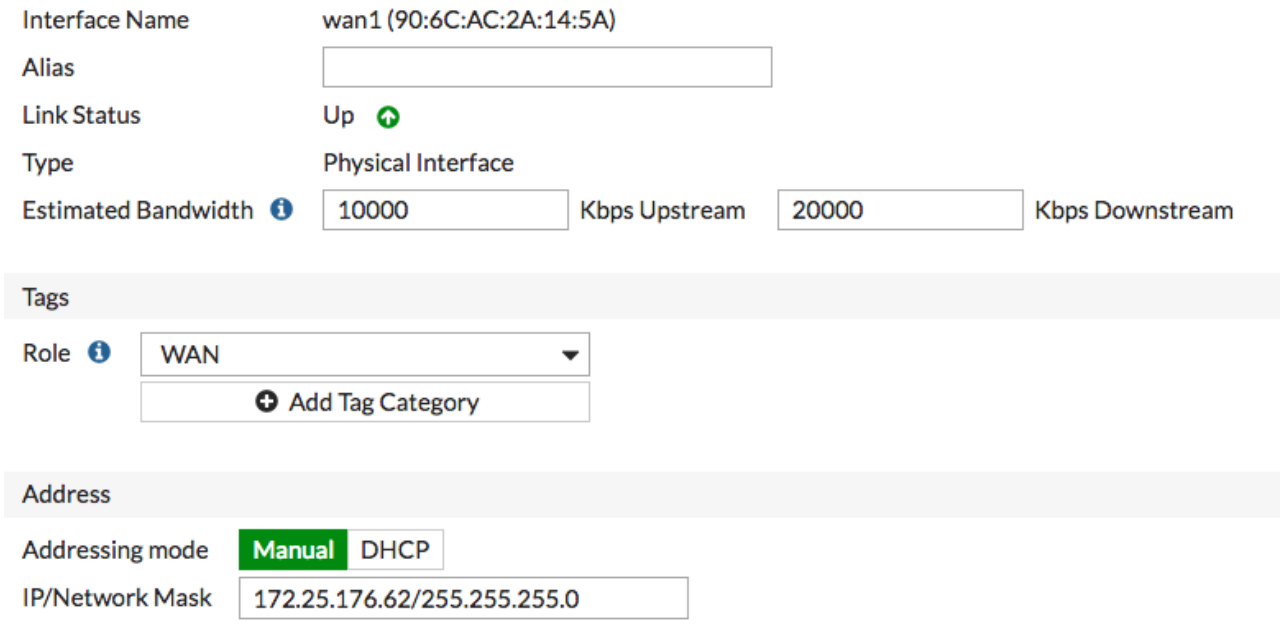


3. Power on the ISP equipment, the FortiGate, and the PC on the internal network.
4. Use the PC to connect to the FortiGate GUI using either FortiExplorer or an Internet browser. For more information about connecting to the GUI, see the QuickStart Guide for you FortiGate model.
5. Log in using an admin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




## Configuring interfaces

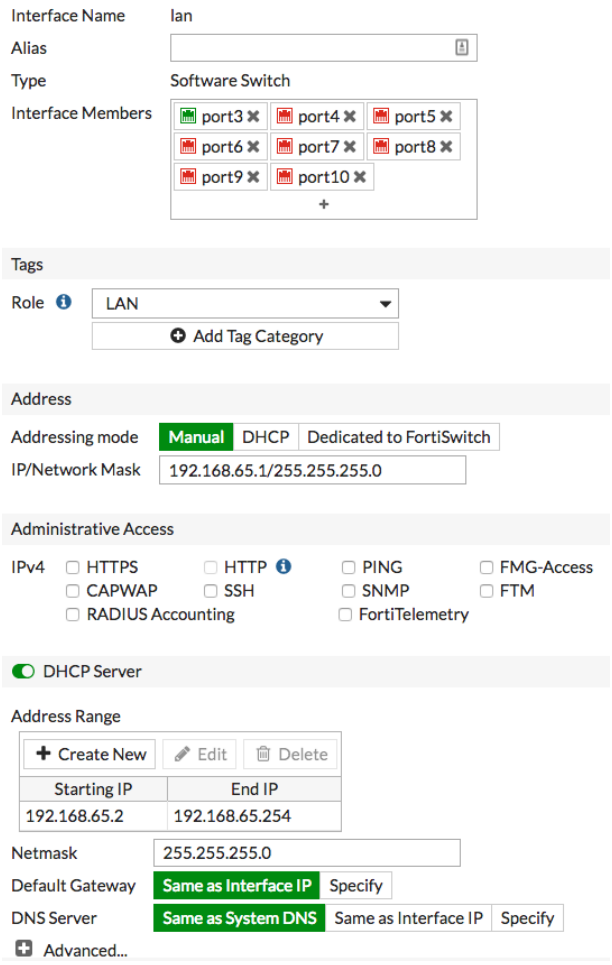
1. To edit the Internet-facing interface (in the example, wan1), go to **Network > Interfaces**.
2. Set the **Estimated Bandwidth** for the interface based on your Internet connection.
3. Set **Role** to **WAN**.




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.
   a. If your ISP provides an IP address, set **Addressing mode** to **Manual** and set the **IP/Network Mask** to that IP address.
   b. 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, for this step, you can use either an individual interface or create a software switch to combine the separate interfaces into a single virtual interface.

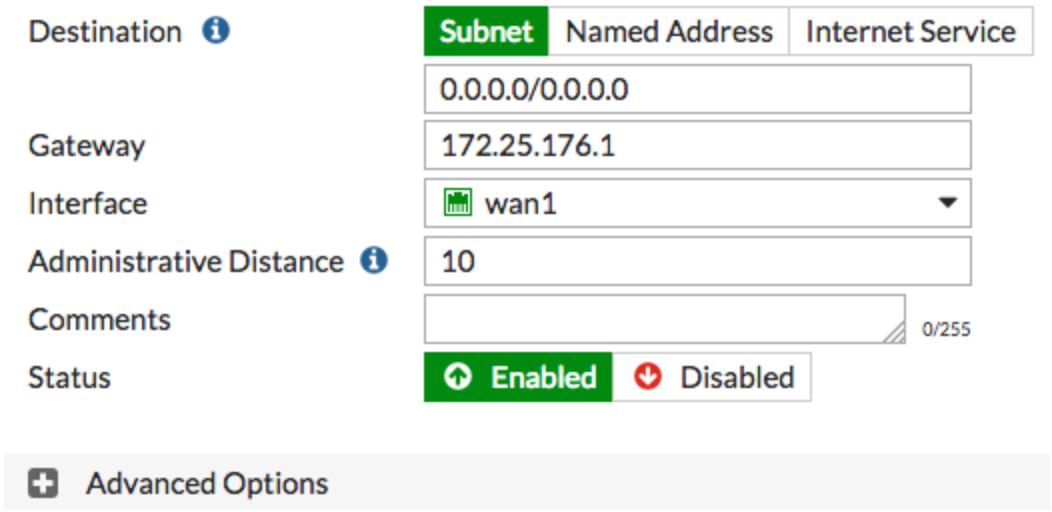
6. Set **Role** to **LAN**.
7. Set **Addressing mode** to **Manual** and set the **IP/Network Mask** to the private IP address that you want to use for the FortiGate.
8. If you need to assign IP addresses to devices on your internal network, enable **DHCP Server**.




## 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 set to 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.




## Selecting DNS servers (optional)

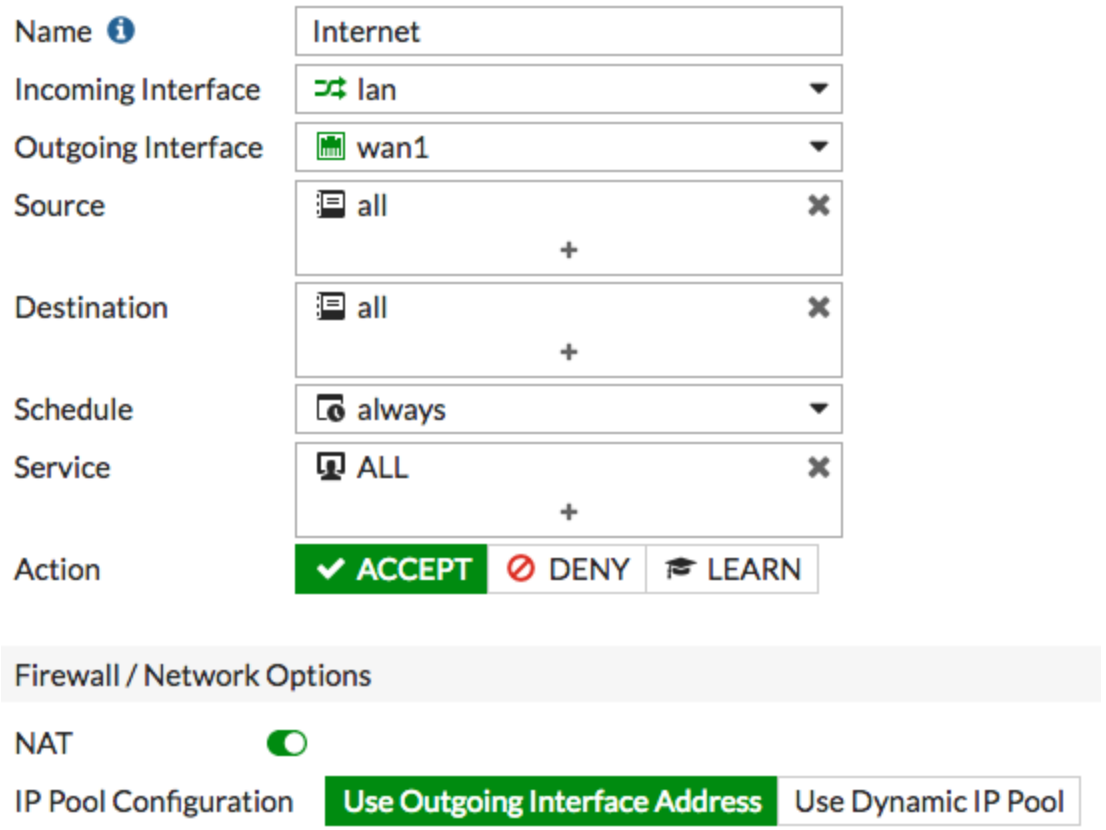
The FortiGate DNS settings are configured to use FortiGuard DNS servers by default, which is sufficient for most networks.

If you need to change the DNS servers, go to **Network > DNS**, select **Specify**, and add **Primary** and **Secondary** 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 the example, Internet).
2. Set the **Incoming Interface** to **lan** and the **Outgoing Interface** to **wan1**. Set **Source**, **Destination Address**, **Schedule**, and **Services**, as required.
3. Ensure the **Action** is set to **ACCEPT**.
4. Turn on **NAT** and select **Use Outgoing Interface Address**.



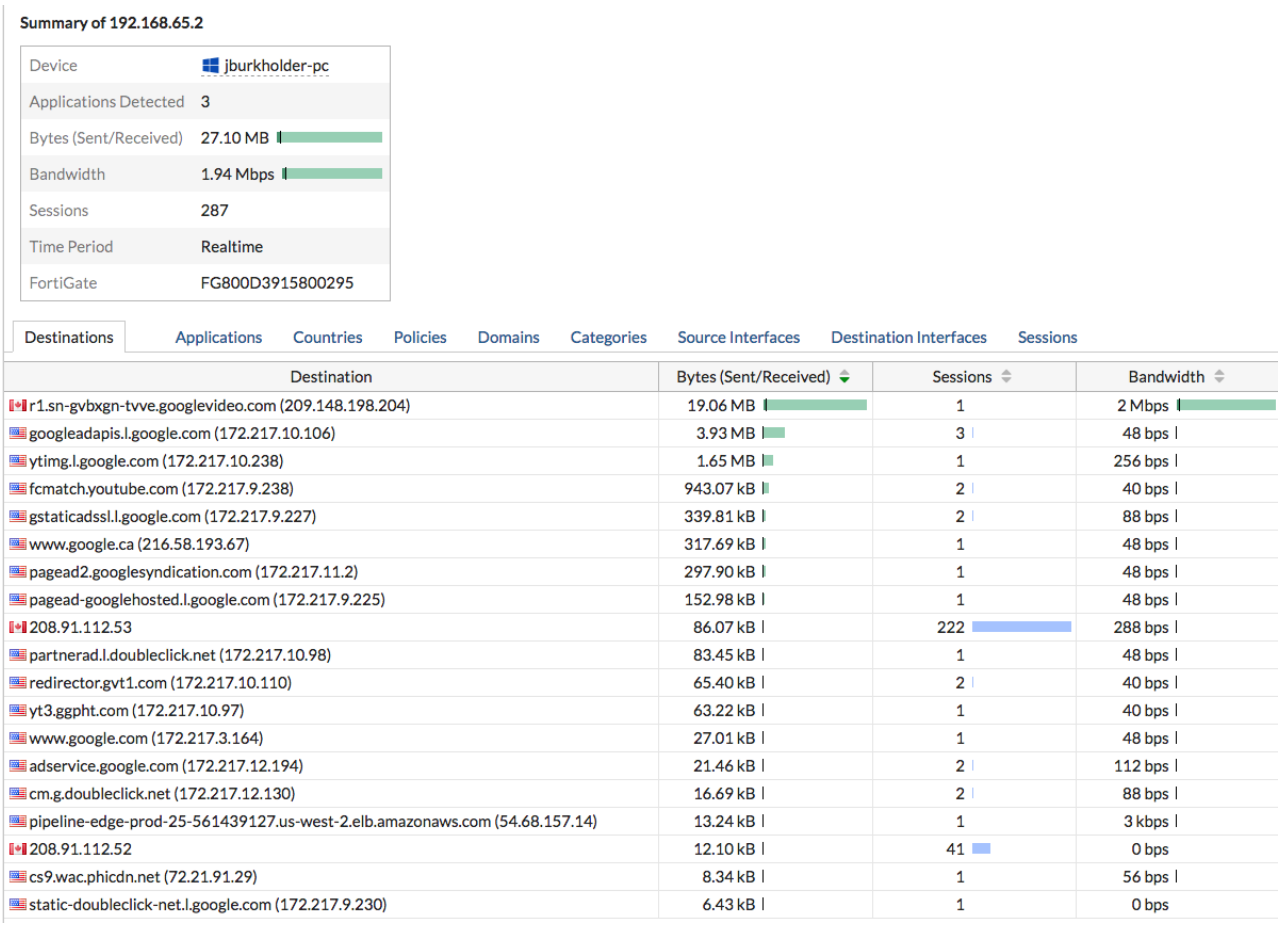

5. Scroll down to view the **Logging Options**. To view the results later, enable **Log Allowed Traffic** and select **All Sessions**.


## Results

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

| Source | Source Device | Bytes (Sent/Received) | Sessions | Bandwidth |
|---|---|---|---|---|
| 192.168.65.2 | jburkholder-pc | 19.92 MB | 300 | 3 Mbps |

4. 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 |

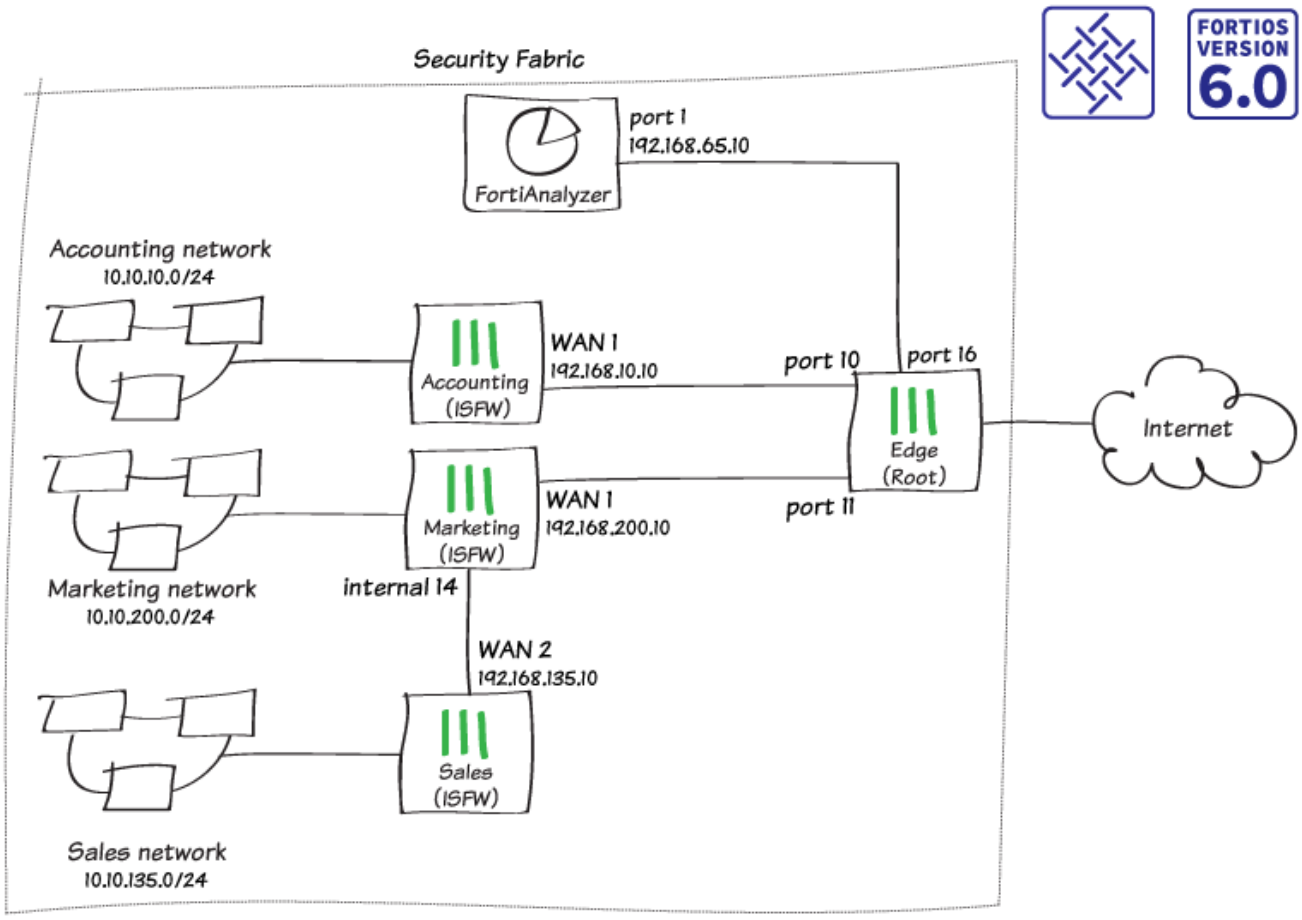
Destinations | Applications | Countries | Policies | Domains | Categories | Source Interfaces | Destination Interfaces | Sessions

| 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 |

5. If your FortiGate model has internal storage and disk logging enabled, a drop-down menu in the top corner allows you to view historical logging information for the previous **5 minutes**, **1 hour**, and **24 hours**.
6. If you're not sure whether your model supports disk logging, check the FortiGate Feature/Platform Matrix.

For further reading, check out NAT mode installation.

# Fortinet Security Fabric installation




In this recipe, you configure a Fortinet Security Fabric that consists of four FortiGate devices and a FortiAnalyzer. One of the FortiGate devices acts as the network edge firewall and root FortiGate of the Security Fabric, while the other FortiGate devices function as Internal Segmentation Firewalls (ISFWs).

The example network uses the following FortiGate aliases:

- **Edge**: the root FortiGate in the Security Fabric. This FortiGate is named “Edge” because it’s the only FortiGate that directly connects to the Internet. This role is also known as the gateway FortiGate.

  This FortiGate has already been installed in NAT mode using Installing a FortiGate in NAT mode on page 10.

- **Accounting**: an ISFW FortiGate that connects to Edge.
- **Marketing**: an ISFW FortiGate that connects to Edge.
- **Sales**: an ISFW FortiGate that connects to Marketing.

Not all FortiGate models can run the FortiGuard Security Rating Service if they are the root FortiGate in a Security Fabric. For more information, see the FortiOS 6.0 Release Notes.

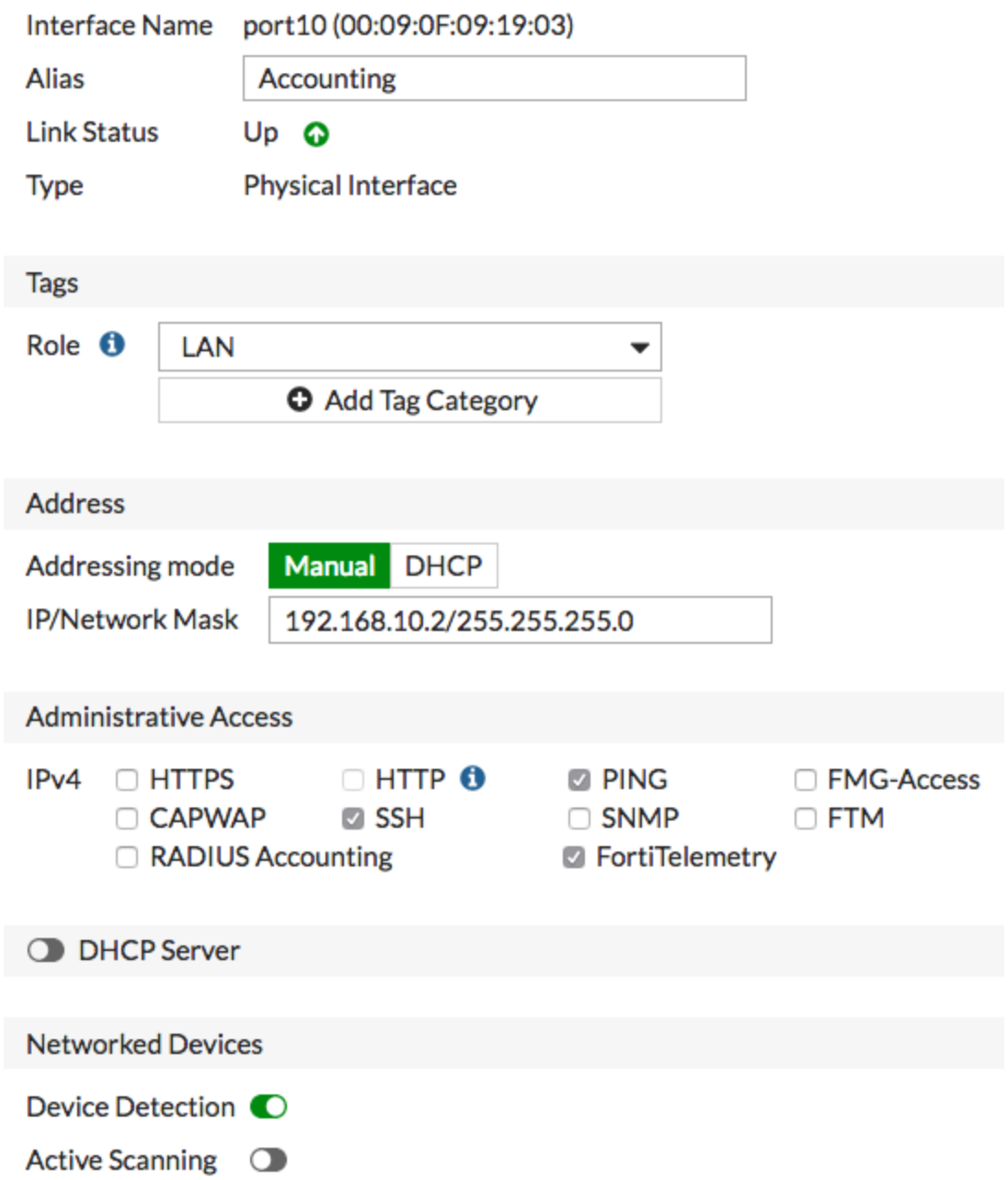
## Configuring Edge

In the Security Fabric, Edge is the root FortiGate. This FortiGate receives information from the other FortiGates in the Security Fabric.

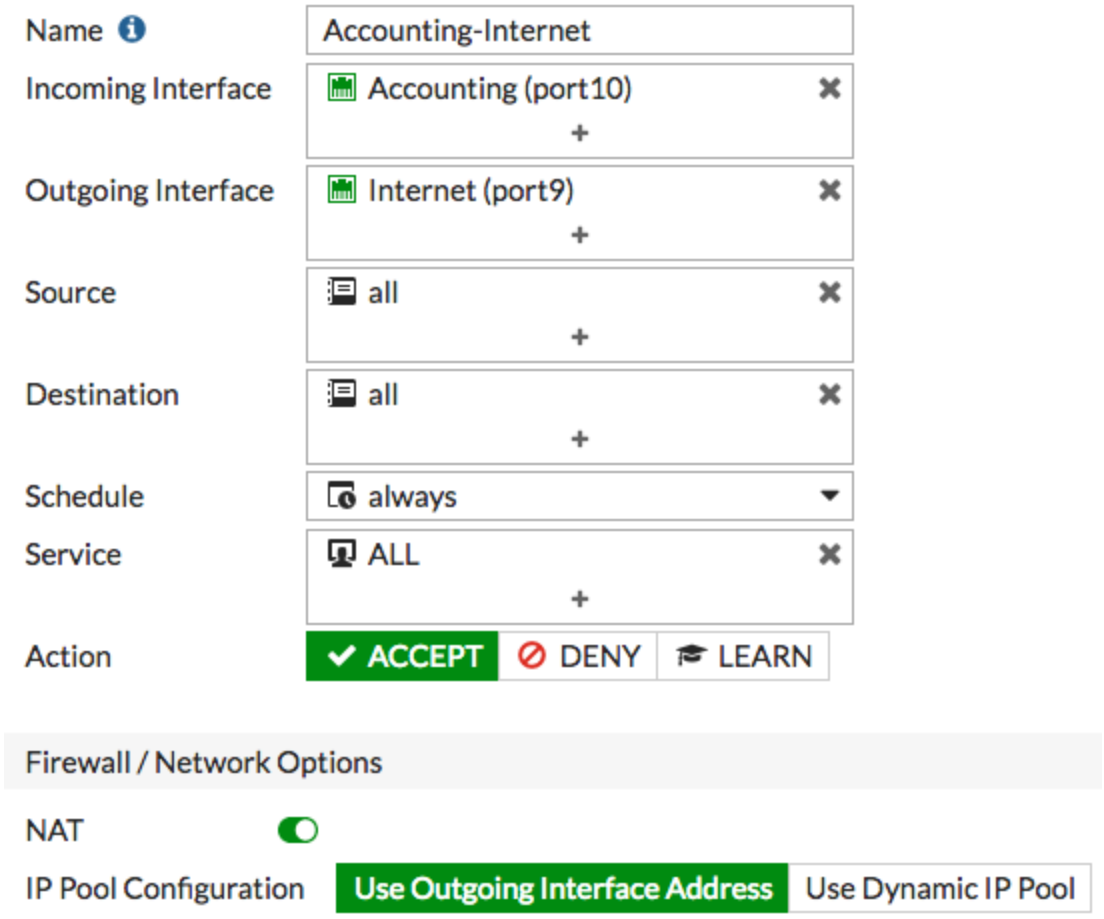
In the example, the following interfaces on Edge connect to other network devices:

- Port 9 connects to the Internet (this interface was configured when Edge was 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)

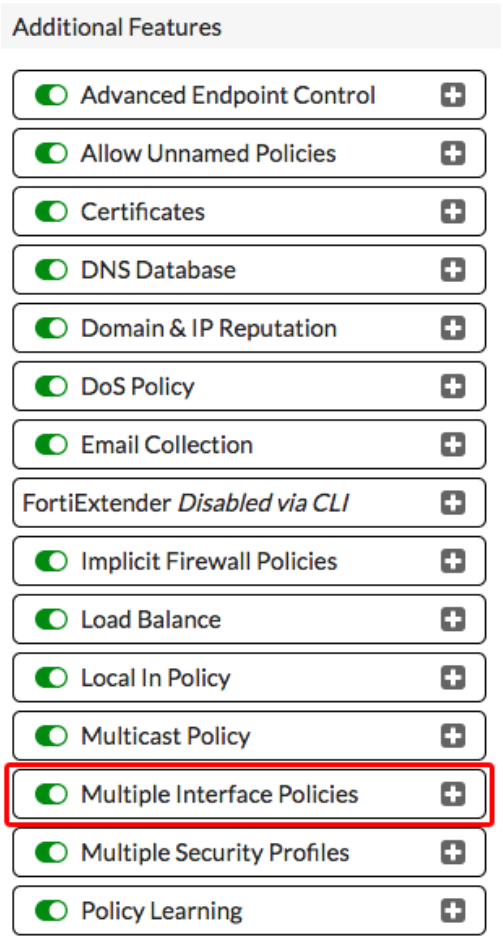
1. To edit port 10 on Edge, go to **Network > Interfaces**. Set an **IP/Network Mask** for the interface (in the example, *192.168.10.2/255.255.255.0*).
2. Set **Administrative Access** to allow **FortiTelemetry**, which is required so that FortiGate devices in the Security Fabric can communicate with each other.



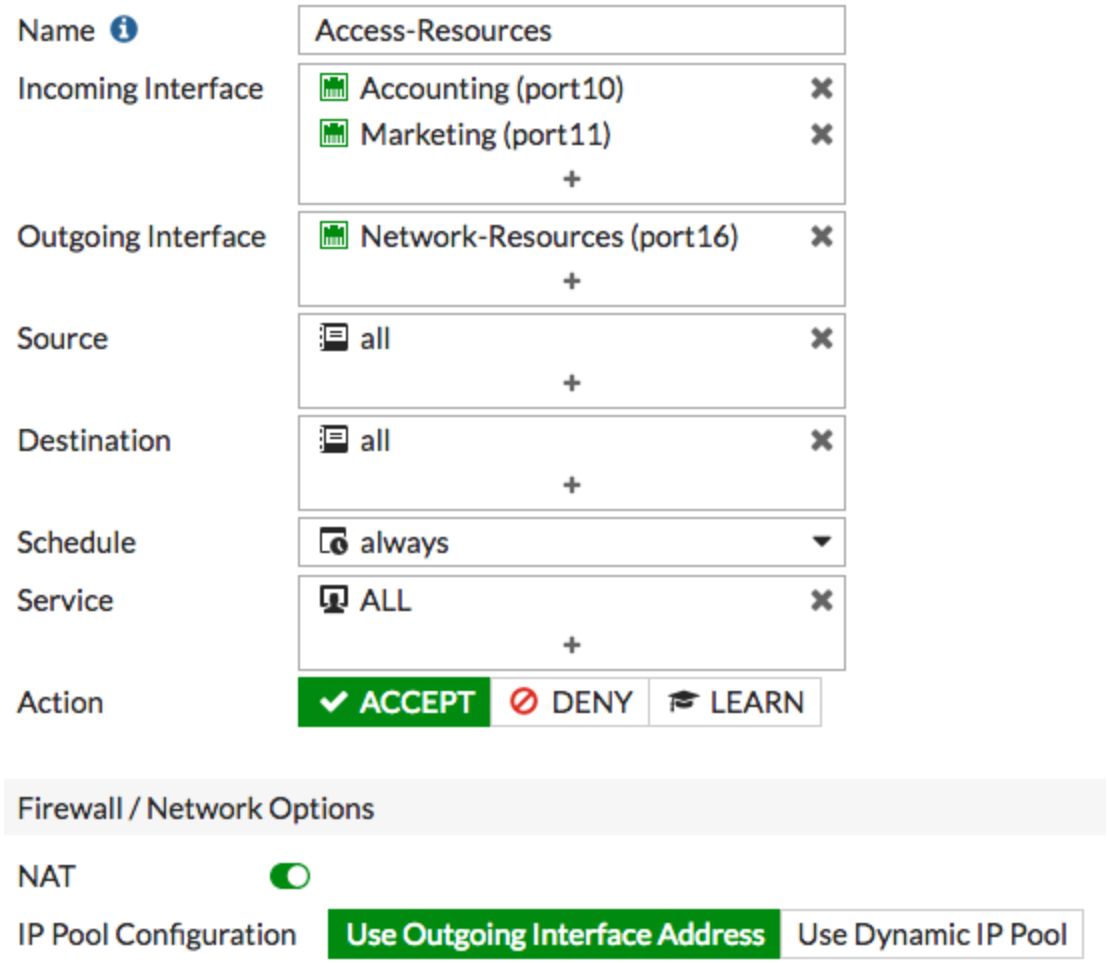

3. Repeat the previous steps to configure the other interfaces with the appropriate IP addresses, as listed above.
4. To create a policy for traffic from Accounting to the Internet, go to **Policy & Objects > IPv4 Policy** and select **Create New**.
5. Set **Incoming Interface** to **port 10** and **Outgoing Interface** to **port 9**.
6. Enable **NAT**.



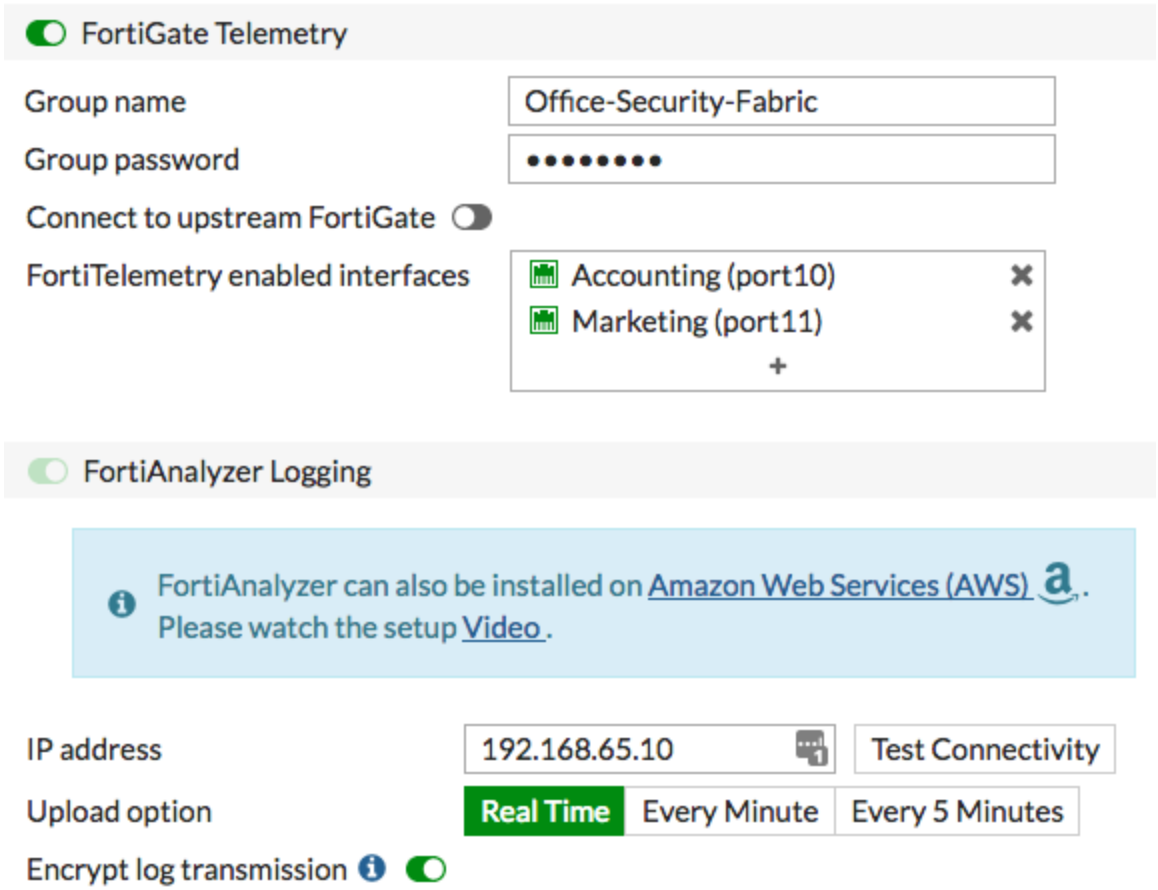

7. Repeat the previous steps to create a similar policy for Marketing.
8. On Edge, go to **System > Feature Select.** Under **Additional Features**, enable **Multiple Interface Policies**.




9. To create a policy that allows Accounting and Marketing to access the FortiAnalyzer, go to **Policy & Objects > IPv4 Policy**.



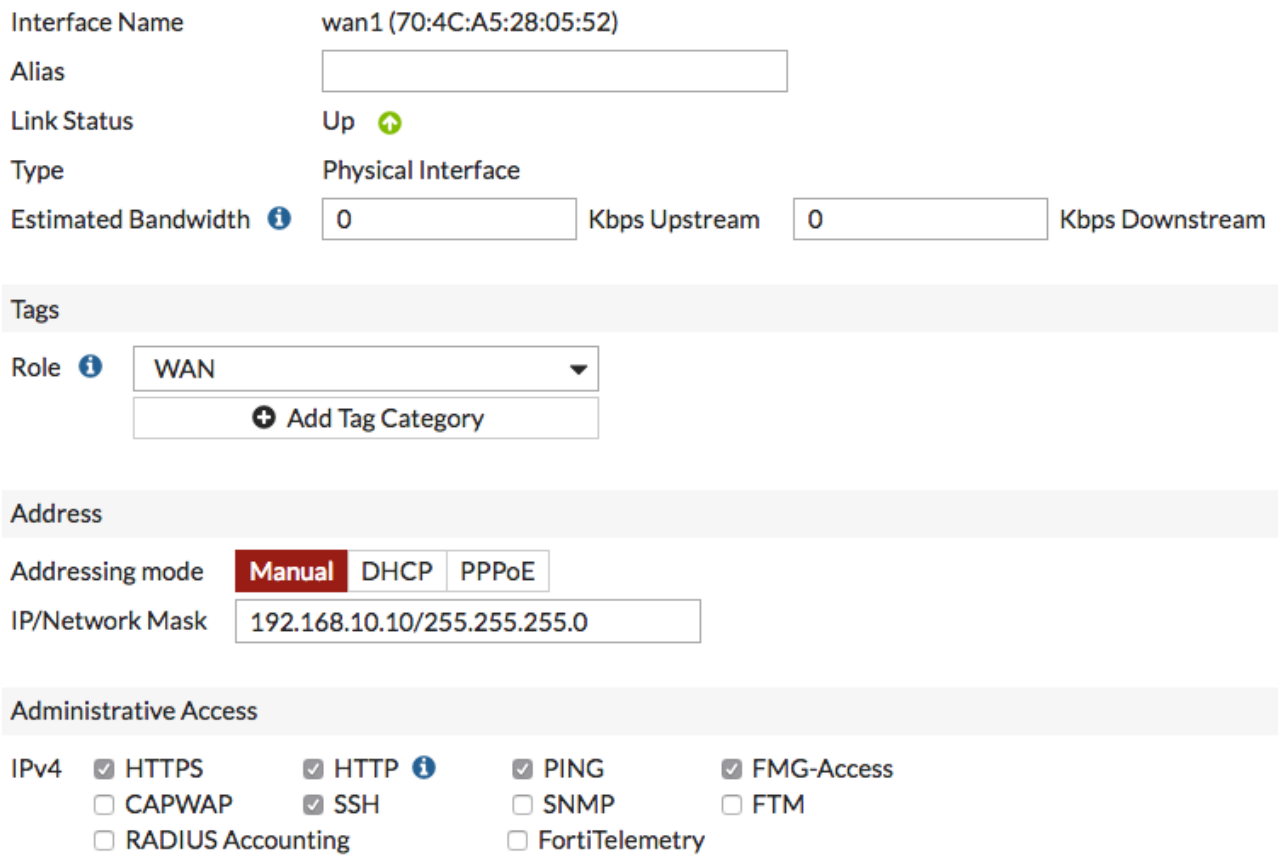

10. To enable communication between the FortiGate devices in the Security Fabric, go to **Security Fabric > Settings** and enable **FortiGate Telemetry**. Set a **Group name** and **Group password** (the **Group password** option isn't available isn't available in FortiOS 6.0.3 and later).
11. **FortiAnalyzer Logging** is enabled by default. Set **IP address** to an internal address that will later be assigned to port 1 on the FortiAnalyzer (in the example, *192.168.65.10*). Set **Upload option** to **Real Time**.




12. Select **Test Connectivity**. An error appears because the FortiGate isn't yet authorized on the FortiAnalyzer. This authorization is configured in a later step.

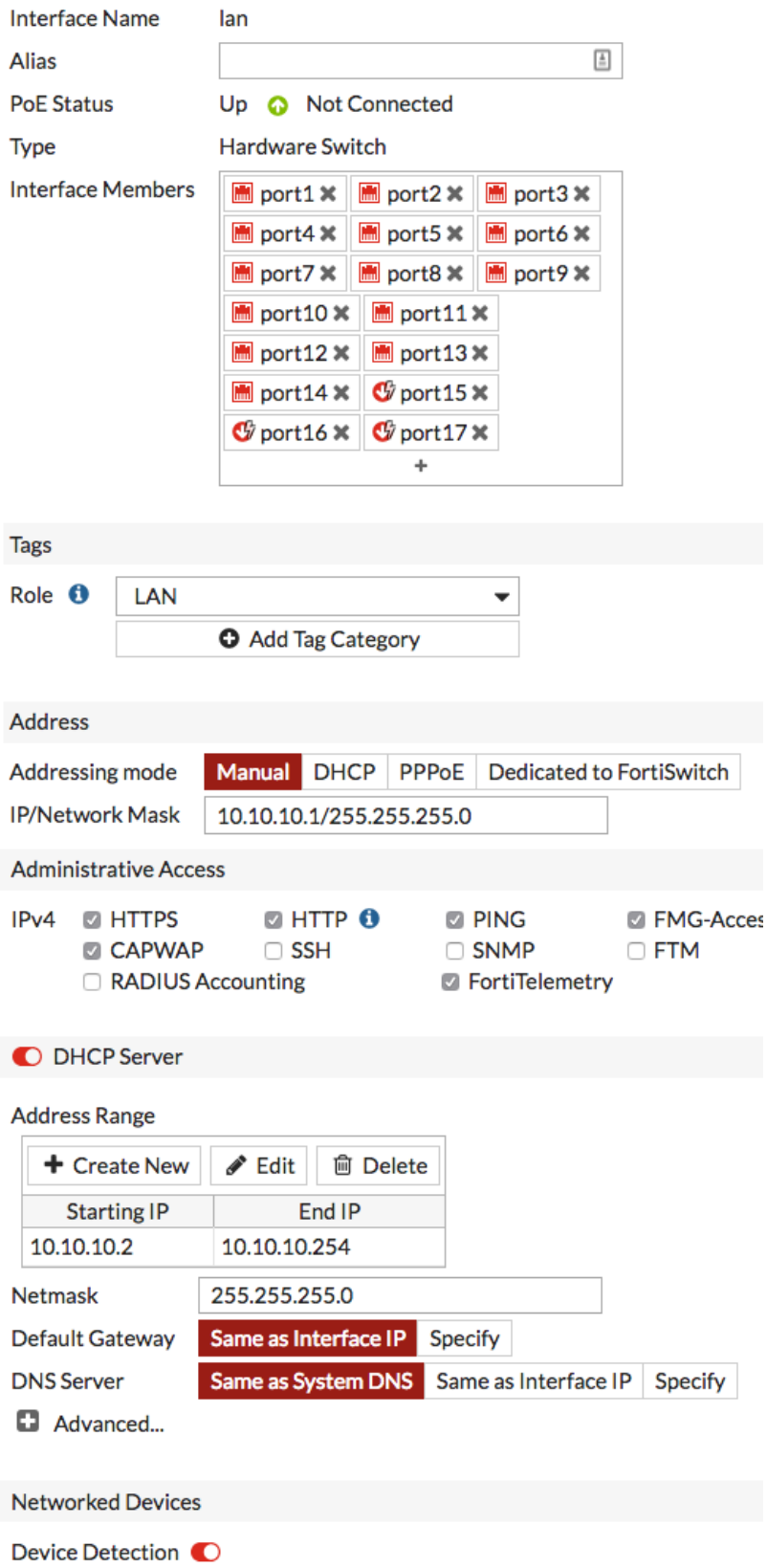
## Installing Accounting and Marketing

1. To edit **wan1** on **Accounting**, go to **Network > Interfaces**.
2. Set an **IP/Network Mask** for the interface that is on the same subnet as port 10 on Edge (in the example, *192.168.10.10/255.255.255.0*).
3. Under **Administrative Access**, select **HTTPS** and **SSH** to allow Edge to use this interface to manage the FortiGate.

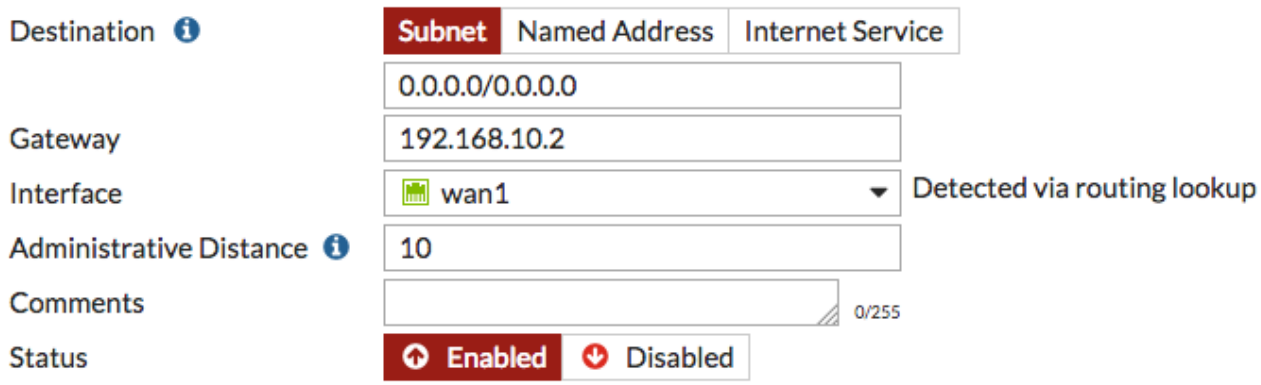



4. Edit the **lan** interface.
5. Set **Addressing mode** to **Manual** and set the **IP/Network Mask** to a private IP address (in the example, *10.10.10.1/255.255.255.0*).
6. Set **Administrative Access** to allow **FortiTelemetry**.
7. If you require the FortiGate to provide IP addresses using DHCP to devices that connect to this interface, enable **DHCP Server**.
8. Under **Networked Devices**, enable **Device Detection**.

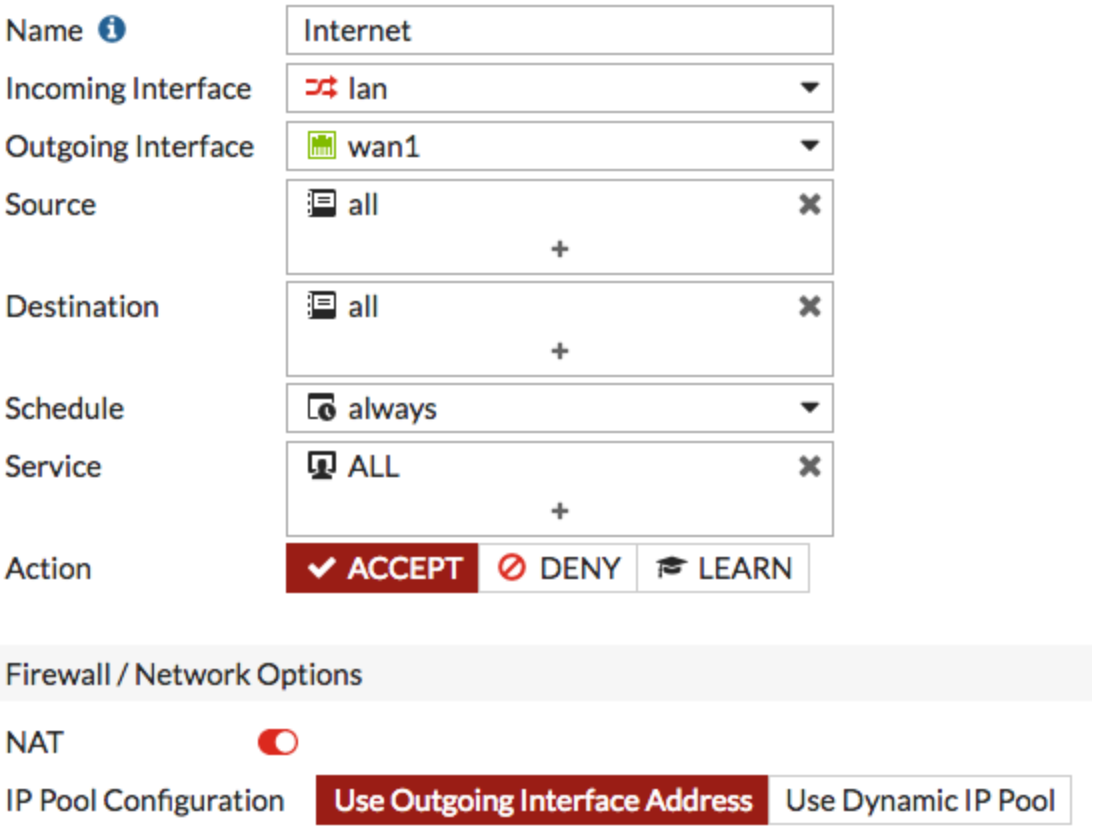
It's a best practice to enable **Device Detection** on all interfaces classified as **LAN** or **DMZ**.



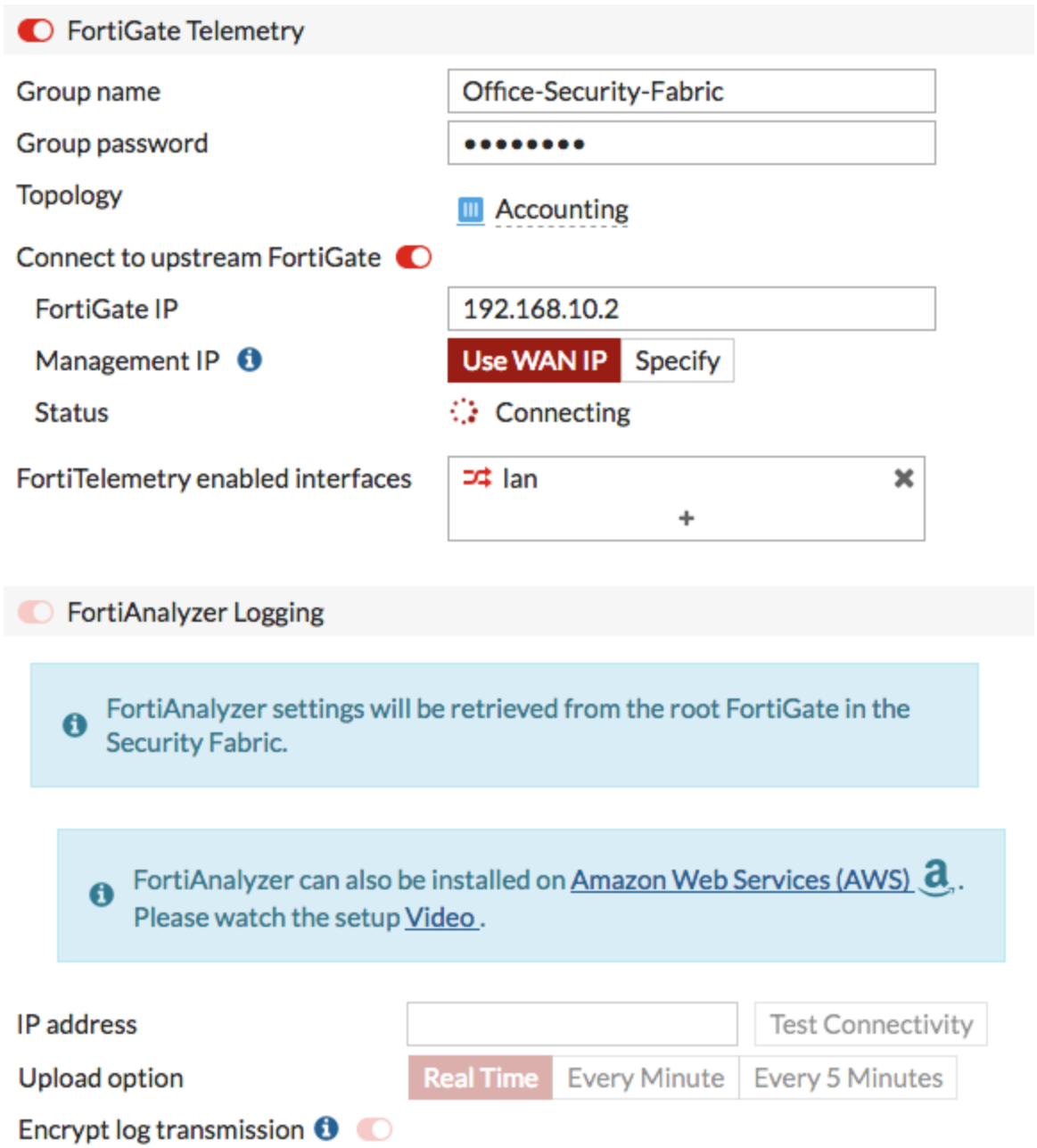

9. To add a static route, go to **Network > Static Routes**. Set **Gateway** to the IP address of port 10 on Edge.




10. To create a policy to allow users on the Accounting network to access Edge, go to **Policy & Objects > IPv4 Policy**.



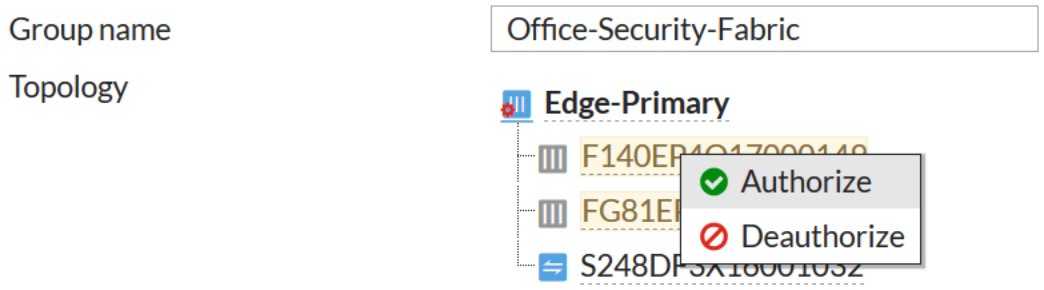

11. To add Accounting to the Security Fabric, go to **Security Fabric > Settings**. Enable **FortiGate Telemetry**, then enter the same **Group name** and **Group password** that you set previously on Edge (the **Group password** option isn't available isn't available in FortiOS 6.0.3 and later).
12. Enable **Connect to upstream FortiGate** and enter the IP address of port 10 on Edge.
13. **FortiAnalyzer Logging** is enabled by default. Settings for the FortiAnalyzer are retrieved when Accounting connects to Edge.




14. Connect WAN 1 on Accounting to port 10 on Edge.
15. Connect and configure Marketing, using the same method that you used to configure Accounting. Make sure you complete the following steps:
    - Configure WAN 1 to connect to Edge (IP address: 192.168.200.10/255.255.255.0) and allow HTTPS and SSH access.
    - Configure the LAN interface for the Marketing network (IP address: 10.10.200.2/255.255.255.0).

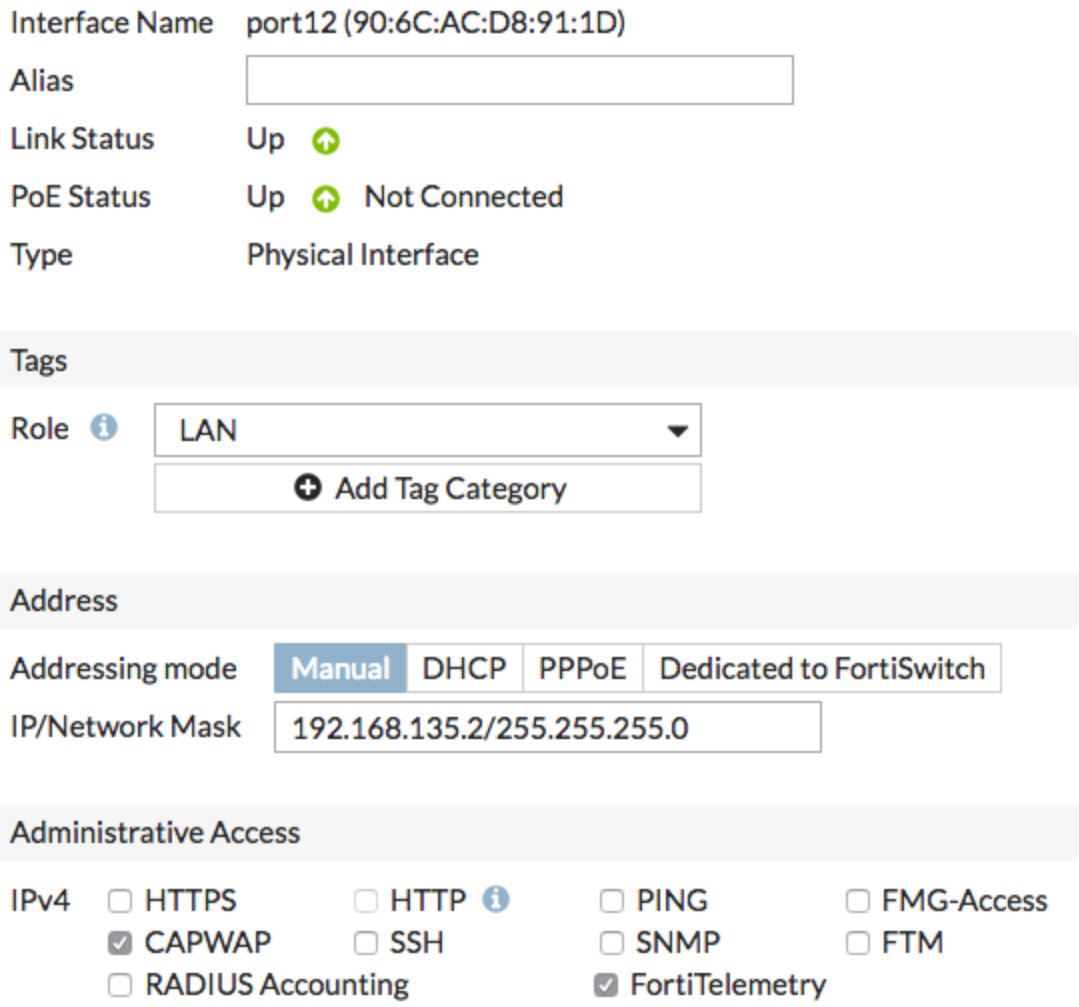
    a. Create a static route pointing traffic to port 11 on Edge.
    b. Create a policy to allow users on the Marketing network to access Edge.
    c. Add Marketing to the Security Fabric.

16. If you're using FortiOS 6.0.3 and later, connect to Edge and go to **Security Fabric > Settings**. Authorize both Accounting and Marketing to join the Security Fabric.

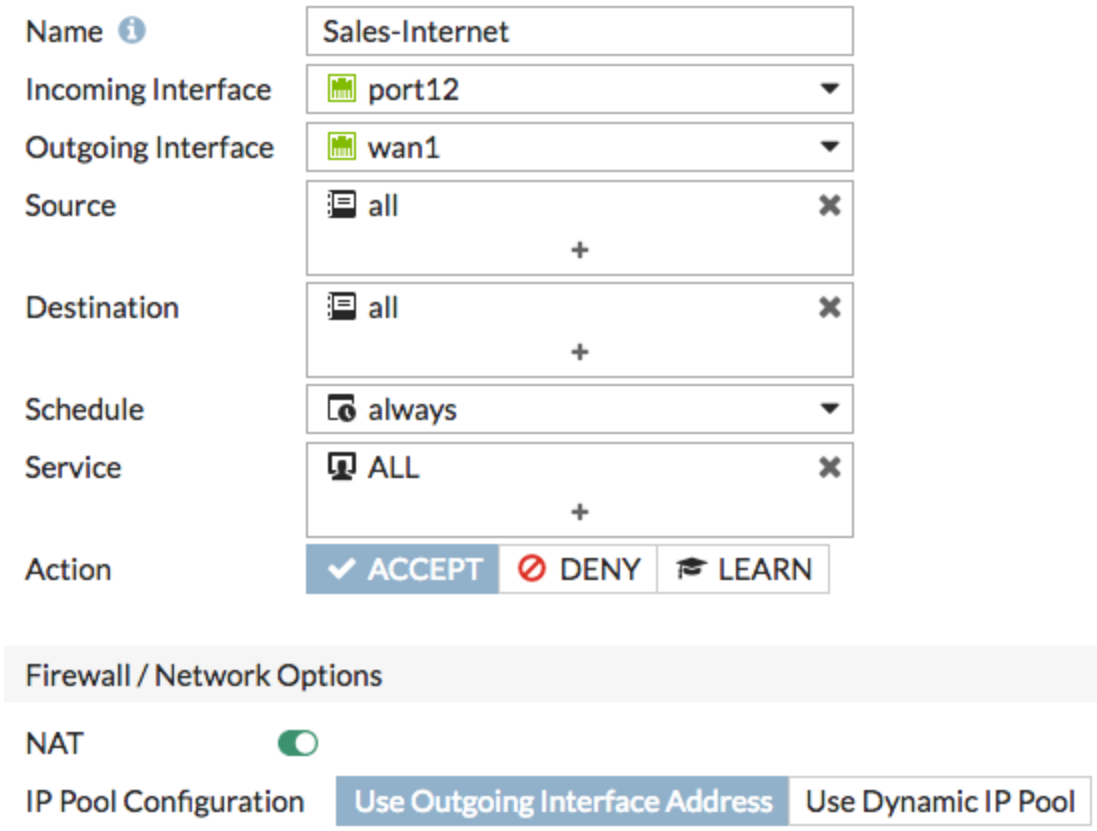



## Installing Sales

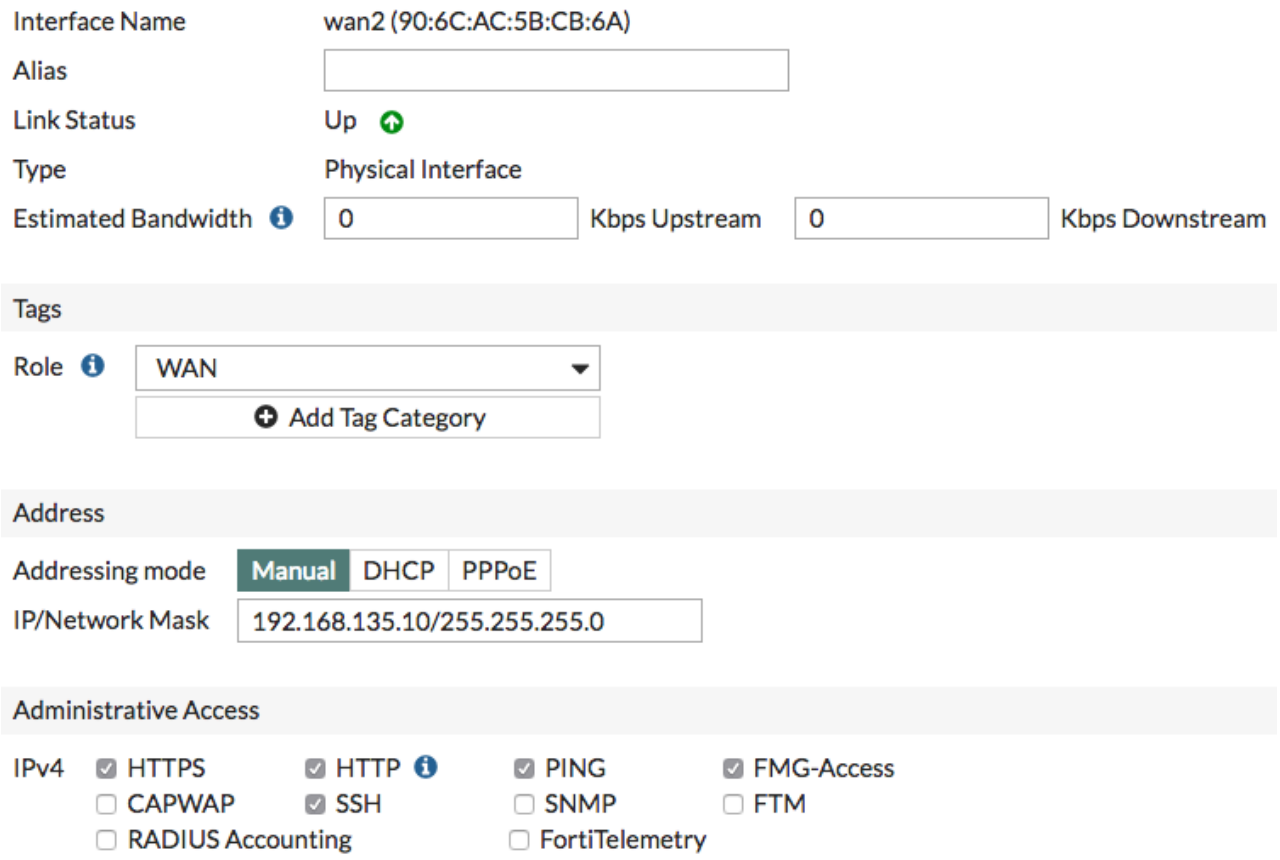
1. To edit the interface on Marketing that connects to Sales (in the example, port12), go to **Network > Interfaces**.
2. Set an **IP/Network Mask** for the interface (in the example, *192.168.135.2/255.255.255.0*).
3. Set **Administrative Access** to allow **FortiTelemetry**.



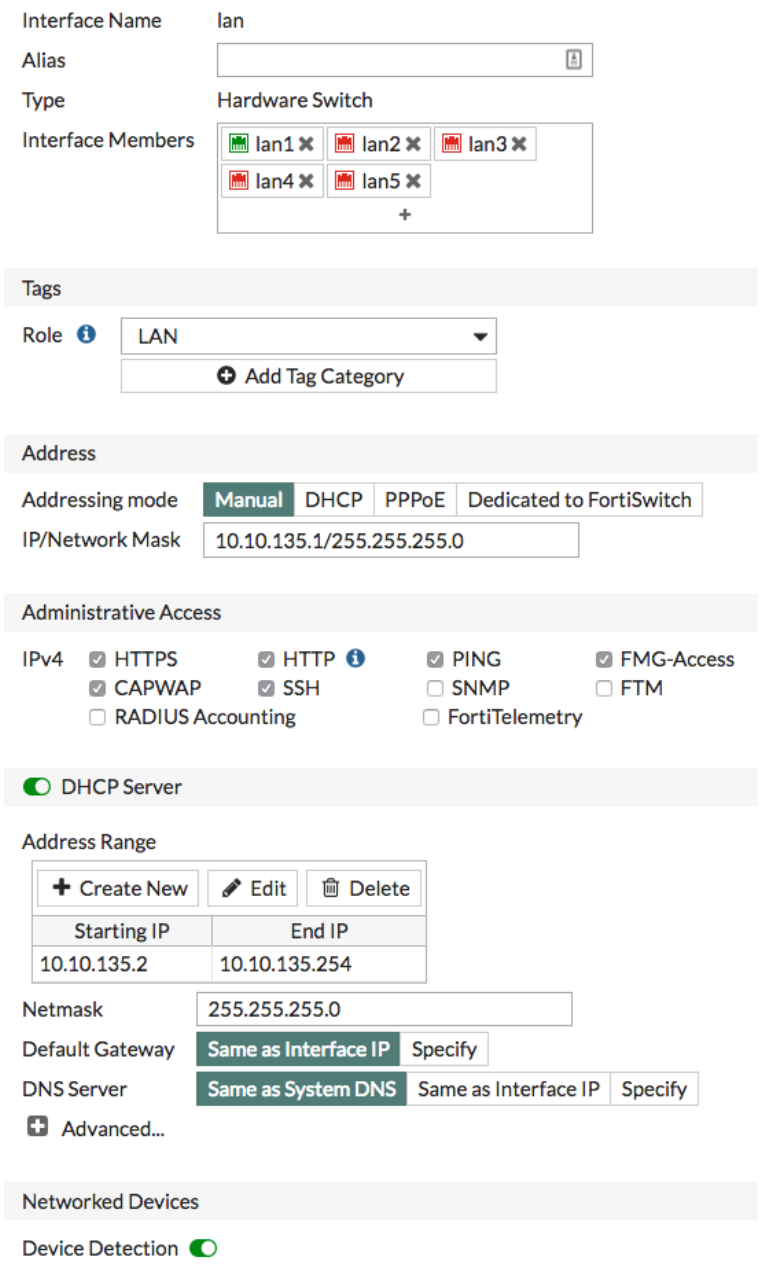
4. To create a policy for traffic from Sales to Edge, go to **Policy & Objects > IPv4 Policy**.
5. Enable **NAT**.



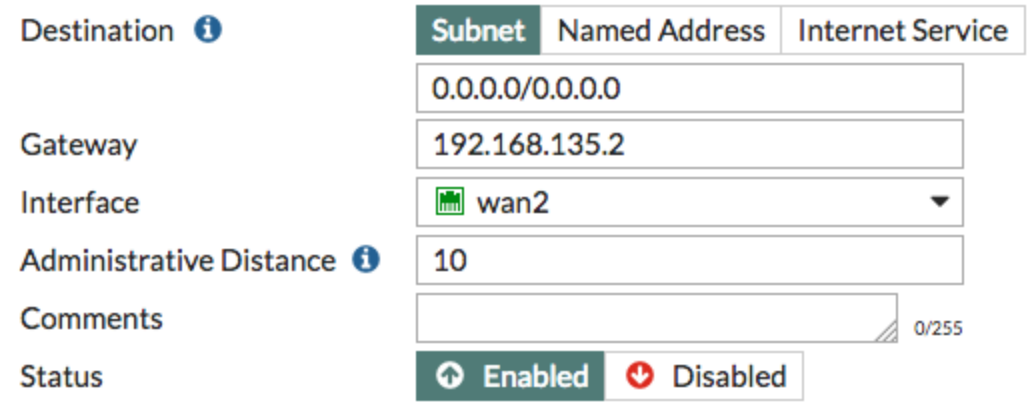

6. To edit wan2 on Sales, go to **Network > Interfaces**.
7. Set an **IP/Network Mask** for the interface that's on the same subnet as the internal 14 interface on Marketing (in the example, *192.168.135.10/255.255.255.0*).
8. Under **Administrative Access**, select **HTTPS** and **SSH**.



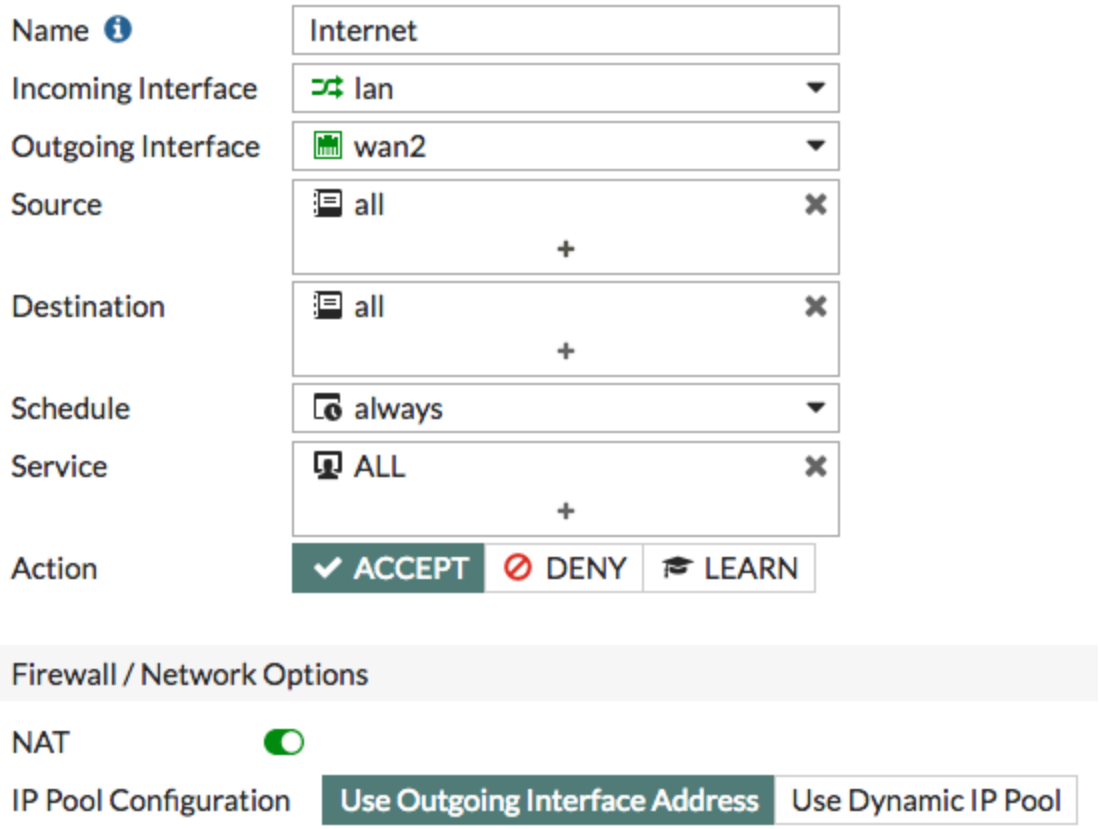

9. Edit the **lan** interface.
10. Set **Addressing Mode** to **Manual**, and set the **IP/Network Mask** to a private IP address (in the example, *10.10.135.1*/255.255.255.0).
11. Set **Administrative Access** to allow **FortiTelemetry**.
12. If you require the FortiGate to provide IP addresses, using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



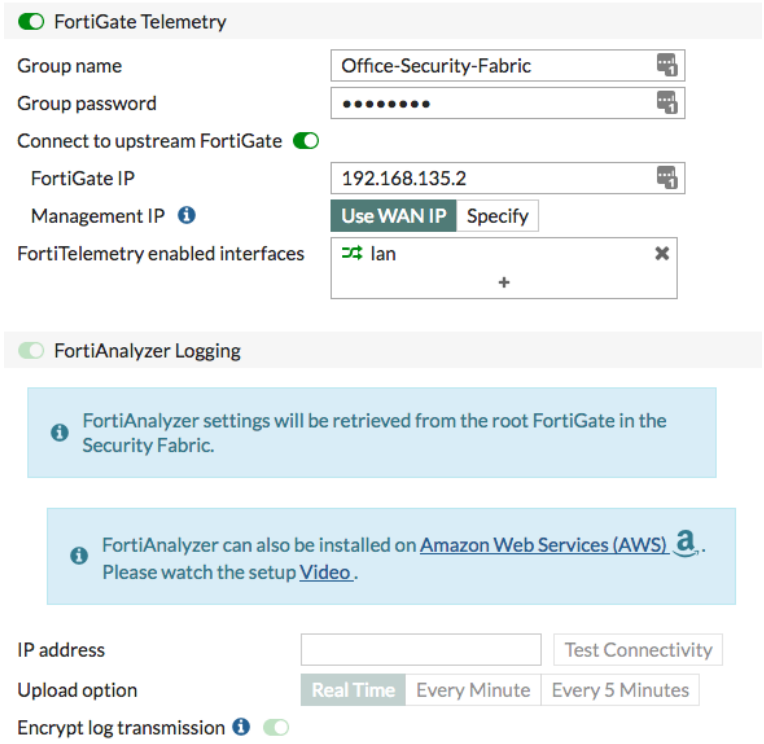

14. To add a default route, go to **Network > Static Routes** and select **Create New**. Set **Gateway** to the IP address of the internal 14 interface on Marketing.



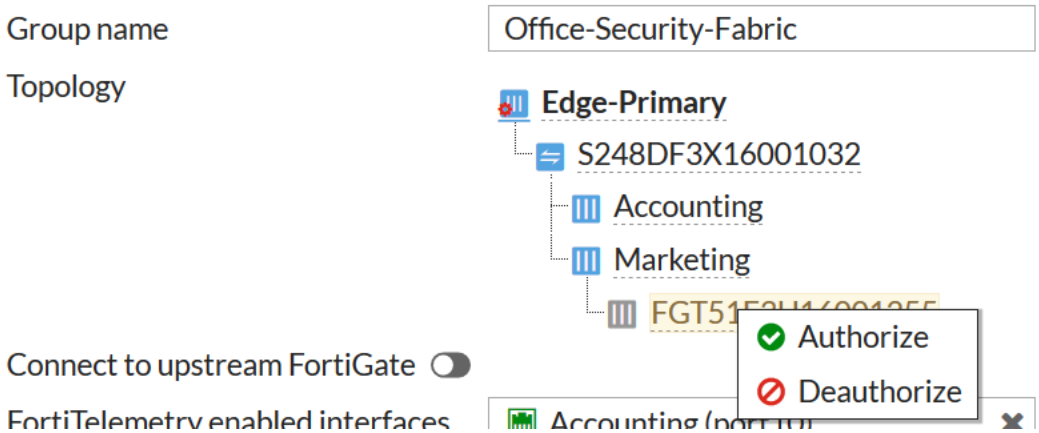

15. To create a policy that allow users on the Sales network to access Marketing, go to **Policy & Objects > IPv4 Policy**.




16. To add Sales to the Security Fabric, go to **Security Fabric > Settings**. Enable **FortiGate Telemetry**, then enter the same **Group name** and **Group password** that you set previously..
17. Enable **Connect to upstream FortiGate** and enter the IP address of the internal 14 interface on Marketing.
18. **FortiAnalyzer Logging** is enabled by default. Settings for the FortiAnalyzer are retrieved when Sales connects to Edge.




19. Connect WAN 2 on Sales to internal 14 on Marketing.
20. If you're using FortiOS 6.0.3 and later, connect to Edge and go to **Security Fabric > Settings**. Authorize Sales to join the Security Fabric.



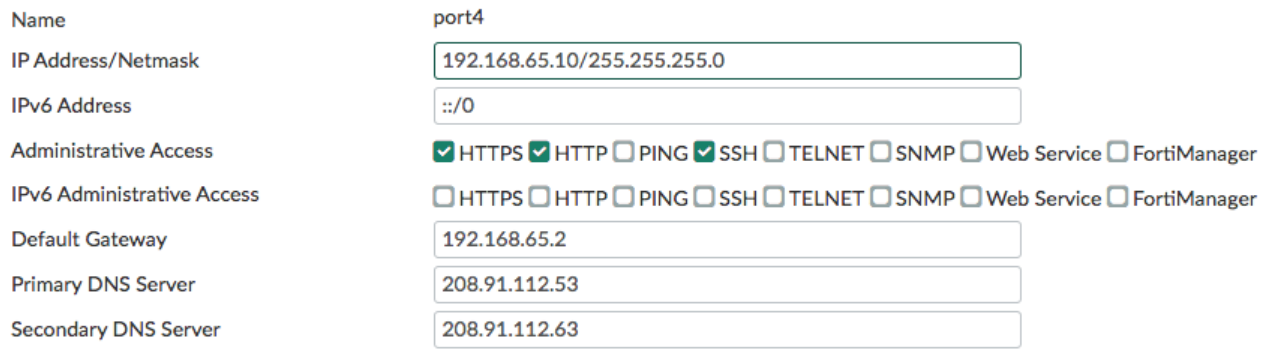

## Configuring the FortiAnalyzer

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.

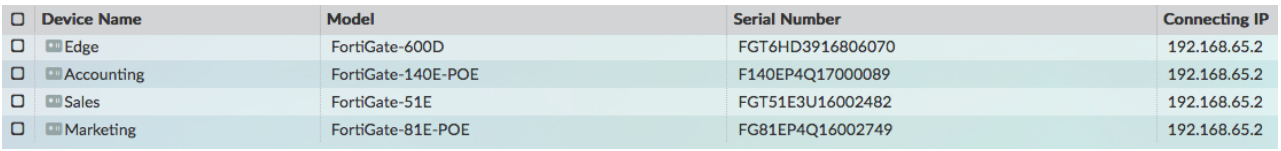
1. To edit the port on FortiAnalyzer that connects to Edge (in the example, port4), go to **System Settings > Network** and select **All Interfaces**.

2. Set **IP Address/Netmask** to the IP address that you use to configure the Security Fabric settings on Edge (*192.168.65.10/255.255.255.0*).
3. Add a **Default Gateway**, using the IP address of port 16 on Edge.

The **Default Gateway** setting may not appear until you save the settings with the new IP address.

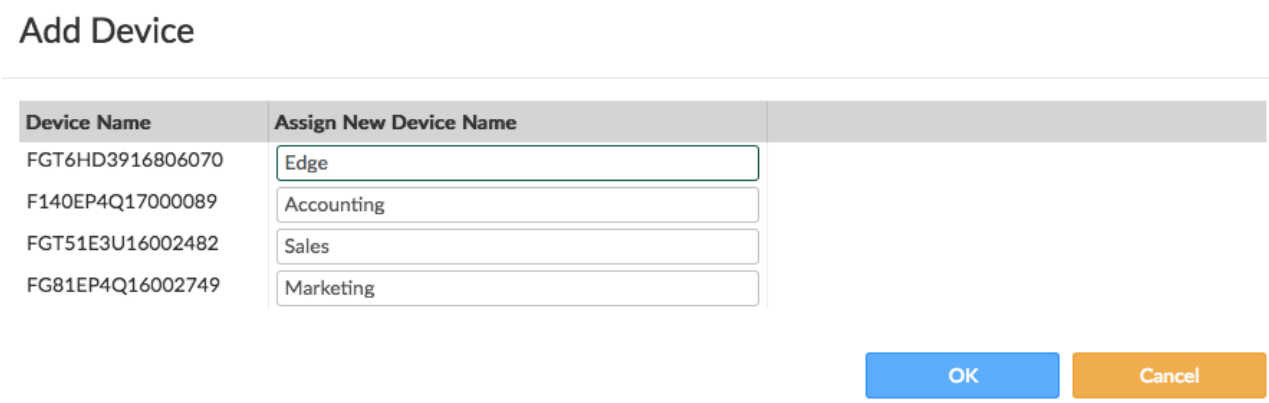



4. Go to **Device Manager**. The FortiGate devices are listed as **Unregistered**.

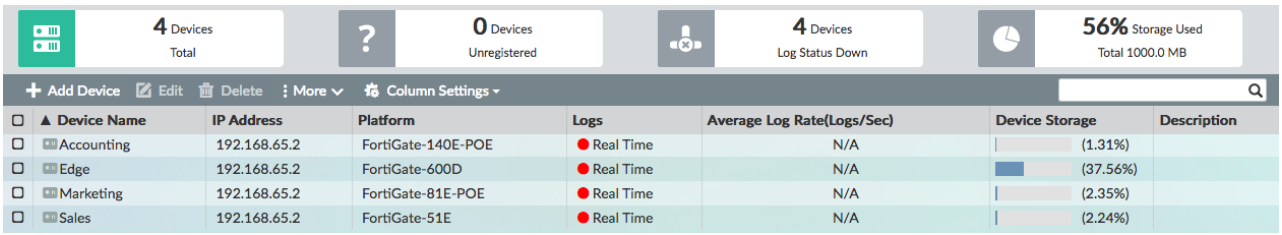


| Device Name | Model | Serial Number | Connecting IP |
|---|---|---|---|
| Edge | FortiGate-600D | FGT6HD3916806070 | 192.168.65.2 |
| Accounting | FortiGate-140E-POE | F140EP4Q17000089 | 192.168.65.2 |
| Sales | FortiGate-51E | FGT51E3U16002482 | 192.168.65.2 |
| Marketing | FortiGate-81E-POE | FG81EP4Q16002749 | 192.168.65.2 |

5. Select the FortiGate devices, then select **+Add**.




6. The FortiGate devices now appear as **Registered**.

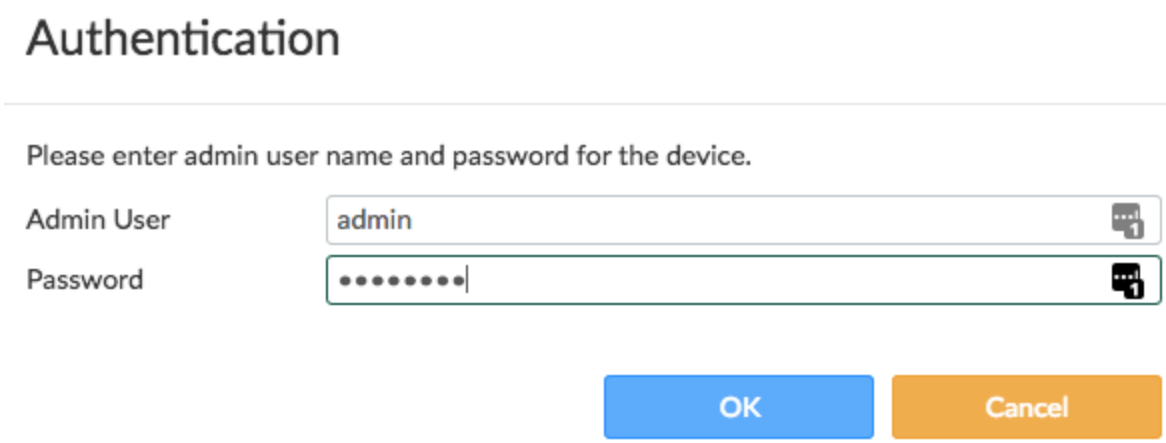



| Device Name | IP Address | Platform | Logs | Average Log Rate(Logs/Sec) | Device Storage | Description |
|---|---|---|---|---|---|---|
| Accounting | 192.168.65.2 | FortiGate-140E-POE | Real Time | N/A | (1.31%) | |
| Edge | 192.168.65.2 | FortiGate-600D | Real Time | N/A | (37.56%) | |
| Marketing | 192.168.65.2 | FortiGate-81E-POE | Real Time | N/A | (2.35%) | |
| Sales | 192.168.65.2 | FortiGate-51E | Real Time | N/A | (2.24%) | |

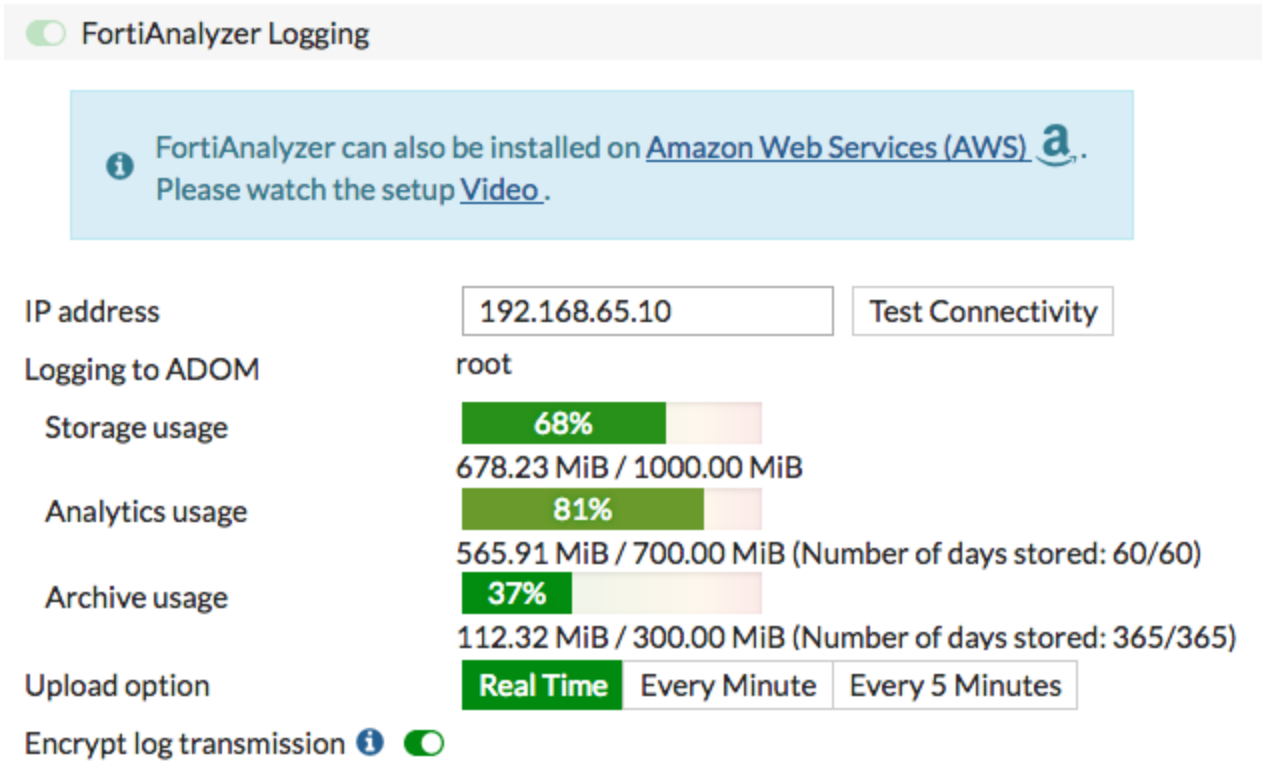
7. After a moment, a warning icon appears beside Edge because the FortiAnalyzer needs administrative access to the root FortiGate in the Security Fabric.

You may need to refresh the page before the icon appears.

8. Double-click on the FortiGate to enter the **Authentication** information.




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



## Adding security profiles (optional)

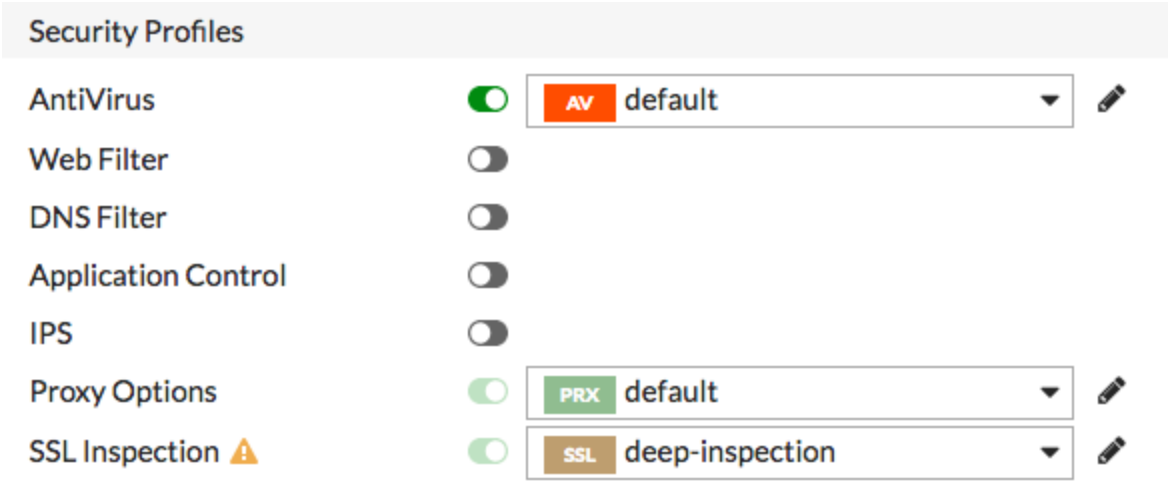
The Security Fabric allows you to distribute security profiles to different FortiGates in your network, which can lessen the workload of each device and avoid creating bottlenecks. For example, you can implement antivirus scanning on Edge while the ISFW FortiGates apply application control and web filtering.

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 since other internal networks may have different application control and web filtering requirements.

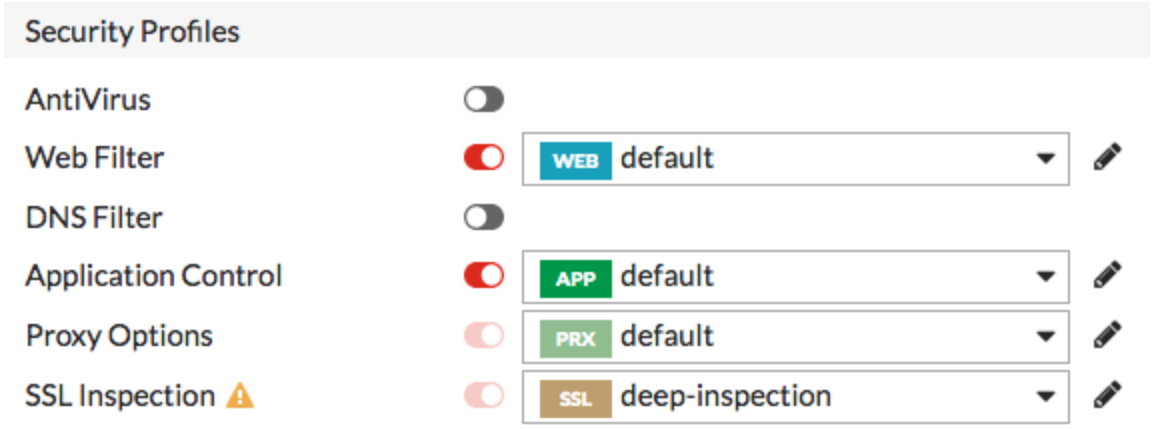
This configuration may result in threats getting through Edge, which means you should very closely limit access to the network connections between the FortiGates in the network.

1. To edit the policy that allows traffic from Accounting to the Internet, connect to Edge and go to **Policy & Objects > IPv4 Policy**.
2. Under **Security Profiles**, enable **AntiVirus** and select the **default** profile.
3. **SSL Inspection** is enabled by default. Set it to the **deep-inspection** profile.

Using the **deep-inspection** profile may cause certificate errors.




4. Do the same for the policy that allows traffic from Marketing to the Internet.
5. To edit the policy that allows traffic from the Accounting network to Edge, connect to Accounting and go to **Policy & Objects > IPv4 Policy**.
6. Under **Security Profiles**, enable **Web Filter** and **Application Control**. Select the **default** profile for both.
7. **SSL Inspection** is enabled by default. Set it to the **deep-inspection** profile.



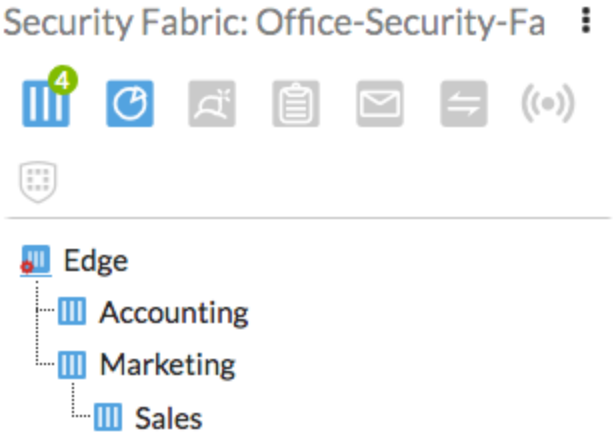

8. Repeat this step for both Marketing and Sales.

## Results

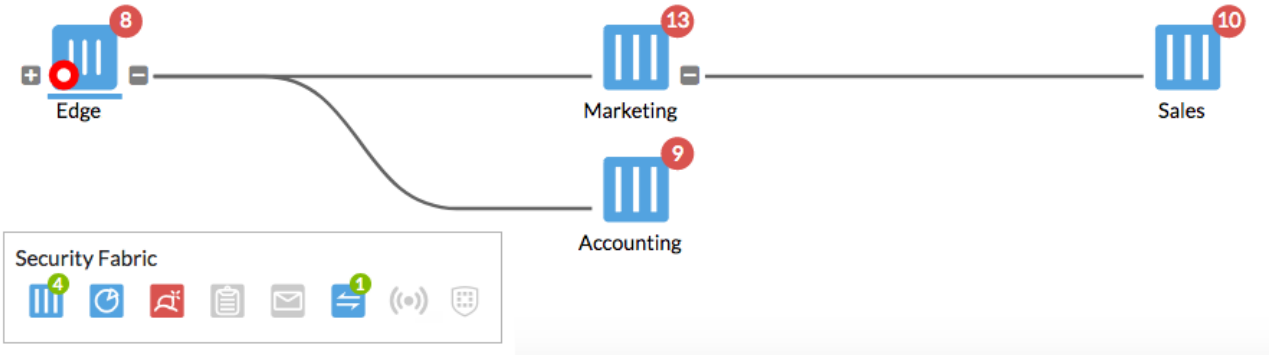
1. On Edge, go to **Dashboard > Main**. The Security Fabric widget displays the names of the FortiGates in the Security Fabric.

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

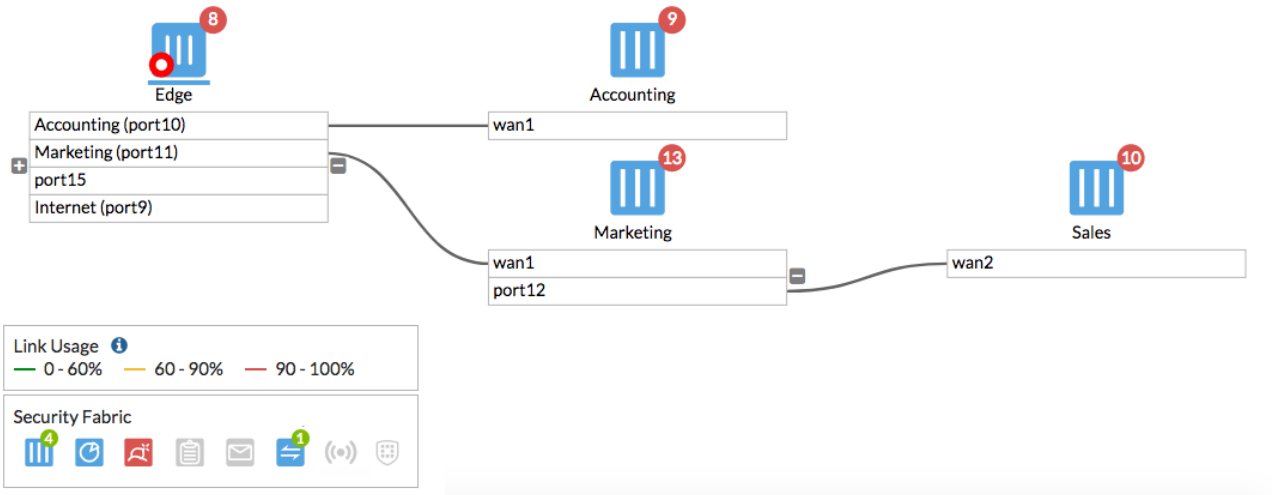
   If either of this widgets doesn't appear on your dashboard, you can add them using the settings button in the bottom right corner.




2. Go to **Security Fabric > Physical Topology**. This page shows a visualization of access layer devices in the Security Fabric.



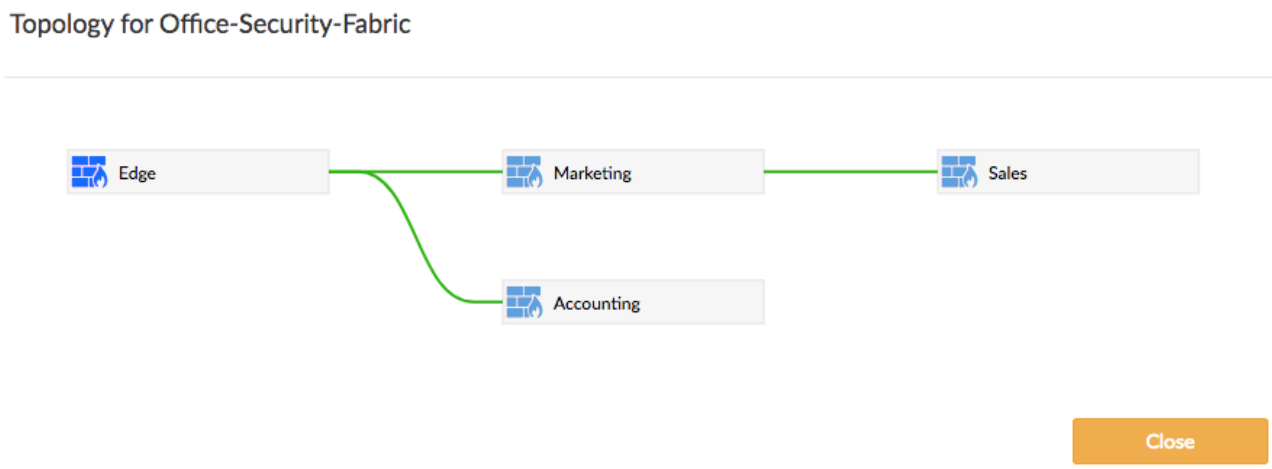

3. Go to **Security Fabric > Logical Topology**. This dashboard displays information about the interface (logical or physical) that each device in the Security Fabric connects.




4. On the FortiAnalyzer, go to **Device Manager**. The FortiGates are now shown as part of a Security Fabric group. The * beside Edge indicates that it's the root FortiGate in the Security Fabric.

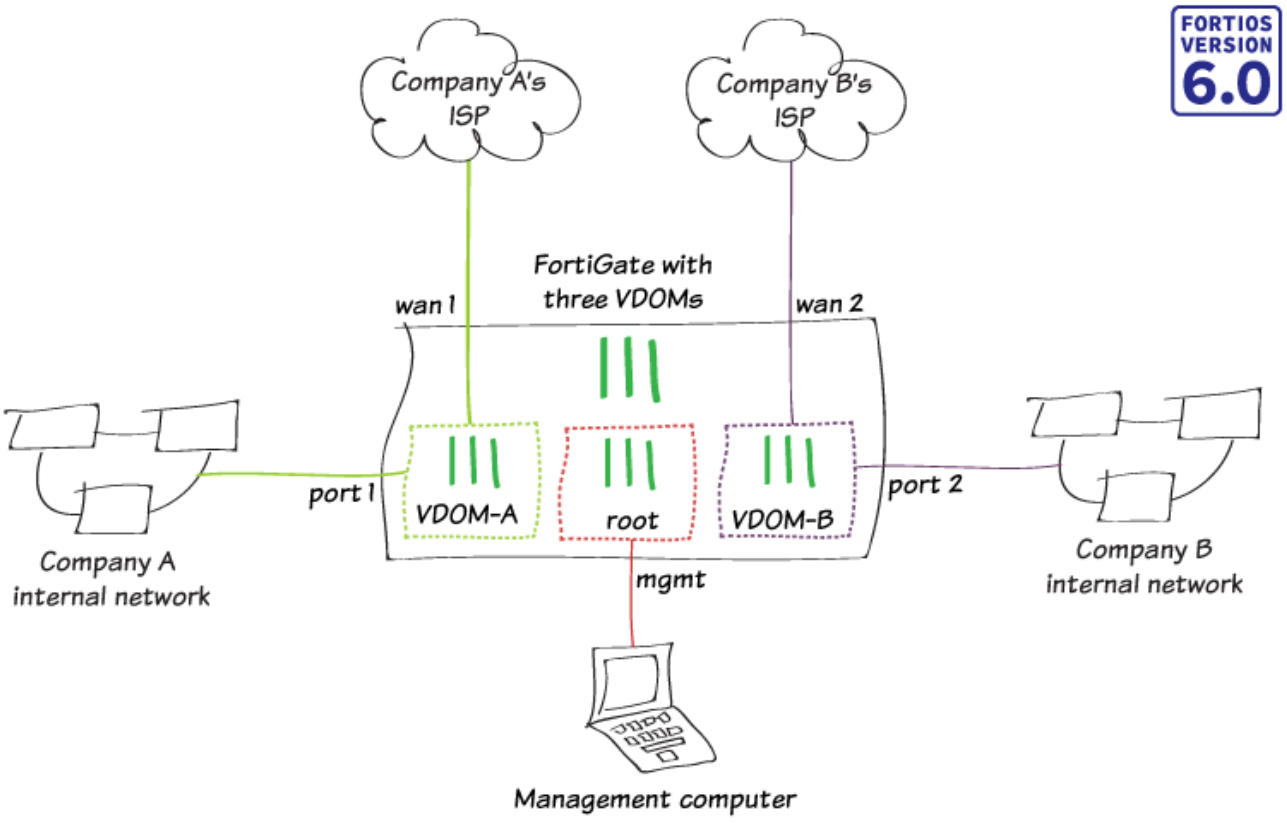
| Device Name | IP Address | Platform | Logs | Average Log Rate(Logs/Sec) | Device Storage |
|---|---|---|---|---|---|
| Office-Security-Fabric | | | | | |
| Accounting | 192.168.65.2 | FortiGate-140E-POE | Real Time | 0 | (1.34%) |
| Edge* | 192.168.65.2 | FortiGate-600D | Real Time | 0 | (47.73%) |
| Marketing | 192.168.65.2 | FortiGate-81E-POE | Real Time | 0 | (2.43%) |
| Sales | 192.168.65.2 | FortiGate-51E | Real Time | 0 | (2.31%) |

5. Right-click on the Security Fabric group and select **Fabric Topology**. The topology of the Security Fabric is displayed.




For further reading, check out Configuring the Security Fabric in the FortiOS 6.0 Online Help.

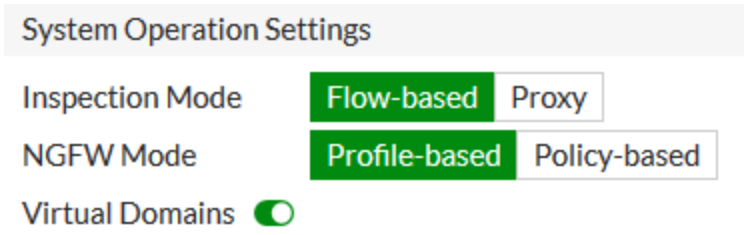
## VDOM configuration



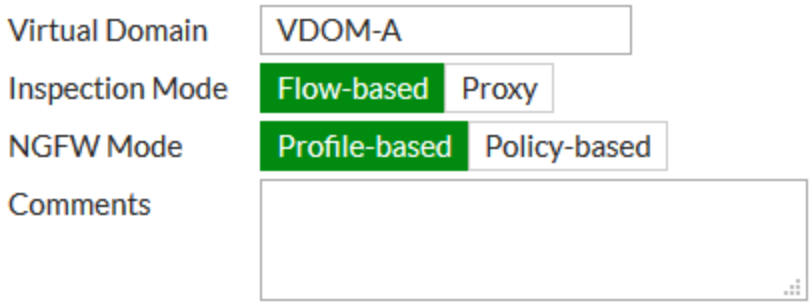

In this recipe, you use virtual domains (VDOMs) to provide Internet access for two different companies (called Company A and Company B) using a single FortiGate.

## Enabling and creating VDOMs

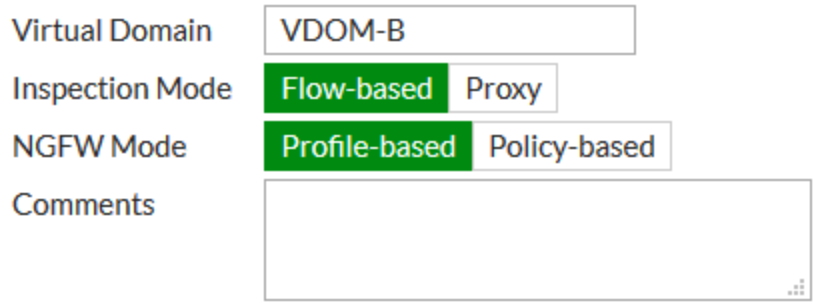
1. To enable VDOMs, go to **System > Settings**. Under **System Operation Settings**, enable **Virtual Domains**.
2. Select **OK** to confirm the VDOM mode change. When the change is applied, you are logged out of the FortiGate.




3. Log back in. To edit global settings, select **Global** from the dropdown menu located in the top-left corner.
4. To create a new VDOM, go to **System > VDOM** and select **Create New**. Enter a name (*VDOM-A*).




5. Create a second VDOM, called *VDOM-B*.

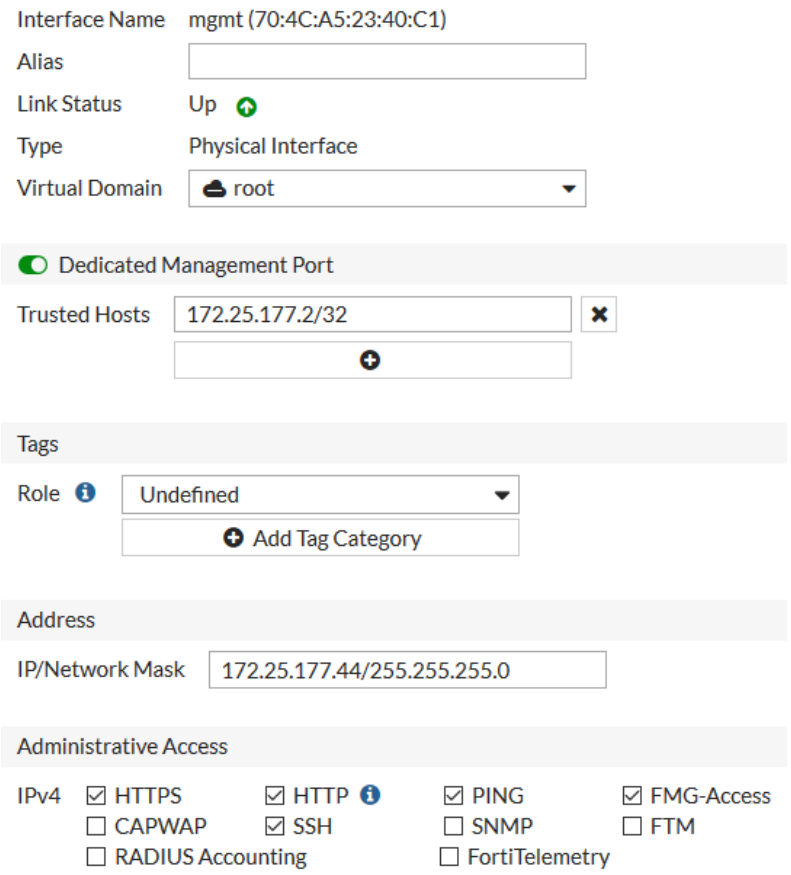



## Configuring a management interface

By default, **root** is the management VDOM. You use the management VDOM to access the global settings for the FortiGate as well as the settings for each VDOM.

1. To configure an interface to connect to the management VDOM, go to **Global > Network > Interfaces** and edit an interface (in the example, **mgmt**).
2. Enable **Dedicated Management Port** and add the management computers as **Trusted Host**.

3. Set **Administrative Access** to **HTTPS**, **PING**, and **SSH**.

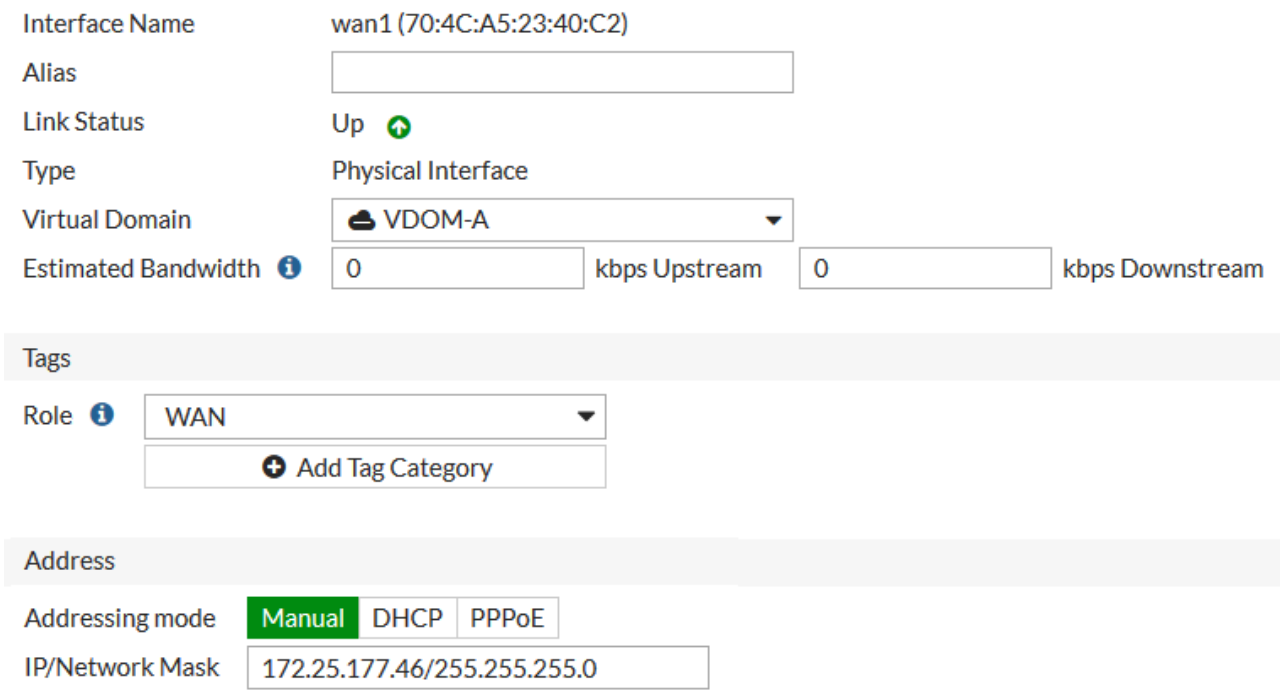



## Assigning interfaces

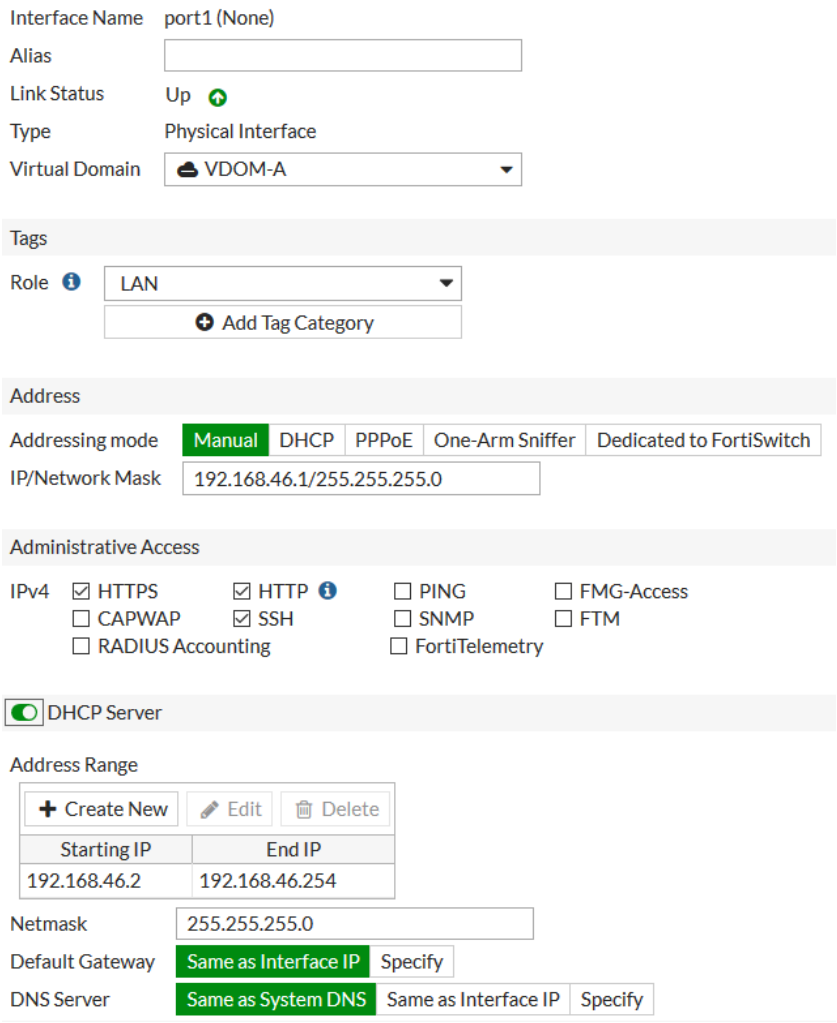
In this example, you assign two interfaces each to VDOM-A and VDOM-B: one for Internet access and one for use by the local network.

You can't change the VDOM assignment if an interface is used in an existing FortiGate configuration. You may need to delete existing policies and routes in order to add a particular interface, as some FortiGate models have default configurations.

1. To assign an interface that provides VDOM-A with Internet access, go to **Network > Interfaces** and edit an interface (in the example, **wan 1**).
2. Set **Virtual Domain** to **VDOM-A** and **Role** to **WAN**.
3. 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.




4. To assign an interface for the VDOM-A internal network, go to **Network > Interfaces** and edit the interface (in the example, **port 1**).
5. Set **Virtual Domain** to **VDOM-A** and **Role** to **LAN**.
6. Set **Addressing Mode** to **Manual**, assign an **IP/Network Mask** to the interface (in the example, *192.168.46.1/255.255.255.0*), and set **Administrative Access** to **HTTPS**, **PING**, and **SSH**.
7. If you need to assign IP addresses to devices on your internal network, enable **DHCP Server**.




8. Repeat the above steps to assign interfaces to VDOM-B.

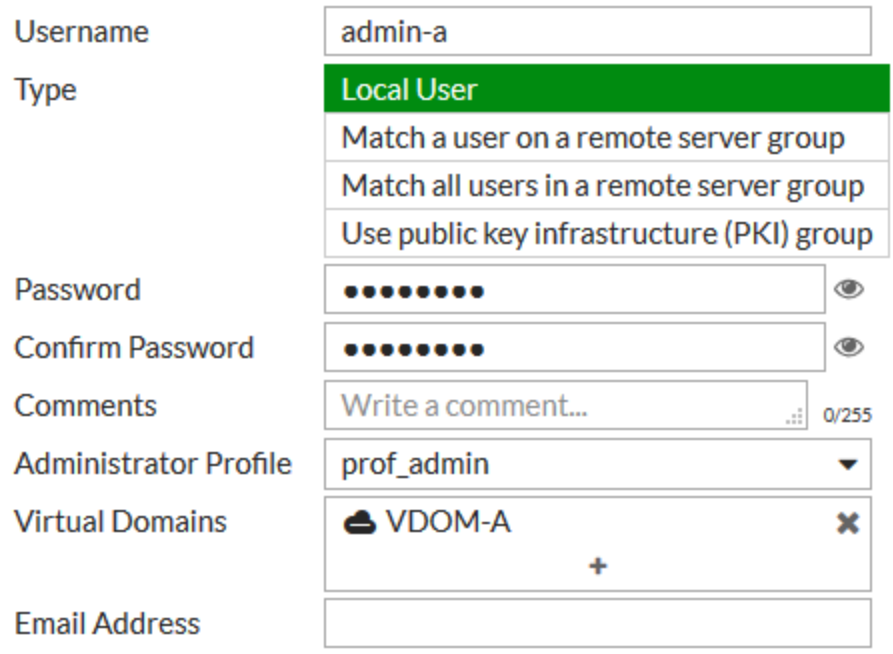
## Creating per-VDOM administrators

Per-VDOM administrator accounts only allow administrative access to specific VDOMs. By creating per-VDOM administrators, you allow both Company A and Company B to manage their respective VDOMs without allowing access to settings for other VDOMs or the global settings.

1. To create a per-VDOM administrator for VDOM-A, go to **System > Administrators** and select **Create New > Administrator**.
2. Enter a **Username** and set **Type** to **Local User**. Enter and confirm a **Password**. Set **Administrator Profile** to **prof_admin**.

You must use either the **prof_admin** or a custom profile for per-VDOM administrators.

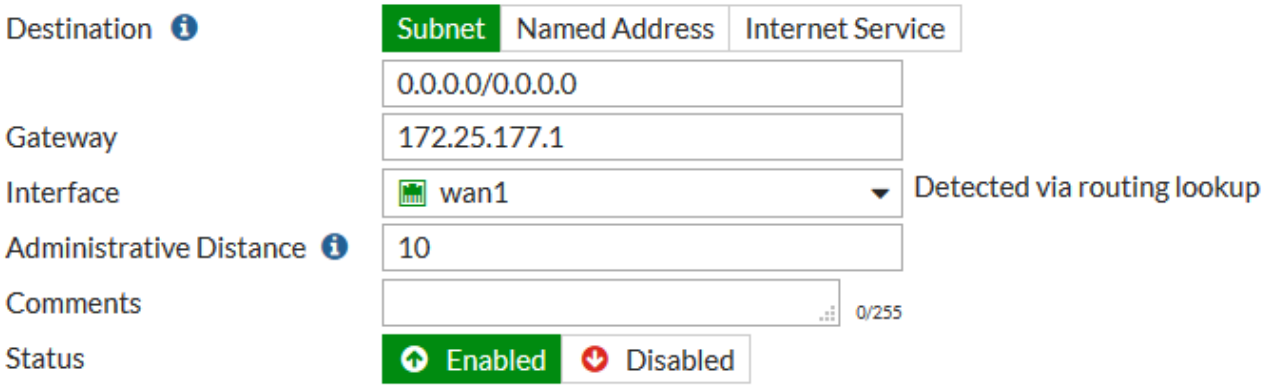
3. Remove the **root** VDOM from the **Virtual Domains** list and add **VDOM-A**.



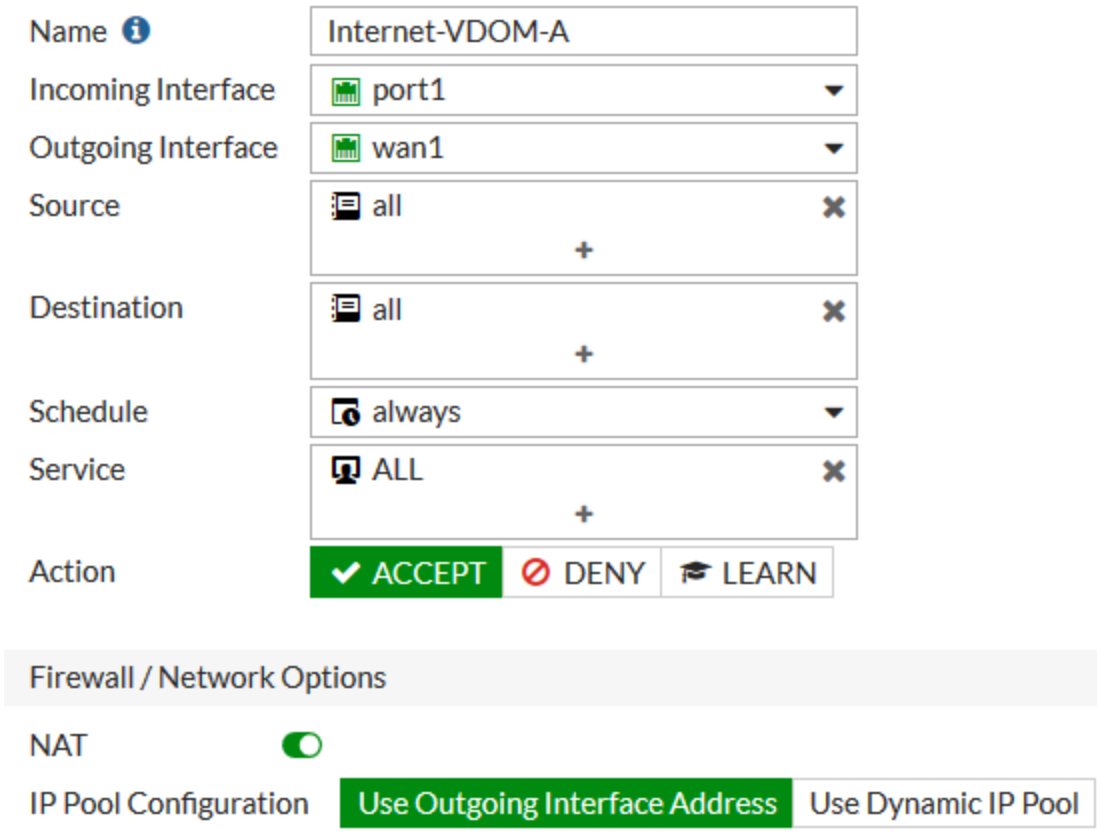

4. Repeat the above steps to create a per-VDOM administrator for VDOM-B.

## Configuring the VDOMs

1. Access VDOM-A using the dropdown menu located in the top-left corner.
2. To add a static route, go to **Network > Static Routes** and select **Create New**.
3. Set **Destination** to **Subnet** and leave the destination IP address set to 0.0.0.0/0.0.0.0.
4. Set **Gateway** to the IP address provided by your ISP and **Interface** to the Internet-facing interface.




5. To create a new policy, go to **Policy & Objects > IPv4 Policy** and select **Create New**.
6. Set the **Incoming Interface** to **port 1** and set the **Outgoing Interface** to **wan 1**.




7. Repeat the above steps to configure VDOM-B.

## Configuring global security profiles

You can create two types of security profiles for VDOMs: per-VDOM profiles that are only available to a specific VDOM, and global security profiles which are available for use by multiple VDOMs. You can use both types of profiles for your configuration.

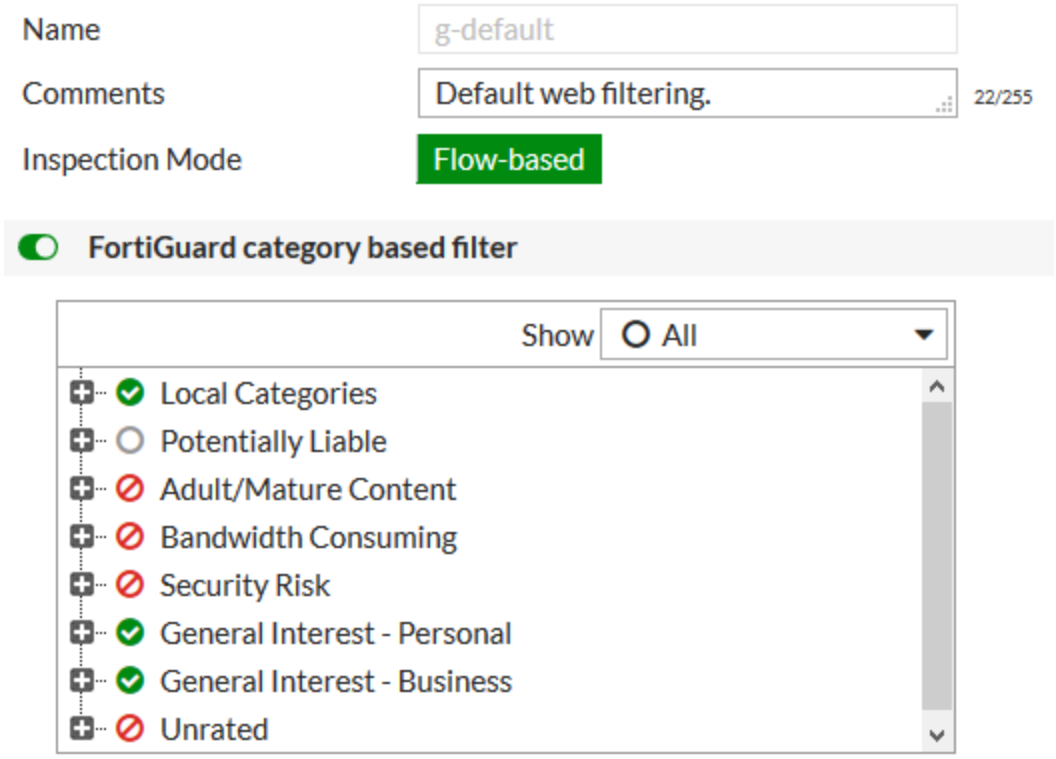
Global profiles are available for the following security features:

- Antivirus
- Application control
- Data leak prevention
- Intrusion prevention
- Web filtering

Each security feature has at least one default global profile. Global profiles are identified by the “g-” at the beginning of the profile name.

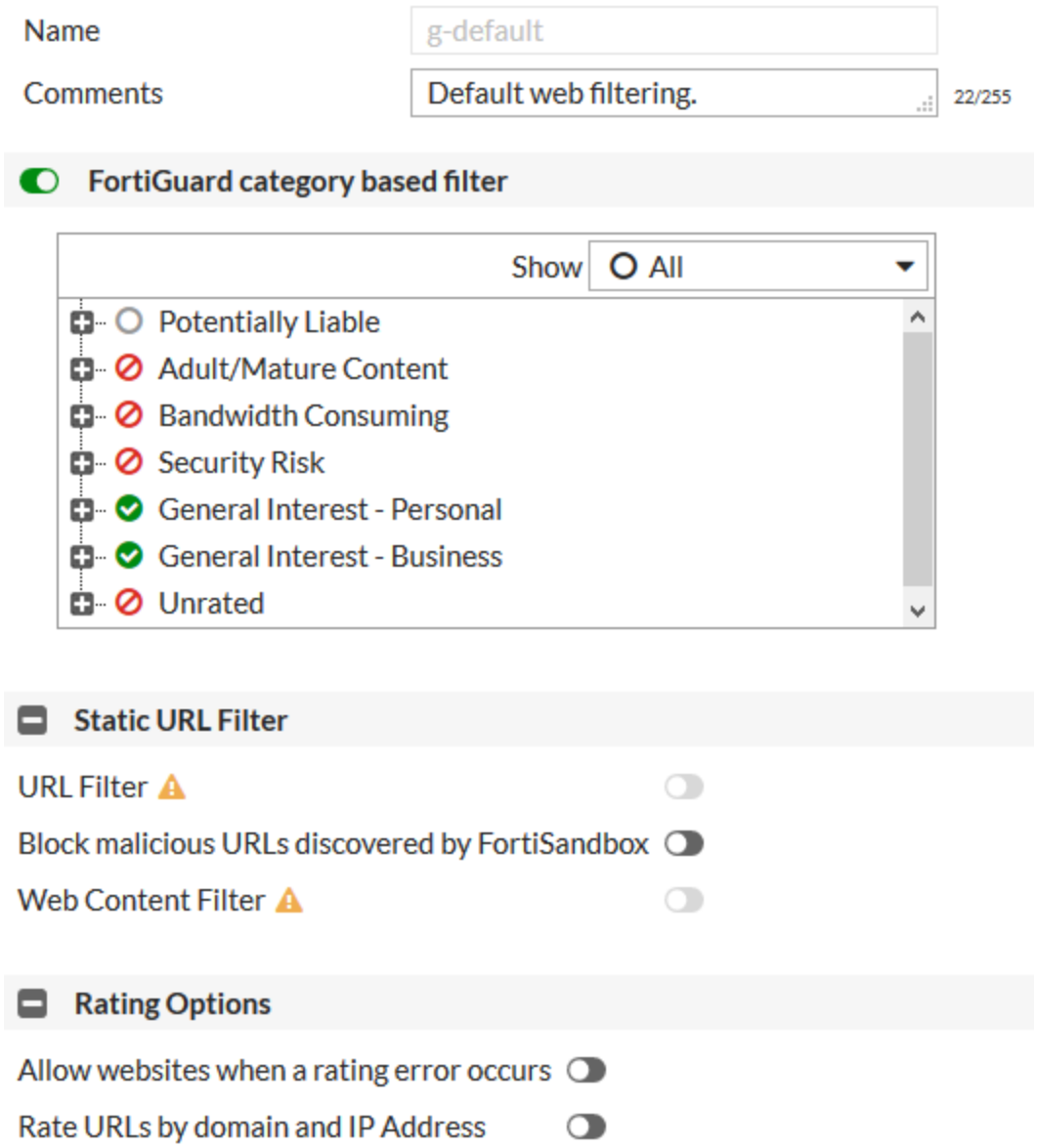
Some security profile features, such as URL filters, are not available for use in a global profile.

1. To edit the default global web filter, go to **Global > Security Profiles > Web Filter** and edit **g-default**.
2. Right-click the **Bandwidth Consuming** category and select **Block**.




## Results

1. Connect to VDOM-A and log in using the VDOM-A administrator account. Only the per-VDOM options are shown.
2. To view the default global web filter, go to **Security Profiles > Web Filter** and select **g-default**. The VDOM-A administrator can't edit the profile.

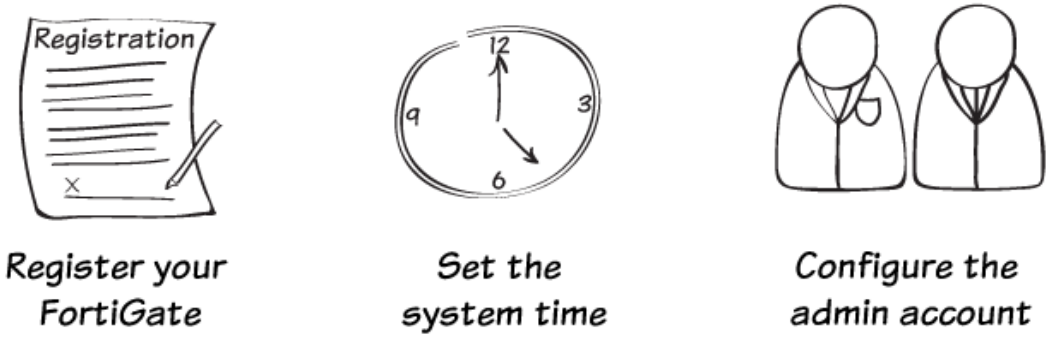



3. To view a summary of the VDOM configuration, connect to the management VDOM and go to **Global > System > VDOM**.

| Name | Operation Mode | Inspection Mode | NGFW Mode | Security Preset | Enable | CPU | Memory | Interfaces | Comments | Ref. |
|---|---|---|---|---|---|---|---|---|---|---|
| VDOM-A | NAT | Flow-based | Profile-based | Custom | ✔ | 0% | 2% | port1<br>ssl.VDOM-A(SSL VPN interface)<br>wan1 | | 5 |
| VDOM-B | NAT | Flow-based | Profile-based | Custom | ✔ | 0% | 2% | port2<br>ssl.VDOM-B(SSL VPN interface)<br>wan2 | | 4 |
| root | NAT | Flow-based | Profile-based | Custom | ✔ | 1% | 16% | dmz ha1 ha2 mgmt modem<br>npu0_vlink0 npu0_vlink1 port3<br>port4 port5 port6 port7 port8<br>port9 port10 port11 port12<br>port13 port14 port15<br>Display More (2 hidden, 22 total) | | 29 |
| | | | | | | Total Usage 1% | Total Usage 20% | | | |

For further reading, check out Virtual domains overview in the FortiOS 6.0 Online Help.

# FortiGate registration and basic settings




In this recipe, you will complete these following basic administrative tasks to get a newly installed FortiGate ready for use:

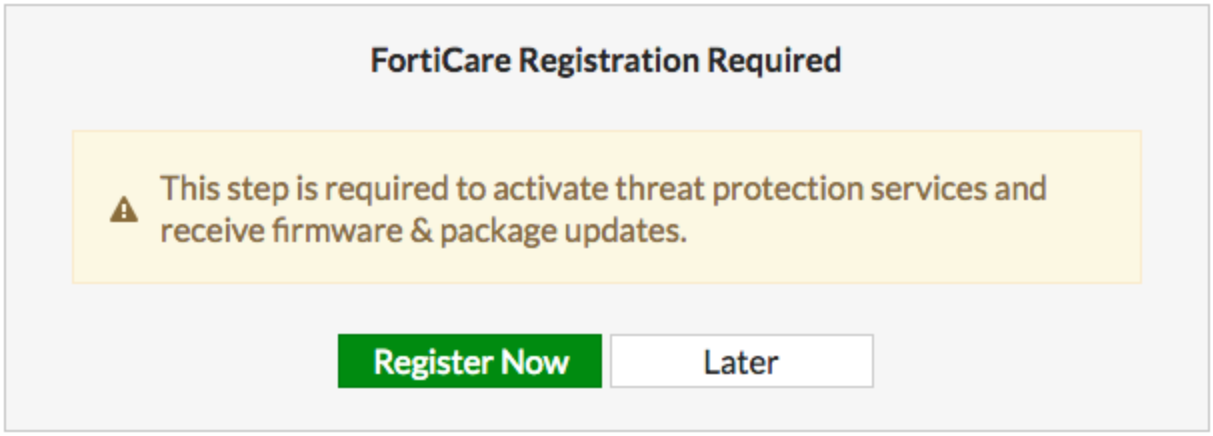
- Register your FortiGate with a Fortinet Support account.
- Set the system time.
- Create a new administrator and edit the default account.
- Restrict administrative access to a trusted host (optional).

## Registering your FortiGate

You must register your FortiGate to receive firmware upgrades, FortiGuard updates, and access to Fortinet Support.

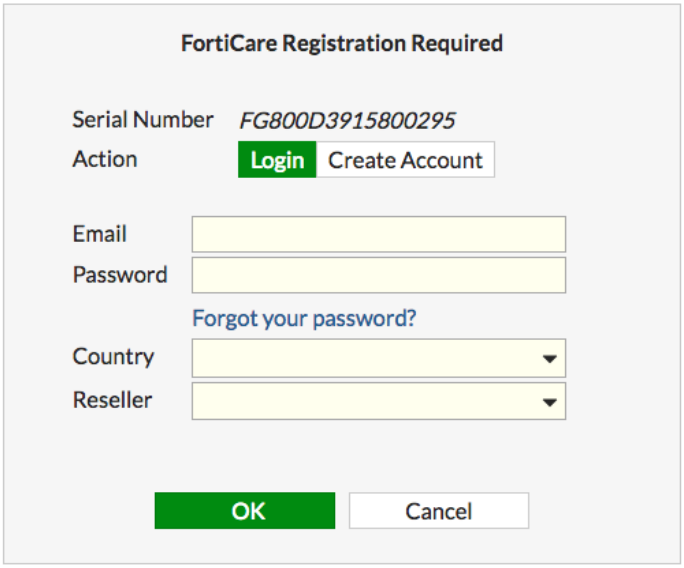
Before you register your FortiGate, it must be connected to the Internet.

1. Connect to your FortiGate. A message appears that states that FortiCare registration is required. Select **Register Now**.

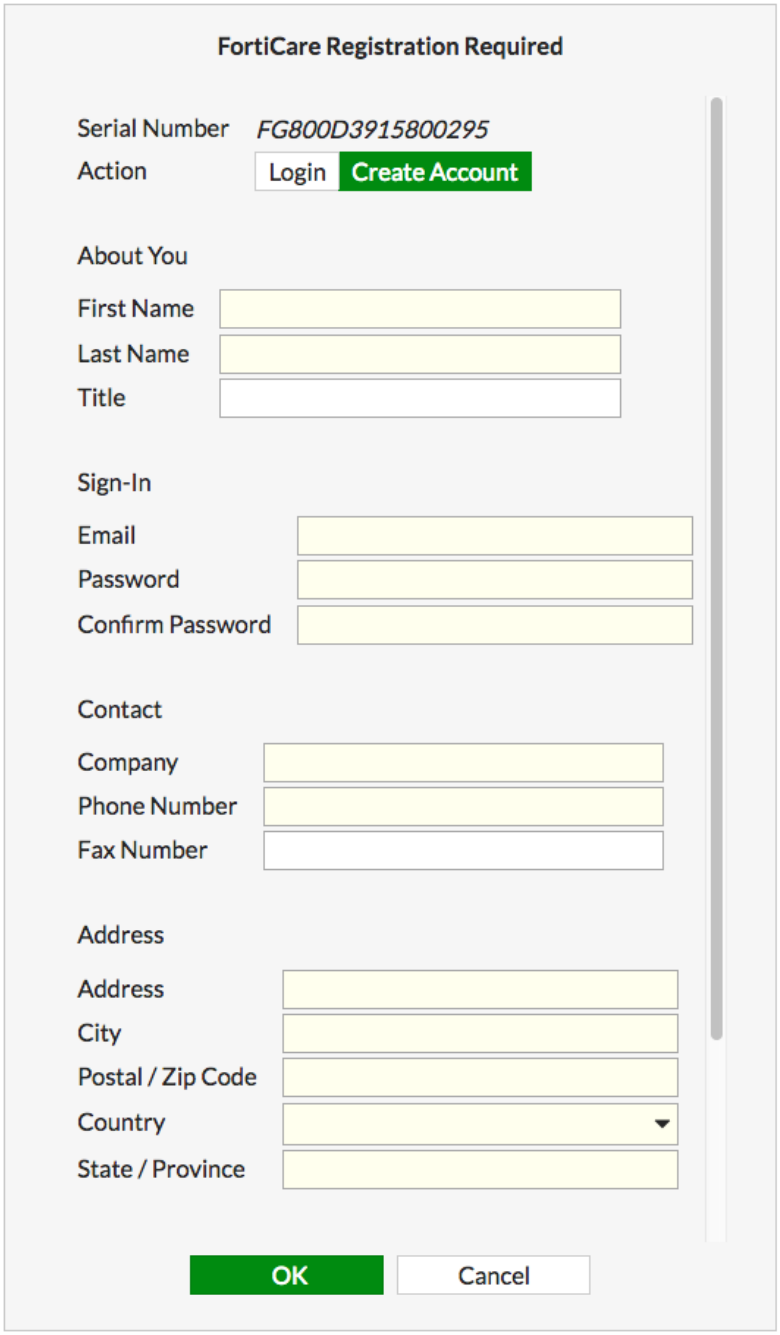



2. To allow Fortinet Support to keep a complete list of your devices, you should use one account to register all of your Fortinet products.

   If you have a Fortinet Support account, set **Action** to **Login**.




   If you need to create an account, set **Action** to **Create Account**.



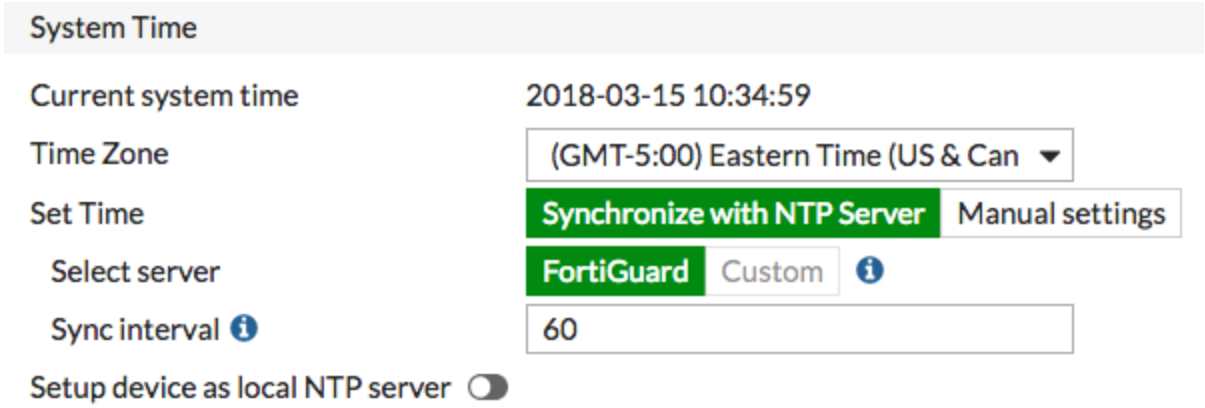

3. Go to **System > FortiGuard**. In **License Information**, **FortiCare Support** appears as **Registered**.

| Contract | Status | |
|---|---|---|
| FortiCare Support | Registered - [redacted] | Launch Portal |

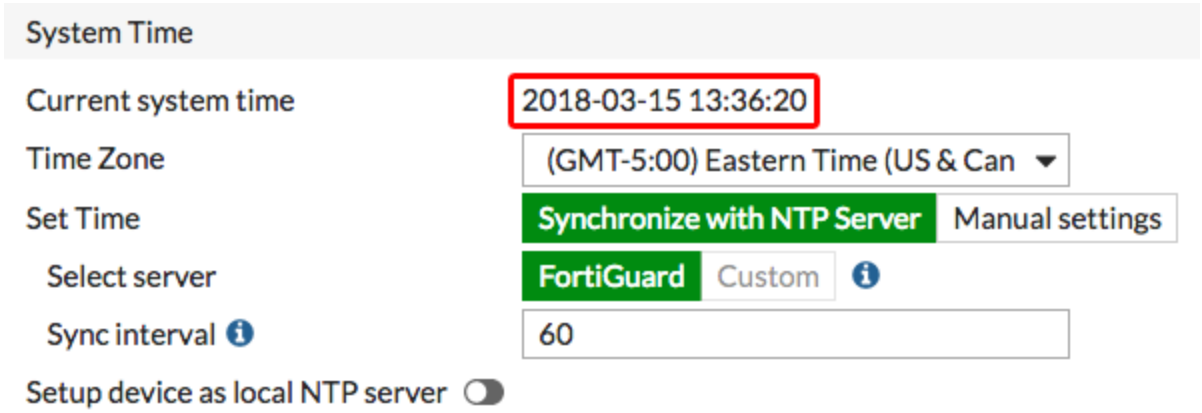
4. Your other FortiGuard licenses now show as licensed. There may be a delay before all of them appear as licensed.

## Setting system time

1. Go to **System > Settings**. Under **System Time**, select your **Time Zone** and either set the time manually or select **Synchronize with NTP Server**.

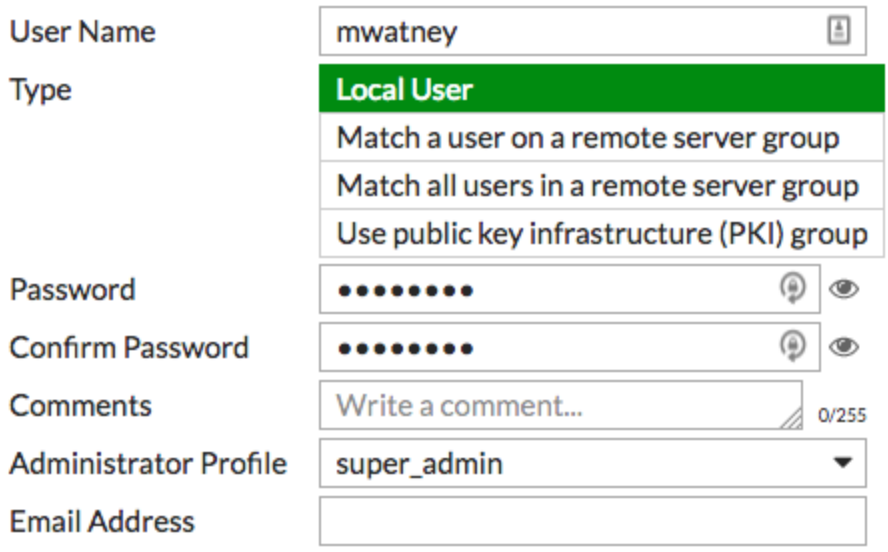



2. **Current system time** displays the correct time.

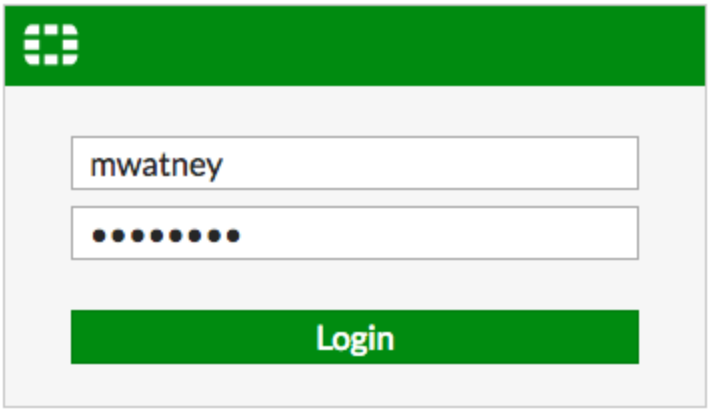



## Creating administrators

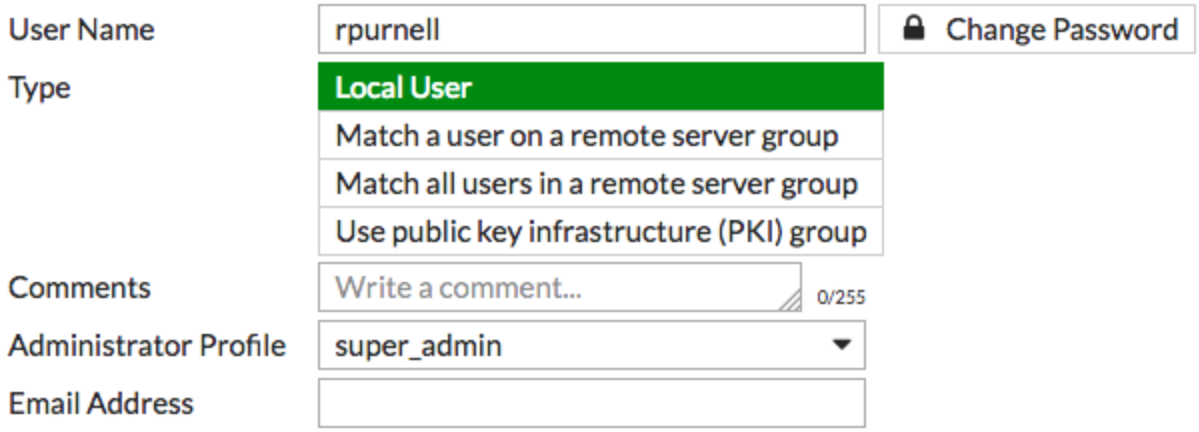
1. Go to **System > Administrators** and create a new account. Set **User Name** and **Password**.
2. Set **Administrator Profile** to **super_admin**. This profile allows the administrator full access to configure the FortiGate.




3. Log out of the FortiGate and log in using your new account.




4. To secure your FortiGate, it's recommended that you change the name and password of the default admin account. Go to **System > Administrators** and edit the default account. Change the **User Name**.

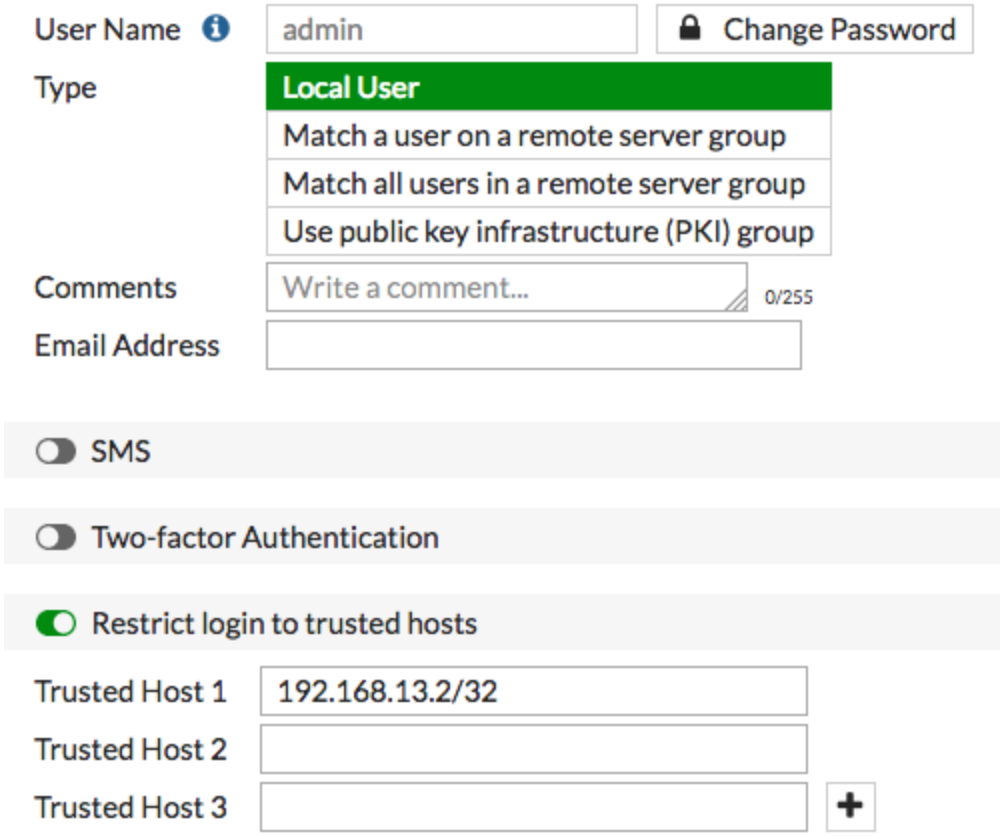



5. Select **Change Password** to add a password to this account.


## Using a trusted host (optional)

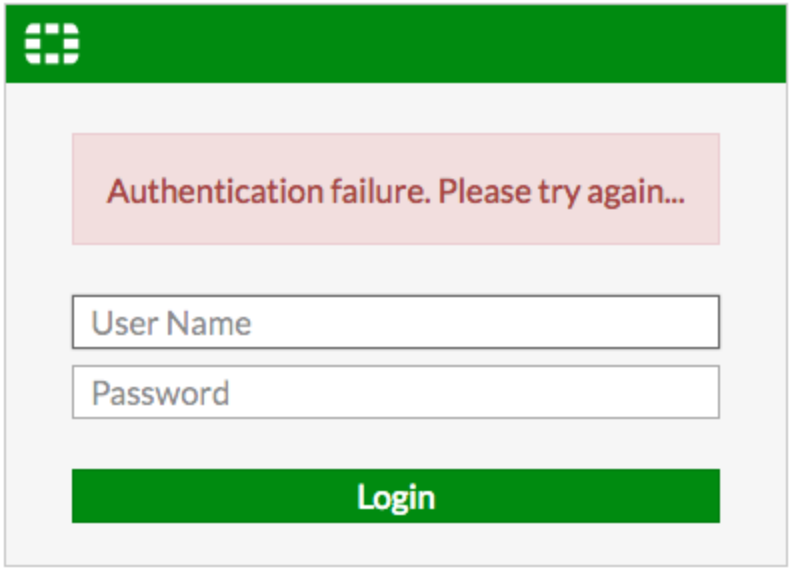
You can configure an administrative account to be accessible only to someone who is using a trusted host. You can set a specific IP address for the trusted host or use a subnet.

1. Go to **System > Administrators** and edit the default admin account.
2. Enable **Restrict login to trusted hosts**. Set **Trusted Host 1** to the static IP address of the computer you use to administer the FortiGate.
3. If required, set additional trusted hosts.

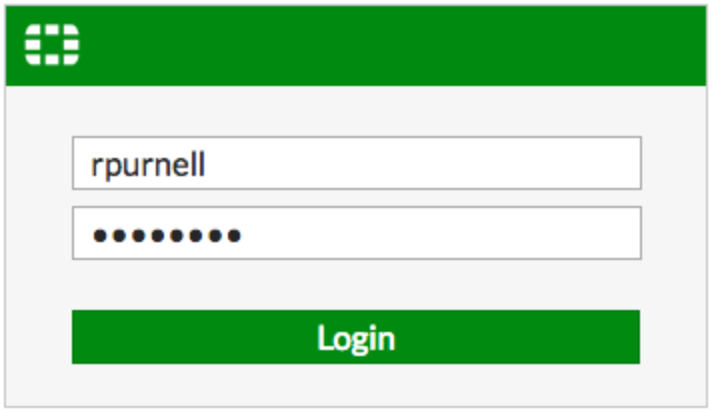


## Results

1. Attempt to log in using the original credentials for the default account. Access is denied.




2. Log in using the new credentials for the default account. Access is granted.




3. Go to **Log & Report > System Events**. You can see the successful and failed login attempts in the events list.

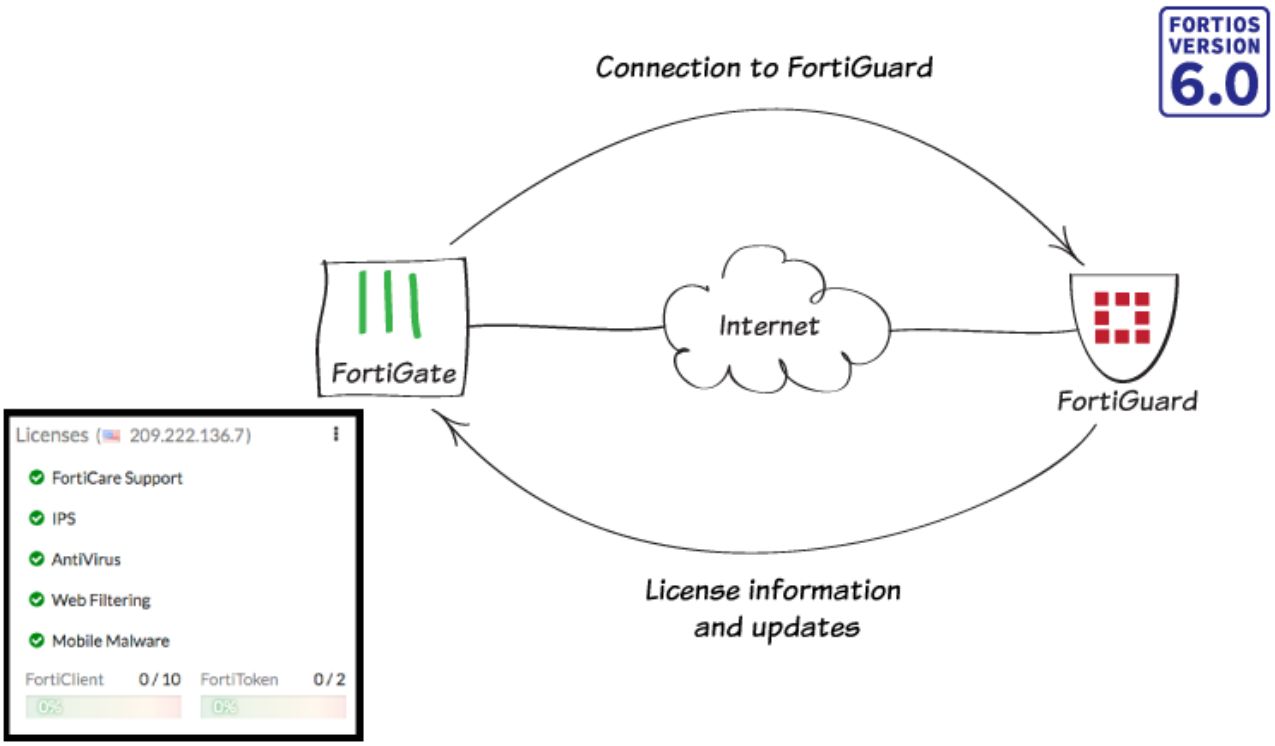
For system events to appear in the GUI, you must configure disk logging in the log settings on the FortiGate. This option is only available on FortiGate models that have an internal hard drive.

| # | Date/Time | Level | User | Message |
|---|---|---|---|---|
| 1 | 14:54:41 | | rpurnell | Administrator rpurnell logged in successfully from https(172.25.177.46) |
| 2 | 14:54:33 | | admin | Administrator admin login failed from https(172.25.177.46) because of invalid user name |

Refresh

For further reading, check out Basic Administration in the FortiOS 6.0 Online Help.

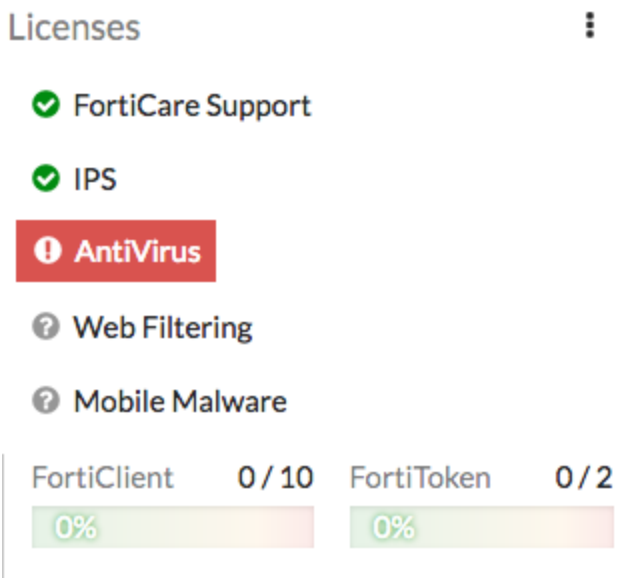
# Verifying FortiGuard licenses and troubleshooting




In this recipe, you verify that your FortiGate displays the correct FortiGuard licenses and troubleshoot any errors. You must register your FortiGate before it can show your FortiGuard licenses.

## Viewing your licenses

1. To view your licenses, go to the **Dashboard** and find the **Licenses** widget. The FortiGuard licenses are listed, with their status indicated:
   - A green check mark indicates an active license.
   - A gray question mark indicates an unavailable license.
   - A license highlighted in orange is either unlicensed or expires soon.
   - A license highlighted in red is expired.




2. The widget only displays licenses for features you enabled in feature visibility. To enable more features, go to **System > Feature Visibility**.
3. The **Web Filtering** license only appears as active when a web filter profile is applied to a firewall policy.

When you apply the profile, a warning will appear stating that web filtering doesn't have a valid license. You can ignore this for the moment.

4. You can also view FortiGuard license information by going to **System > FortiGuard**.

License Information

| Contract | Status | |
|---|---|---|
| FortiCare Support | Registered | Launch Portal |
| Hardware Version | Advanced hardware - expires on 2019/03/17 | |
| Firmware | Web/online - expires on 2019/03/17 | |
| Enhanced Support | 24x7 support - expires on 2019/03/17 | |
| Comprehensive Support | 24x7 support - expires on 2019/03/17 | |
| Application Control Signatures | Version 6.00741 | Upgrade Database |
| IPS | Licensed - expires on 2019/03/17 | Upgrade Database |
| IPS Definitions | Version 6.00741 | |
| IPS Engine | Version 3.00510 | |
| Malicious URLs | Version 1.00930 | |
| AntiVirus | Expired - expired on 2017/07/27 | Upgrade Database |
| AV Definitions | Version 1.00000 | |
| AV Engine | Version 5.00350 | |
| Botnet IPs | Version 3.00300 | View List |
| Botnet Domains | Version 1.00946 | View List |
| Mobile Malware | Unavailable | |
| Mobile Malware Definitions | Version 56.00524 | |
| Web Filtering | Unavailable | |
| FortiClient | Free License | 0% 0 / 10 |

## Troubleshooting

If you need to add or renew a subscription, go to Fortinet Support.

If a license that should be active isn't currently available, you can use the following steps to troubleshoot your connection. After each troubleshooting step, go to **System > FortiGuard** to check if the licenses are now showing as available.

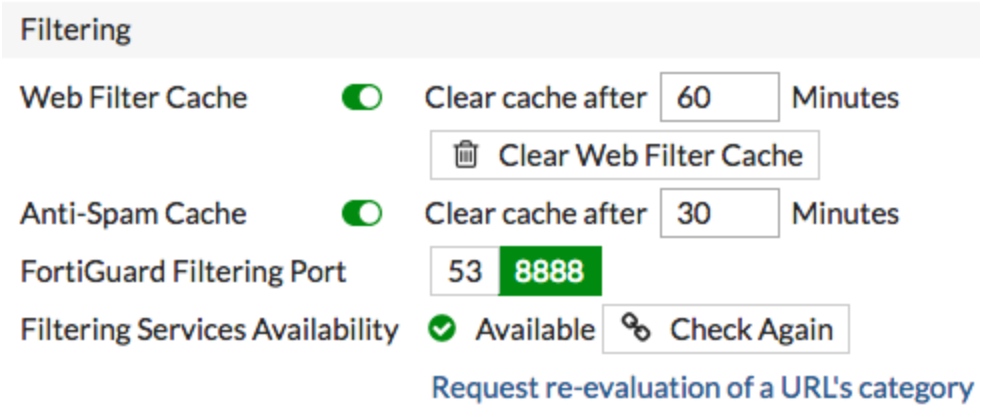
### Connecting to FortiGuard

1. To prompt your FortiGate to connect to FortiGuard, connect to the CLI and use the following command:
```
diagnose debug application update -1
diagnose debug enable
execute update-now
```
2. If your FortiGate has multiple VDOMs, make sure that you use the management VDOM and that the VDOM has Internet access. To set the proper VDOM as the management VDOM, use the following command:
```
config system global
   set management-vdom
end
```

### Checking FortiGuard filtering

1. To test if FortiGuard is reachable, go to **System > FortiGuard**.
2. Under **Filtering**, check **Filtering Services Availability.** If you don't see a green check mark, select **Check Again**.
3. If you still don't see a green check mark, change the **FortiGuard Filtering Port** to the alternate port (8888). Select **Apply** and see if the services become available.

If you're updating FortiGuard using a FortiManager, the **FortiGuard Filtering Port** can also be 80.




### Testing the DNS

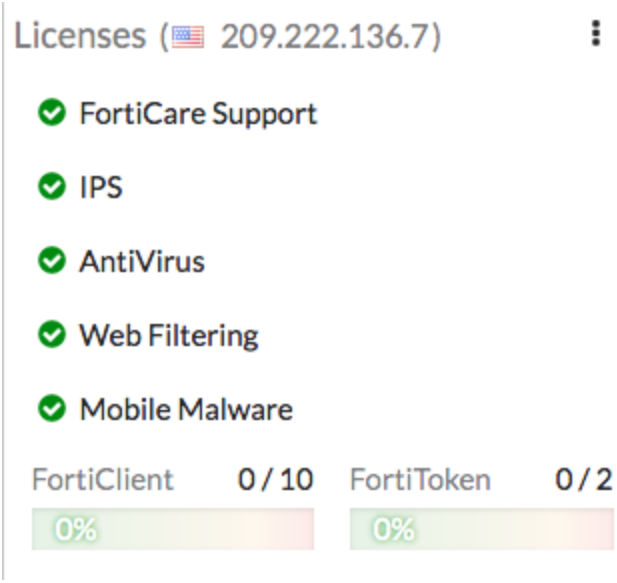
1. To test if your DNS can reach FortiGuard, use the following CLI command:
```
execute ping guard.fortinet.net
```
2. If you can reach the address, run the following command:
```
diagnose debug application update -1
diagnose debug enable
execute update-now
```
3. If you can't reach the address, go to **System > DNS** and verify that the settings are correct. Then run the PING test again.

### Contacting Support

If you still can't connect, contact Fortinet Support.

## Results

1. Go to the **Dashboard** and view the **Licenses** widget. Any subscribed services should have a green check mark beside it.




2. Go to **System > FortiGuard**. Features and services you're subscribed to should have a green check mark beside

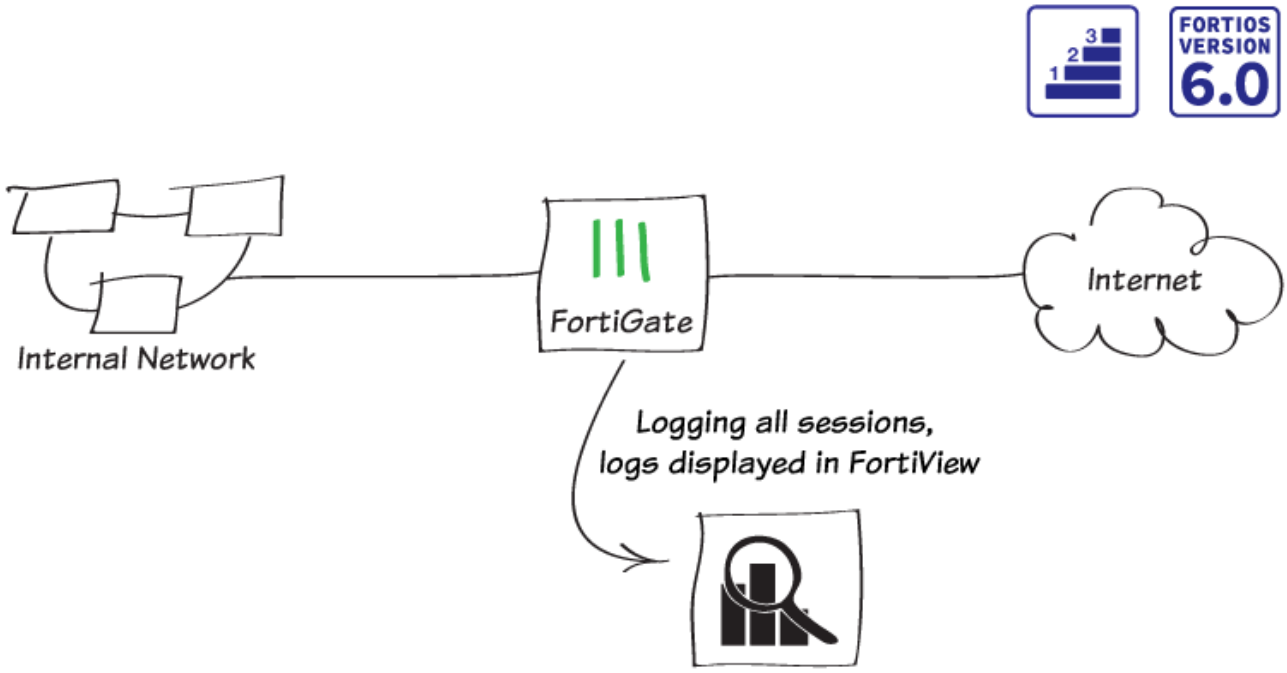
them.

License Information

| Contract | Status | |
|---|---|---|
| FortiCare Support | Registered | Launch Portal |
| Hardware Version | Advanced hardware - expires on 2019/03/17 | |
| Firmware | Web/online - expires on 2019/03/17 | |
| Enhanced Support | 24x7 support - expires on 2019/03/17 | |
| Comprehensive Support | 24x7 support - expires on 2019/03/17 | |
| Application Control Signatures | Version 6.00741 | Upgrade Database |
| IPS | Licensed - expires on 2019/03/17 | Upgrade Database |
| IPS Definitions | Version 6.00741 | |
| IPS Engine | Version 3.00510 | |
| Malicious URLs | Version 1.00930 | |
| AntiVirus | Licensed - expires on 2019/03/17 | Upgrade Database |
| AV Definitions | Version 1.00000 | |
| AV Engine | Version 5.00350 | |
| Botnet IPs | Version 3.00300 | View List |
| Botnet Domains | Version 1.00946 | View List |
| Mobile Malware | Licensed | |
| Mobile Malware Definitions | Version 56.00524 | |
| Web Filtering | Licensed - expires on 2019/03/17 | |
| FortiClient | Free License | 0% 0 / 10 |

For further reading, check out FortiGuard in the FortiOS 6.0 Handbook.

# Logging FortiGate traffic and using FortiView



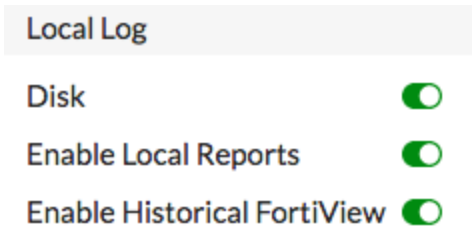

In this example, you will configure logging to record information about sessions processed by your FortiGate. You will then use FortiView to look at the traffic logs and see how your network is being used.

FortiView is a logging tool that contains dashboards that show real time and historical logs. You can filter the dashboards to show specific results and also drill down for more information about a particular session. Each dashboard focuses on a different aspect of your network traffic, such as traffic sources of WiFi clients.

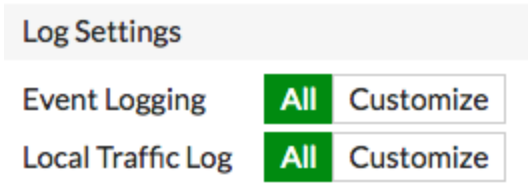
Some FortiView dashboards, such as applications and web sites, require you to apply security profiles to traffic before you can view results.

## Configuring log settings

1. To configure log settings, go to **Log & Report > Log Settings**.
2. Select where you want to record log messages. This example uses **Local Log**, because it is required by FortiView. You can also use **Remote Logging and Archiving** to send logs to either a FortiAnalyzer/FortiManager, FortiCloud, or a syslog server.
3. Enable **Disk**, **Local Reports**, and **Historical FortiView**.




4. Under **Log Settings**, set both **Event Logging** and **Local Traffic Log** to **All**.




## Enabling logging

Because logging all sessions uses more system resources, it is typically recommended to log only security events. However, for the purpose of this recipe, all sessions will be logged to ensure that logging has been configured correctly.

1. To edit the Internet policy, go to **Policy & Objects > IPv4 Policy**.
2. Under **Logging Options**, enable **Log Allowed Traffic** and select **All Sessions**.


## Results

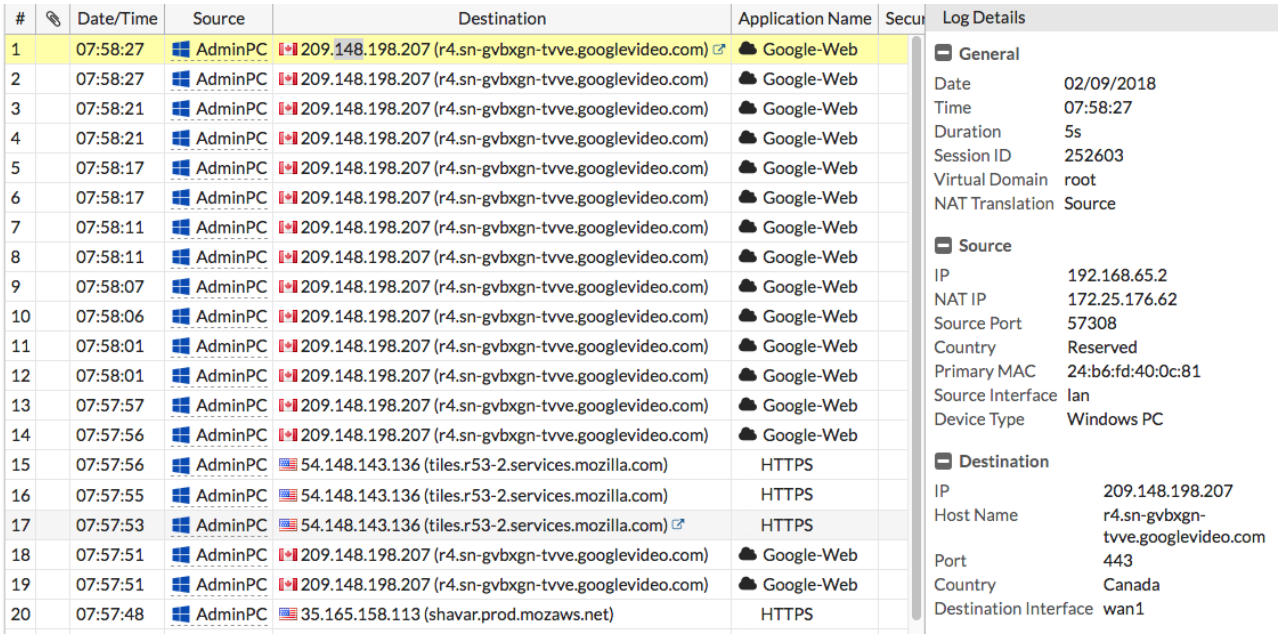
1. Browse the Internet to generate traffic through the FortiGate.
2. To view a realtime display of all active sessions, go to **FortiView > All Segments > All Sessions**.

| Source | Source Device | Source Interface | Destination | Destination Device | Destination Interface | Application | Bytes (Sent/Received) | Policy |
|---|---|---|---|---|---|---|---|---|
| 192.168.65.2 | AdminPC | lan | 172.217.6.227 | | wan1 | TCP/443 | 166.03 kB | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 172.217.10.2 | | wan1 | TCP/443 | 6.98 kB | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 208.91.112.52 | | wan1 | UDP/53 | 432 B | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 8.253.151.248 | | wan1 | TCP/80 | 73.28 kB | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 8.253.151.248 | | wan1 | TCP/80 | 1.31 MB | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 208.91.112.52 | | wan1 | UDP/53 | 249 B | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 208.91.112.52 | | wan1 | UDP/53 | 408 B | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 208.91.112.52 | | wan1 | UDP/53 | 197 B | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 208.91.112.53 | | wan1 | UDP/53 | 410 B | Internet (1) |
| 192.168.65.2 | AdminPC | lan | 208.91.112.52 | | wan1 | UDP/53 | 410 B | Internet (1) |

3. If you right-click a session in the list, you can choose to end the session, end all sessions, ban the source IP, or filter logs by the source device.

4. Select the **24 hours view**. You can see a historical view of your traffic. To see more information, doubleclick a session.

Historical views are only available on FortiGate models with internal hard drives.



| # | Date/Time | Source | Destination | Application Name | Secu |
|---|---|---|---|---|---|
| 1 | 07:58:27 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 2 | 07:58:27 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 3 | 07:58:21 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 4 | 07:58:21 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 5 | 07:58:17 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 6 | 07:58:17 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 7 | 07:58:11 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 8 | 07:58:11 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 9 | 07:58:07 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 10 | 07:58:06 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 11 | 07:58:01 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 12 | 07:58:01 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 13 | 07:57:57 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 14 | 07:57:56 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 15 | 07:57:56 | AdminPC | 54.148.143.136 (tiles.r53-2.services.mozilla.com) | HTTPS | |
| 16 | 07:57:55 | AdminPC | 54.148.143.136 (tiles.r53-2.services.mozilla.com) | HTTPS | |
| 17 | 07:57:53 | AdminPC | 54.148.143.136 (tiles.r53-2.services.mozilla.com) | HTTPS | |
| 18 | 07:57:51 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 19 | 07:57:51 | AdminPC | 209.148.198.207 (r4.sn-gvbxgn-tvve.googlevideo.com) | Google-Web | |
| 20 | 07:57:48 | AdminPC | 35.165.158.113 (shavar.prod.mozaws.net) | HTTPS | |

Log Details

General

| | |
|---|---|
| Date | 02/09/2018 |
| Time | 07:58:27 |
| Duration | 5s |
| Session ID | 252603 |
| Virtual Domain | root |
| NAT Translation | Source |

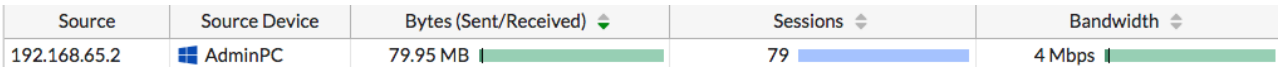
Source

| | |
|---|---|
| IP | 192.168.65.2 |
| NAT IP | 172.25.176.62 |
| Source Port | 57308 |
| Country | Reserved |
| Primary MAC | 24:b6:fd:40:0c:81 |
| Source Interface | lan |
| Device Type | Windows PC |

Destination

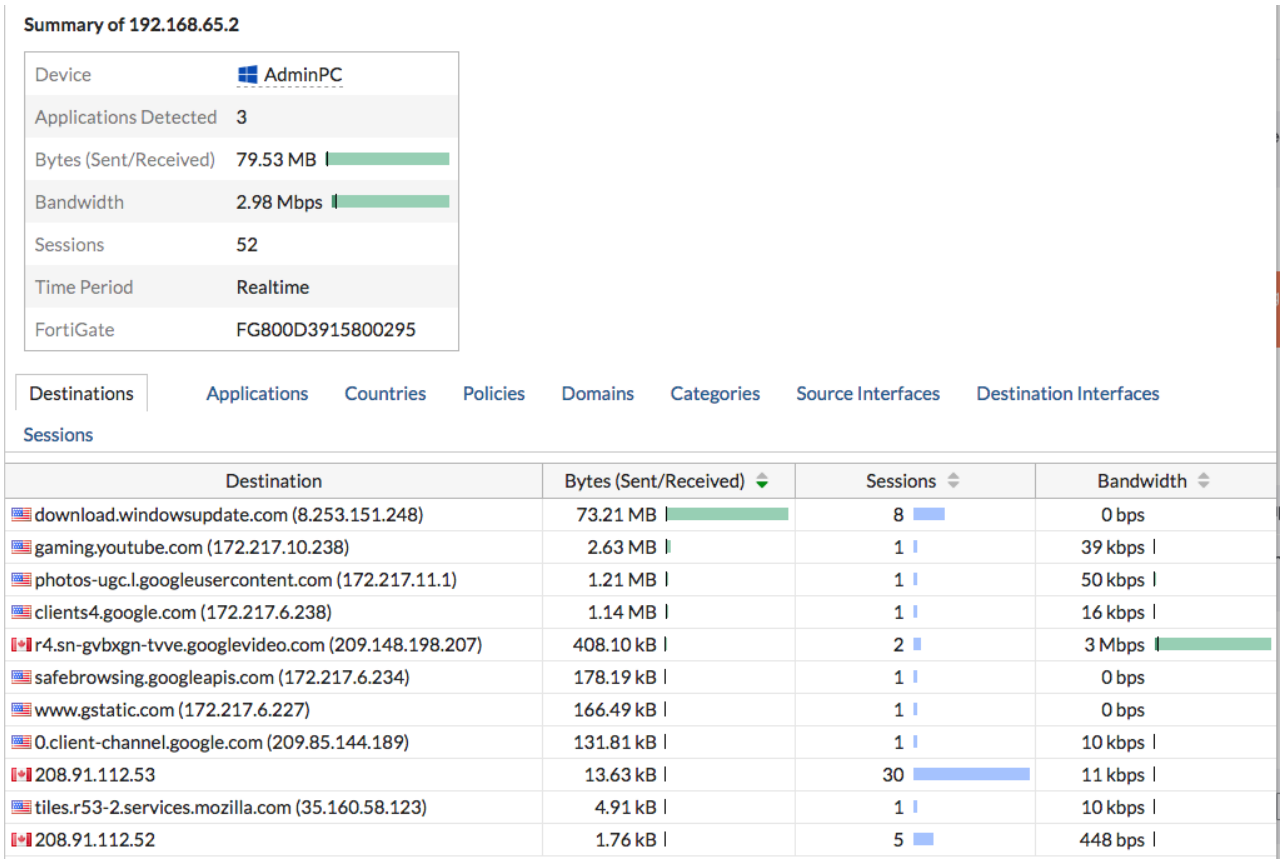
| | |
|---|---|
| IP | 209.148.198.207 |
| Host Name | r4.sn-gvbxgn-tvve.googlevideo.com |
| Port | 443 |
| Country | Canada |
| Destination Interface | wan1 |

5. To view a list of the sources in your network traffic, go to **FortiView > Traffic from LAN/DMZ > Sources**.



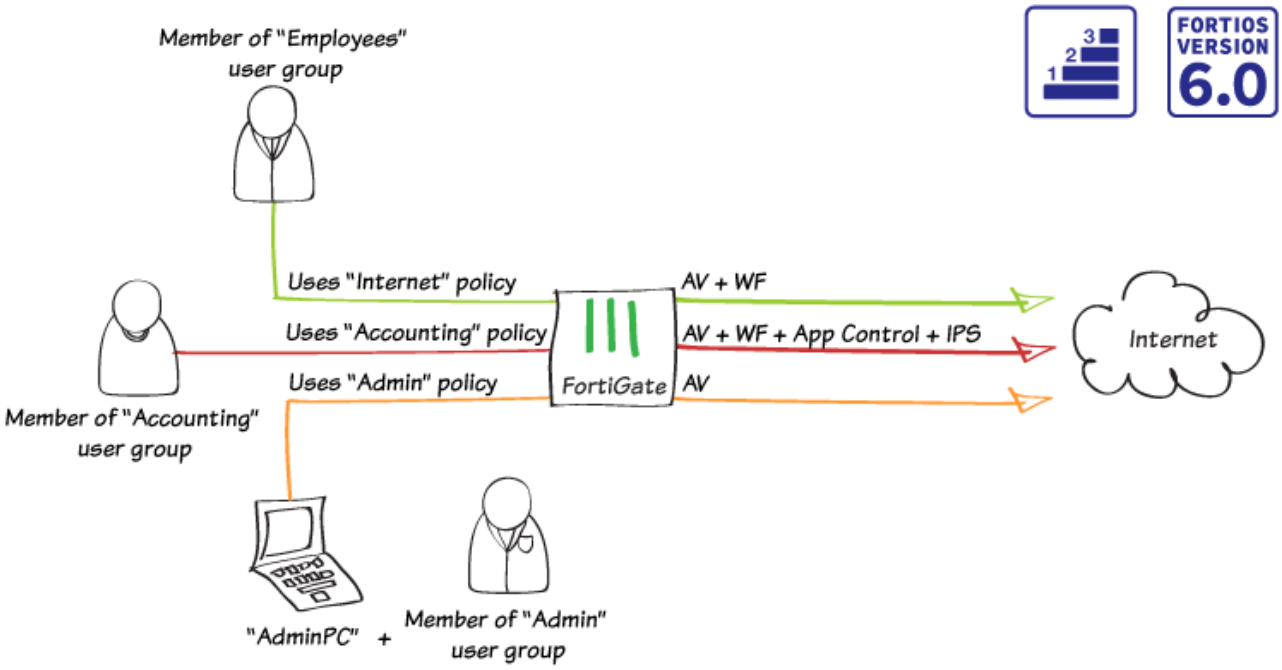
| Source | Source Device | Bytes (Sent/Received) | Sessions | Bandwidth |
|---|---|---|---|---|
| 192.168.65.2 | AdminPC | 79.95 MB | 79 | 4 Mbps |

6. Right-click on any source listed and select Drill Down to Details. You can view a variety of information about the source address, including traffic destinations, security policies used, and if any threats are linked to traffic from this address.




For further reading, check out FortiView in the FortiOS 6.0 Online Help.

# Creating security policies for different users




In this recipe, you will create multiple security policies, which will apply security inspection to different users based on which user group they belong to.

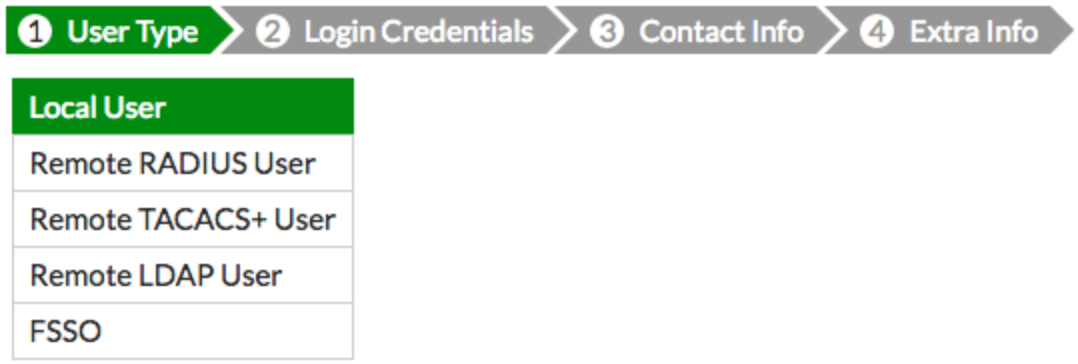
This example contains three IPv4 policies:

- *Internet*: The policy that the *Employee* user group uses to access the Internet. You use the FortiGate to apply some security inspection to traffic.
- *Accounting*: The policy that the *Accounting* user group uses to access the Internet. You use the FortiGate to apply increased security inspection to protect sensitive information.
- *Admin*: The policy that the *Admin* user group uses, connecting from a specific computer, to access the Internet. You use the FortiGate to apply limited security inspection.

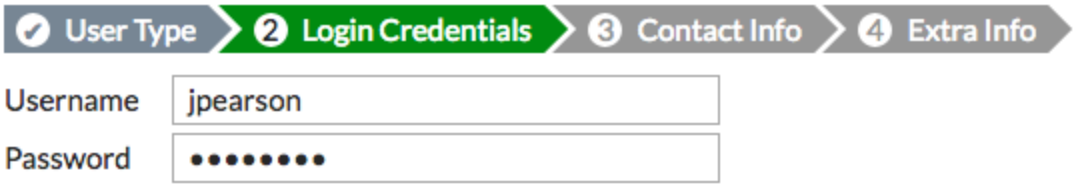
For information about creating the Internet policy, see Installing a FortiGate in NAT mode on page 10.

## Creating the Employee user and policy

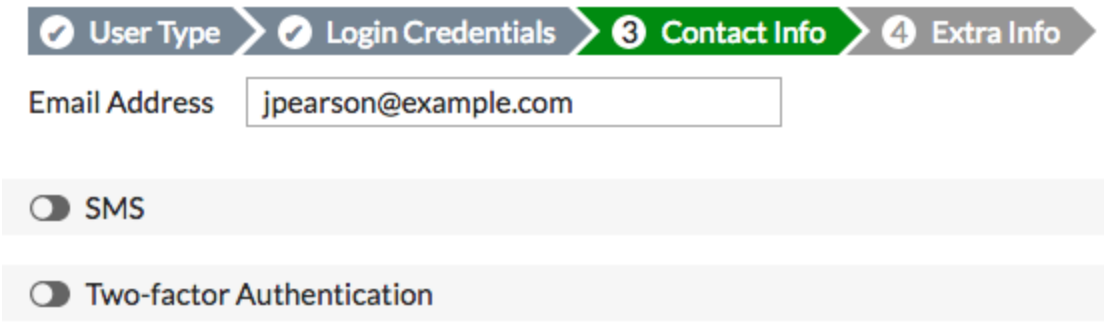
1. To create a new user, go to **User & Device > User Definition** (in the example, this account is called *jpearson*).
2. In the **User Type** section, select **Local User**.



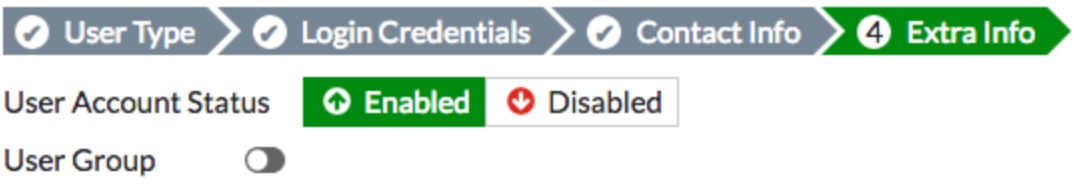

3. In the **Login Credentials** section, set **Username** and set a **Password**.




4. In the **Contact info** section, set the user's **Email Address**.



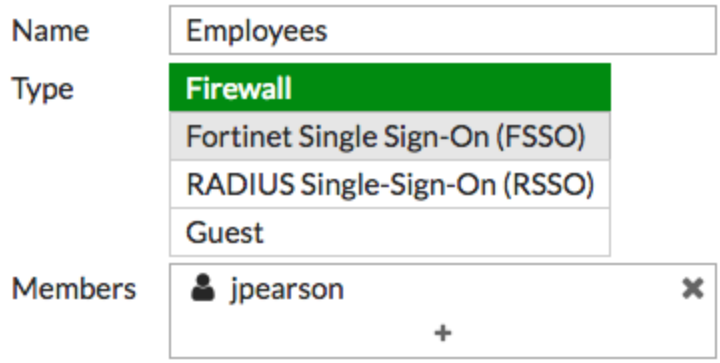

5. In the **Extra Info** section, verify that **User Account Status** is **Enabled**.




6. Your FortiGate now lists the new user.

| User Name | Type | Two-factor Authentication | Ref. |
|---|---|---|---|
| guest | LOCAL | | 1 |
| jpearson | LOCAL | | 0 |

7. To create a new user group, go to **User & Device > User Groups** (in the example, this group is called *Employees*). Add user **jpearson** to the **Members** list.

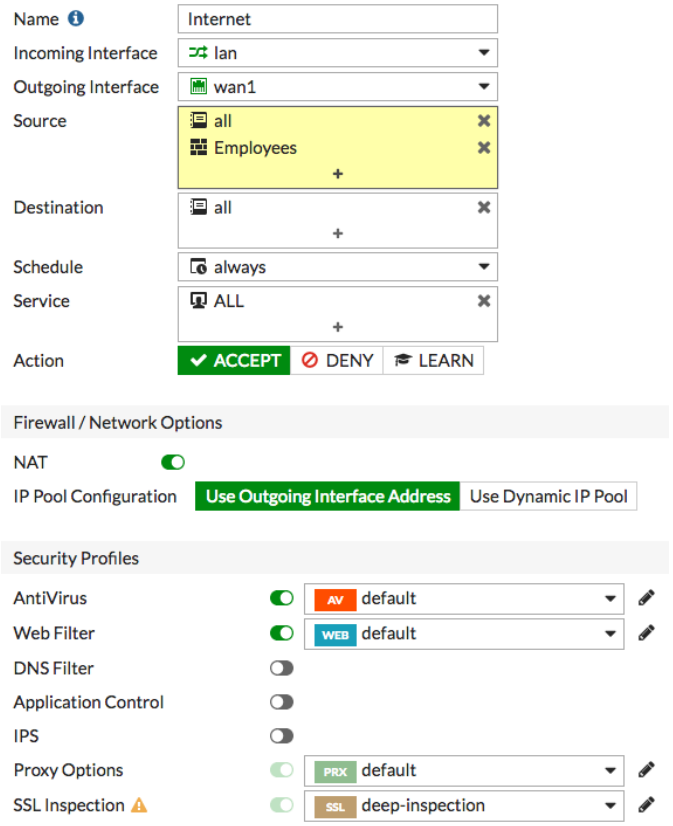



8. The FortiGate now lists the new user group.

| Group Name | Group Type | Members | Ref. |
|---|---|---|---|
| Employees (1 Members) | Firewall | jpearson | 0 |
| Guest-group (1 Members) | Firewall | guest | 0 |
| SSO_Guest_Users (0 Members) | Fortinet Single Sign-On (FSSO) | | 1 |

9. To edit the Internet policy, go to **Policy & Objects > IPv4 Policy**.
10. For **Source**, set **Address** to **all** and **User** to the **Employees** group.
11. Under **Security Profiles**, enable **AntiVirus** and **Web Filter**. Set both to use the default profile.
12. **SSL Inspection** is enabled by default. Set it to the **deep-inspection** profile.

Using the **deep-inspection** profile may cause certificate errors.




## Creating the Accounting user and policy

1. To create another user, go to **User & Device > User Definition** and select **Create New** (in the example, *akeating*).

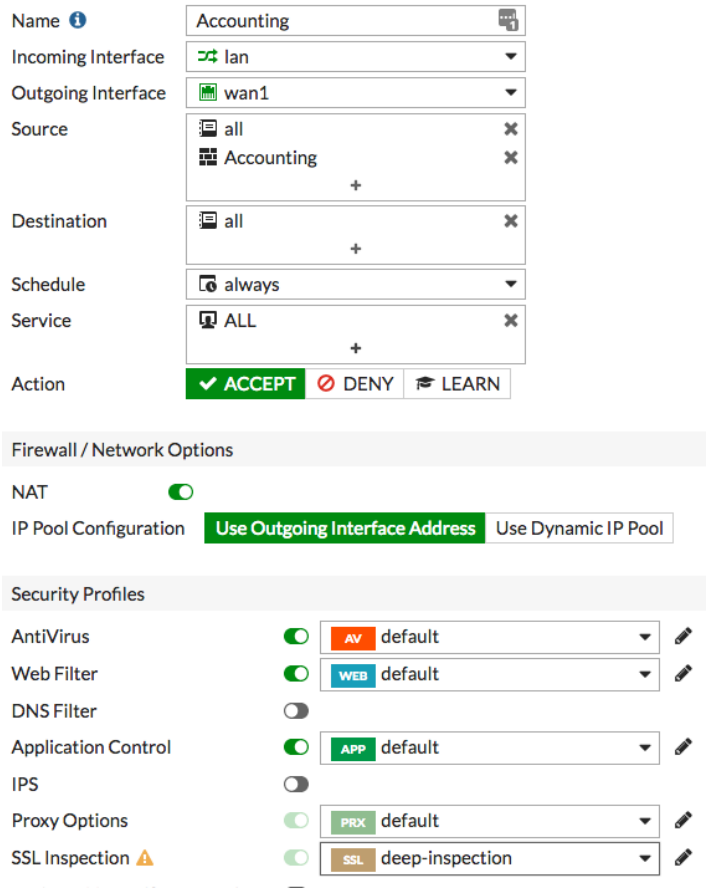
| User Name | Type | Two-factor Authentication | Ref. |
|---|---|---|---|
| akeating | LOCAL | | 0 |
| guest | LOCAL | | 1 |
| jpearson | LOCAL | | 2 |

2. To create another user group, go to **User & Device > User Groups** and select **Create New** (in the example, *Accounting*). Add user **akeating** to the **Members** list.

| Group Name | Group Type | Members | Ref. |
|---|---|---|---|
| Accounting (1 Members) | Firewall | akeating | 0 |
| Employees (1 Members) | Firewall | jpearson | 1 |
| Guest-group (1 Members) | Firewall | guest | 0 |
| SSO_Guest_Users (0 Members) | Fortinet Single Sign-On (FSSO) | | 1 |

3. To create a new *Accounting* policy, go to **Policy & Objects > IPv4 Policy** and **select Create New.**
4. For **Source**, set **Address** to **all** and **User** to the **Accounting** group.

5. Under **Security Profiles**, enable **AntiVirus**, **Web Filter**, **Application Control**, and **IPS**. Set all of these to use the **default** profile.
6. **SSL Inspection** is enabled by default. Set it to the **deep-inspection** profile.




## Creating the Admin user, device, and policy

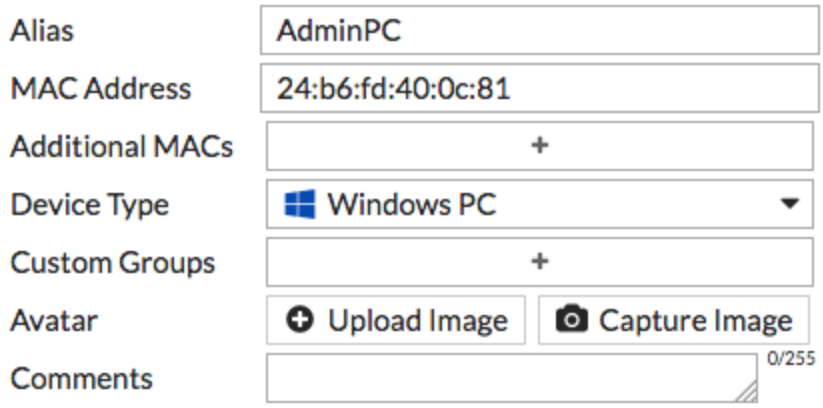
1. To create another user, go to **User & Device > User Definition** and select **Create New** (in the example, *tal-jamil*).

| User Name | Type | Two-factor Authentication | Ref. |
|---|---|---|---|
| akeating | LOCAL | | 1 |
| guest | LOCAL | | 1 |
| jpearson | LOCAL | | 1 |
| tal-jamil | LOCAL | | 0 |

2. To create another user group, go to **User & Device > User Groups** and select **Create New** (in the example, *Admin*). Add user **tal-jamil** to the Members list.

| Group Name | Group Type | Members | Ref. |
|---|---|---|---|
| Accounting (1 Members) | Firewall | akeating | 1 |
| Admin (1 Members) | Firewall | tal-jamil | 0 |
| Employees (1 Members) | Firewall | jpearson | 1 |
| Guest-group (1 Members) | Firewall | guest | 0 |
| SSO_Guest_Users (0 Members) | Fortinet Single Sign-On (FSSO) | | 1 |

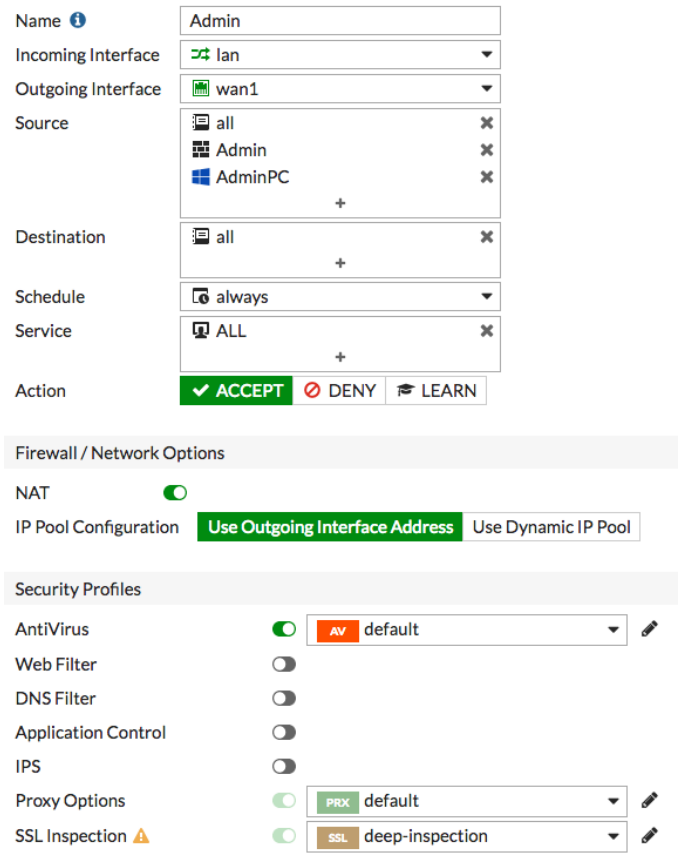
3. To add a new device, go to **User & Device > Custom Devices & Groups** and select **Create New**.
4. Set **Alias** to *AdminPC* and enter the **MAC Address** of the PC. Select the appropriate **Device Type**.




5. The PC is now listed under **Custom Devices**.

| Custom Devices (1) | | |
|---|---|---|
| AdminPC | 192.168.65.2 | |
| **Custom Device Groups (3)** | | |
| Mobile Devices *8 Members* | Android Phone, Android Tablet, BlackBerry Phone, BlackBerry PlayBook, iPad, iPhone, Windows Phone, Windows Tablet | Phones, tablets, etc. |
| Network Devices *3 Members* | Fortinet Device, Other Network Device, Router/NAT Device | Routers, firewalls, gateways, e… |
| Others *2 Members* | Gaming Console, Media Streaming | Other devices. |

6. To create a new *Admin* policy, go to **Policy & Objects > IPv4 Policy** and select **Create New**.
7. For **Source**, set **Address** to **all**, **User** to the **Admin** group, and **Device** to the **AdminPC**.
8. Under **Security Profiles**, enable **AntiVirus** and set it to use the **default** profile.
9. **SSL Inspection** is enabled by default. Set it to the **deep-inspection** profile.




## Ordering the policy table

1. To view the policy table, go to **Policy & Objects > IPv4 Policy**. Select the **By Sequence** view, which shows the policies in the order that they are used by your FortiGate.

   Currently, the policies are arranged in the order you created them, with the oldest policy at the top of the list.

| ID | Name | From | To | Source | Destination | Schedule | Service | Action | NAT | Security Profiles | Log | Bytes |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Internet | lan | wan1 | all<br>Employees | all | always | ALL | ACCEPT | Enabled | AV default<br>WEB default<br>SSL deep-inspection | UTM | 478.00 MB |
| 2 | Accounting | lan | wan1 | all<br>Accounting | all | always | ALL | ACCEPT | Enabled | AV default<br>WEB default<br>APP default<br>SSL deep-inspection | UTM | 0 B |
| 3 | Admin | lan | wan1 | all<br>Admin<br>AdminPC | all | always | ALL | ACCEPT | Enabled | AV default<br>SSL deep-inspection | UTM | |
| 0 | Implicit Deny | any | any | all | all | always | ALL | DENY | | | Disabled | 467.88 kB |

2. To have the correct traffic flowing through each policy, you must arrange them so that the more specific policies are located at the top.

   To rearrange the policies, select the column on the far left (in the example, ID) and drag the policy to the required

position, as shown on the right.

| ID | Name | From | To | Source | Destination | Schedule | Service | Action | NAT | Security Profiles | Log | Bytes |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | Admin | lan | wan1 | all<br>Admin<br>AdminPC | all | always | ALL | ACCEPT | Enabled | AV default<br>SSL deep-inspection | UTM | 0 B |
| 2 | Accounting | lan | wan1 | all<br>Accounting | all | always | ALL | ACCEPT | Enabled | AV default<br>WEB default<br>APP default<br>SSL deep-inspection | UTM | 0 B |
| 1 | Internet | lan | wan1 | all<br>Employees | all | always | ALL | ACCEPT | Enabled | AV default<br>WEB default<br>SSL deep-inspection | UTM | 478.00 MB |
| 0 | Implicit Deny | any | any | all | all | always | ALL | DENY | | | Disabled | 529.54 kB |

## Results

1. From any PC in the internal network, attempt to browse the Internet. A log in screen will appear. Use the **jpearson** account to log in. After authentication, you can connect to the Internet.

If a certificate error occurs during the authentication process, browse to a different site and re-attempt user authentication.


2. Go to **Monitor > Firewall User Monitor**. The list shows **jpearson** is online.

| User Name | User Group | Duration | IP Address | Traffic Volume | Method |
|---|---|---|---|---|---|
| jpearson | Employees | 1 minute 39 seconds | 192.168.65.3 | 3.52 MB | Firewall |

3. Right-click the account and select **Deauthenticate**.
4. On the same PC, attempt to browse the Internet again. This time, log in using the **akeating** account.

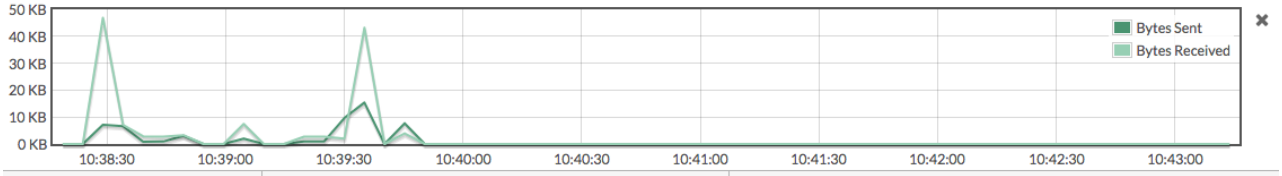
5. The **Firewall User Monitor** now shows **akeating** is online and you can access the Internet.

| User Name | User Group | Duration | IP Address | Traffic Volume | Method |
|---|---|---|---|---|---|
| akeating | Accounting | 51 seconds | 192.168.65.3 | 291.08 kB | Firewall |

6. From the **AdminPC**, attempt to browse the Internet. Log in using the **tal-jamil** account.
7. The **Firewall User Monitor** now shows **tal-jamil** is online and you can access the Internet.

| User Name | User Group | Duration | IP Address | Traffic Volume | Method |
|---|---|---|---|---|---|
| tal-jamil | Admin | 1 minute 32 seconds | 192.168.65.2 | 334.73 kB | Firewall |

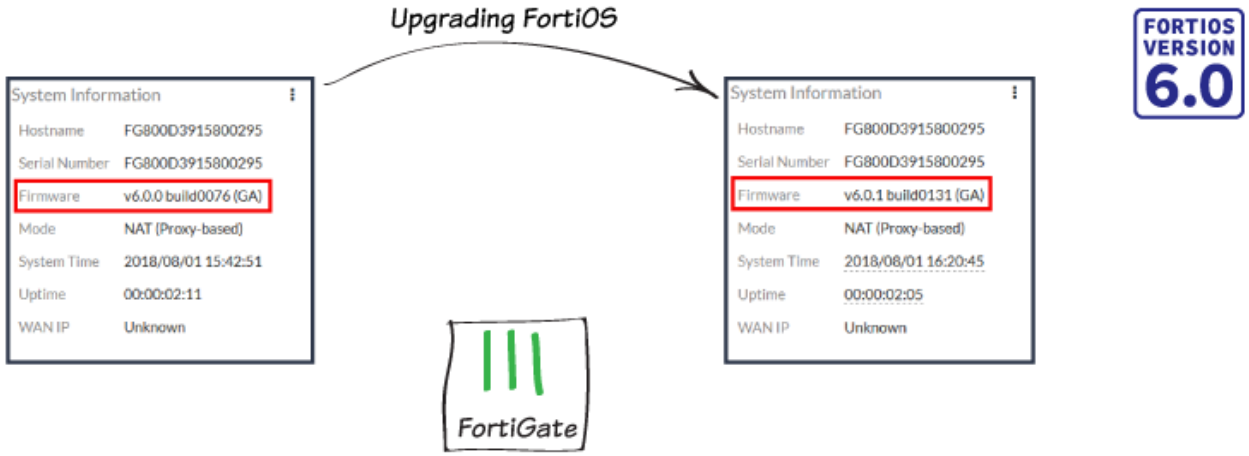
8. If you attempt to log in from any other device using the **tal-jamil** account, the account will authenticate; however, you will not have Internet access.
9. Go to **FortiView >All Segments> Policies** and select the **5 minutes** view. You can see traffic hitting all three policies and that each user's traffic is flowing through the correct policy.




| Policy | Bytes (Sent/Received) | Sessions (Blocked/Allowed) |
|---|---|---|
| Admin (3) | 10.66 kB | 10 |
| Accounting (2) | 182.05 kB | 27 |
| Internet (1) | 2.36 kB | 1 |

For further reading, check out Firewall policies in the FortiOS 6.0 Online Help.

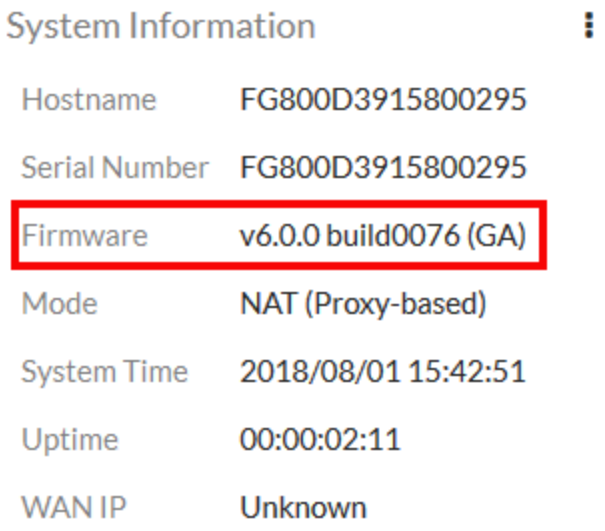
# Upgrading FortiGate firmware




In this example, you upgrade your FortiGate firmware from FortiOS 6.0.0 to 6.0.1.

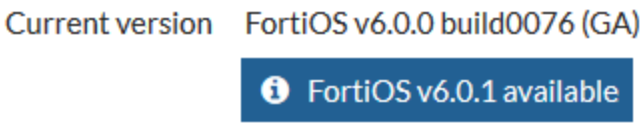
## Checking the current FortiOS firmware

1. To check which firmware version you're using, go to the **Dashboard** and view the **System Information** widget, which shows the current **Firmware**.




2. To find out if a new FortiOS version is available, go to **System > Firmware**. If new firmware is available, a notice appears under **Current version**.

When a new FortiOS version is released, it may not be listed on your FortiGate right away. If this occurs, download the firmware from Fortinet Support, then use **Upload Firmware** to upgrade your FortiGate.

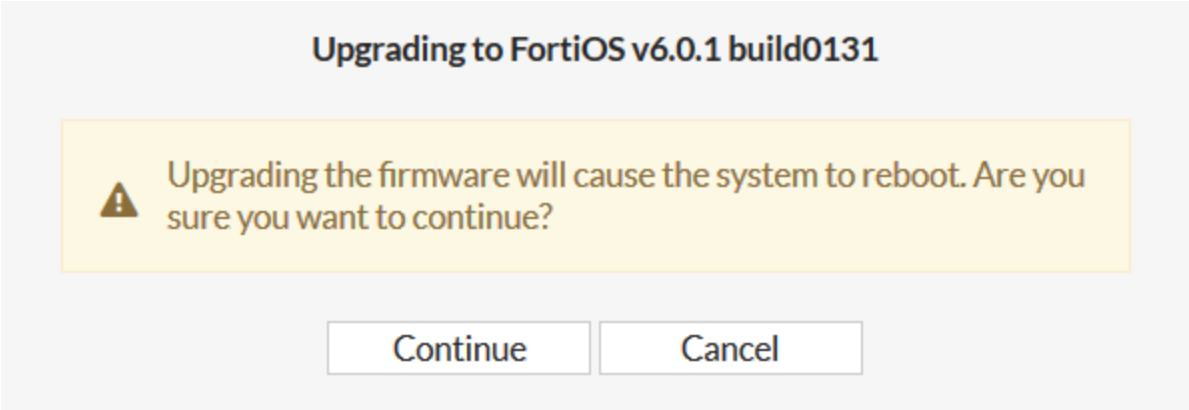



## Upgrading to the latest version

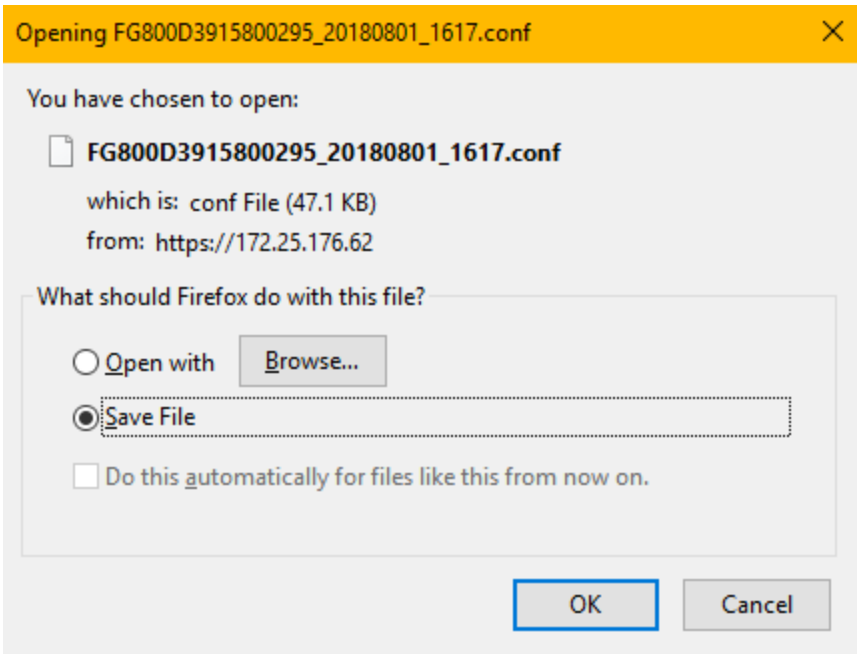
1. Under **FortiGuard Firmware**, select Latest. A notice may appear stating that there is no valid upgrade path for this firmware version. If this is the case, select All available instead and find a suitable firmware version for your FortiGate.

   For more information about the upgrade path, go to Fortinet Support.
2. If no warning appears, select **Release notes** to learn more about the firmware build. Release notes are also available at the Fortinet Documentation Library.


3. To upgrade your FortiGate, select **Backup config and upgrade**. When prompted, select **Continue**.

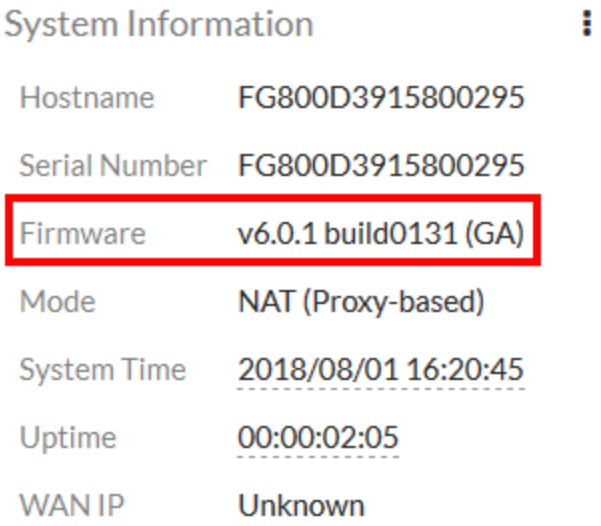



4. Save the backup of your current FortiGate configuration, in case you need to restore it after the upgrade process.

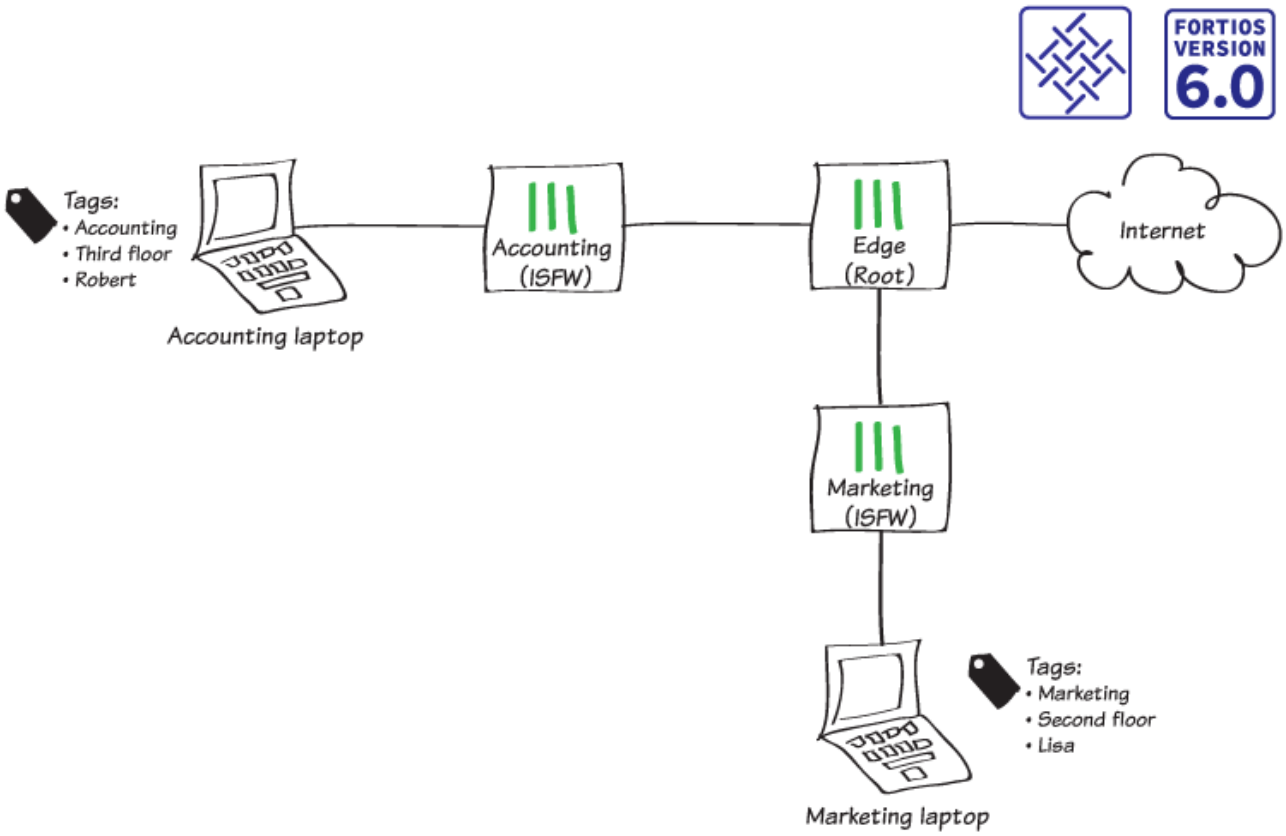


## Results

1. The FortiGate uploads and installs the firmware, then restarts. This process takes a few minutes. When the firmware is installed, the FortiGate login appears.
2. Go to the **Dashboard**. The **System Information** widget shows the new **Firmware** version.



# Tags in the Fortinet Security Fabric



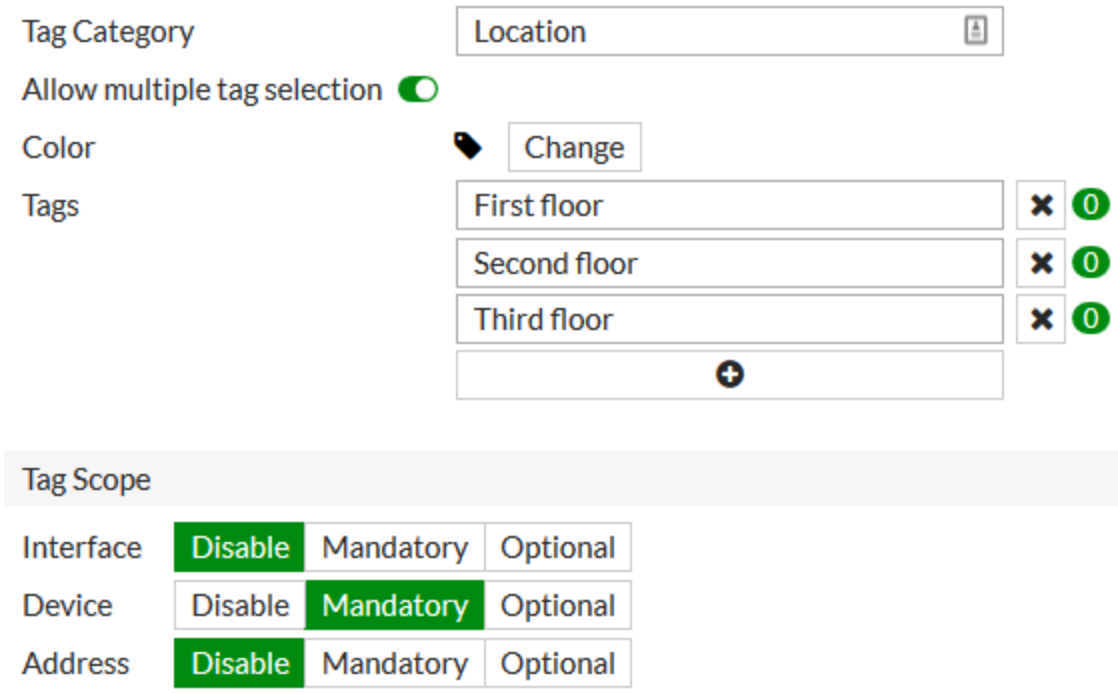

In this recipe, you create tag categories and tags for your network. By applying these tags to different devices, interfaces, and addresses, you identify the location and function of each part of your Security Fabric and increase network visibility.

## Creating tag categories and tags

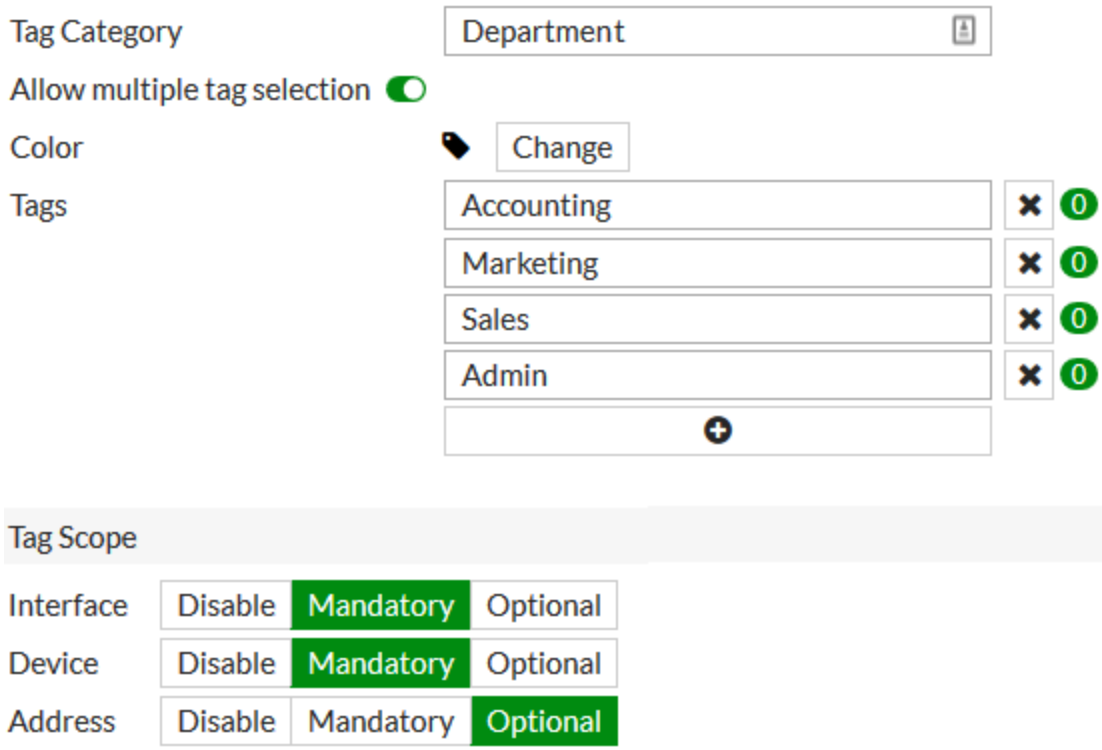
In this example, you use tags to identify the following things about devices in the Security Fabric:

- Physical location
- Department
- Network administrators

1. To create the tag category for physical location, connect to Edge and go to **System > Tags**.
2. Set **Tag Category** to **Location**. Because each device in the network can only have one location, disable **Allow multiple tag selection**.
3. Add **Tags** for the first floor, second floor, and third floor.
4. Under **Tag Scope**, set **Device** to **Mandatory**.

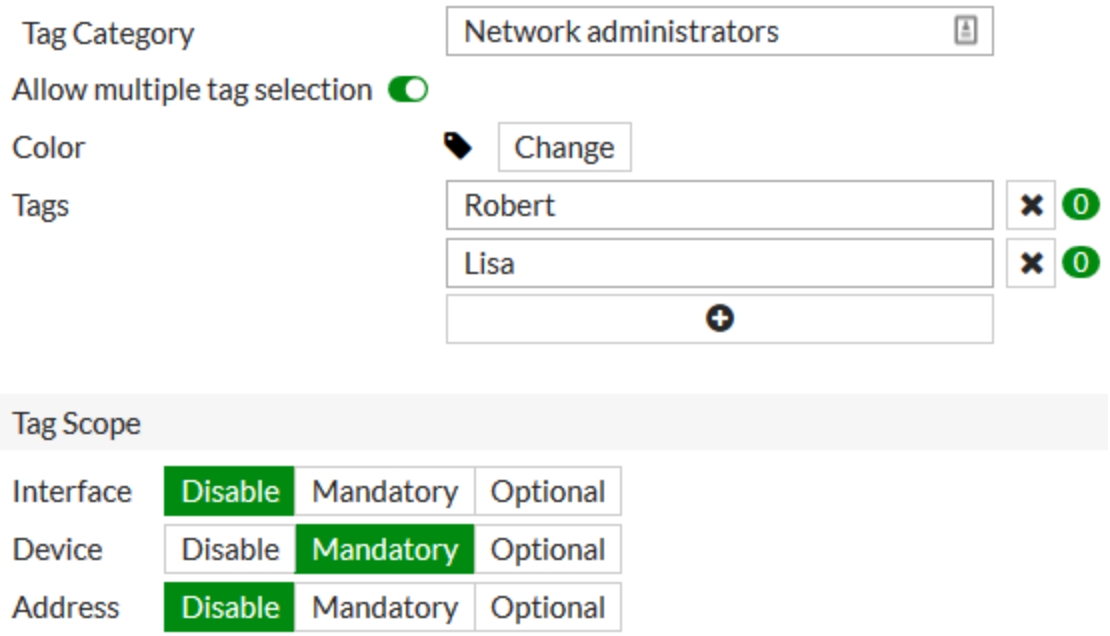



5. For the department tag, enable **Allow multiple tag selection**.
6. Add **Tags** for the following departments: *Accounting*, *Marketing*, *Sales*, and *Admin*.
7. Under **Tag Scope**, set **Interface** to **Mandatory** and set **Device** to **Mandatory**. Because the FortiGate configuration includes default addresses, set **Address** to **Optional**.




8. For the network administrators tag, enable **Allow multiple tag selection**.

9. Add **Tags** for *Robert* and *Lisa*.
10. Under **Tag Scope**, set **Device** to **Mandatory**.



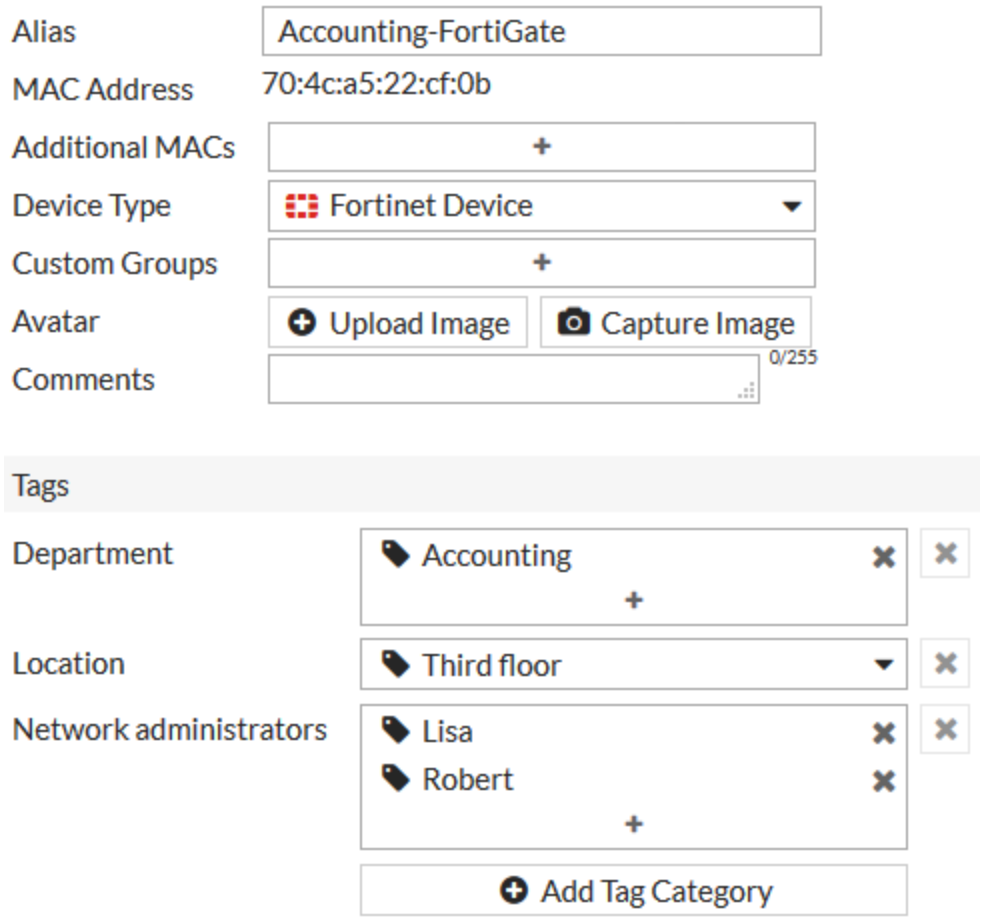

11. Because the configuration of tag categories and tags isn't synchronized across the Security Fabric, you must connect to each FortiGate device separately and add the appropriate tags for the part of your network that uses that FortiGate.

    Connect to Accounting and repeat the previous steps to create the tags that are shown.

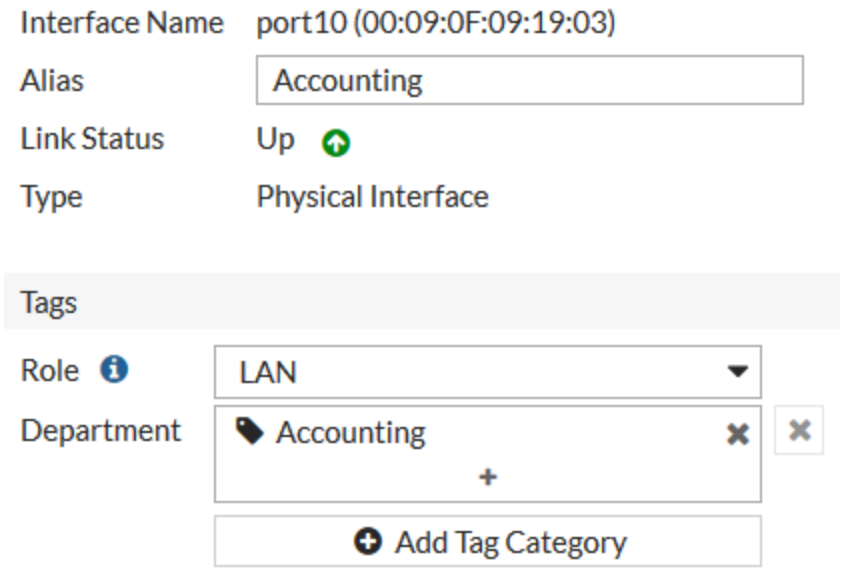
| Tag Category | Allow Multiple Tag Selection | Interface | Address | Device | Tags |
|---|---|---|---|---|---|
| default | Enable | Optional | Optional | Optional | |
| Department | Enable | Mandatory | Optional | Mandatory | Accounting |
| Location | Disable | Disable | Disable | Mandatory | Third floor |
| Network administrators | Enable | Disable | Disable | Mandatory | Lisa<br>Robert |

## Applying tags

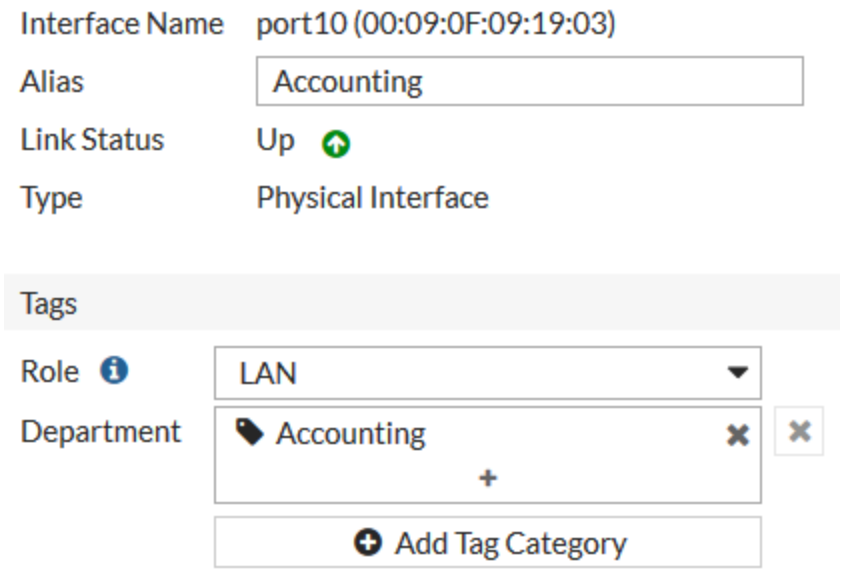
1. To apply tags to devices in your network, go to **User & Device > Device Inventory**.
2. Edit the Accounting FortiGate.
3. Under **Tags**, add the following tags:
   - For **Department**, add the **Accounting** tag
   - For **Location**, add the **Third floor tag**
   - For **Network administrators**, add the **Robert** and **Lisa** tags




4. Edit all other devices listed and apply the appropriate tags for department, location, and administrators.
5. To apply tags to interfaces in your network, go to **Network > Interfaces**. Edit the interface that connects Edge and Accounting (in the example, **port 10**).
6. Under **Tags**, set **Department** to **Accounting**.



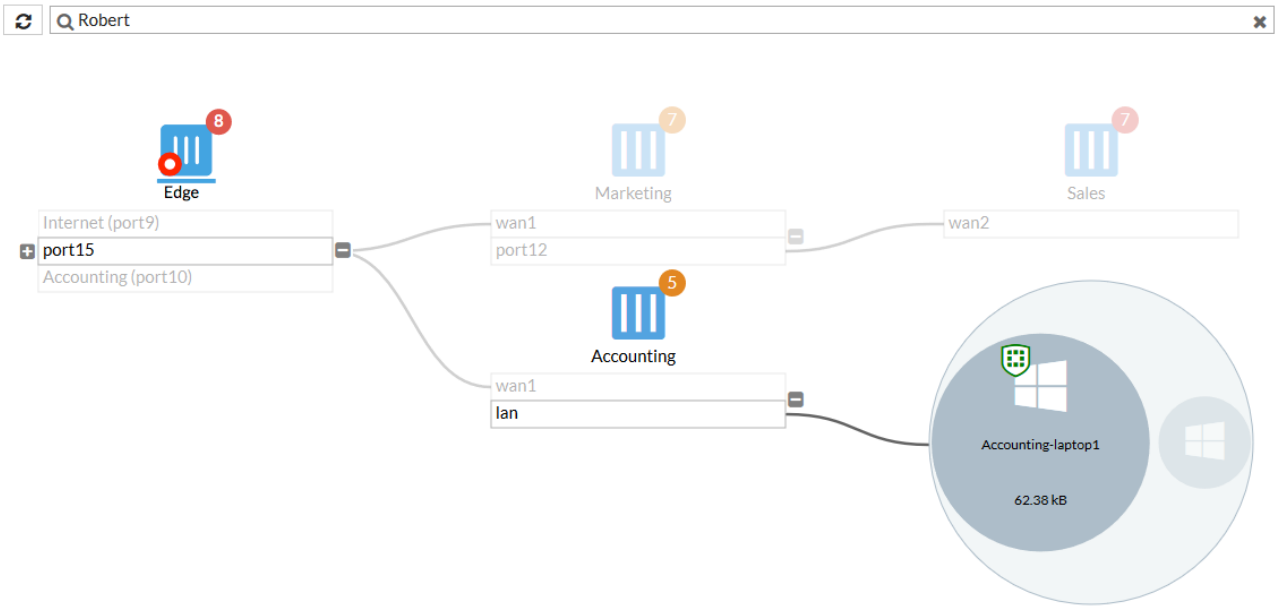
7. Edit all other interfaces and apply the appropriate tag for department.
8. To apply tags to addresses in your network, go to **Policy & Objects > Addresses**. Edit the address for the Accounting subnet.
9. Under **Tags**, set **Department** to **Accounting**.



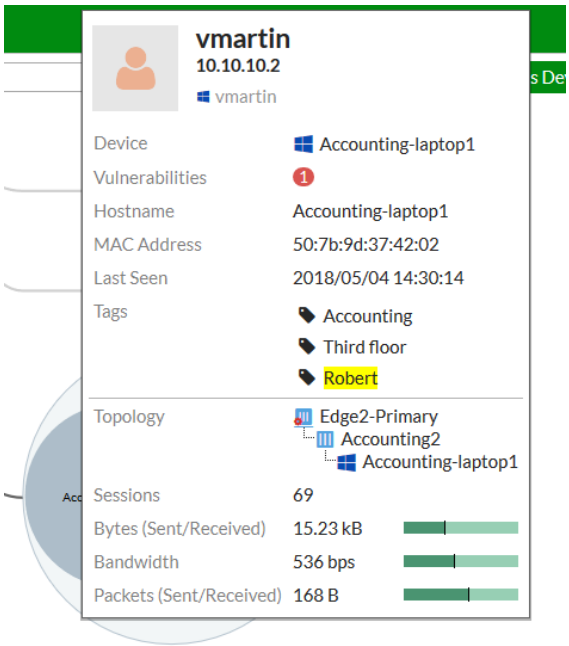

10. Edit all other addresses and apply the appropriate tag for department.
11. To apply tags to devices in on the accounting network, connect to Accounting and go to **User & Device > Device Inventory**.
12. Edit a computer on this network.
13. Under **Tags**, add the following tags:
    - For **Department**, add the **Accounting** tag
    - For **Location**, add the **Third floor** tag
    - For **Network administrators**, add the **Robert** tag
14. Apply the appropriate tags to other devices, interfaces, and addresses on this network.

## Results

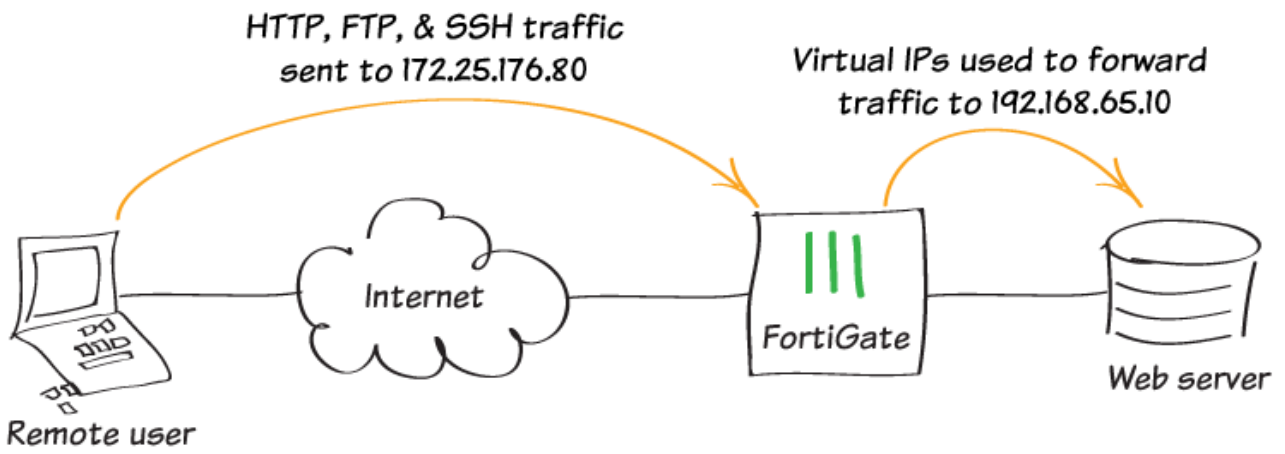
1. To sort devices and interfaces by tags, connect to Edge and go to **Security Fabric > Logical Topology**.
2. In the **Search** field, enter *Robert*. The devices that have the **Robert** tag are highlighted.




3. To view more information about a highlighted device, including tags, hover over that device in the topology. The **Robert** tag is highlighted.



# Port forwarding

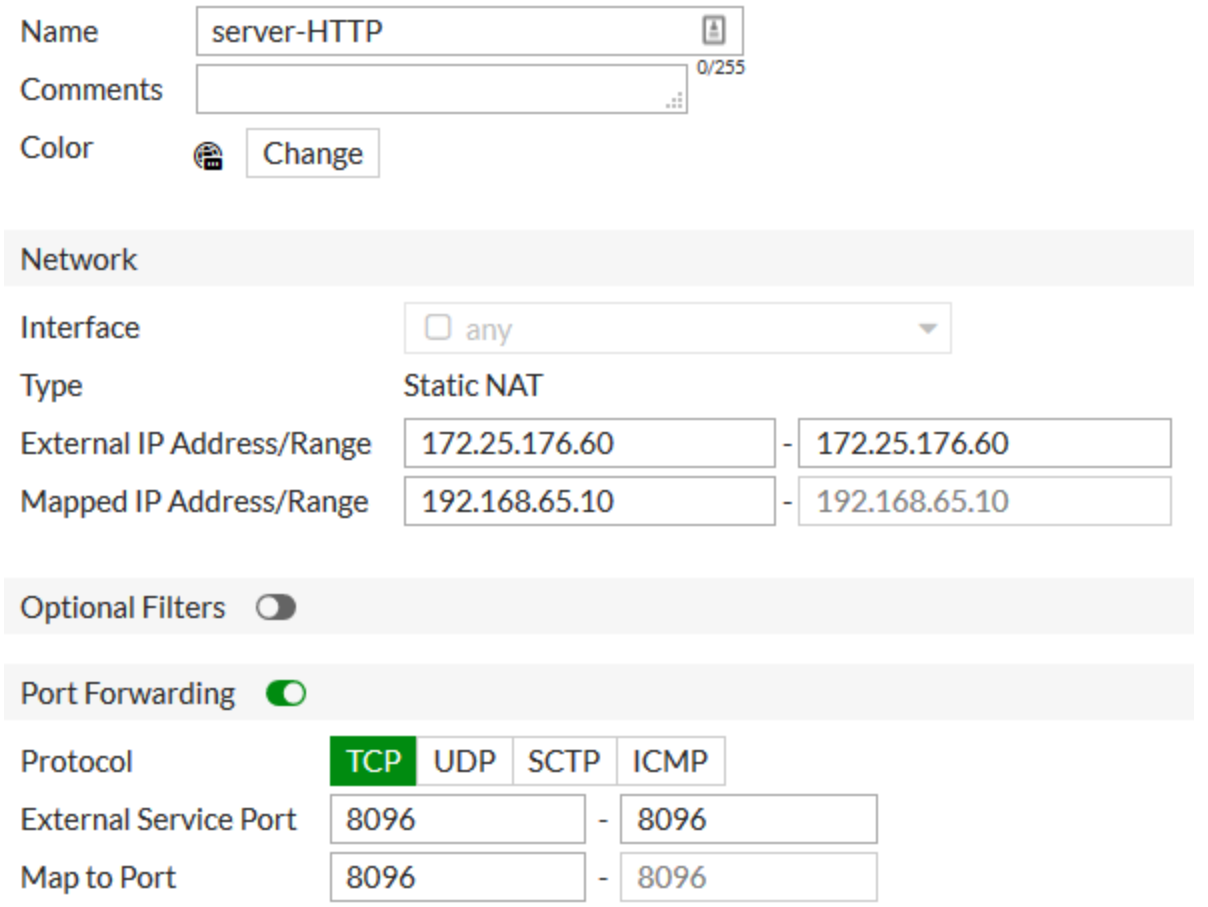



In this recipe, you configure port forwarding to open specific ports and allow connections from the Internet to reach a server located behind the FortiGate. This allows Internet users to reach the server through the FortiGate without knowing the server's internal IP address. Users can also connect using only the ports that you choose.

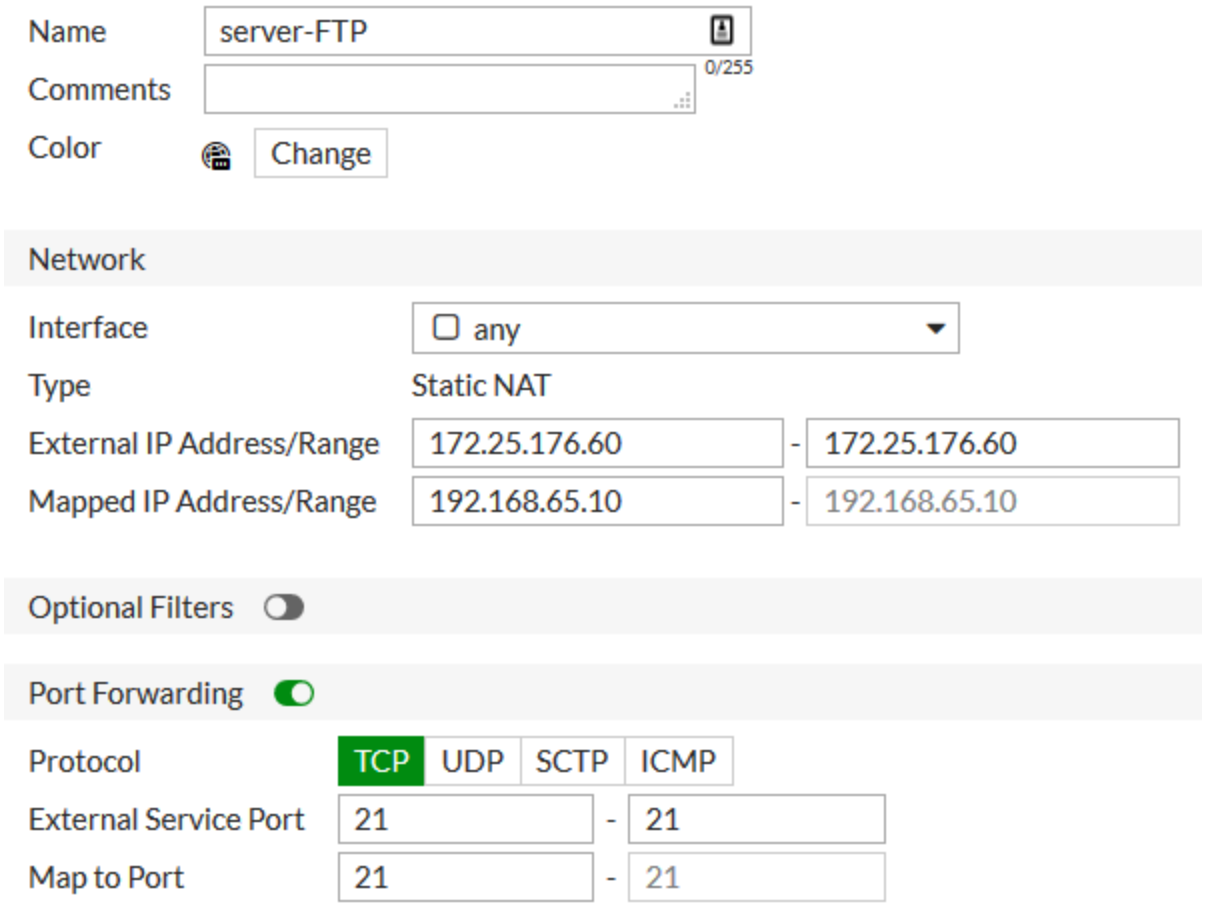
## Creating virtual IP addresses

In this example, you open TCP ports 8096 (HTTP), 21 (FTP), and 22 (SSH) for remote users to communicate with the server behind the firewall. The external IP address of the server is 172.25.176.60, which is mapped to the internal IP address 192.168.70.10.

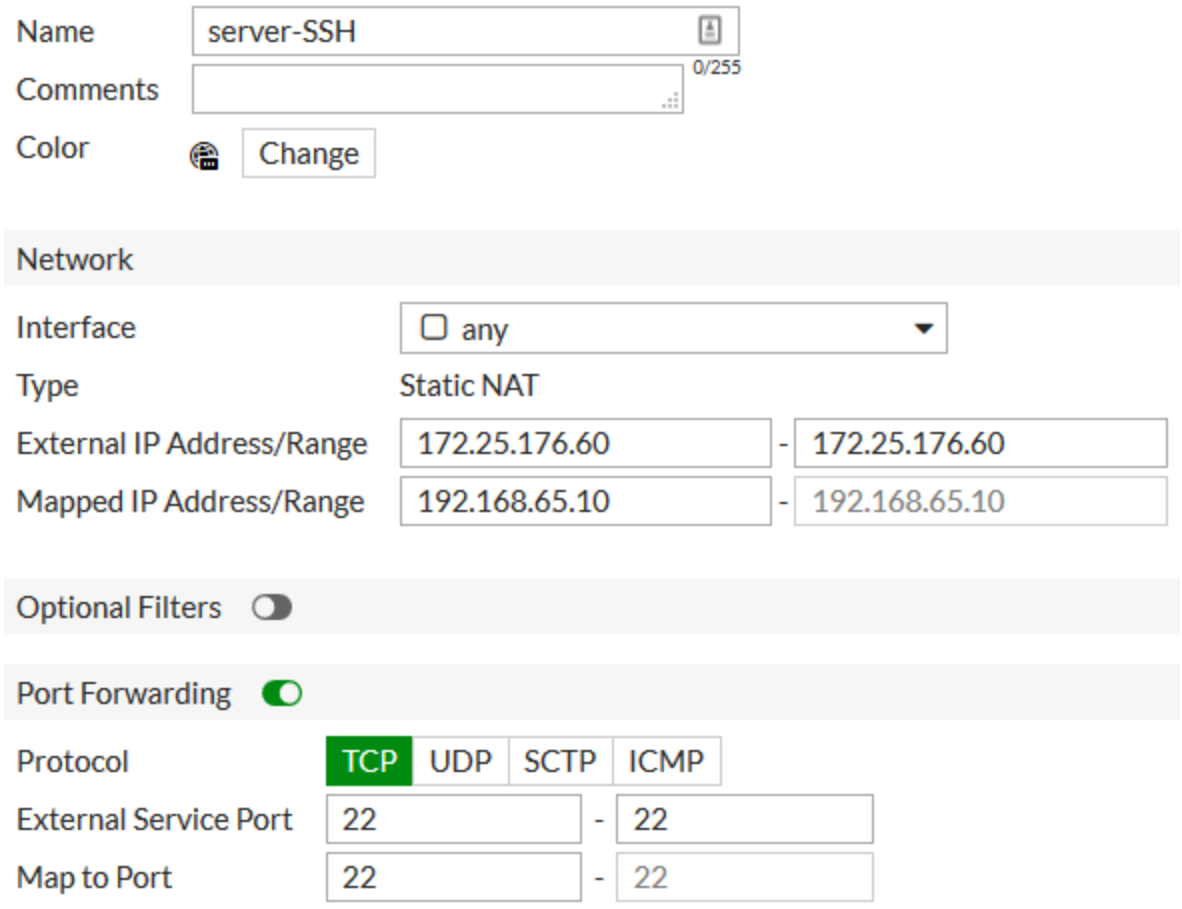
1. To create a virtual IP (VIP) address for port 8096, go to **Policy & Objects > Virtual IPs** and create a new virtual IP address.
2. Set **External IP Address/Range** to *172.25.176.60* and set **Mapped IP Address/Range** to *192.168.65.10*.
3. Enable **Port Forwarding**. Set **Protocol** to **TCP**, set **External Service Port** to **8096**, and set **Map to Port** to *8096*.




4. Create a second VIP address for port 21. Set both **External Service Port** and **Map to Port** to *21*.

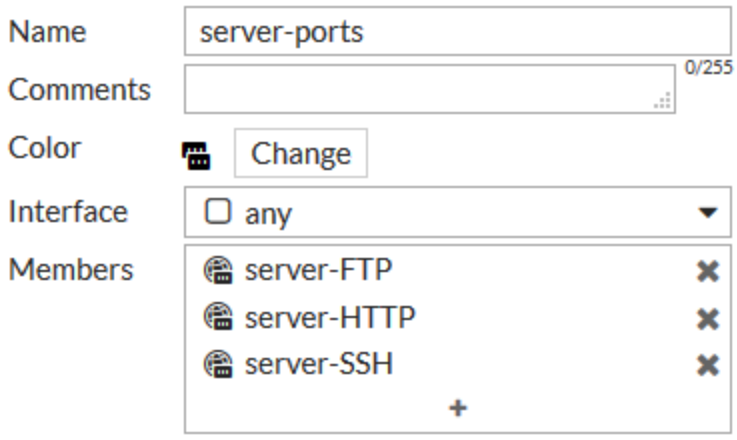



5. Create a third VIP address for port 22. Set both **External Service Port** and **Map to Port** to 22.




## Creating a virtual IP group

1. To add the new virtual IP addresses to a virtual IP group, go to **Policy & Objects > Virtual IPs** and create a new group.
2. Set the new virtual IP addresses as **Members** of the group.

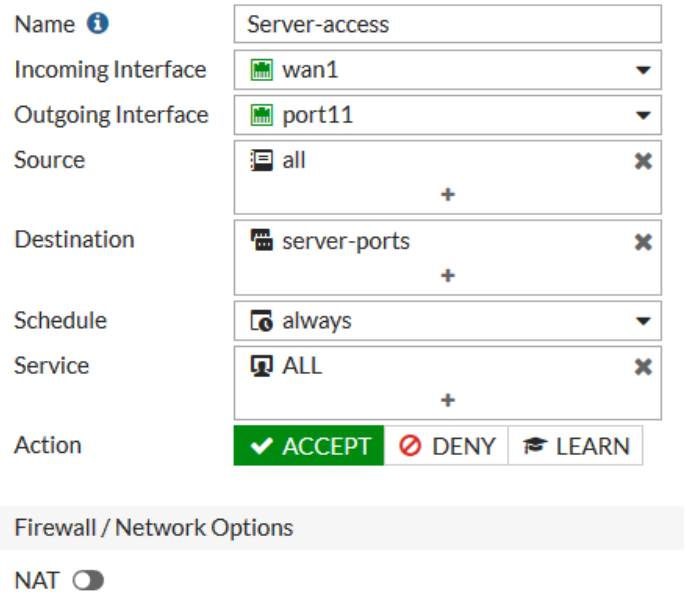


## Creating a security policy

1. To allow Internet users to reach the server, go to **Policy & Objects > IPv4 Policy** and create a new policy.
2. Set **Incoming Interface** to your Internet-facing interface, **Outgoing Interface** to the interface connected to the server, and **Destination Address** to the VIP group.

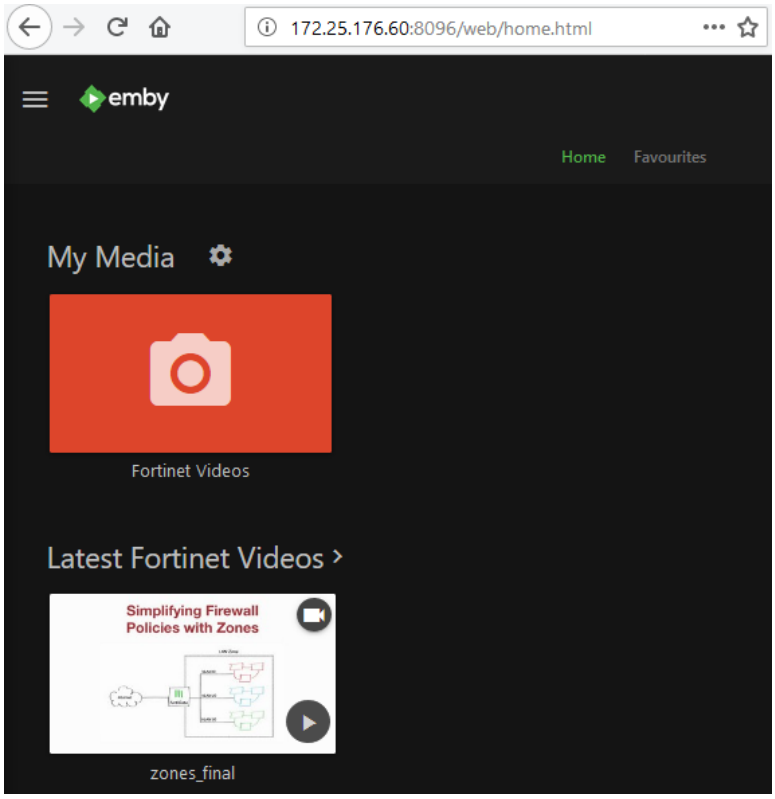
   NAT is disabled for this policy so that the server sees the original source addresses of the packets it receives. This is the preferred setting for a number of reasons. For example, the server logs are more meaningful if they record the actual source addresses of your users.

If the FortiGate has Central NAT enabled, the VIP objects won't be available for selection in the policy editing window.

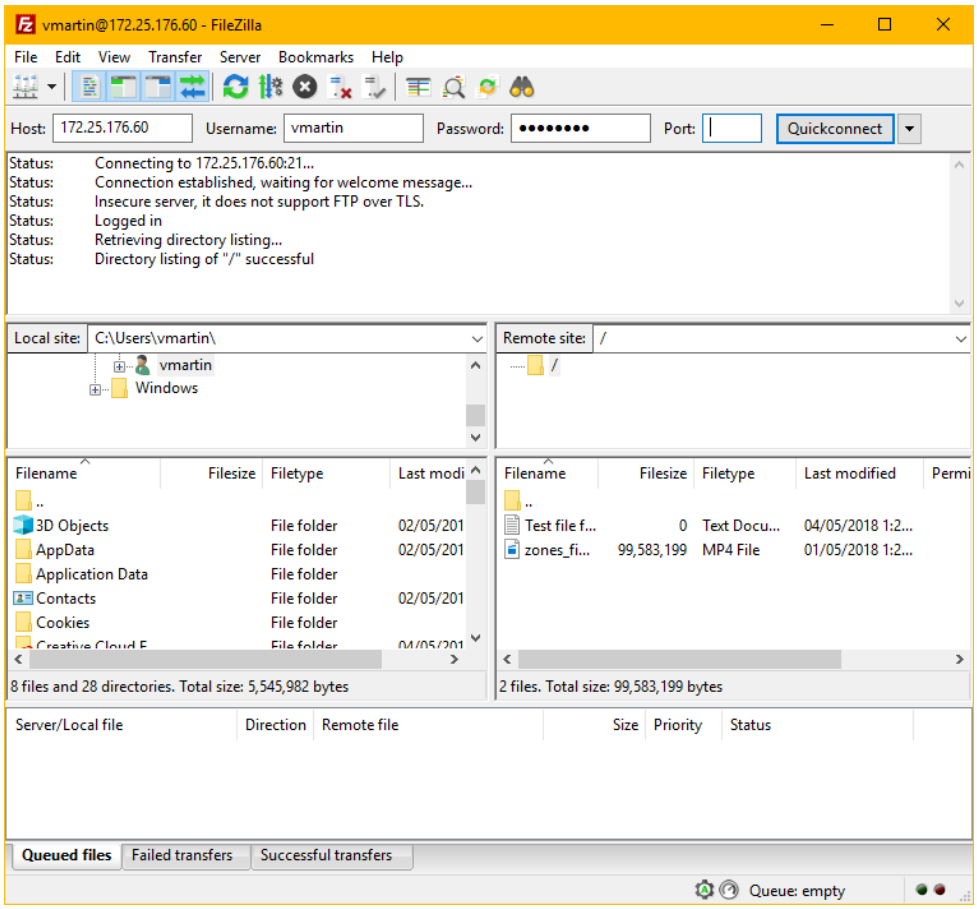


## Results

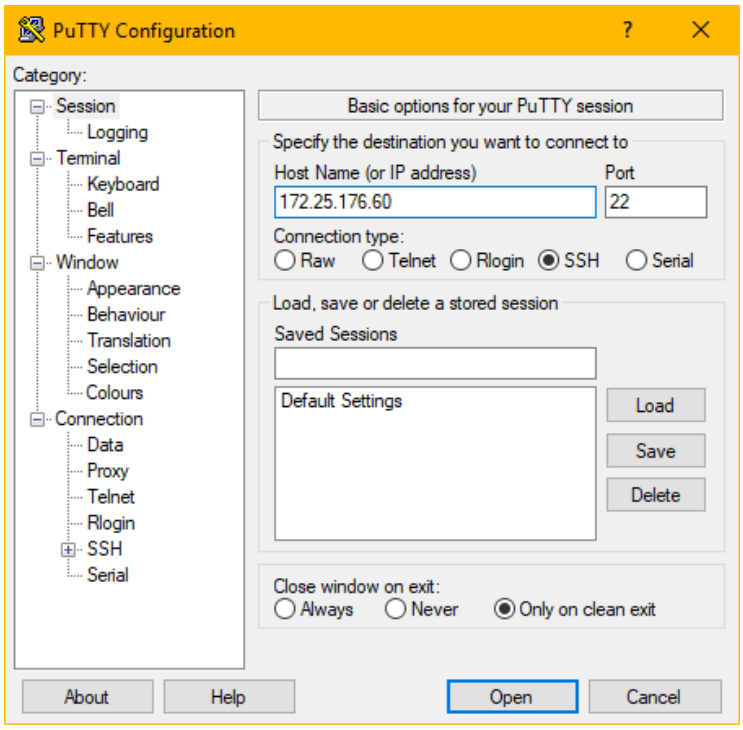
1. To ensure that TCP port 8096 is open, browse to http://172.25.176.60:8096.

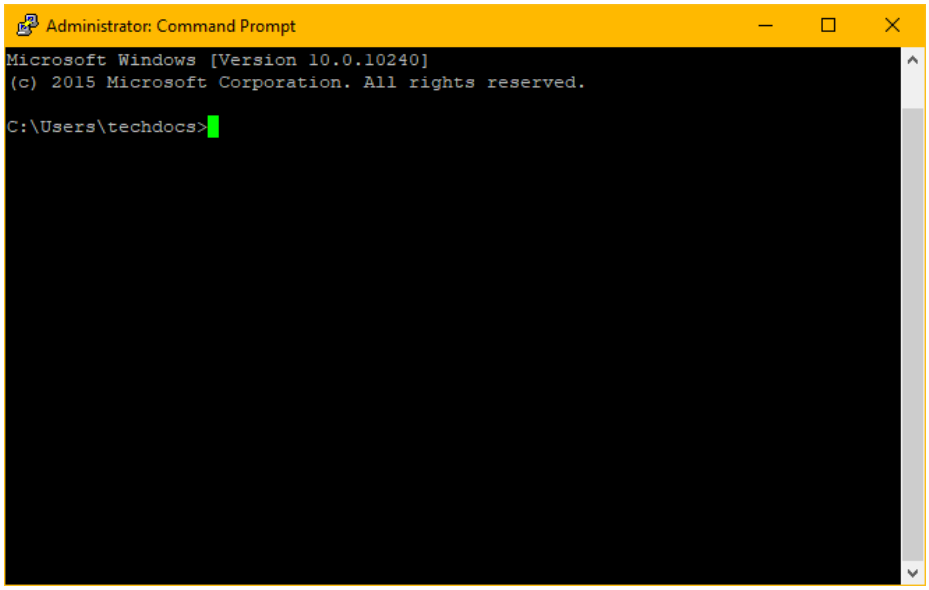



2. Next, ensure that TCP port 21 is open by using an FTP client to connect to the FTP server from a remote connection on the other side of the firewall.



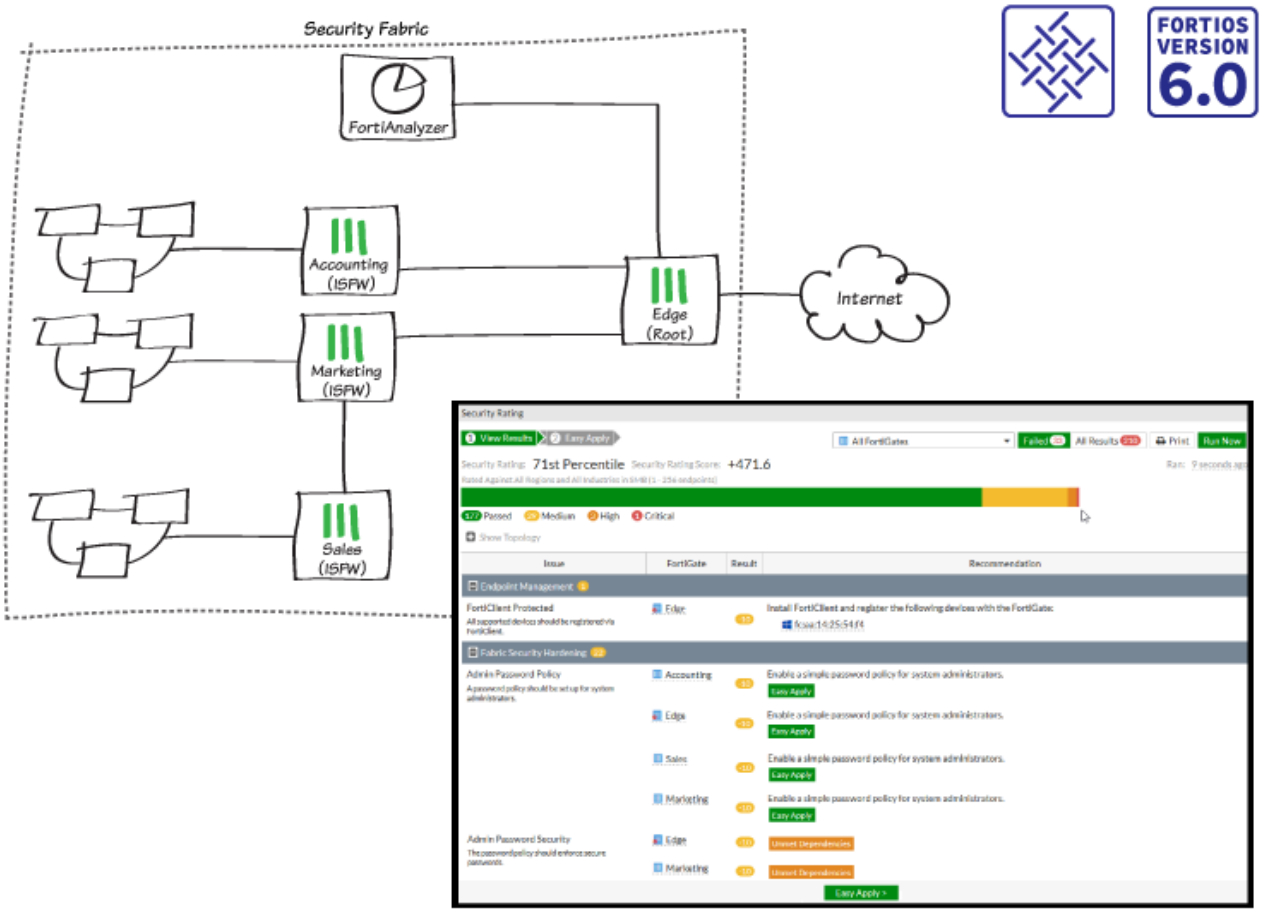

3. Finally, ensure that TCP port 22 is open by connecting to the SSH server from a remote connection on the other side of the firewall.




For further reading, check out Virtual IPs in the FortiOS 6.0 Online Help.

# Security Rating




In this recipe, you run a Security Rating check, which analyzes the Fortinet Security Fabric deployment to identify potential vulnerabilities and highlight best practices.

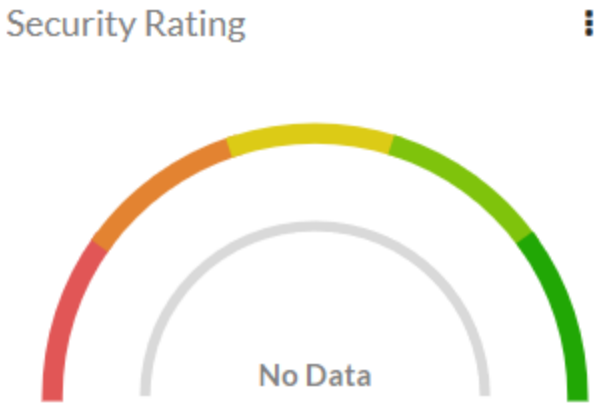
Using the Security Rating can help you improve your network configuration, deploy new hardware and software, and gain more visibility and control over your network. By regularly checking your Security Rating and your Security Rating Score, and making the recommended improvements, you can have confidence that your network is getting more secure over time.

To run all available checks, you must have a valid Security Rating license from FortiGuard. If you don't have a license, only certain checks are available. For more information about these checks, see Security Best Practices & Security Rating Feature.

Not all FortiGate models can run the FortiGuard Security Rating Service if they are the root FortiGate in a Security Fabric. For more information, see the FortiOS 6.0 Release Notes.

## Checking the Security Rating widget

1. Go to the **Dashboard** and locate the **Security Rating** widget. In the example, the widget doesn't display any information because it's not properly configured.



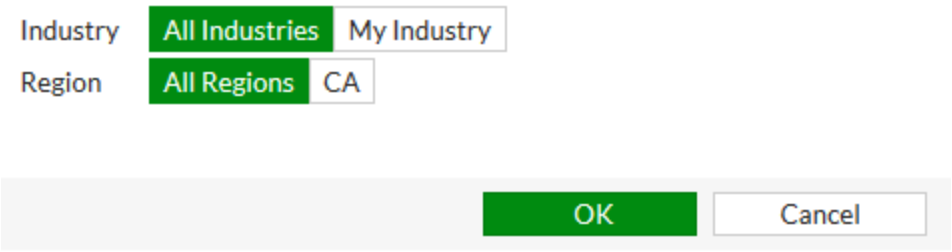

2. Once you configure the widget, it displays a comparison between your Security Rating and the ratings of other organizations. You can compare your rating to the ratings of organizations that belong to all industries or the same industry as your organization. You can also compare your rating with organizations in your region or all regions.

---

Your FortiCare account settings determine your industry categorization.

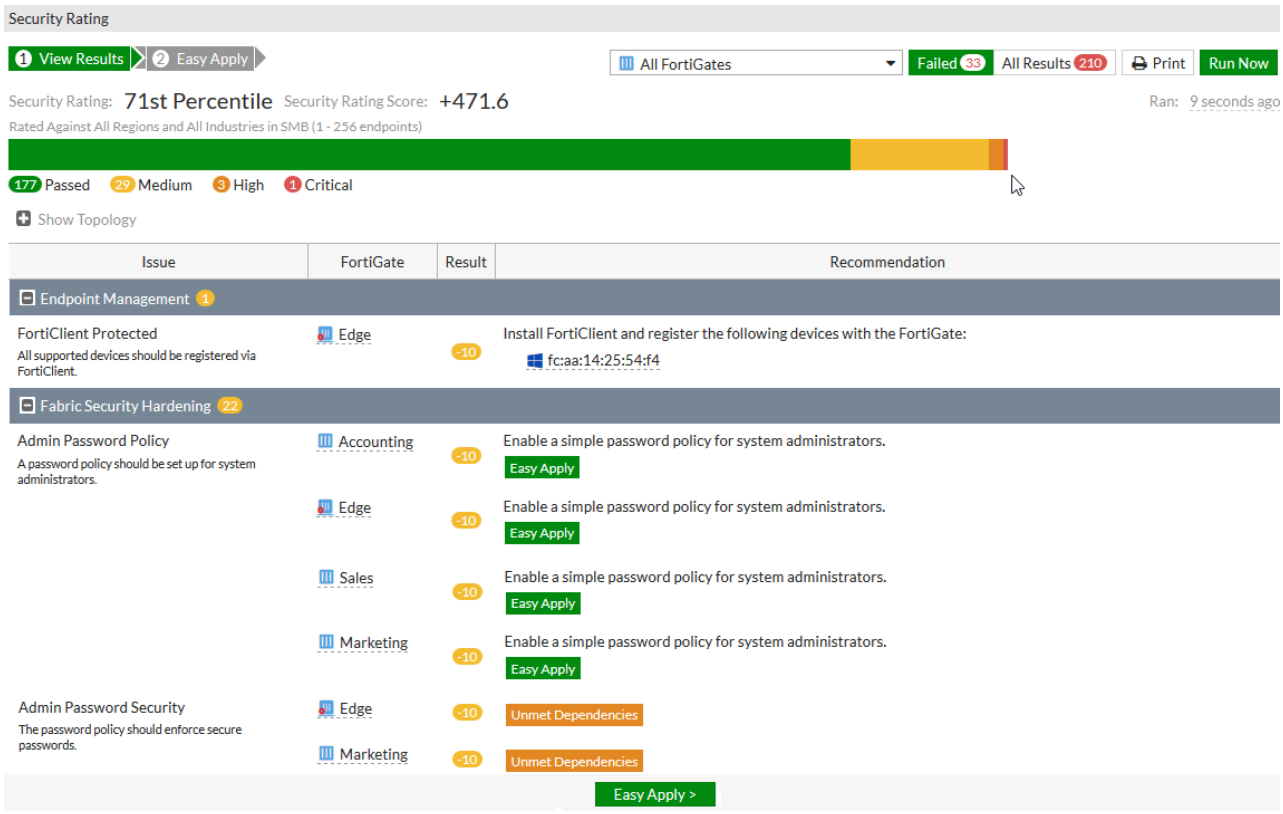
---

3. To change which organizations your score is compared to, select the options menu in the top right corner, then select **Settings**.

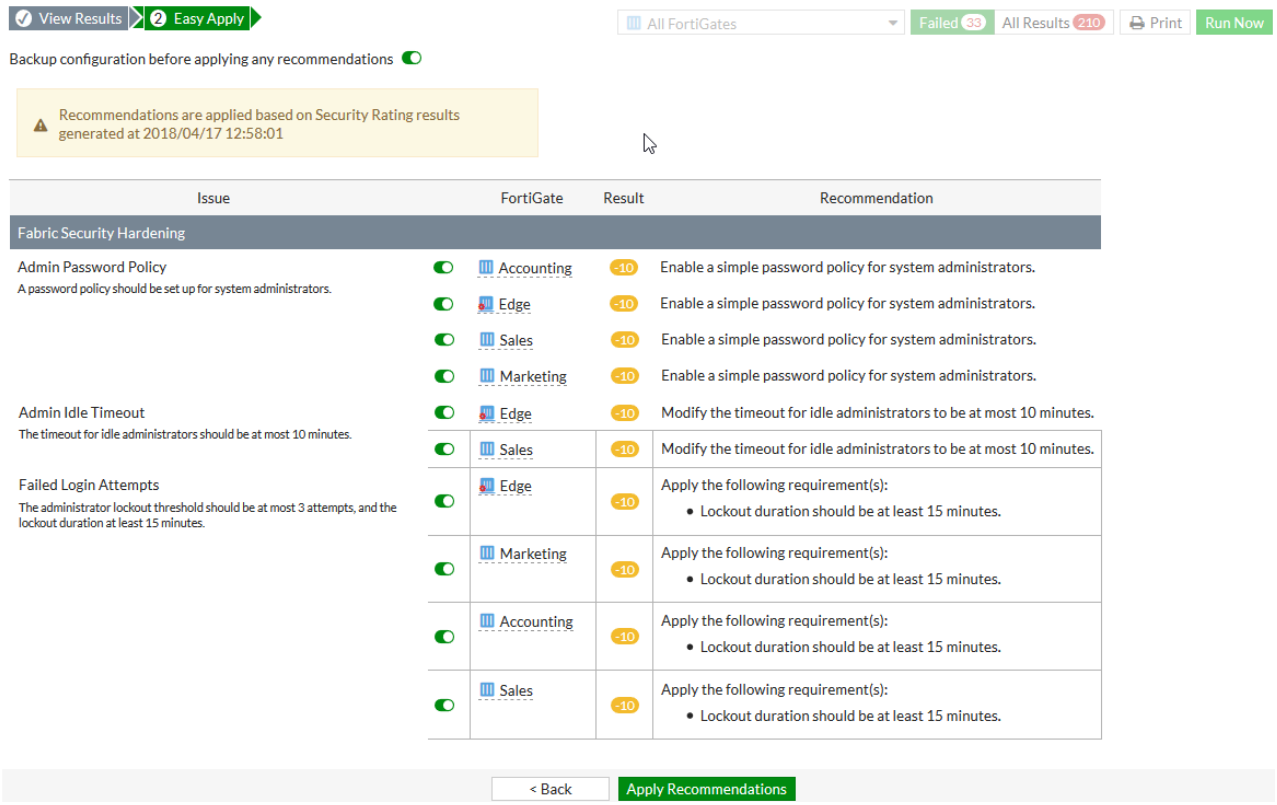



## Checking your Security Rating

1. On Edge, go to **Security Fabric > Security Rating**. The Security Rating runs automatically on the root FortiGate. However, if you want more recent results, select **Run Now** to run another Security Rating.
2. You can also select whether to run the Security Rating on **All FortiGates** or on specific FortiGate devices in the Security Fabric.

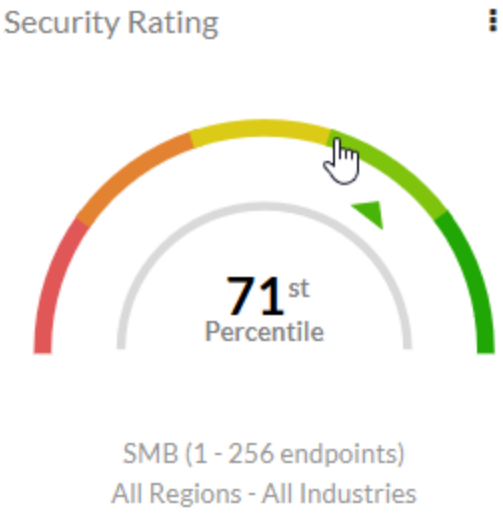



3. At the top of the page, you can see your network's **Security Rating**, which shows which percentile your network is in compared to other organizations. You can also see your **Security Rating Score**, which is based on how many checks your Security Fabric passed or failed, and how many FortiGate units are in your network.
4. Further down the page, you can see information about each failed check, including which FortiGate failed the check, the effect on your Security Rating Score, and recommendations for how you can the issue.
5. In the next step of the Security Rating, you can apply recommendations marked as **Easy Apply** to any FortiGate in the Security Fabric. However, if the Security Rating results are older than 30 minutes, you must first run it again to make sure all information is current and accurate.
6. By using **Easy Apply**, you can change the configuration of any FortiGate in the Security Fabric from the root FortiGate.
7. Select all the changes that you want to make, then select **Apply Recommendations**.

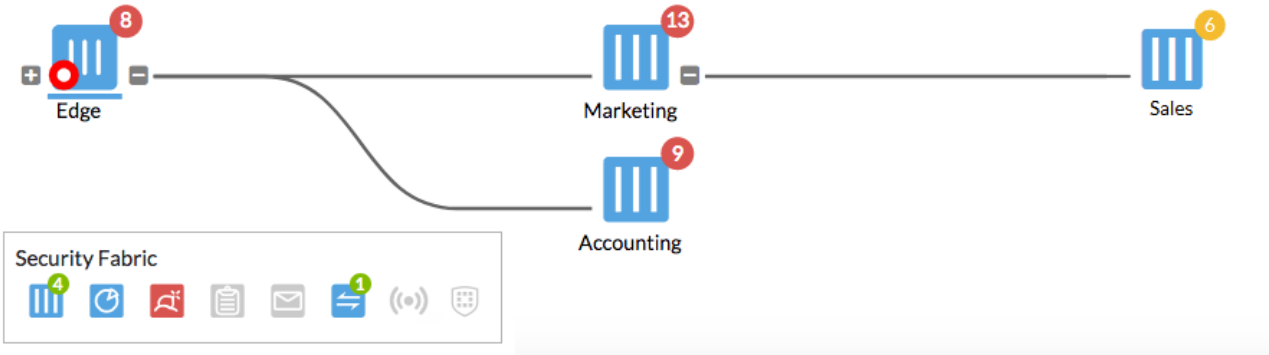



## Results

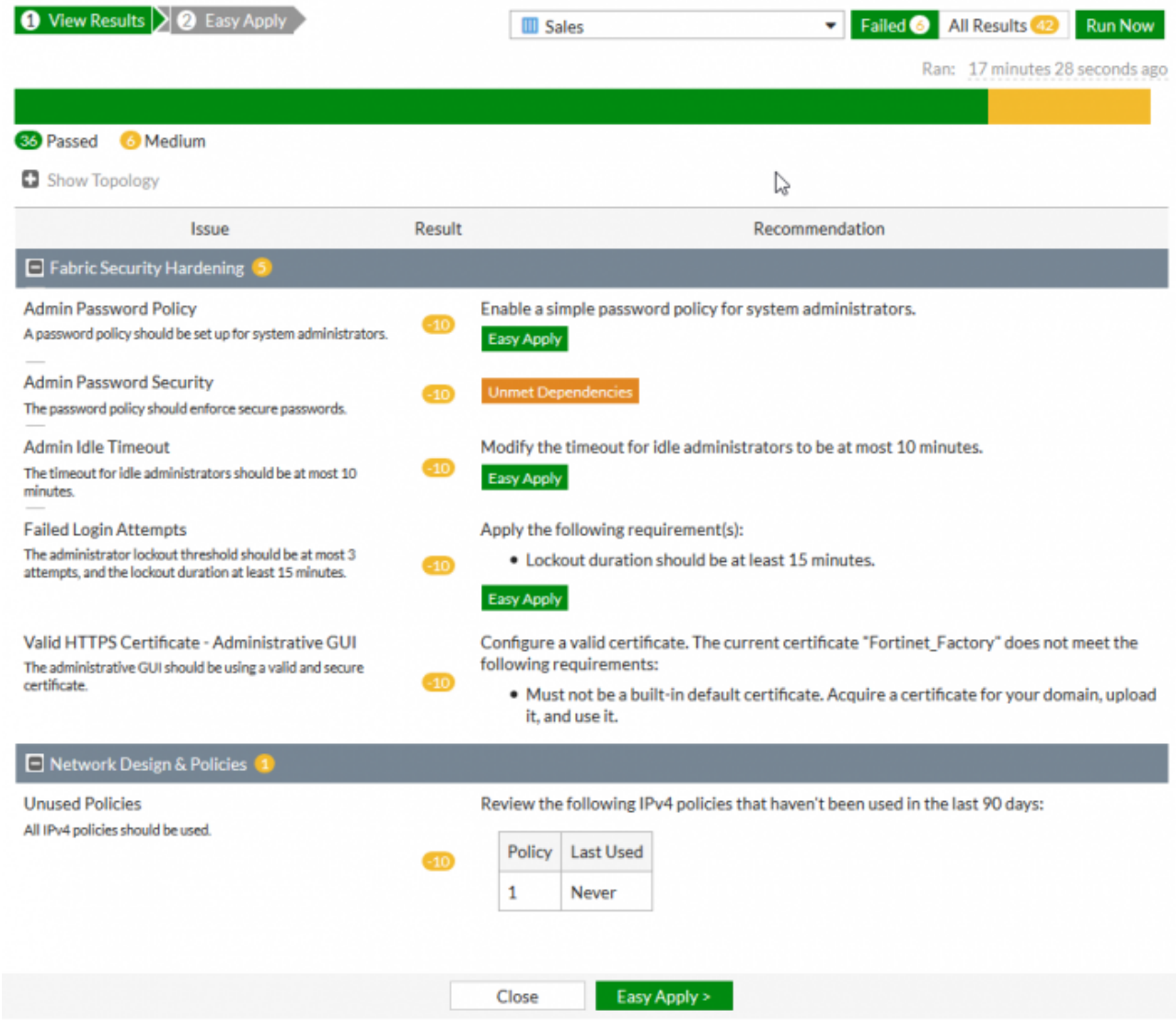
1. Go to the **Dashboard**. The **Security Rating** widget displays information from the most recent Security Rating check.




2. Go to **Security Fabric > Physical Topology**. Each FortiGate has a Security Rating indicator, which is circle that contains a number. The number shows how many checks the FortiGate failed and the color shows the severity of failed checks (red for critical, orange for high, yellow for medium, and blue for low).

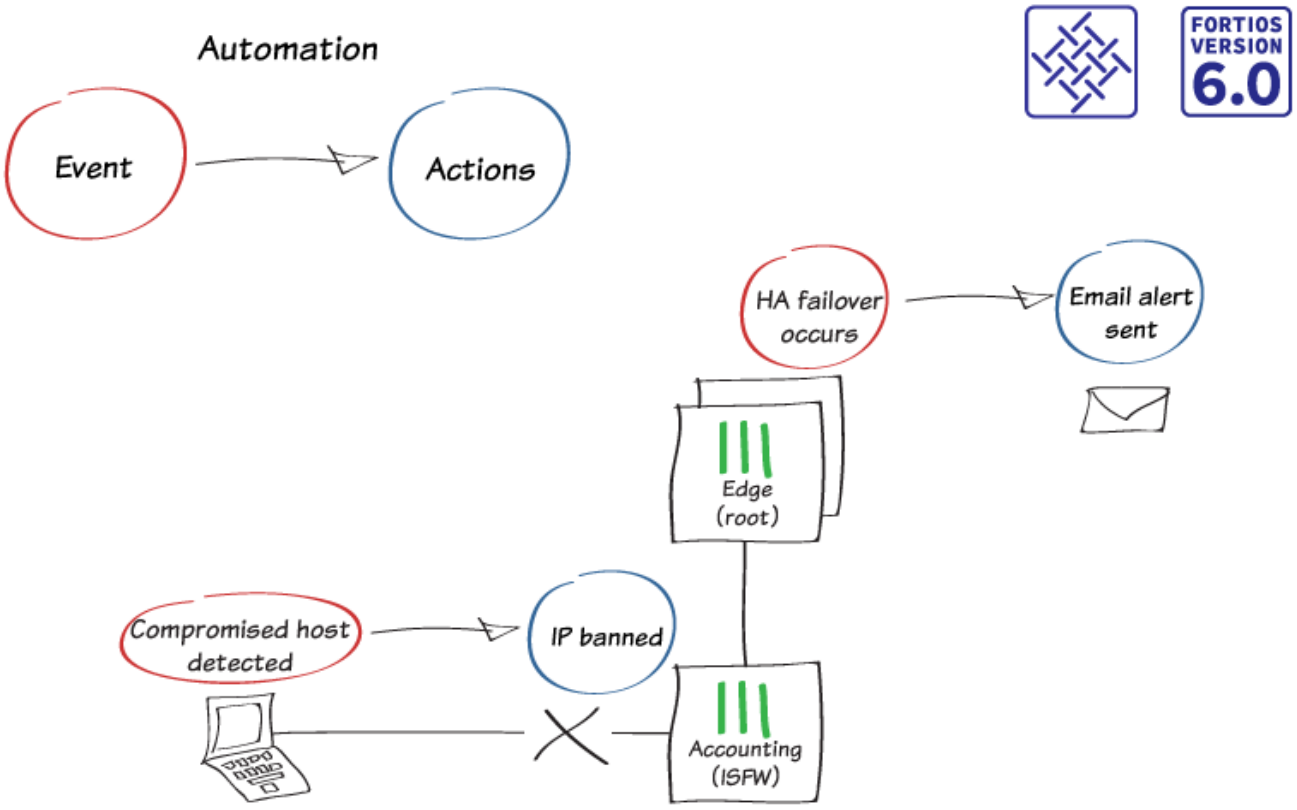



3. To view the failed checks on a specific FortiGate device, select the Security Rating indicator on the FortiGate in the topology.
4. A screen appears, showing the Security Rating recommendations for that unit. You can also apply **Easy Apply** recommendations from here.



For further reading, check out Running a Security Fabric Rating in the FortiOS 6.0 Online Help.

## Automation stitches




In this recipe, you configure Automation stitches for your Fortinet Security Fabric. Each Automation pairs an event trigger and one or more actions, which allows you to monitor your network and take appropriate action when the Security Fabric detects a threat. You can use Automation stitches to detect events from any source in the Security Fabric and apply actions to any destination.

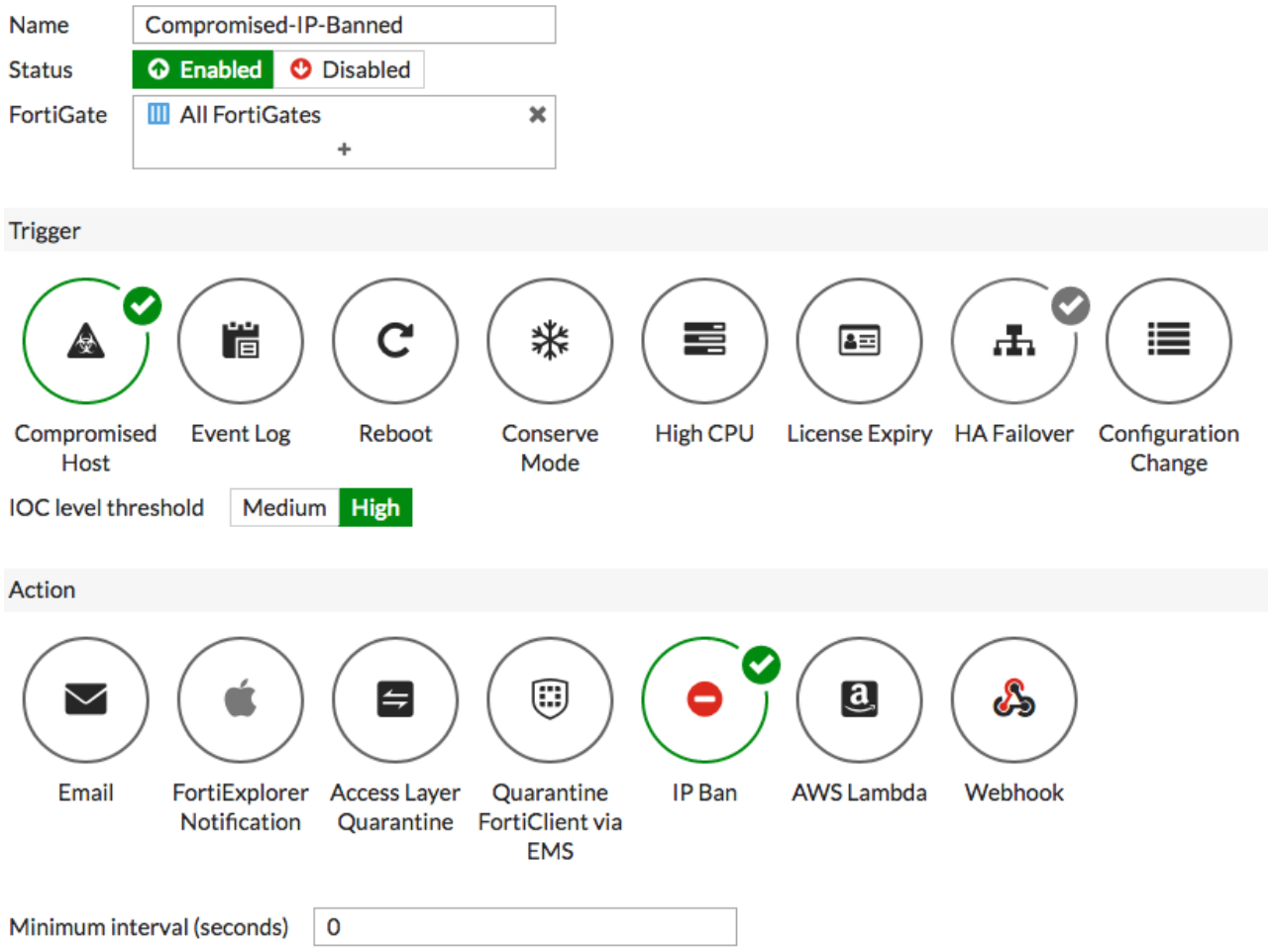
In this example, you create the following Automation stitches:

- Ban a compromised host's IP address.
- Send an email alert when HA failover occurs.

In this example, the Security Fabric consists of Edge, an HA cluster that is the root FortiGate of the Security Fabric, and three ISFW FortiGate devices (Accounting, Marketing, and Sales). You configure the Automation stitches on the root FortiGate and the settings are synchronized with the other FortiGate devices in the Security Fabric.

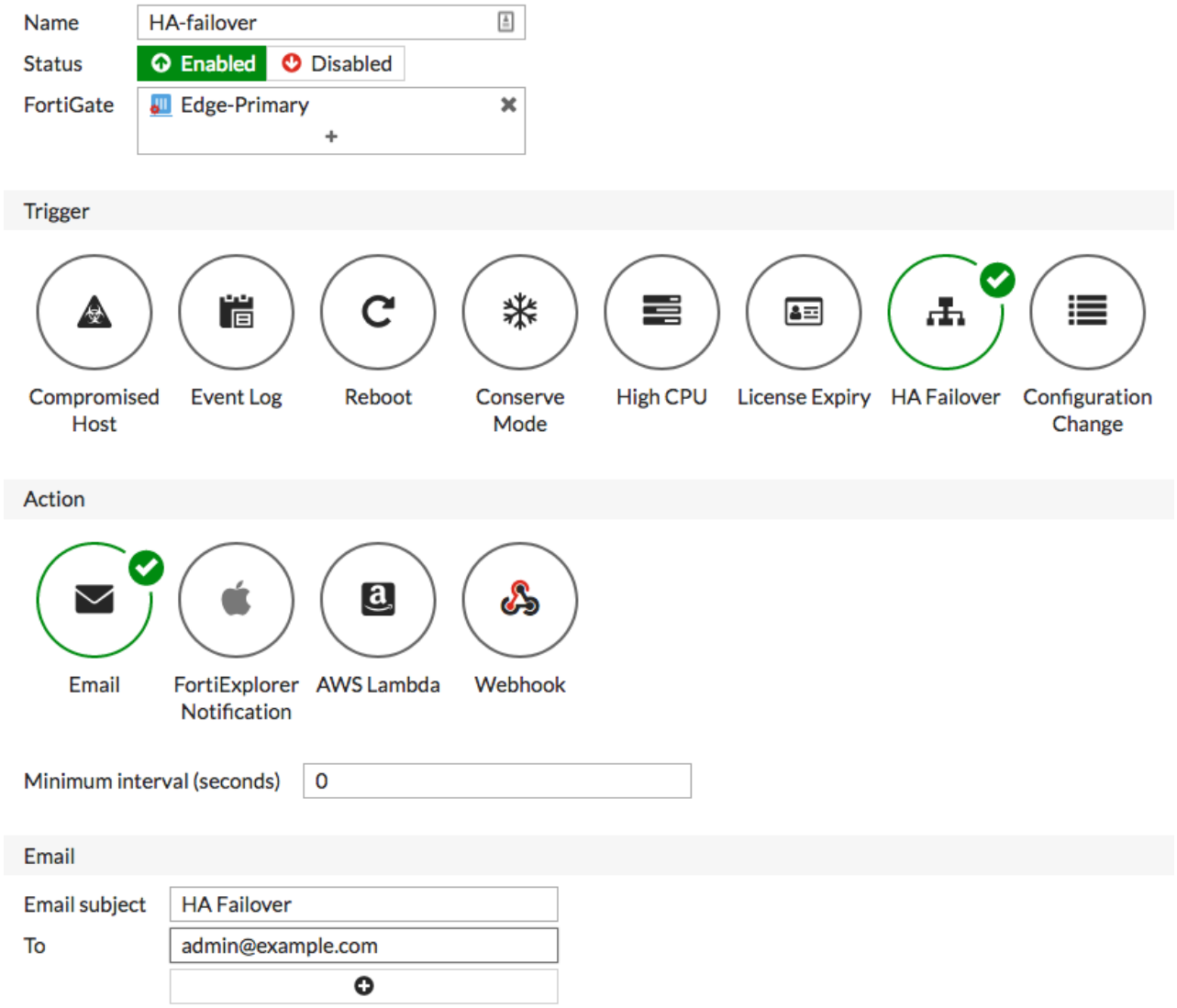
## Creating the Automation stitches

1. To create a new Automation that bans the IP address of a compromised host, go to **Security Fabric > Automation** and select **Create New**.
2. Set **FortiGate** to **All FortiGates**.
3. Set **Trigger** to **Compromised Host**. Set **IOC level threshold** to **High**.
4. Set **Action** to **IP Ban**.



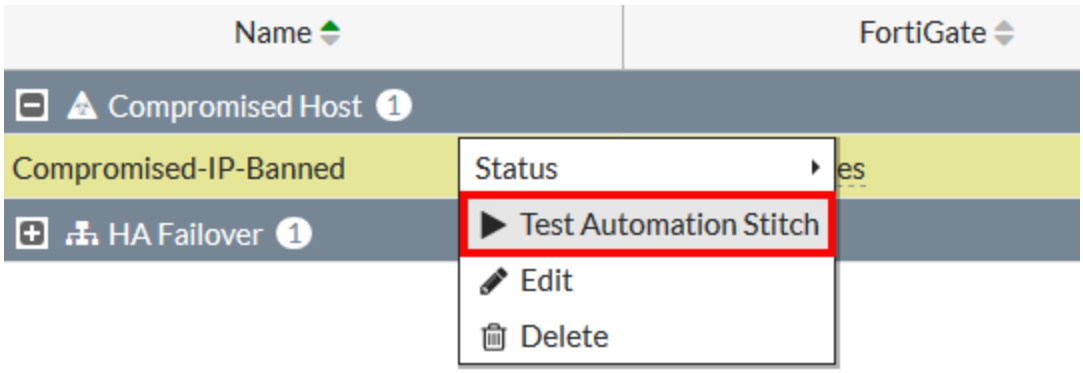

5. Create a second Automation that sends an email alert when HA failover occurs.
6. Set **FortiGate** to **Edge-Primary**, which is part of the only HA cluster in the Security Fabric.
7. Set **Trigger** to **HA Failover**. Set **Action** to **Email**.

8. Set the **Email subject** and **email address**.



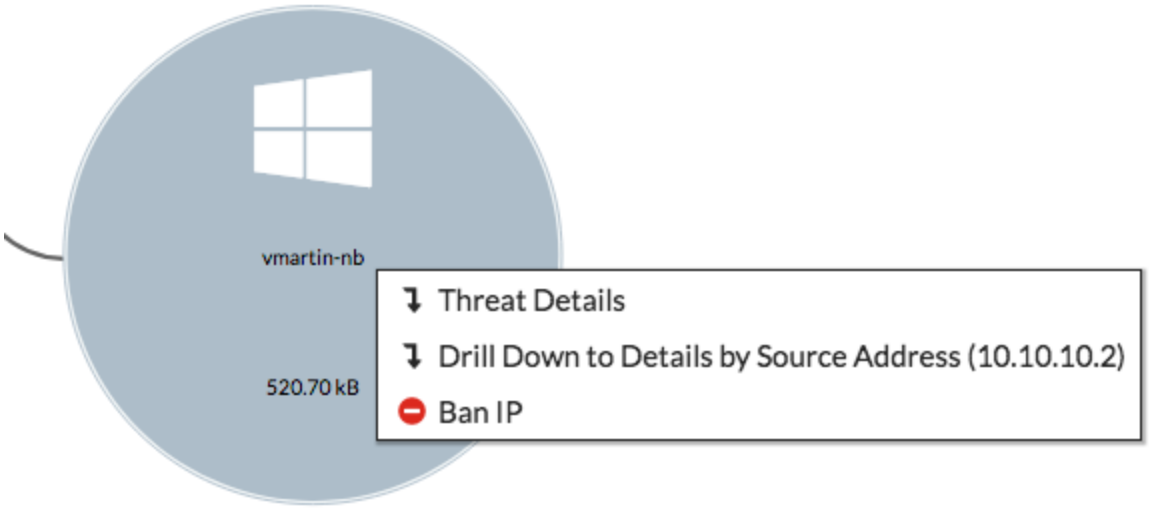

## Testing the Automation stitches

1. If your FortiOS version is 6.0.2 or higher, to test the Automation stitches go to **Security Fabric > Automation**, right-click the Automation, and select **Test Automation Stitch**.

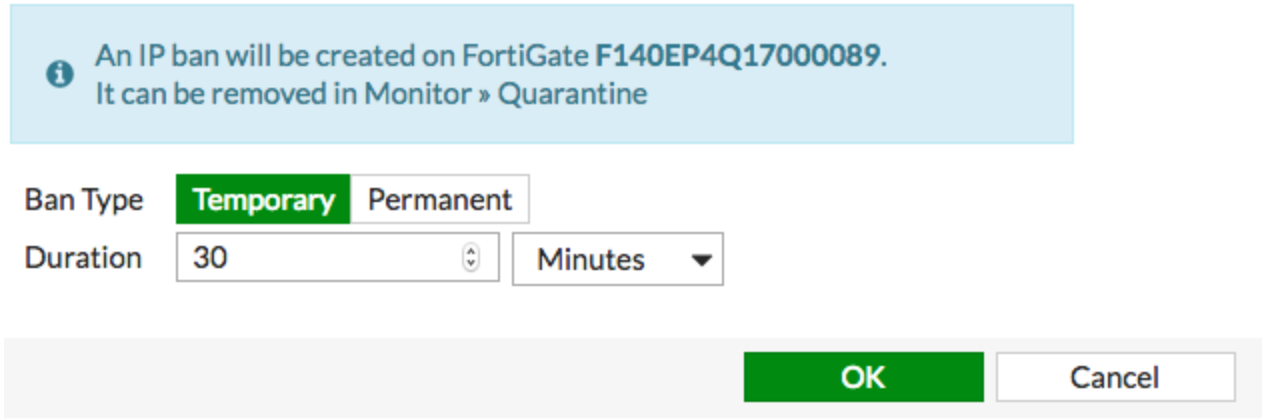



2. If your FortiOS version is 6.0.0 or 6.0.1, use the following instructions to test the automation stitches.

   Instead of testing the Automation that blocks compromised hosts, the following steps simulate its effects by manually blocking the IP address of a PC on your network. Go to **Security Fabric > Physical Topology** and locate a PC on your network. Right-click the PC and select **Ban IP**.

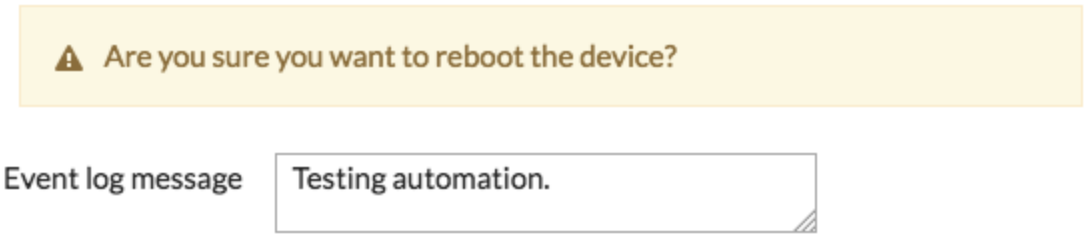



3. Set **Ban Type** to **Temporary**. Set **Duration** to **30 minutes**.




4. To test the Automation for HA failover, go to Edge-Primary. In the administrative drop-down menu, select **System > Reboot**.

5. Set an **Event log message**.

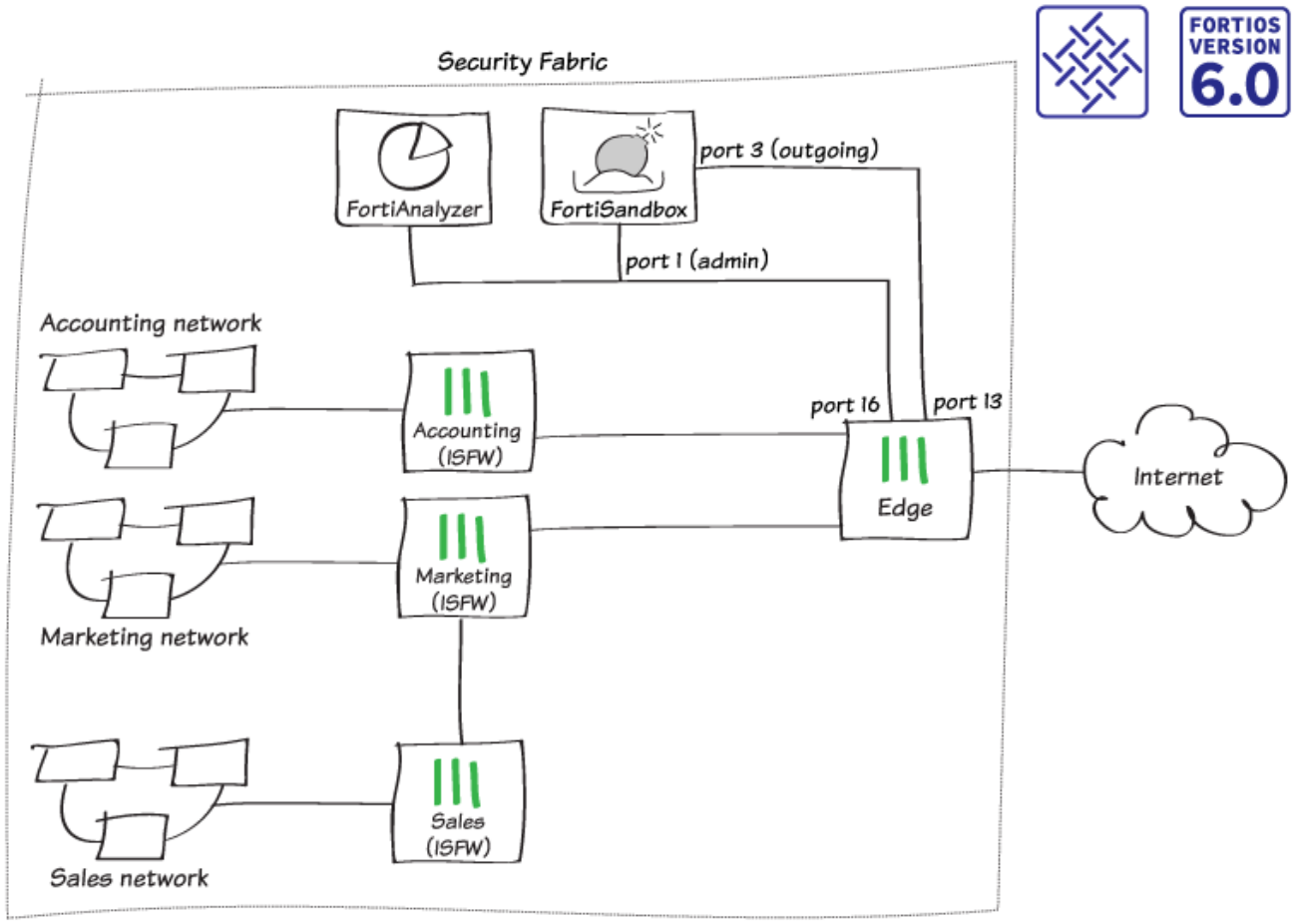



## Results

1. If you have simulated the the Automation that blocks compromised hosts, the banned device can no longer access the Internet.
2. When HA failover occurs or when the Automation is tested, an email similar to the one shown is sent to the email that you configured in the Automation.

```
FGT[FGT6HD3916806098] Automation Stitch:HA-failover is triggered.
log: logid="0108037892" type="event" subtype="ha" level="notice" vd="root"
eventtime=1522173378 logdesc="Virtual cluster member state moved"
msg="Virtual cluster's member state moved" ha_role="master" vcluster=1
vcluster_state="work" vcluster_member=0 hostname="Edge-Backup"
sn="FGT6HD3916806098"
```

# FortiSandbox in the Fortinet Security Fabric




In this recipe, you will add a FortiSandbox to the Fortinet Security Fabric and configure each FortiGate in the network to send suspicious files to FortiSandbox for sandbox inspection. The FortiSandbox scans and tests these files in isolation from your network.

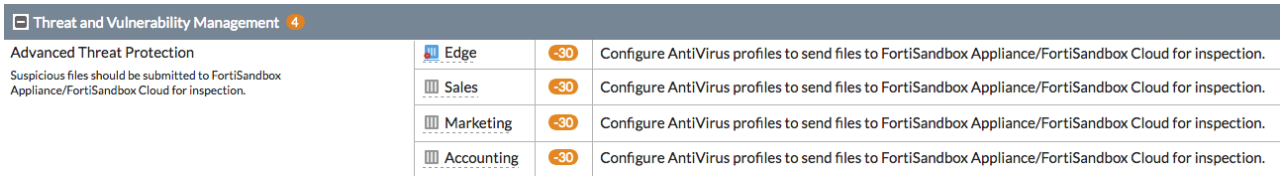
This example uses the Security Fabric configuration created in Fortinet Security Fabric installation on page 16. The FortiSandbox connects to the root FortiGate in the Security Fabric, known as Edge. There are two connections between the devices:

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

If possible, you can also use a separate Internet connection for FortiSandbox port 3, rather than connecting through the Edge FortiGate to use your main Internet connection. This configuration avoids having IP addresses from your main network blacklisted if malware that's tested on the FortiSandbox generates an attack. If you use this configuration, you can skip the steps listed for FortiSandbox port 3.

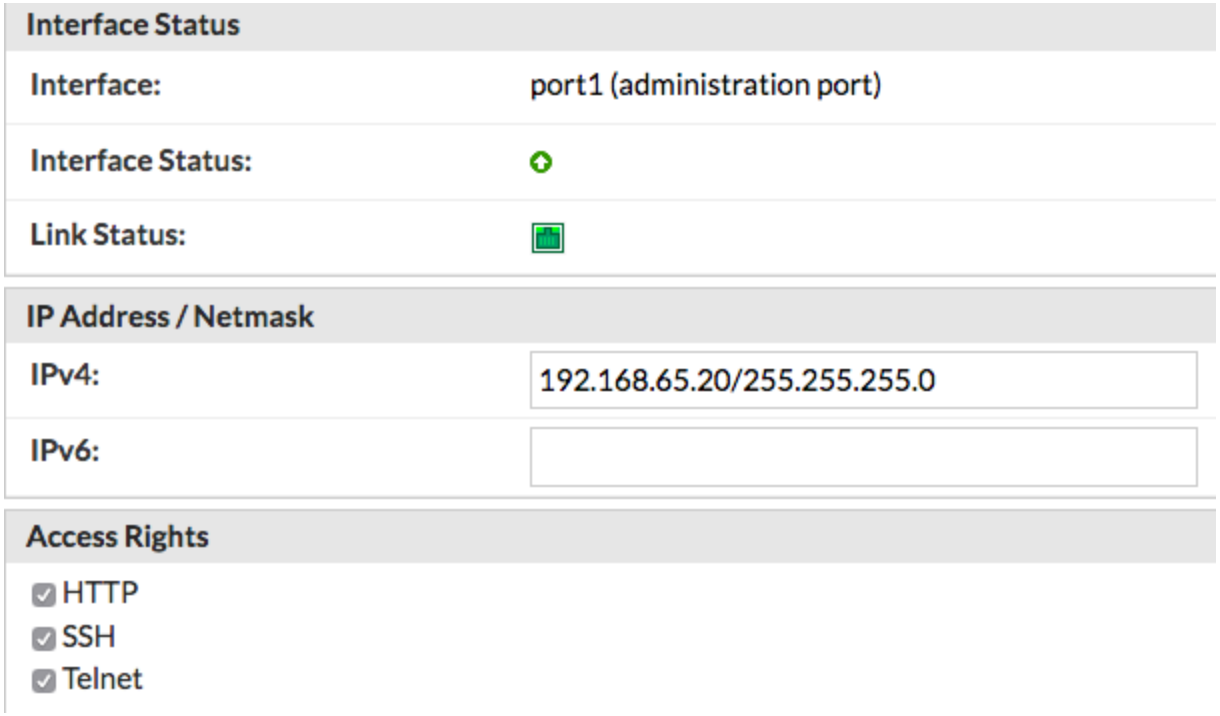
## Checking your Security Rating

1. On Edge (the root FortiGate in the Security Fabric), go to **Security Fabric > Security Rating**.
2. Since you haven't yet installed a FortiSandbox in your network, the Security Fabric fails the **Advanced Threat Protection** check. In the example, the **Security Rating Score** decreases by 30 points for each of the four FortiGates in the Security Fabric.

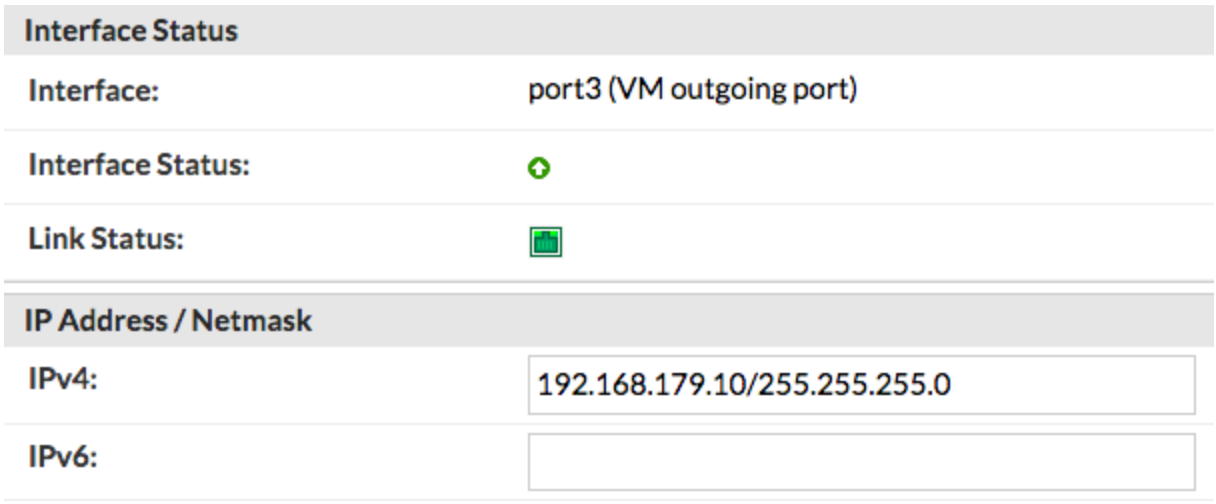



## Connecting the FortiSandbox

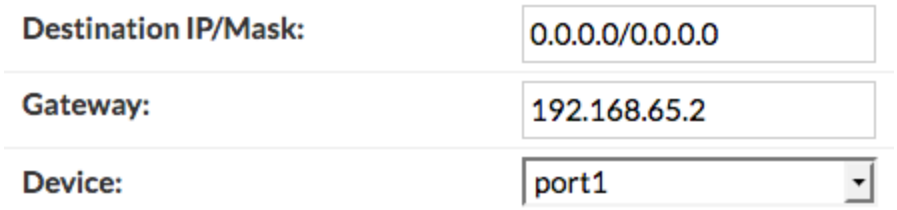
1. Connect to the FortiSandbox.
2. To edit **port 1**, which is used for communication between the FortiSandbox and the rest of the Security Fabric, go to **Network > Interfaces**.
3. Set **IP Address/Netmask** to an internal IP address. In this example, the FortiSandbox connects to the same subnet as the FortiAnalyzer that you installed previously, using the IP address *192.168.65.20*.



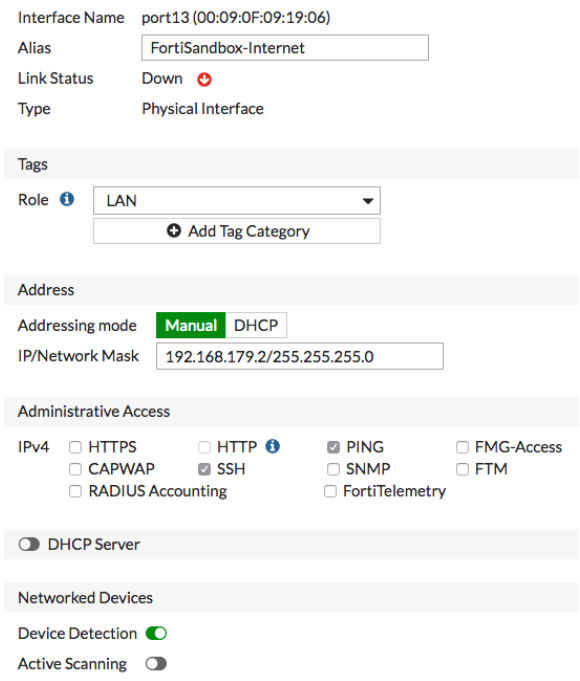

4. Edit **port 3**. This port is used for outgoing communication by the virtual machines (VMs) running on the FortiSandbox. It's recommended that you connect this port to a dedicated interface on your FortiGate to protect the rest of the network from threats that the FortiSandbox is currently investigating.
5. Set **IP Address/Netmask** to an internal IP address (in the example, *192.168.179.10/255.255.255.0*).




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



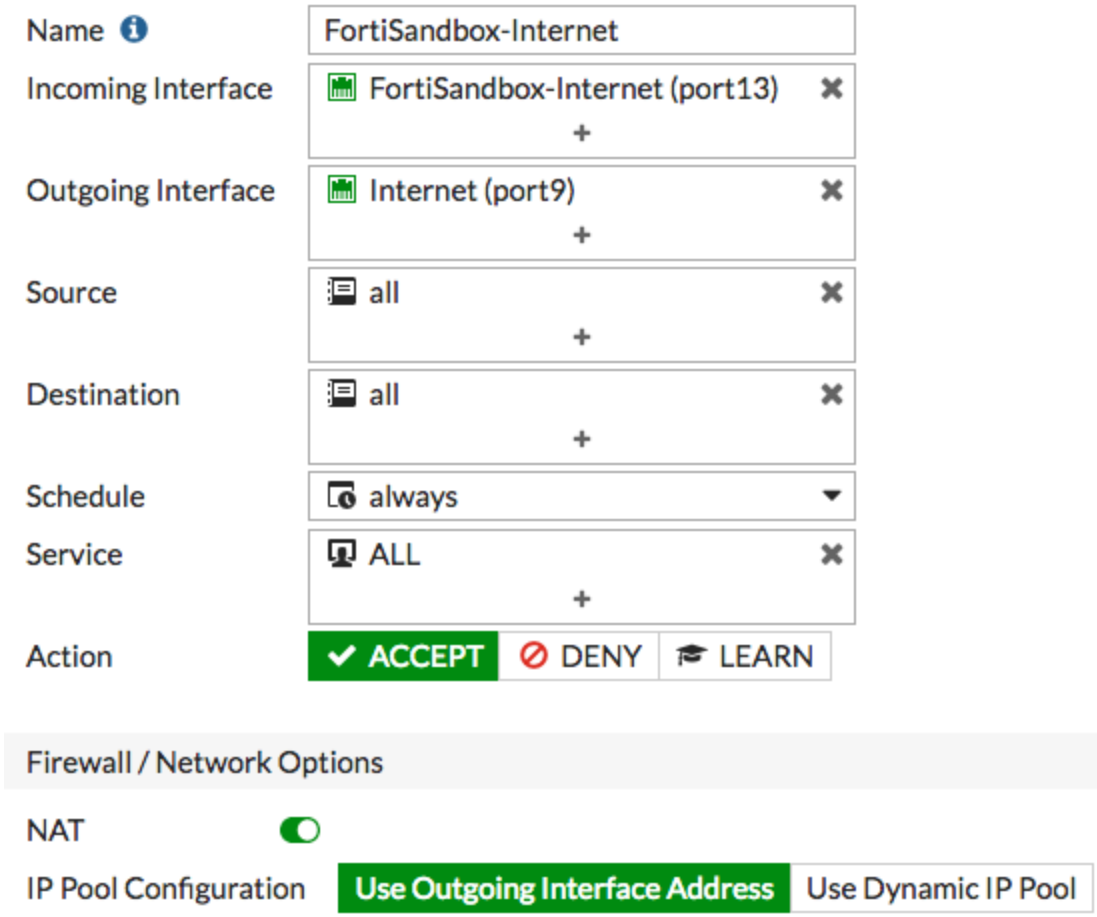

7. Connect to Edge.
8. To configure the port that connects to port3 on the FortiSandbox (in the example, port13), go to **Network > Interfaces**. Set **IP/Network Mask** to an address on the same subnet as port 3 on the FortiSandbox (in the example, *192.168.179.2/255.255.255.0*)



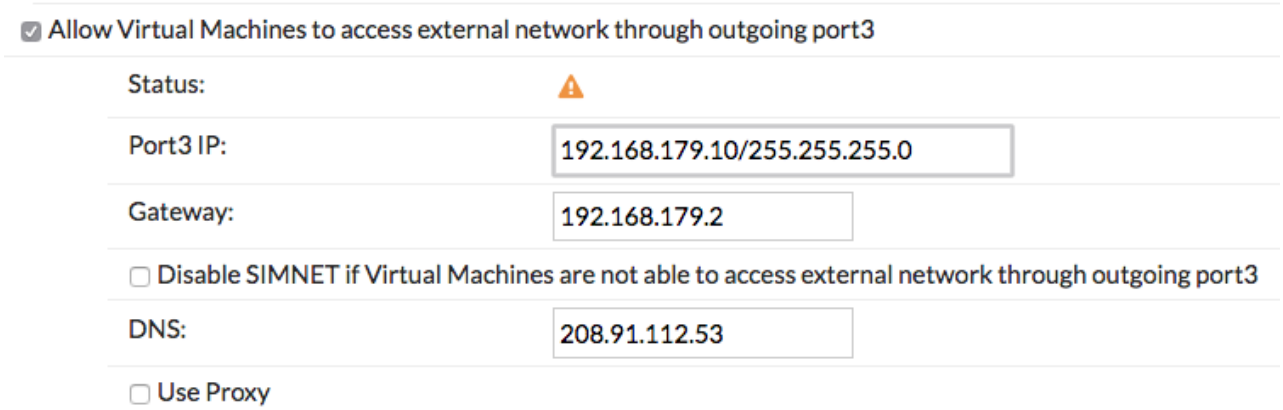

9. Connect the FortiSandbox to the Security Fabric.

## Allowing VM Internet access

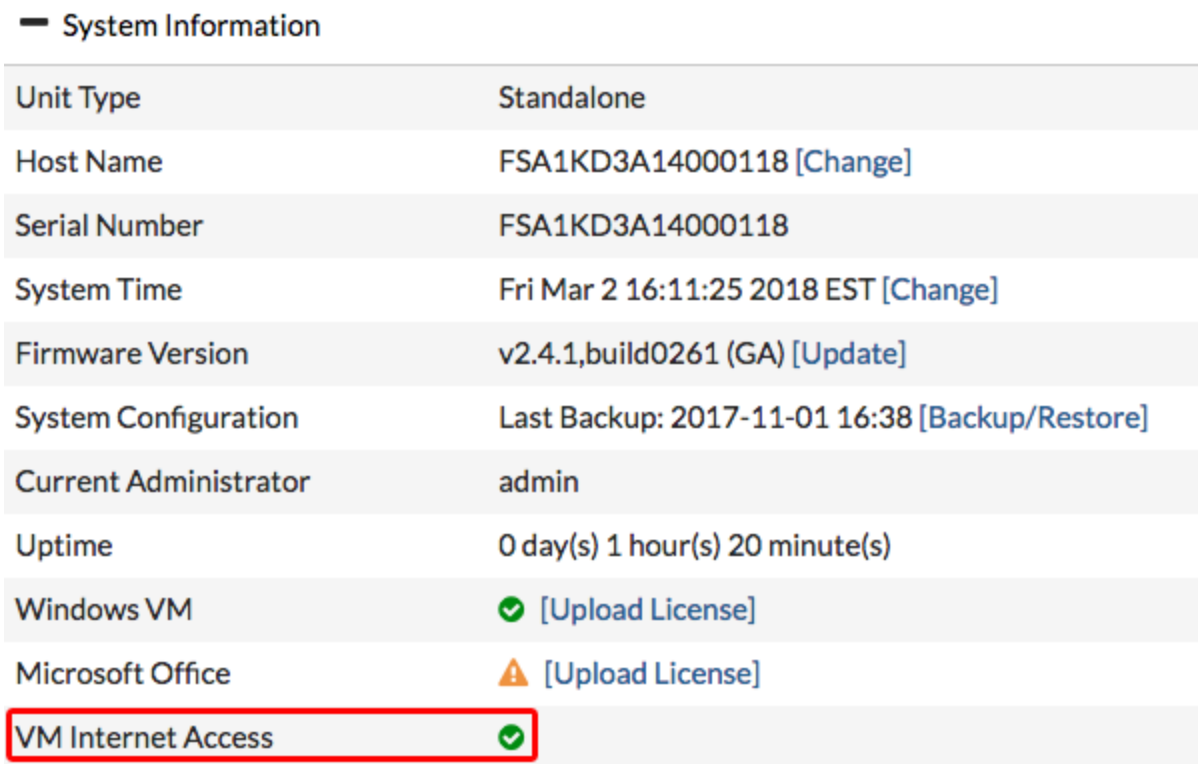
1. Connect to Edge.
2. To create a policy that allows connections from the FortiSandbox to the Internet, go to **Policy & Objects > IPv4 Policy**.




3. Connect to FortiSandbox.
4. 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.

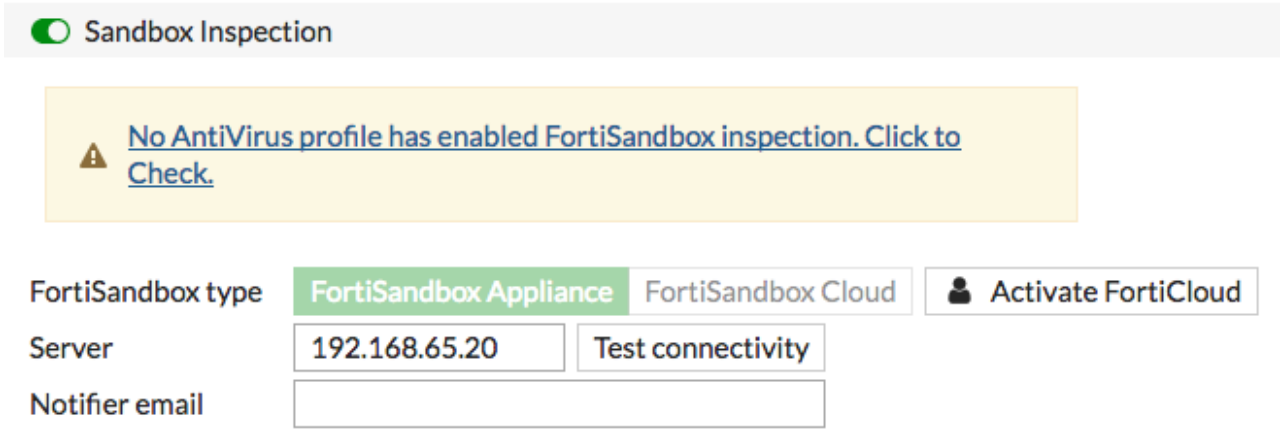


5. Go to the **Dashboard** and locate the **System Information** widget. Verify that **VM Internet Access** has a green check mark beside it.



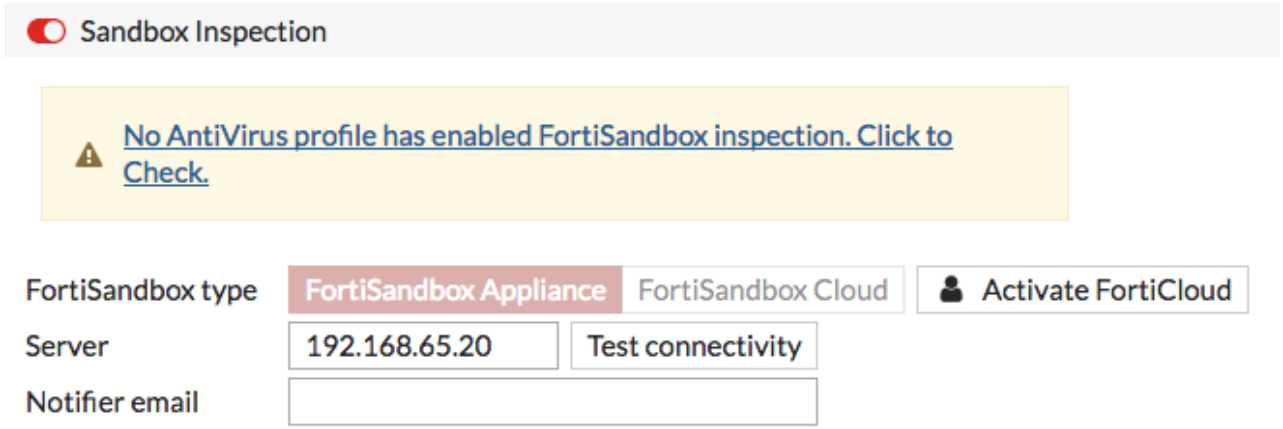

## Adding FortiSandbox to the Security Fabric

1. Connect to Edge.
2. To add FortiSandbox to the Security Fabric, go to **Security Fabric > Settings**. Enable **Sandbox Inspection**.
3. Make sure **FortiSandbox Appliance** is selected and set **Server** to the IP address of port 1 on the FortiSandbox.




4. Select **Test Connectivity**. An error message appears because Edge hasn't been authorized on the FortiSandbox.

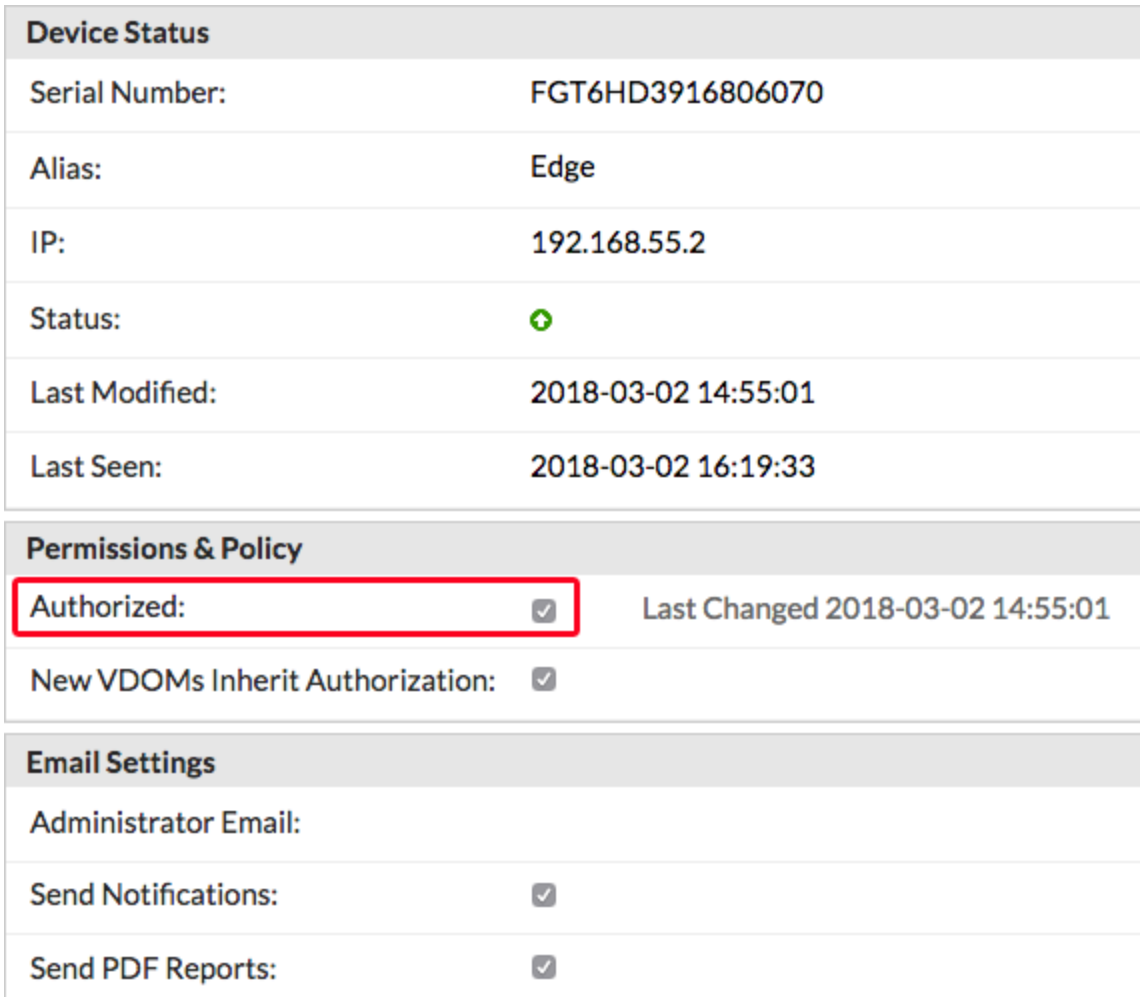

5. Edge, as the root FortiGate, pushes FortiSandbox settings to the other FortiGates in the Security Fabric. To verify this, connect to Accounting and go to **Security Fabric > Settings**.



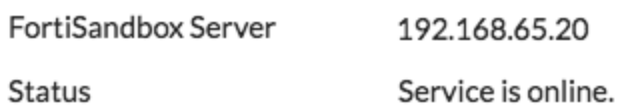

6. On the FortiSandbox, go to **Scan Input > Device**. The FortiGates in the Security Fabric (Edge, Accounting, Marketing, and Sales) are listed but the **Auth** column indicates that the devices are unauthorized.

| 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 | |

7. Select and edit **Edge**. Under **Permissions & Policies**, select **Authorized**.




8. Repeat this for the other FortiGate devices.
9. On Edge, go to **Security Fabric > Settings** and test the **Sandbox Inspection** connectivity again. Edge is now connected to the FortiSandbox.



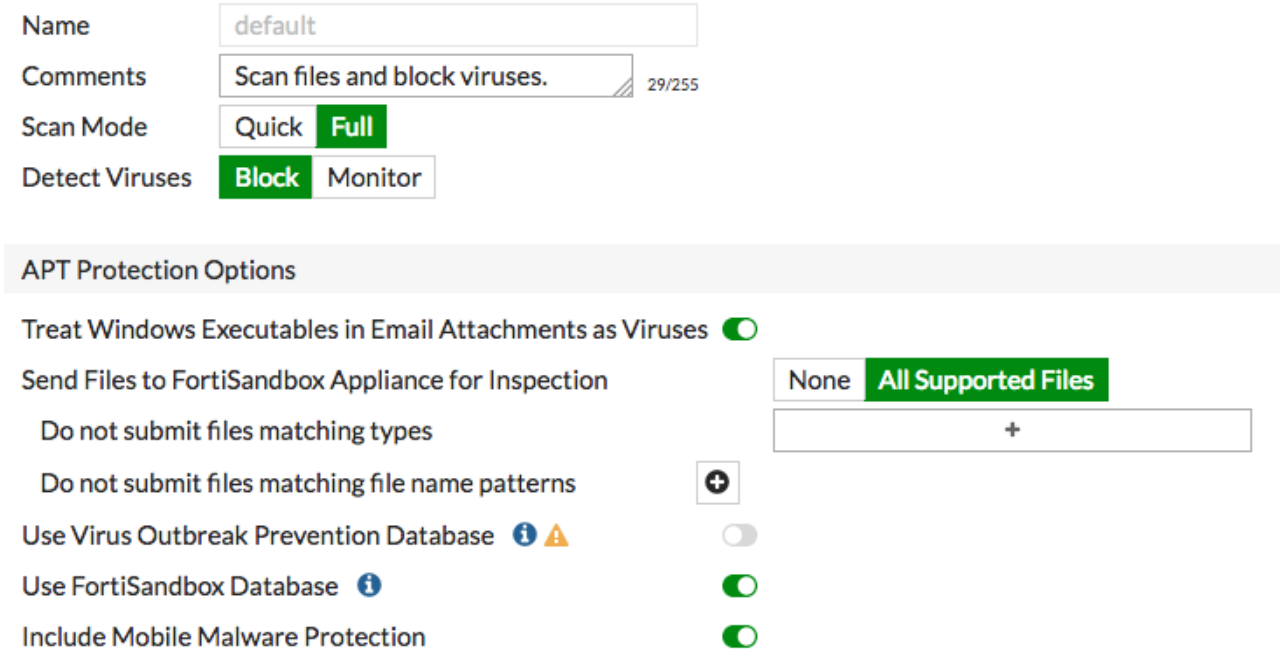

## Adding sandbox inspection to security profiles

You can apply sandbox inspection with three types of security inspection: antivirus, web filter, and FortiClient compliance profiles. In this step, you add sandbox to all FortiGate devices in the Security Fabric individually, using the profiles that each FortiGate applies to network traffic.

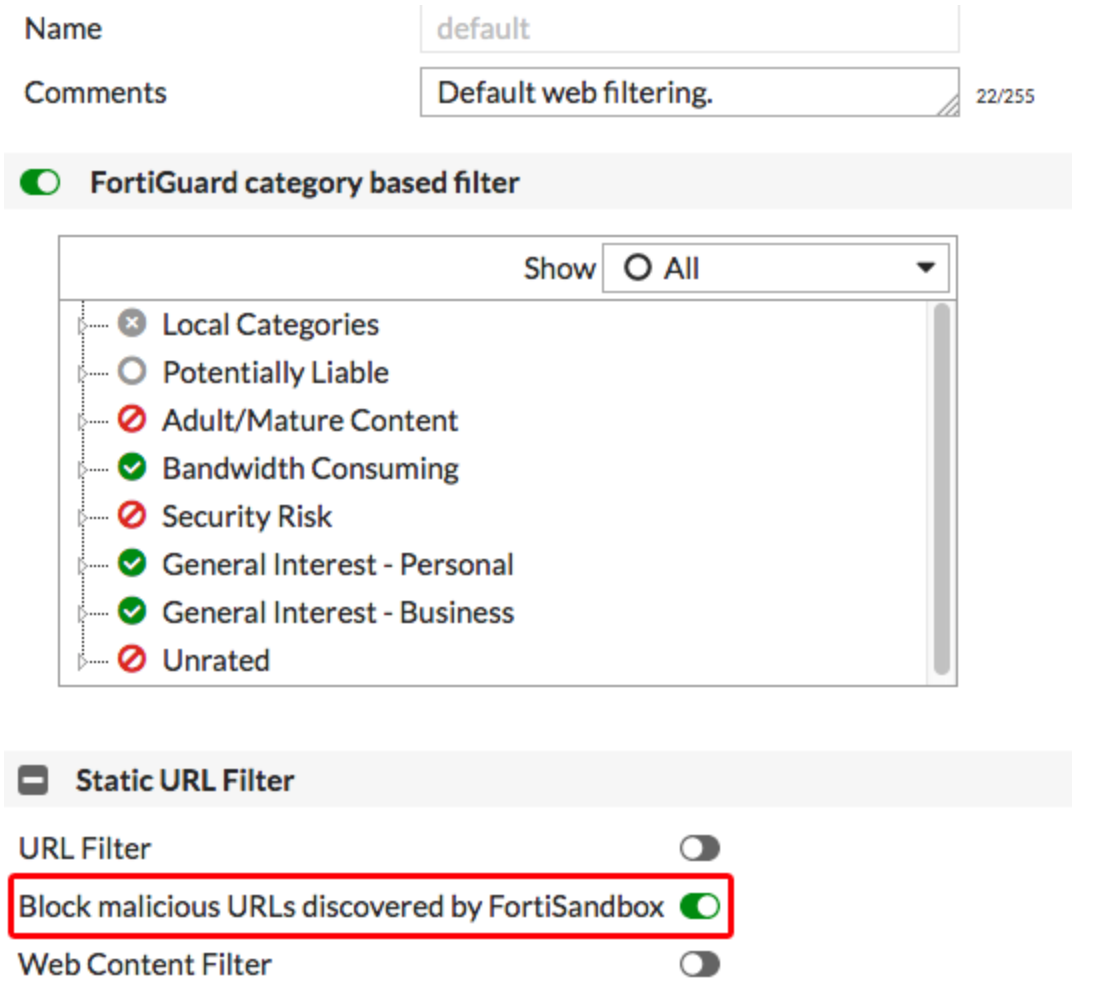
In order to pass the **Advanced Threat Protection** check, you must add sandbox inspection to antivirus profiles for all FortiGate devices in the Security Fabric.

1. Go to **Security Profiles > AntiVirus** and edit the **default** profile.
2. Under **Inspection Options**, set **Send Files to FortiSandbox Appliance for Inspection** to **All Supported Files**.

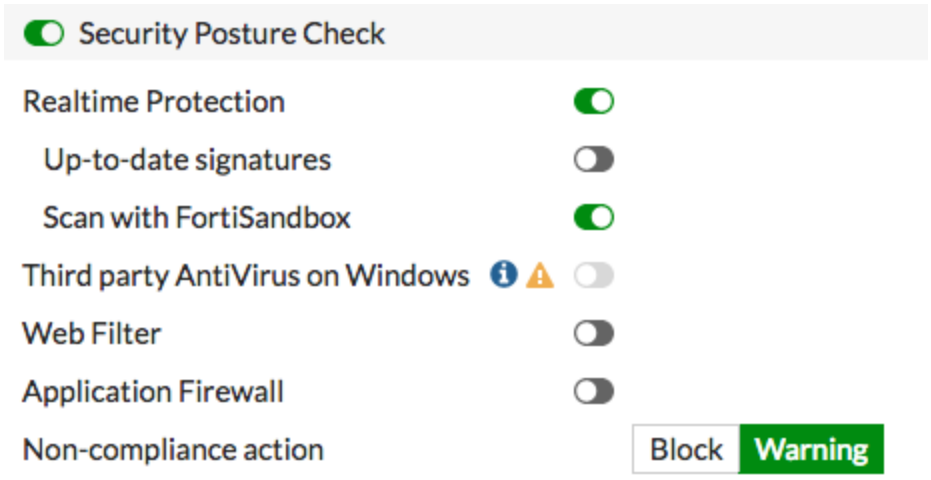
3. Enable **Use FortiSandbox Database**, so that if the FortiSandbox discovers a threat, it adds a signature for that file to the antivirus signature database on the FortiGate.




4. Go to **Security Profiles > Web Filter** and edit the **default** profile.
5. Under **Static URL Filter**, enable **Block malicious URLs discovered by FortiSandbox**. If the FortiSandbox discovers a threat, the URL that threat came from is added to the list of URLs that are blocked by the FortiGate.

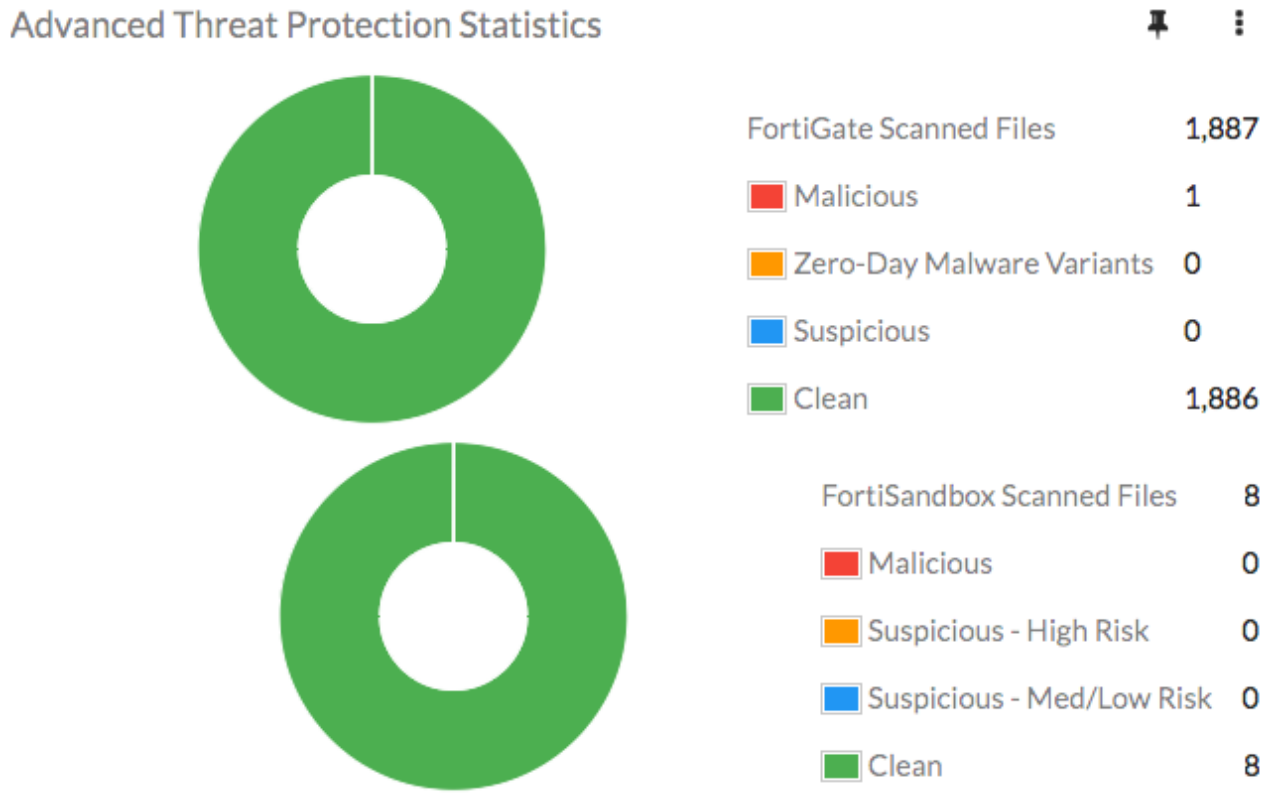



6. Go to **Security Profiles > FortiClient Compliance Profiles** and edit the **default** profile. Enable **Security Posture Check**.
7. Enable **Realtime Protection** and **Scan with FortiSandbox**.



## Results

1. If a FortiGate in the Security Fabric discovers a suspicious file, it sends the file to the FortiSandbox.
   You can view information about scanned files on either the FortiGate that sent the file or the FortiSandbox. On one of the FortiGate devices, go to the **Dashboard** and locate the **Advanced Threat Protection Statistics** widget. This widget shows files that both the FortiGate and FortiSandbox scan.

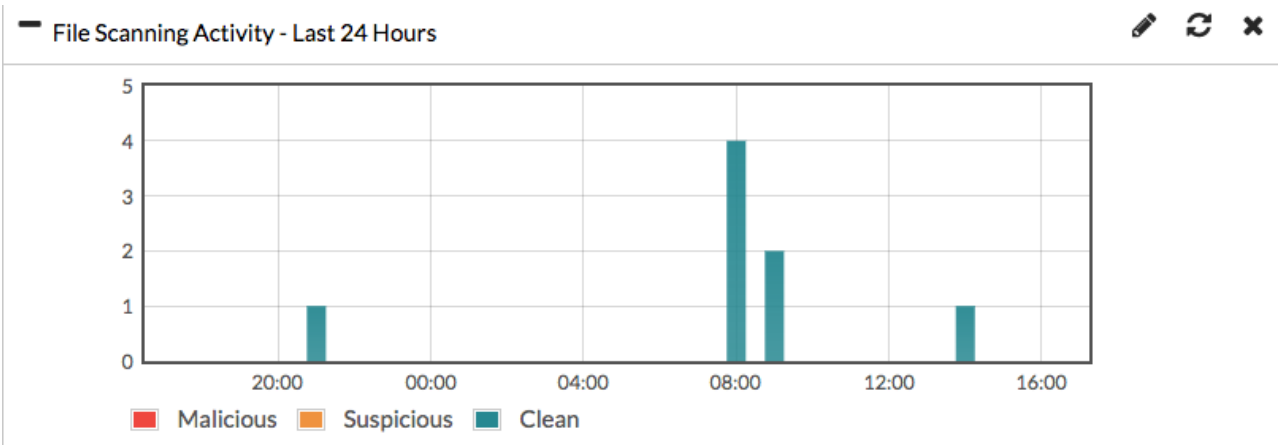



2. On the FortiSandbox, go to **System > Status** and view the **Scanning Statistics** widget for a summary of scanned files.

Scanning Statistics - Last 24 Hours

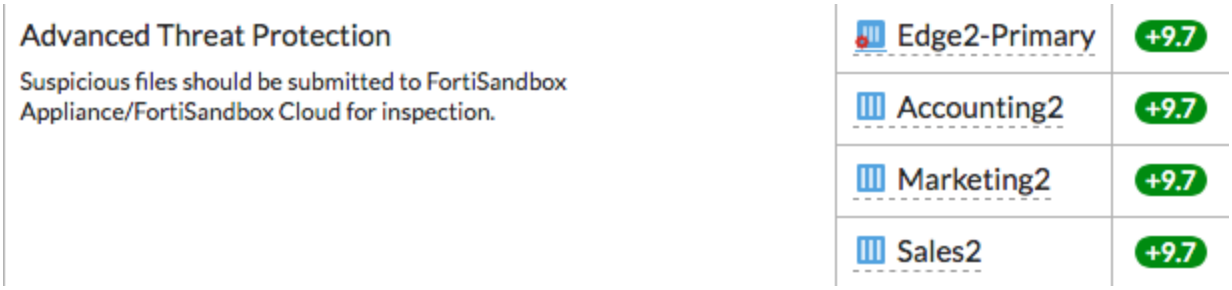
| Rating | Sniffer | Device(s) | On Demand | Network | Adapter | URL | All |
|---|---|---|---|---|---|---|---|
| Malicious | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Suspicious - High Risk | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Suspicious - Medium Risk | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Suspicious - Low Risk | 0 | 0 | 0 | 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* |

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

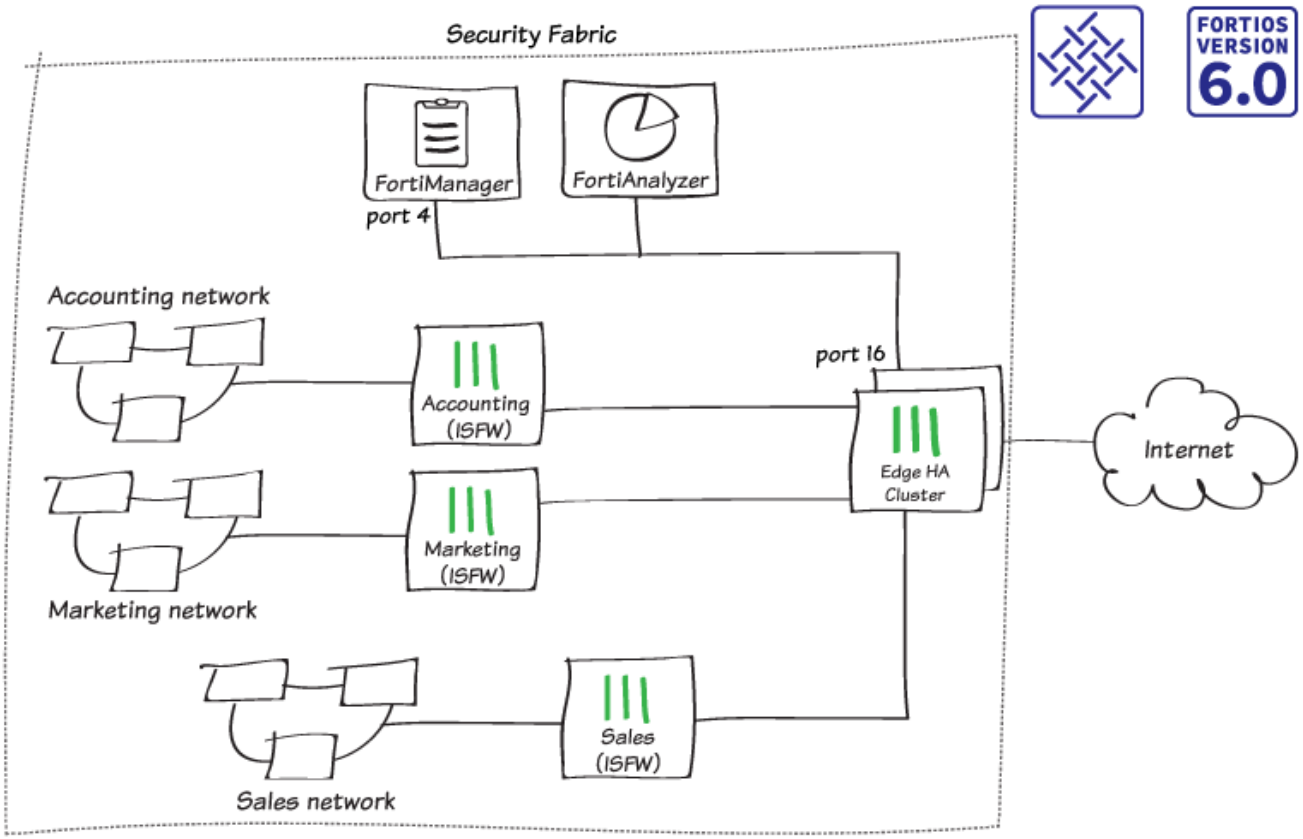



4. On Edge, go to **Security Fabric > Security Rating** and run a rating. When it is finished, select the **All Results** view.

   In the example, all four FortiGate devices in the Security Fabric pass the **Advanced Threat Protection** check and the **Security Rating Score** increases by 9.7 points for each FortiGate.



# FortiManager in the Fortinet Security Fabric



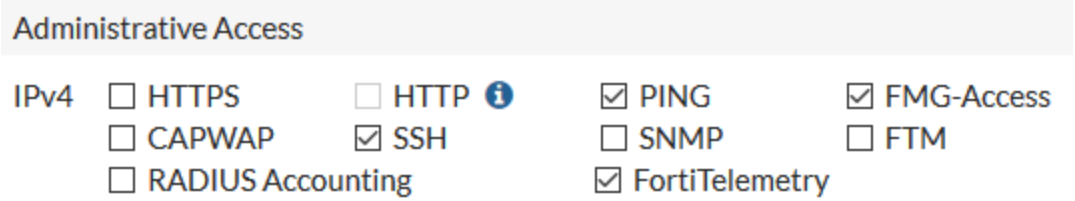

In this recipe, you add a FortiManager to the Security Fabric. This simplifies network administration because you manage all of the FortiGate devices in your network from the FortiManager.

In this example, you add the FortiManager to an existing Security Fabric, with an HA cluster called Edge as the root FortiGate and three internal FortiGates: Accounting, Marketing, and Sales. Network resources, such as a FortiManager, are located on the subnet 192.168.65.x.

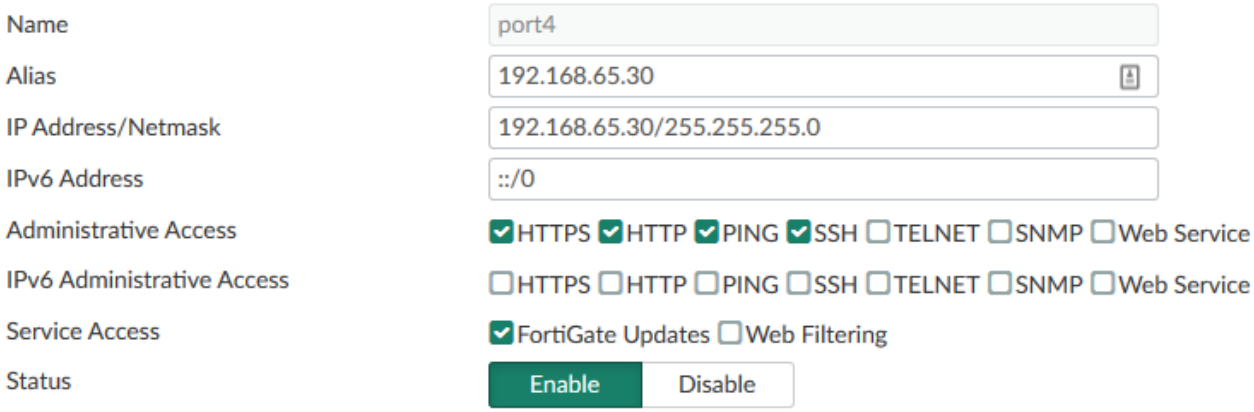
## Connecting the FortiManager

In this example, port 16 on Edge connects to port 4 on the FortiManager.

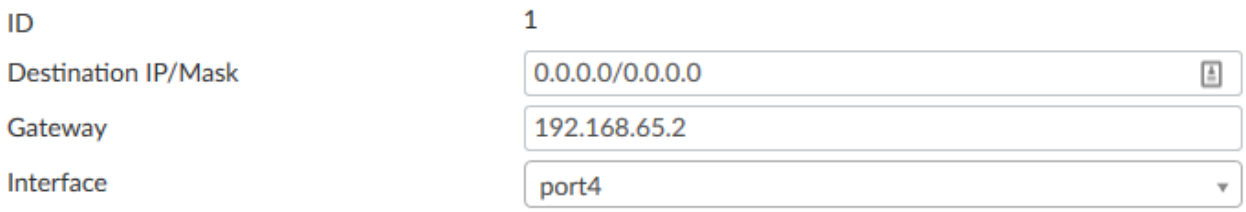
1. To configure the interface on the root FortiGate, connect to Edge, go to **Network > Interfaces**, and edit **port 16**.
2. Configure **Administrative Access** to allow **FMG-Access** and **FortiTelemetry**.



3. To configure the interface on the FortiManager, connect to the FortiManager, go to **System Settings > Network**, select **All Interfaces**, and edit **port 4**.
4. Set **IP Address/Netmask** to an internal IP address (in the example, *192.168.65.30/255.255.255.0*).




5. Select **Routing Table** and add a default route for port 4. Set **Gateway** to the IP address of port 16 on Edge.

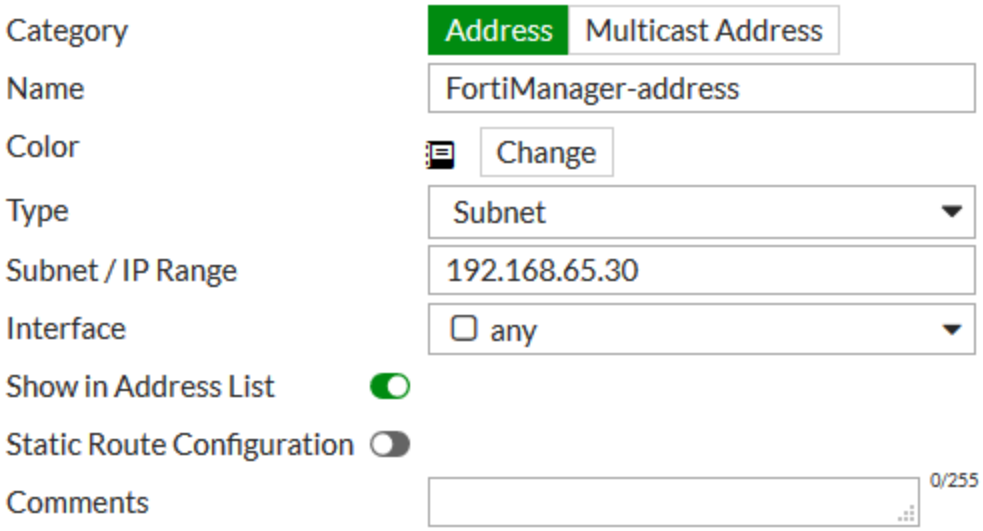



6. If you haven't already done so, connect the FortiManager and Edge.

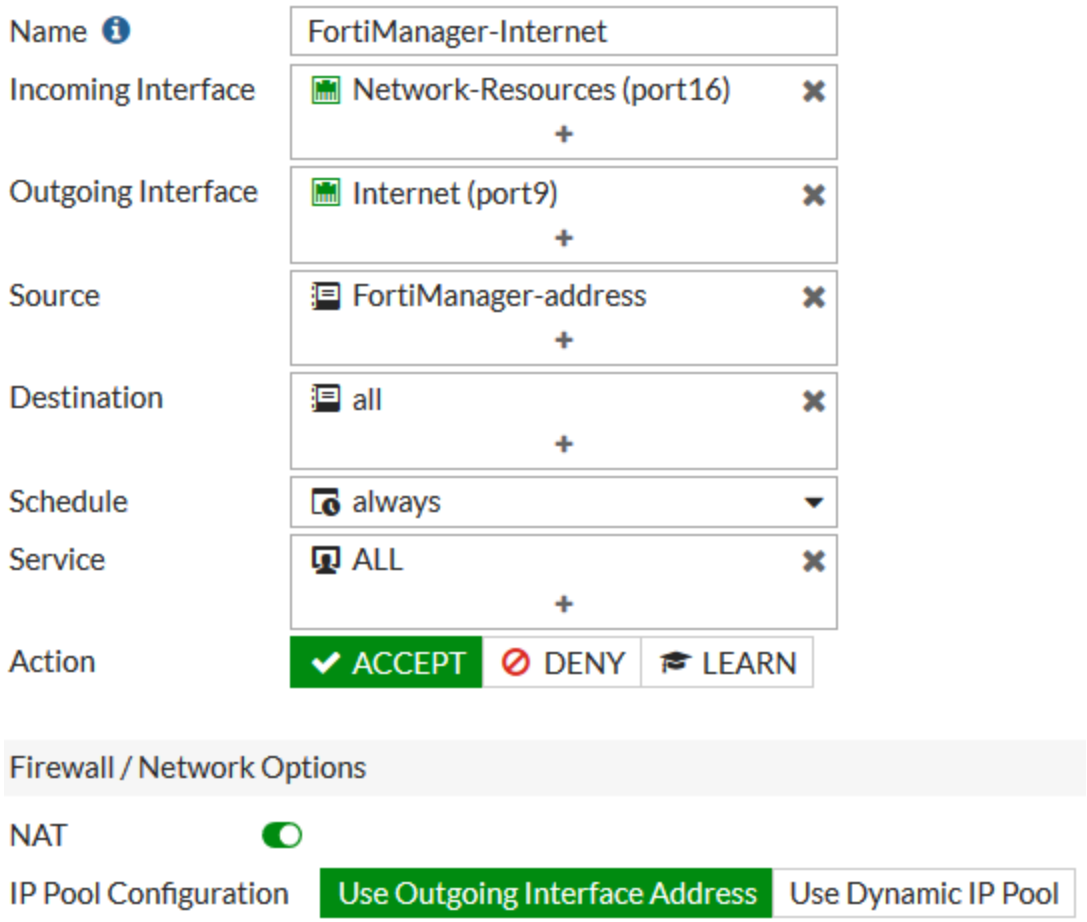
## Allowing Internet access

In order to communicate with FortiGuard, the FortiManager requires Internet access.

1. To create an address for the FortiManager, connect to Edge, go to **Policy & Objects > Addresses**, and create a new address.

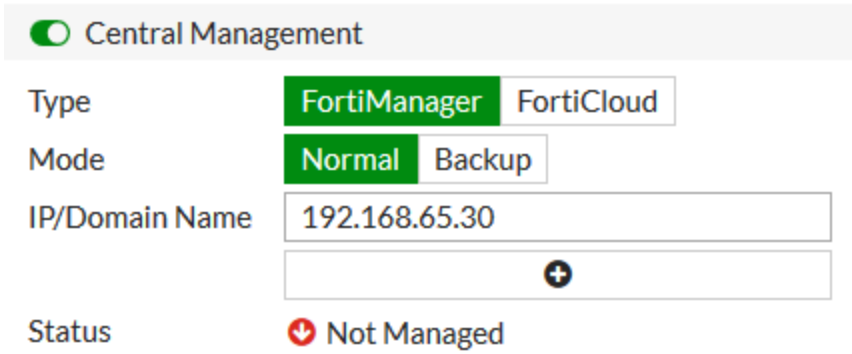


2. To allow the FortiManager to access the Internet, go to **Policy & Objects > IPv4 Policy**, and create a new policy.

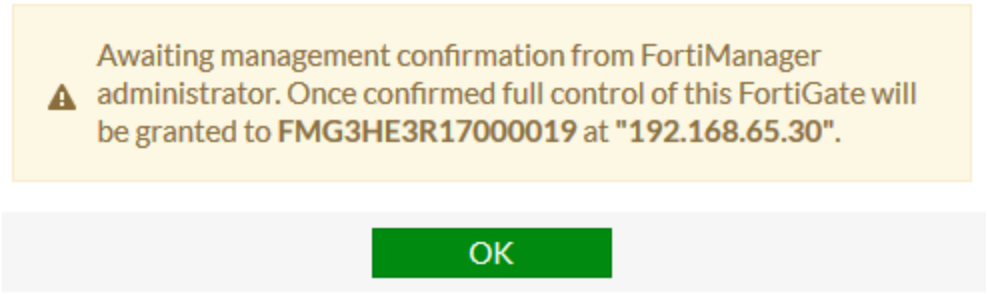



## Configuring central management

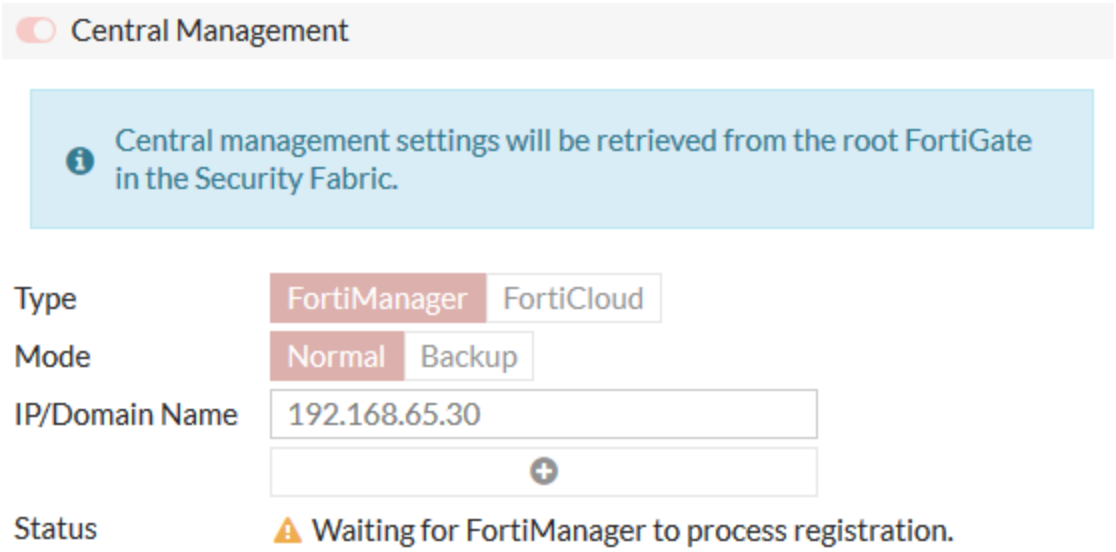
1. To enable central management, connect to Edge, go to **Security Fabric > Settings**, and enable **Central Management**.
2. Set **Type** to **FortiManager**, **Mode** to **Normal**, and set **IP/Domain Name** to the IP address of port 4 on the FortiManager.



3. After you select **Apply**, a message appears stating that the FortiManager received the message and Edge is waiting for management confirmation.



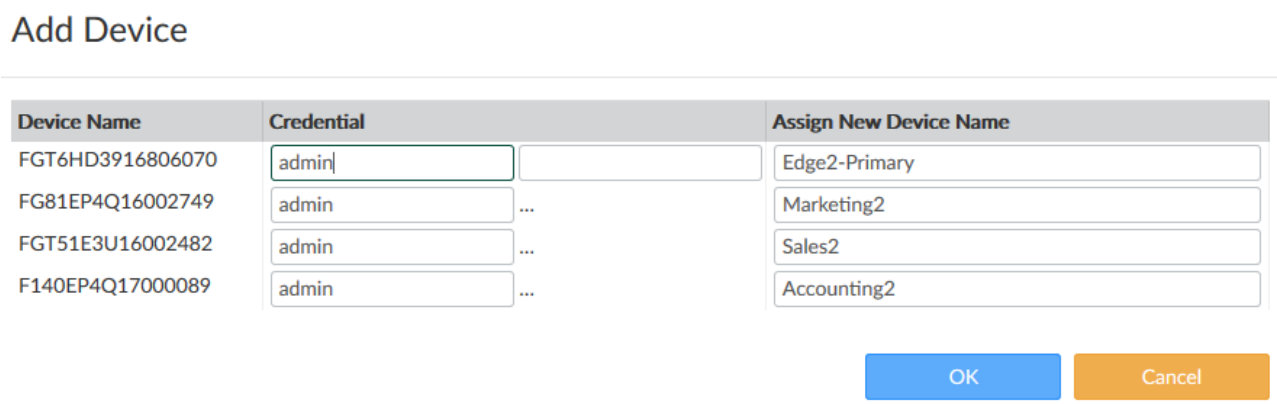

4. Edge, as the root FortiGate, pushes FortiManager settings to the other FortiGate devices in the Security Fabric. To verify this, connect to Accounting and go to **Security Fabric > Settings**.



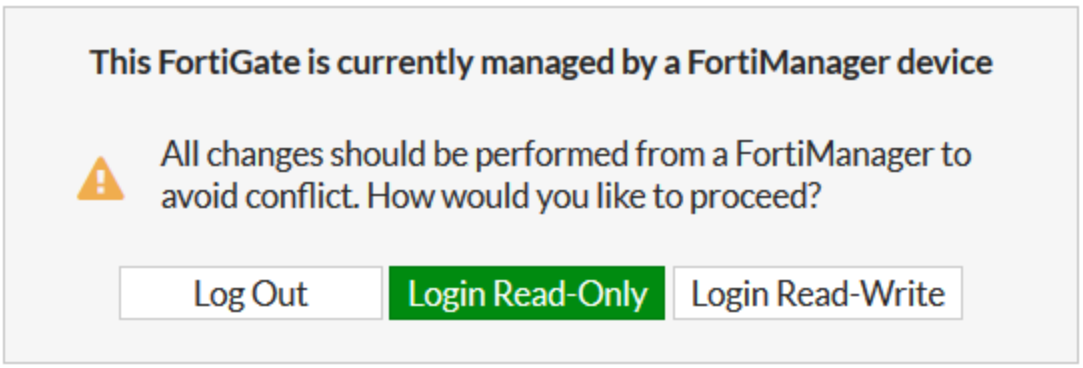

5. To confirm the management connection, connect to the FortiManager and go to **Device Manager > Unregistered Devices**. Select the FortiGate devices and select **+ Add**.

| Device Name | Model | Management Mode | Serial Number | Connecting IP | Firmware Version |
|---|---|---|---|---|---|
| Accounting2 | FortiGate-140E-POE | Configuration & Logging | F140EP4Q17000089 | 192.168.65.2 | FortiGate 6.0.0,build0076 (GA) |
| Edge2-Primary | FortiGate-600D | Configuration & Logging | FGT6HD3916806070 | 192.168.65.2 | FortiGate 6.0.0,build0076 (GA) |
| Marketing2 | FortiGate-81E-POE | Configuration & Logging | FG81EP4Q16002749 | 192.168.65.2 | FortiGate 6.0.0,build0076 (GA) |
| Sales2 | FortiGate-51E | Configuration & Logging | FGT51E3U16002482 | 192.168.65.2 | FortiGate 6.0.0,build0076 (GA) |

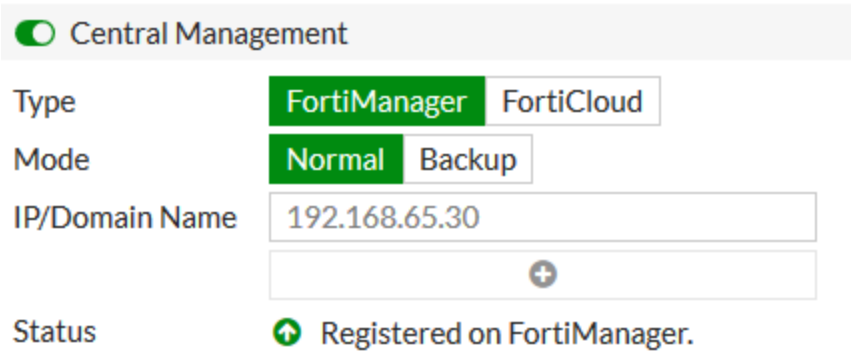
6. Add the FortiGate devices to the FortiManager.




7. Connect to Edge. A warning message appears stating that the FortiGate is now managed by a FortiManager. Select **Login Read-Only**.




8. Go to **Security Fabric > Settings**. Under **Central Management**, the **Status** is now **Registered on FortiManager**.

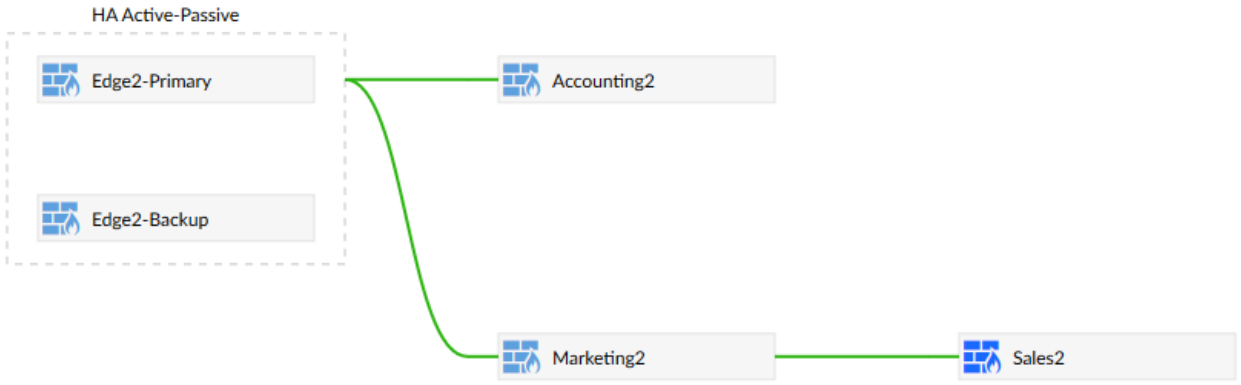



## Results

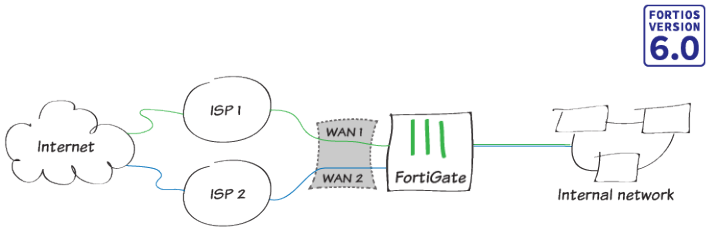
1. The FortiGate devices are on the **Managed FortiGate** list and appear as part of a Security Fabric group. The * beside Edge indicates that it's the root FortiGate in the Security Fabric.

| Device Name | Config Status | Policy Package Status | Host Name | IP Address | Platform |
|---|---|---|---|---|---|
| FGT6HD3916806070 | | | | | |
| Accounting2 | Synchronized | Never installed | Accounting2 | 192.168.65.2 | FortiGate-140E-POE |
| Edge2-Primary* | Auto-update | Never installed | Edge2-Primary | 192.168.65.2 | FortiGate-600D |
| Marketing2 | Synchronized | Never installed | Marketing2 | 192.168.65.2 | FortiGate-81E-POE |
| Sales2 | Synchronized | Never installed | Sales2 | 192.168.65.2 | FortiGate-51E |

2. Right-click on any of the FortiGate devices and select **Fabric Topology**. The topology of the Security Fabric is displayed.

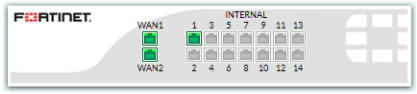



# Redundant Internet with SD-WAN




This recipe provides an example of how you can configure redundant Internet connectivity for your network using SD-WAN. This allows you to load balance your Internet traffic between multiple ISP links and provides redundancy for your network's Internet connection if your primary ISP is unavailable.

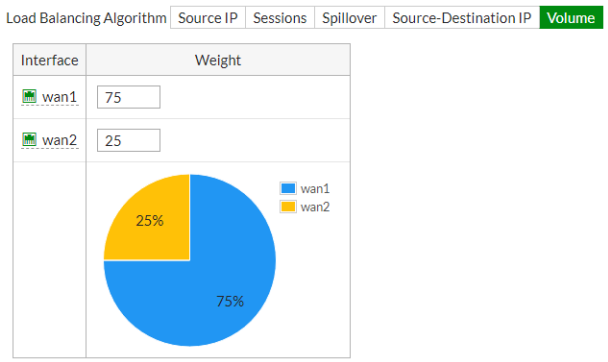
1. Connect the FortiGate to your ISP devices by connecting the Internet-facing (WAN) ports on the FortiGate to your ISP devices. Connect WAN1 to the ISP that you want to use for most traffic, and connect WAN2 to the other ISP.




2. Before you can configure FortiGate interfaces as SD-WAN members, you must remove or redirect existing configuration references to those interfaces in routes and security policies. This includes the default Internet access policy that's included with many FortiGate models. Note that after you remove the routes and security policies, traffic can't reach the WAN ports through the FortiGate. Redirecting the routes and policies to reference other interfaces avoids your having to create them again later. After you configure SD-WAN, you can reconfigure the routes and policies to reference the SD-WAN interface. Remove existing configuration references to interfaces:

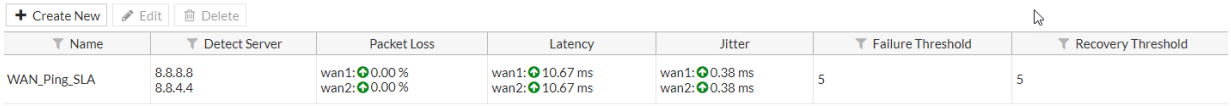
a. Go to *Network* > *Static Routes* and delete any routes that use WAN1 or WAN2.
b. Go to *Policy & Objects* > *IPv4 Policy* and delete any policies that use WAN1 or WAN2.

3. Create the SD-WAN interface:
   a. Go to *Network* > *SD-WAN* and set *Status* to *Enable*.
   b. Under *SD-WAN Interface Members*, select + and select *wan1*. Set the *Gateway* to the default gateway for this interface. This is usually the default gateway IP address of the ISP that this interface is connected to. Repeat these steps to add *wan2*.
   c. Go to *Network* > *Interfaces* and verify that the virtual interface for *SD-WAN* appears in the interface list. You can expand SD-WAN to view the ports that are included in the SD-WAN interface.
4. Configure SD-WAN load balancing:
   a. Go to *Network* > *SD-WAN Rules* and edit the rule named sd-wan.
   b. In the *Load Balancing Algorithm* field, select *Volume*, and prioritize WAN1 to serve more traffic. the 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.

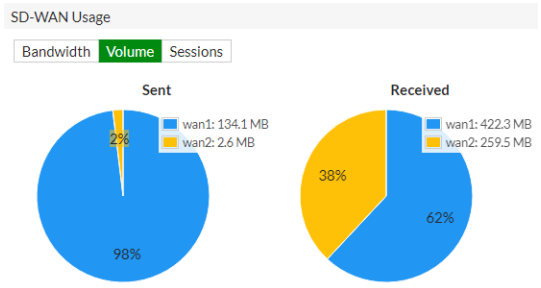



5. Create a static route for the SD-WAN interface:
   a. Go to *Network* > *Static Routes* and create a new route.
   b. In the *Destination* field, select *Subnet*, and leave the destination IP address and subnet mask as 0.0.0.0/0.0.0.0.
   c. In the *Interface* field, select the SD-WAN interface from the dropdown list.
   d. Ensure that *Status* is set to *Enable*. If you previously removed or redirected existing references in routes to interfaces that you wanted to add as SD-WAN interface members, you can now reconfigure those routes to reference the SD-WAN interface.
6. Configure a security policy that allows traffic from your organization's internal network to the SD-WAN interface.
   a. Go to *Policy & Objects* > *IPv4 Policy* and create a new policy.
   b. Set *Incoming Interface* to the interface that connects to your organization's internal network and set *Outgoing Interface* to the SD-WAN interface.
   c. Enable *NAT* and apply *Security Profiles* as required.
   d. Enable *Log Allowed Traffic* for *All Sessions* to allow you to verify the results later. If you previously removed or redirected existing references in security policies to interfaces that you wanted to add as SD-WAN interface members, you can now reconfigure those policies to reference the SD-WAN interface.
7. You can configure link health monitoring to verify the health and status of the links that make up the SD-WAN link:
   a. Go to *Network* > *Performance SLA* and create a new performance SLA.
   b. Set the *Protocol* for the health checks. In the *Server* fields, enter the IP addresses of up to two servers that you want to use to test the health of each SD-WAN member interface.* In the *Participants* field, select the SD-WAN interface members that you want the health check to apply to.
   c. You can view link quality measurements on the *Performance SLA* page. The table displays information about configured health checks. The values in the *Packet Loss*, *Latency*, and *Jitter* columns apply to the server that

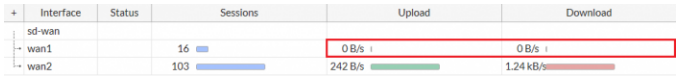
the FortiGate is using to test the health of the SD-WAN member interfaces. The green (up) arrows indicate only that the server is responding to the health checks, regardless of the packet loss, latency, and jitter values, and do not indicate that the health checks are being met.



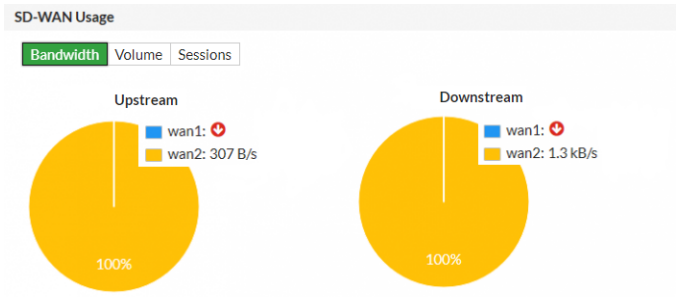

8. View the results:
   a. Browse the Internet using a computer on your internal network and then go to *Network* > *SD-WAN*.
   b. In the *SD-WAN Usage* section, you can see the bandwidth, volume, and sessions for traffic on the SD-WAN interfaces.




   c. Go to *Monitor* > *SD-WAN Monitor* to view the number of sessions, bit rate, and more information for each interface.
9. To test failover of the redundant Internet configuration, you must simulate a failed Internet connection to one of the ports. Do so by physically disconnecting the Ethernet cable connected to WAN1:
   a. Verify that users still have Internet access by navigating to *Monitor* > *SD-WAN Monitor*. The *Upload* and *Download* values for WAN1 show that traffic is not going through that interface.




   b. Go to *Network* > *SD-WAN*. In the *SD-WAN Usage* section, you can see that bandwidth, volume, and sessions have diverted entirely through WAN2.




   c. Users on the internal network should not notice the WAN1 failure. Likewise, if you are using the WAN1 gateway IP address to connect to the admin dashboard, nothing should change from your perspective. It appears as though you are still connecting through WAN1. After you verify successful failover, reconnect the WAN1 Ethernet cable.

# Blocking malicious domains using threat feeds

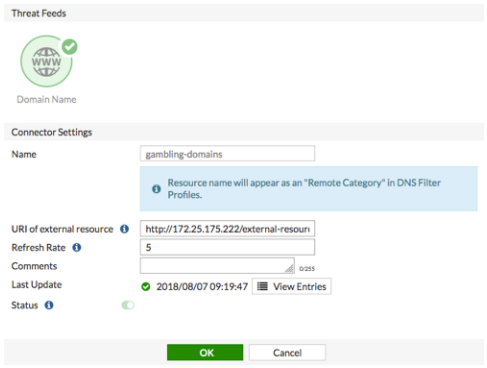
This example uses a domain name threat feed and FortiGate DNS filtering to block malicious domains. The text file in this example is a list of gambling site domain names.

Threat feeds allow you to dynamically import external block lists in the form of a text file into your FortiGate. These text files, stored on an HTTP server, can contain a list of web addresses or domains. You can use threat feeds to deny access to a source or destination IP address in Web Filter and DNS Filter profiles, SSL inspection exemptions, and as a source/destination in proxy policies. You can use Fabric connectors for FortiGates that do not belong to a Fortinet Security Fabric.

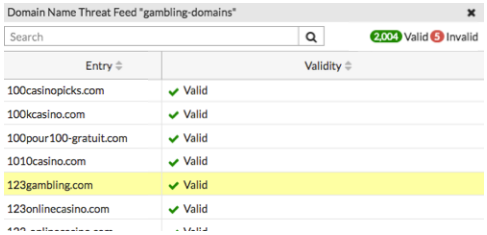
1. Create an external block list. The external block list should be a plain text file with one domain name per line. The use of simple wildcards is supported. You can create your own text file or download it from an external service. Upload the text file to the HTTP file server.

```
100casinopicks.com
100kcasino.com
100pour100-gratuit.com
1010casino.com
123gambling.com
123onlinecasino.com
```

2. Configure the threat feed:
   a. In FortiOS, go to *Security Fabric* > *Fabric Connectors*. Click *Create New*.
   b. Under *Threat Feeds*, select *Domain Name*.
   c. Configure the *Name*, *URI of external resource*, and *Refresh Rate* fields. In the *URI of external resource* field, enter the location of the text file on the HTTP file server. By default, the FortiGate rereads the file and uploads any changes every five minutes.

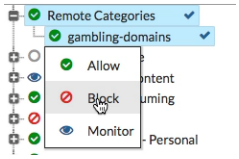



   d. Click *View Entries* to see the text file's domain list.




   e. Click *OK*.
3. Add the threat feed to the DNS filter:
   a. Go to *Security Profiles* > *DNS Filter*.
   b. Scroll to the list of preconfigured FortiGuard filters.

c. The resource file uploaded earlier is listed under *Remote Categories*. Set the action for this category to *Block*.




4. Configure the outgoing Internet policy:
   a. Go to *Policy & Objects* > *IPv4 Policy*.
   b. Under *Security Profiles*, enable *DNS Filter*.
   c. From the *SSL Inspection* dropdown list, select an SSL inspection profile.
5. View the results:
   a. Visit a domain on the external resource file. This example visits 123gambling.com. A *Web Page Blocked!* message appears.

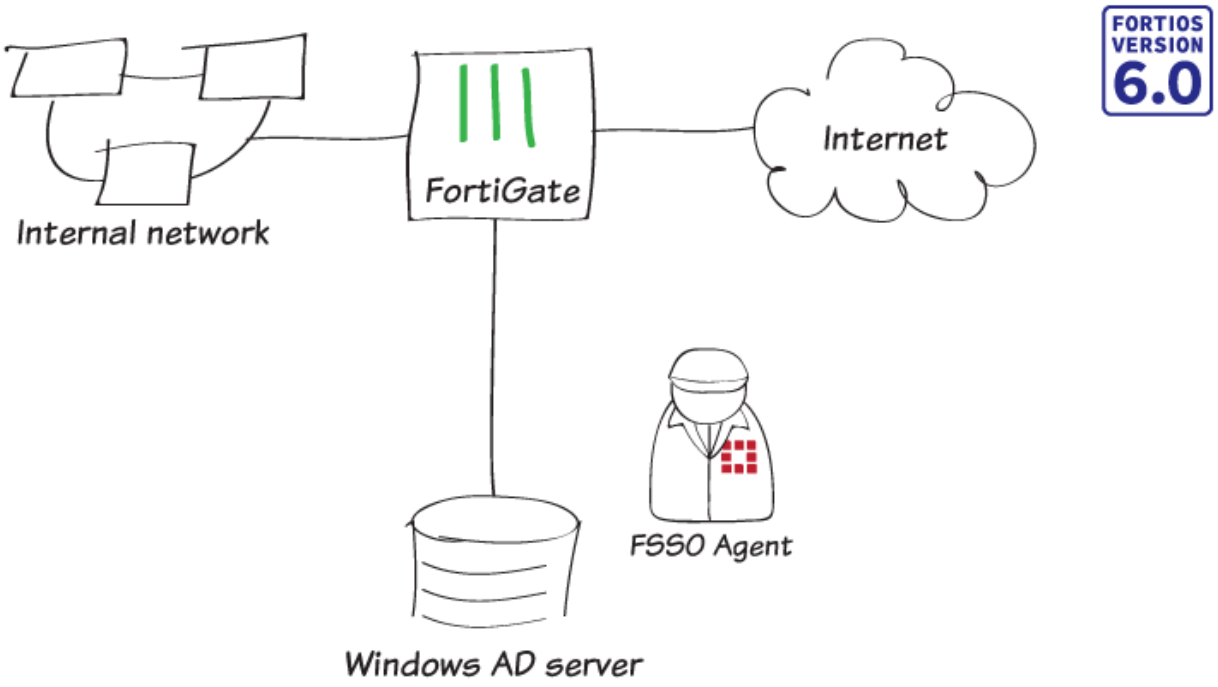

   b. In FortiOS, go to *Log & Report* > *DNS Query*. The logs show that the 123gambling.com domain belongs to a blocked category.

| # | Date/Time | DNS Type | Source | Domain Name | Query Type | Policy | Message |
|---|---|---|---|---|---|---|---|
| 1 | Hour ago | dns-response | writer 38:c9:86:39:b5:98 | 123gambling.com | A | 1 | Domain belongs to a denied category in policy |
| 2 | Hour ago | dns-response | writer 38:c9:86:39:b5:98 | 123gambling.com | A | 1 | Domain belongs to a denied category in policy |
| 3 | Hour ago | dns-response | writer 38:c9:86:39:b5:98 | www.richcasino.com | A | 1 | Domain belongs to a denied category in policy |
| 4 | Hour ago | dns-response | writer 38:c9:86:39:b5:98 | www.richcasino.com | A | 1 | Domain belongs to a denied category in policy |

# Authentication

This section contains information about authenticating users and devices.

## Agent-based FSSO for Windows AD




In this recipe, you use agent-based Fortinet single sign-on (FSSO) to allow users to login to the network once with their Windows AD credentials and seamlessly access all appropriate network resources.

This example uses the FSSO agent in advanced mode. The main difference between advanced and standard mode is the naming convention used when referring to username information. Standard mode uses Windows convention: Domain\Username. Advanced mode uses LDAP convention: CN=User, OU=Name, DC=Domain.

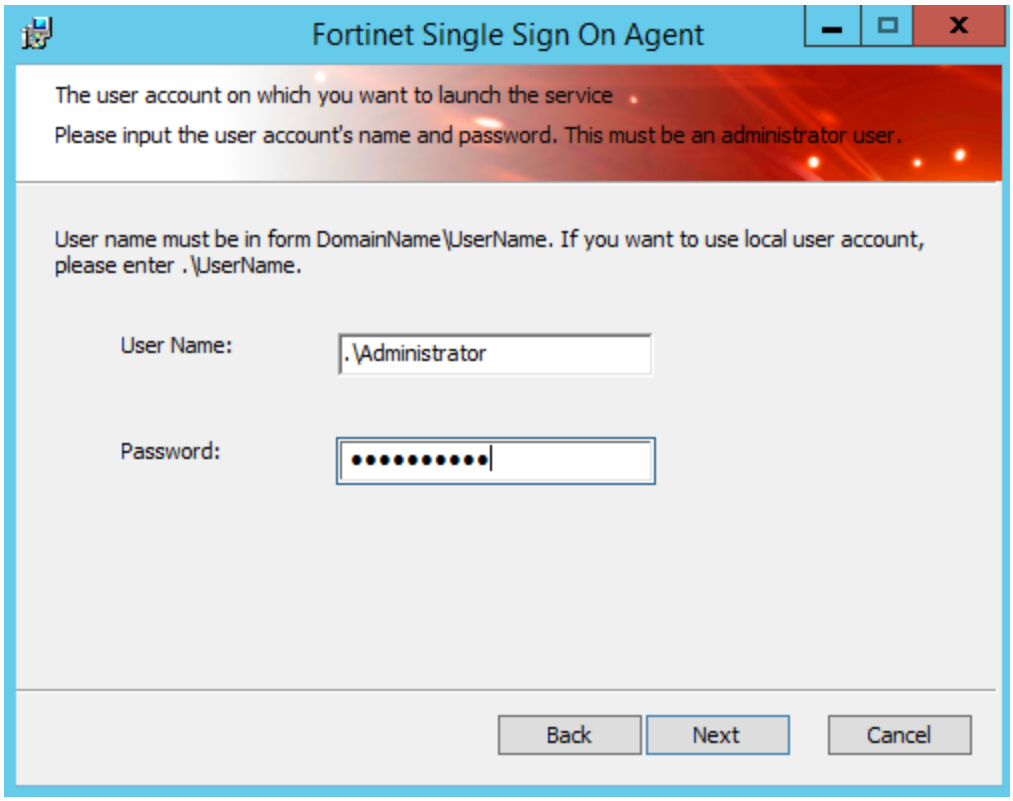
Standard mode supports device names up to 15 characters long. Advanced mode supports device names longer than 15 characters.

Advanced mode is required for multi-domains environments.

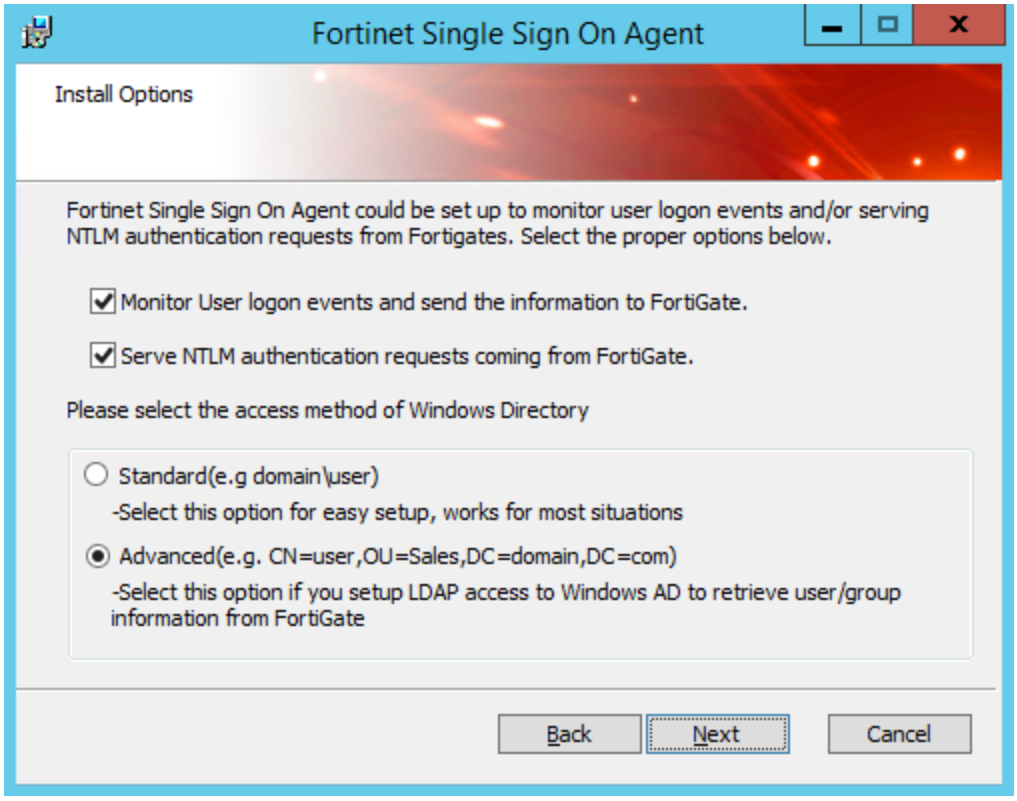
### Installing the FSSO agent

Connect to the Windows AD server and download the FSSO agent from Fortinet Support.

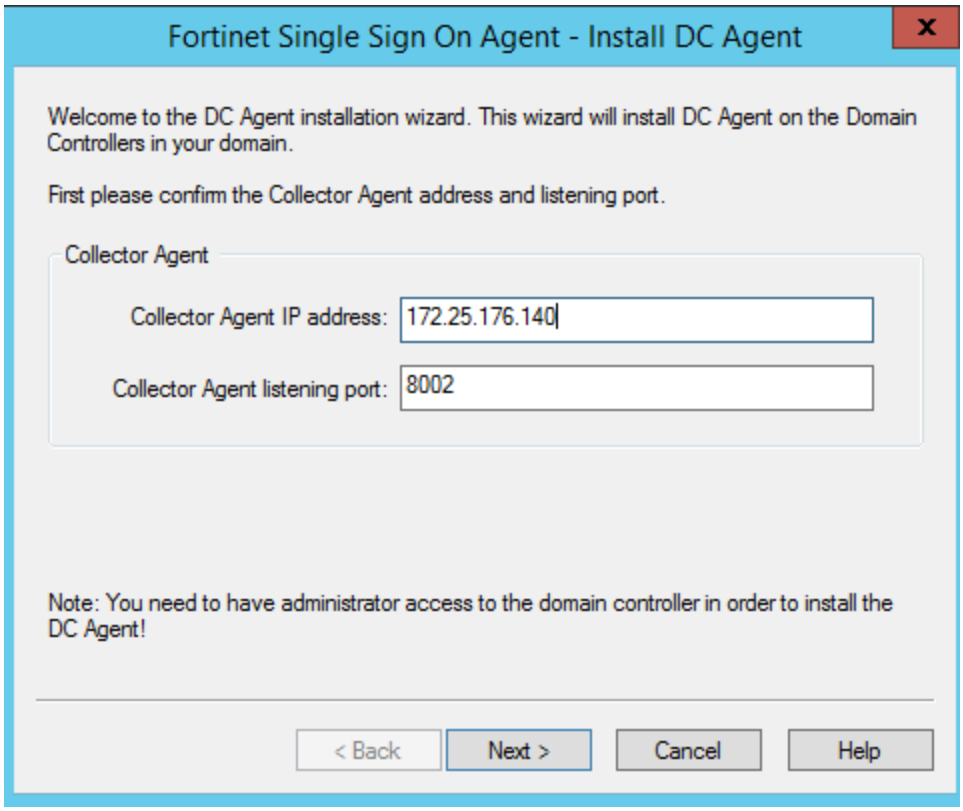
1. To install the agent, open the installer file and use the installation wizard.
2. Set a **User Name** and **Password** for the FSSO domain administrator.




3. For the **Install Options**, select **Advanced** to use advanced mode instead of standard.

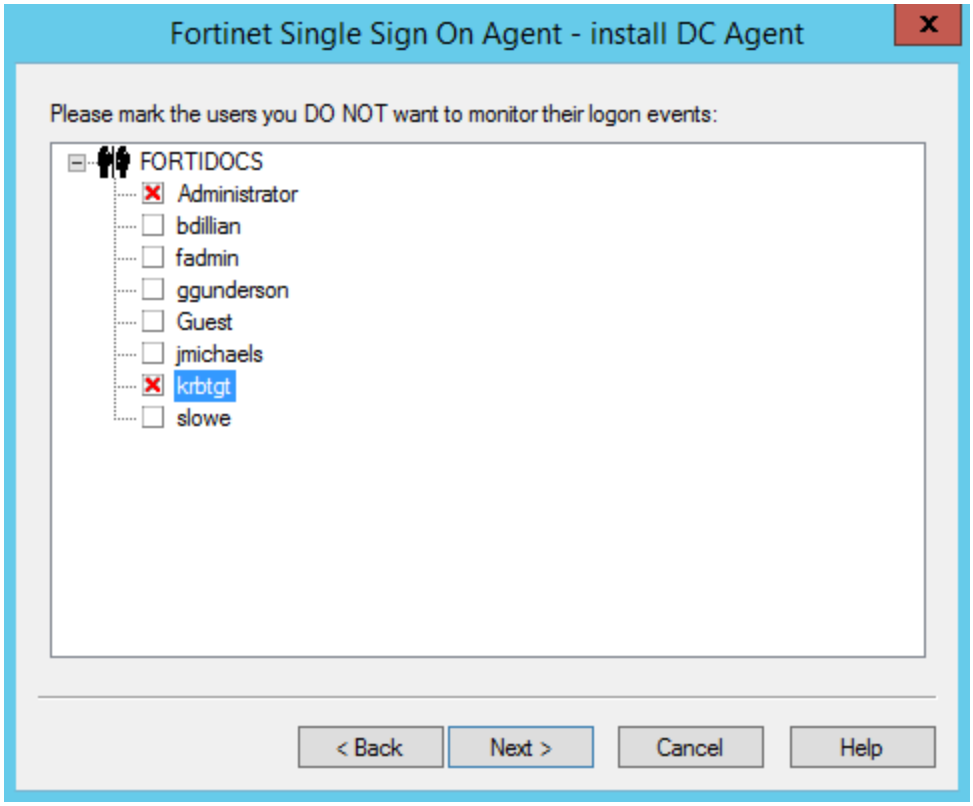


4. After installing the FSSO agent, run **Install DC Agent**.
5. Set the **Collector Agent IP address** and the **Collector Agent listening port**.

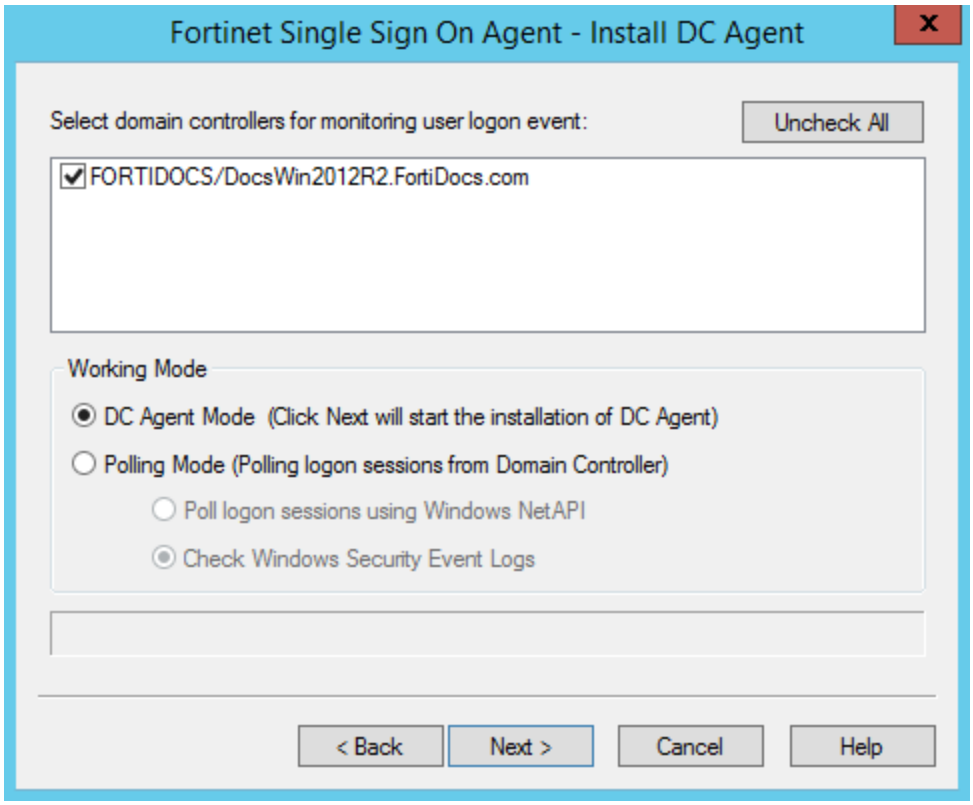



6. Select the domain you wish to monitor.


7. Exclude any users that you don't want to monitor, including the administrator.



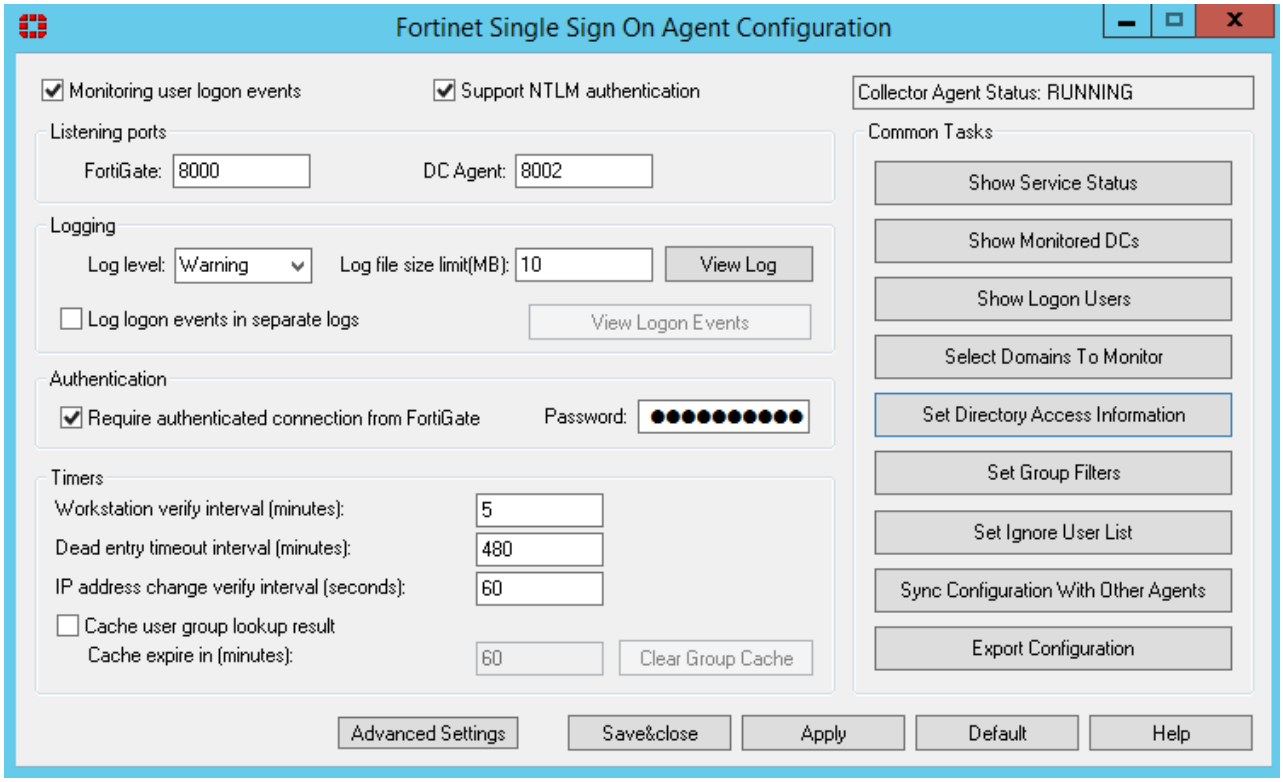

8. Set **Working Mode** to **DC Agent Mode**



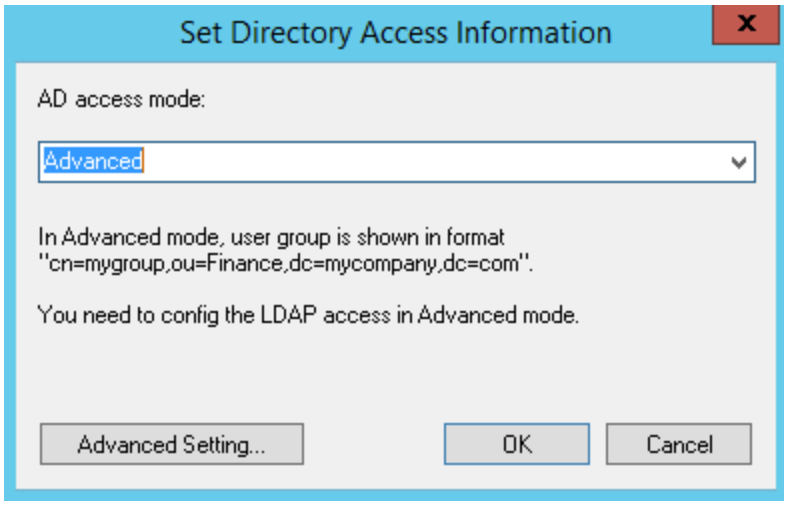

9. Restart your server to apply all changes.

## Configuring the FSSO agent

1. To configure the settings for your network, open the FSSO agent. You can use the default for most settings.



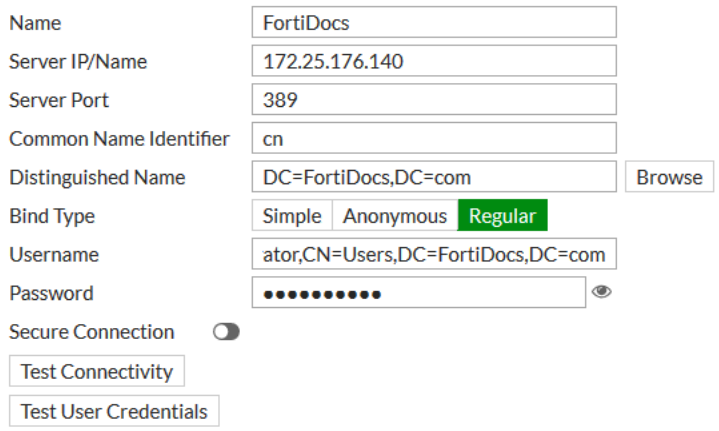

2. Select **Set Directory Access Information**. Set **AD access mode** to **Advanced**.



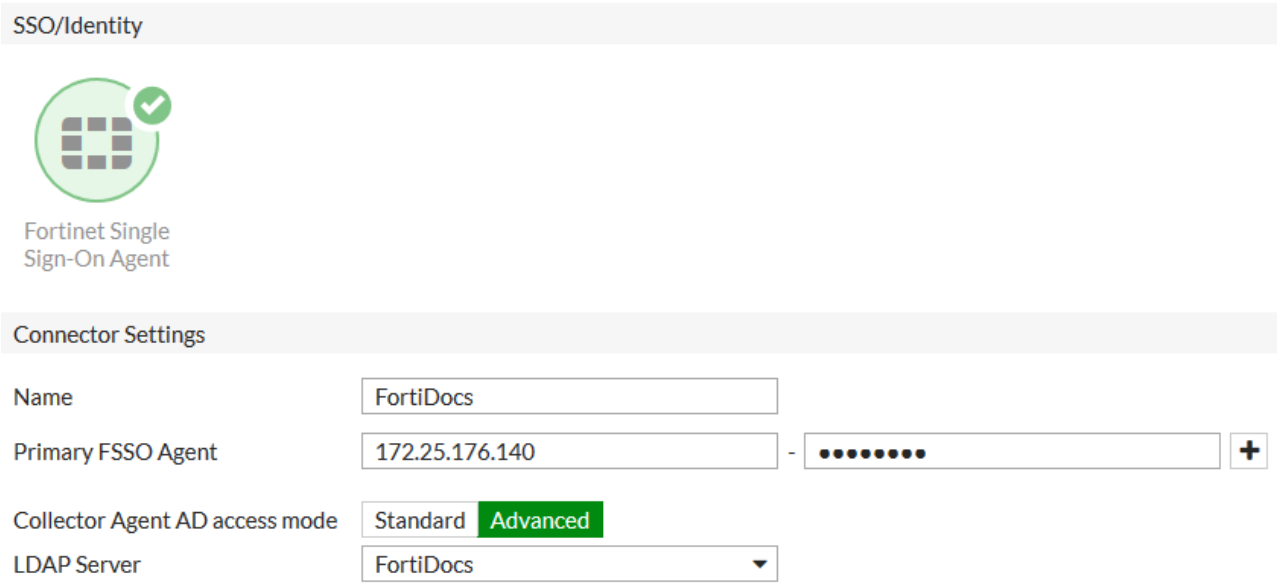

## Setting up your FortiGate for FSSO

Because you have installed FSSSO in advanced mode, you need to configure LDAP to use with FSSO.

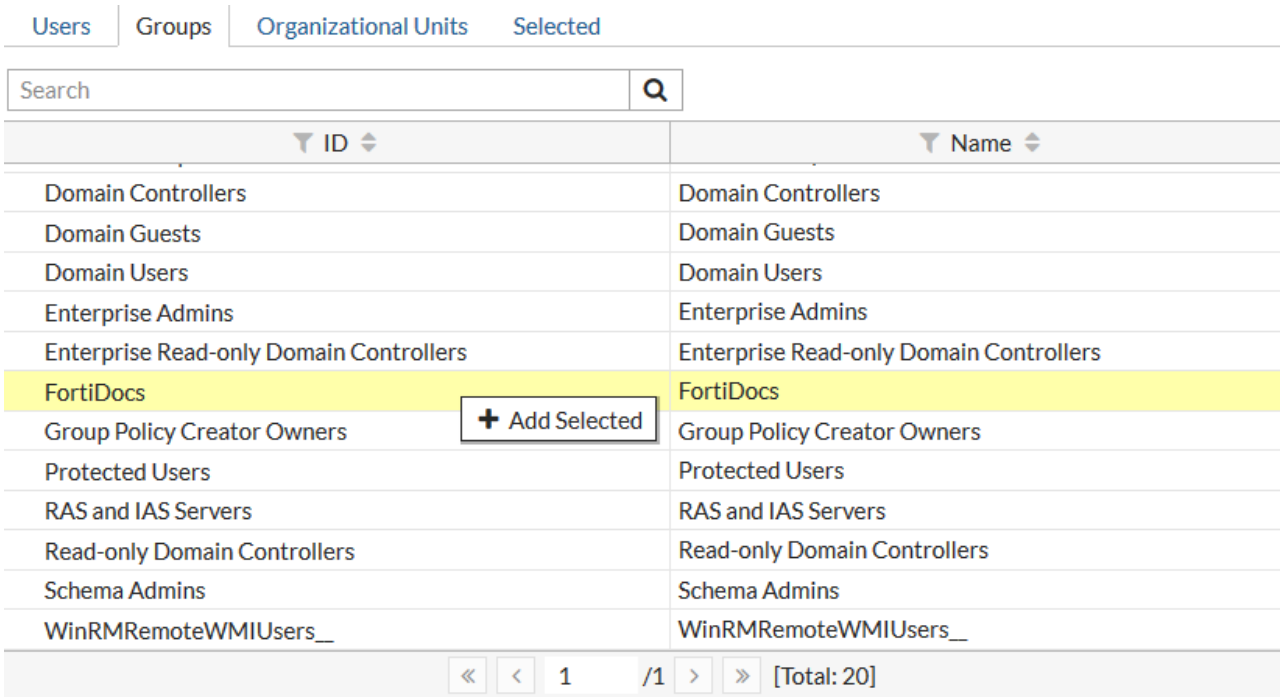
1. To configure the LDAP service, go to **User & Device > LDAP Servers** and select **Create New**.
2. Enter all information about your LDAP server. Select **Test Connectivity**. If your information is correct, **Connection status** is **Successful**.



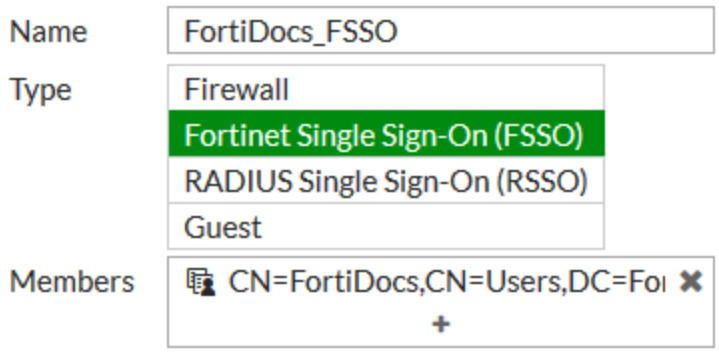

3. Create a Fabric Connector to the FSSO agent by going to **Security Fabric > Fabric Connectors** and select **+ Create New**.
4. Under **SSO/Identity**, select **Fortinet Single Sign-On Agent**.
5. Set the **Name** and enter the IP address and password for the **Primary FSSO Agent**.
6. Set **Collector Agent AD access mode** to **Advanced** and set **LDAP Server** to the new LDAP service.



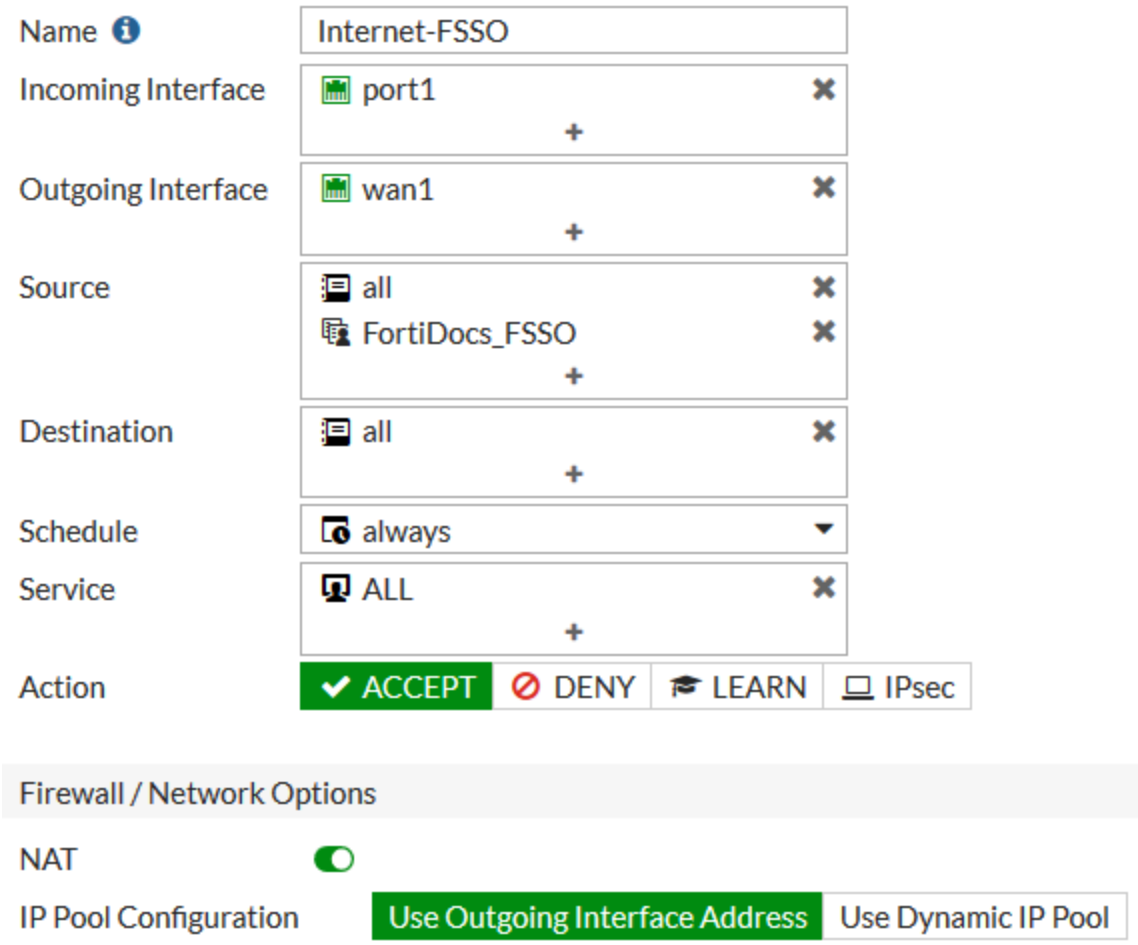

7. Your FortiGate displays information retrieved from the AD server. Select **Groups**, then right-click the FSSO group and select **+ Add Selected**.
8. Select **Selected**.
   The FSSO group is shown.




9. To create a user group for FSSO users, go to **User & Device > User Groups** and select **Create New**.
10. Enter a group **Name** and set **Type** to **Fortinet Single Sign-On (FSSO)**. Add the FSSO users to **Members**.



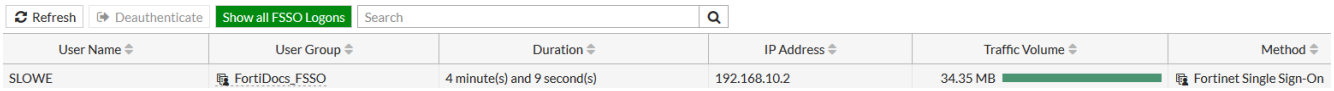

11. To create a policy for FSSO users, go to **Policy & Objects > IPv4 Policy** and select **Create New**.
12. For **Source**, set **User** to the FSSO user group.



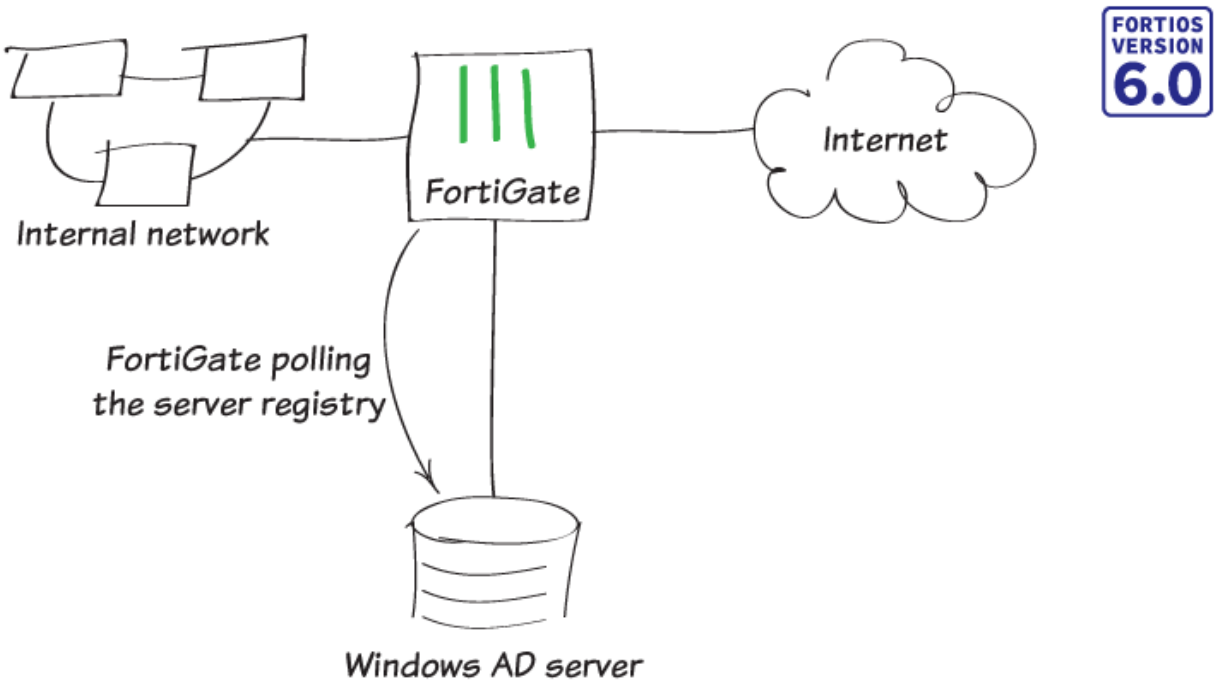

## Results

Log into a computer on the domain and access the Internet. The FortiGate uses FSSO for authentication and doesn't require your credentials to be entered again.

On the FortiGate, go to **Monitor > Firewall User Monitor** and select **Show all FSSO Logons**.



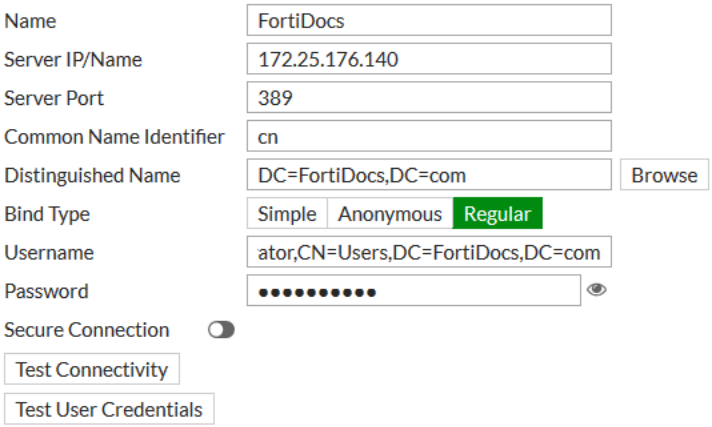
# FSSO in polling mode for Windows AD




In this recipe, you use Fortinet single sign-on (FSSO) in polling mode to allow users to log in to the network once with their Windows Active Directory (AD) credentials and seamlessly access all appropriate network resources.

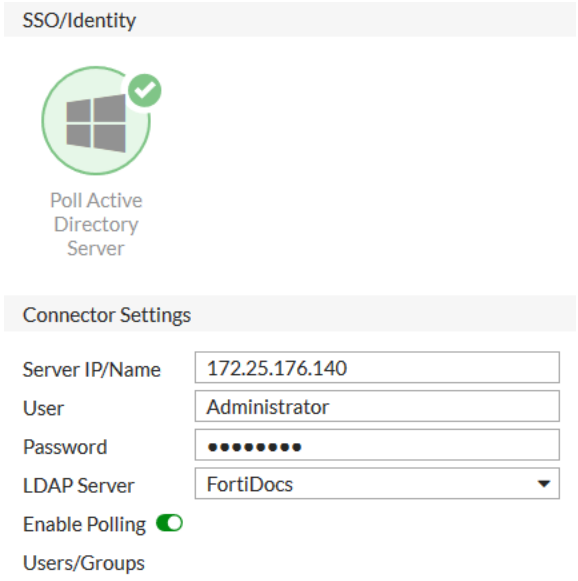
## Creating a Fabric Connector

1. To configure the LDAP service, go to **User & Device > LDAP Servers** and select **Create New**.
2. Enter all information about your LDAP server. Select **Test Connectivity**. If your information is correct, **Connection status** is **Successful**.

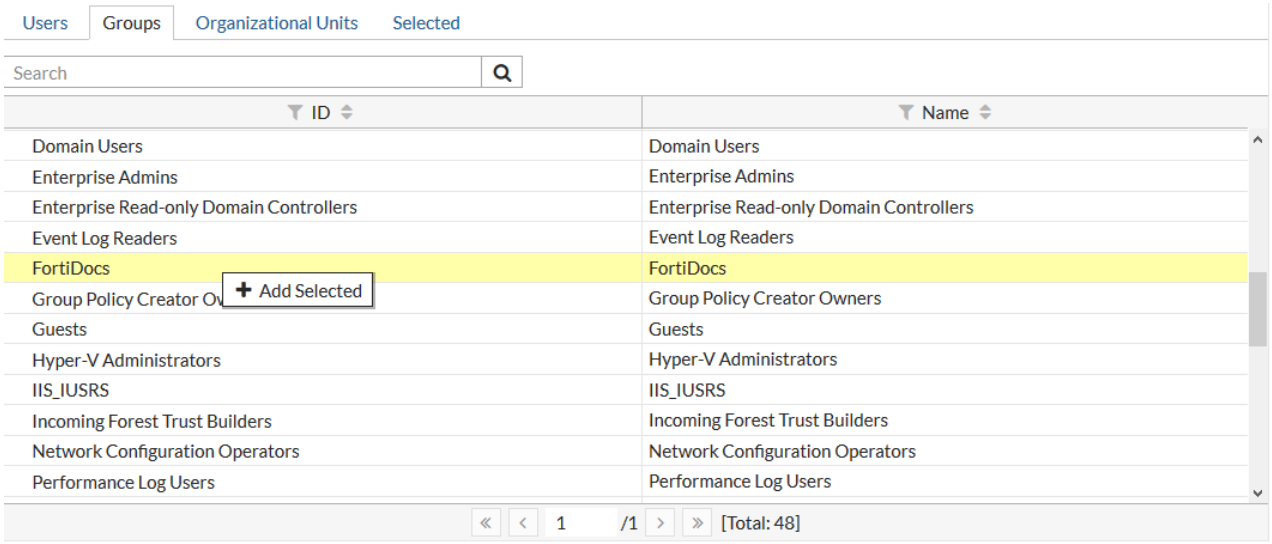



3. To create a Fabric Connector, go to **Security Fabric > Fabric Connectors** and select **Create New**.

4. Under **SSO/Identity**, select **Poll Active Directory Server**.
5. Set the **Server IP/Name** and enter the credentials for the administrator account. Set **LDAP Server** to the new LDAP service.

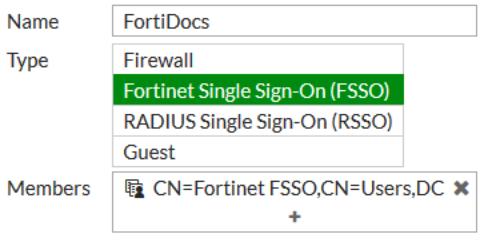



6. Your FortiGate displays information retrieved from the AD server. Select **Groups**, then right-click the FSSO group and select **+ Add Selected**.
7. Select **Selected**. The list includes the FSSO group.



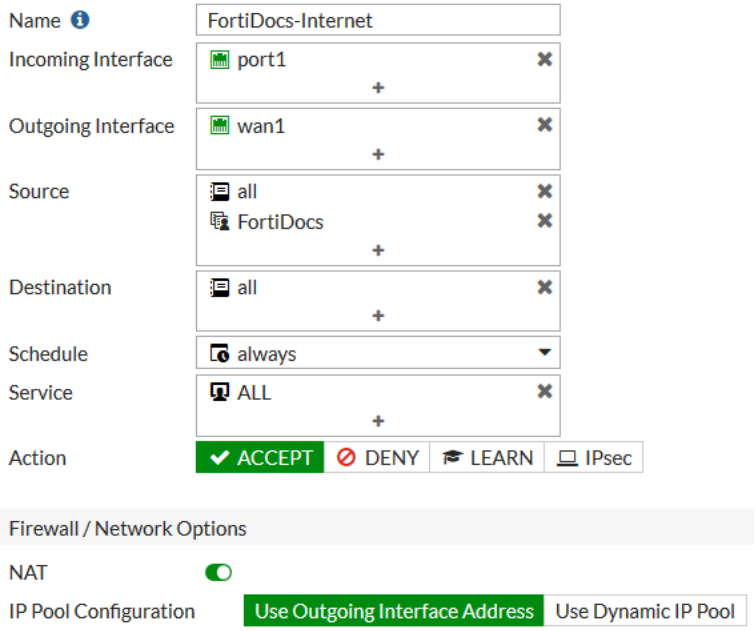

## Creating a user group

1. To create a user group for FSSO users, go to **User & Device > User Groups** and select **Create New**.
2. Enter a group **Name** and set **Type** to **Fortinet Single Sign-On (FSSO)**. Add the FSSO users to **Members**.



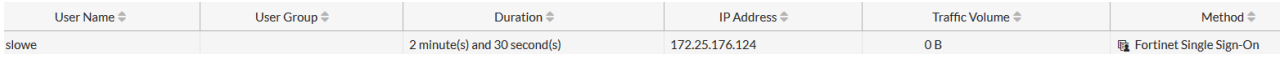

## Creating a policy

1. To create a policy for FSSO users, go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. For **Source**, set **User** to the FSSO user group.




## Results

1. Log in to a computer on the domain and access the Internet. The FortiGate uses FSSO for authentication and doesn't require your credentials to be entered again.
2. On the FortiGate, go to **Monitor > Firewall User Monitor** and select **Show all FSSO Logons**.

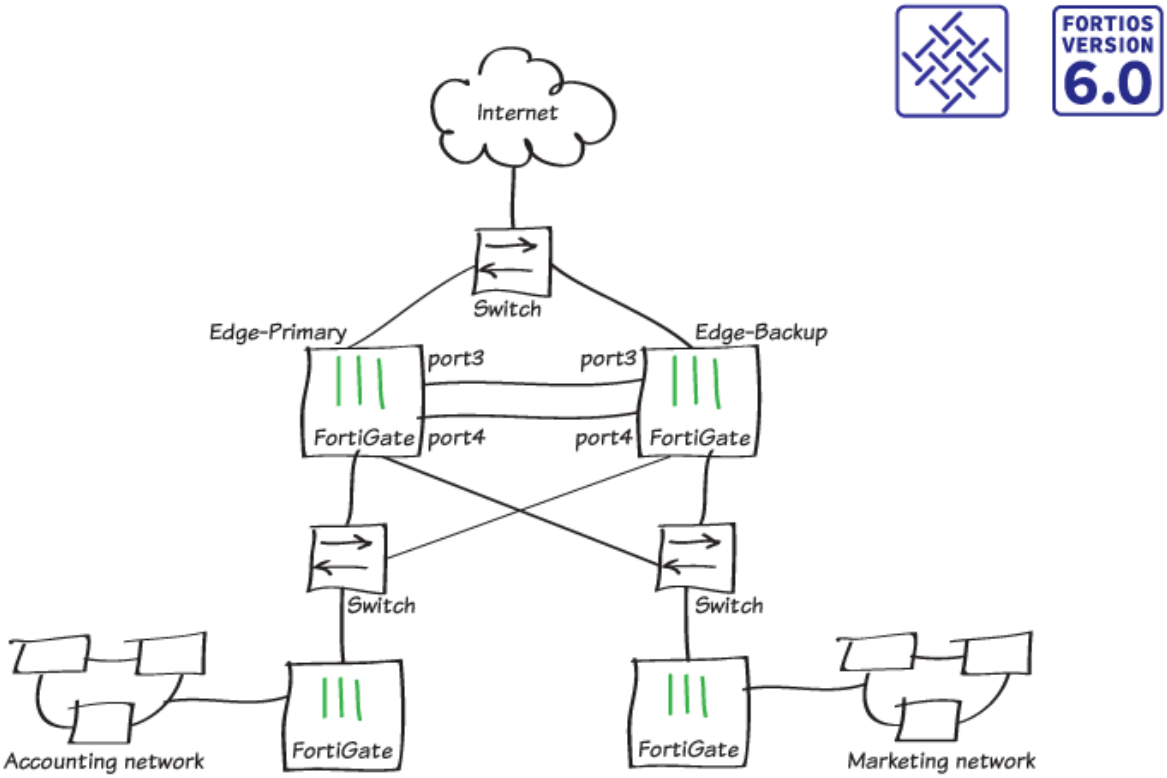



For further reading, check out Single sign-on to Windows AD in the FortiOS 6.0 Online Help.

# High availability

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

## High availability with two FortiGates




This recipe 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, make sure that the FortiGates are running the same FortiOS firmware version and interfaces are not configured to get their addresses from DHCP or PPPoE. Also, you can't use a switch port as an HA heartbeat interface. If necessary, convert the switch port to individual interfaces.

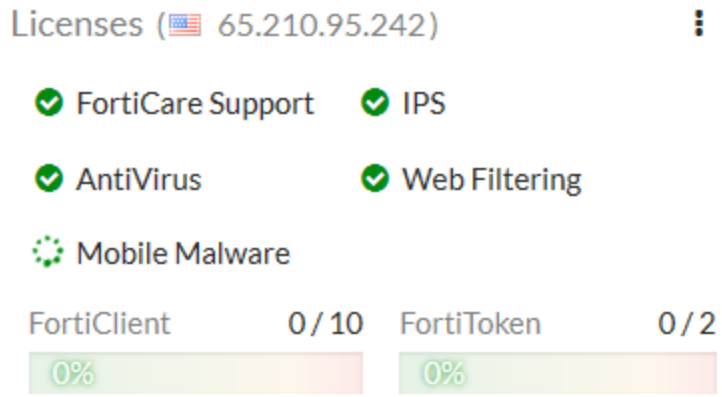
This recipe is in the Fortinet Security Fabric collection. It can also be used as a standalone recipe.

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

For a more advanced HA recipe 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 141.

## Setting up registration and licensing

1. Make sure both FortiGates are running the same FortiOS firmware version. Register and apply licenses to the new FortiGate unit before you add it to the HA cluster.




   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 to all cluster members.

   If the FortiGates in the cluster will run FortiOS Carrier, apply the FortiOS Carrier license before you configure the cluster (and before you apply other licenses). 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.

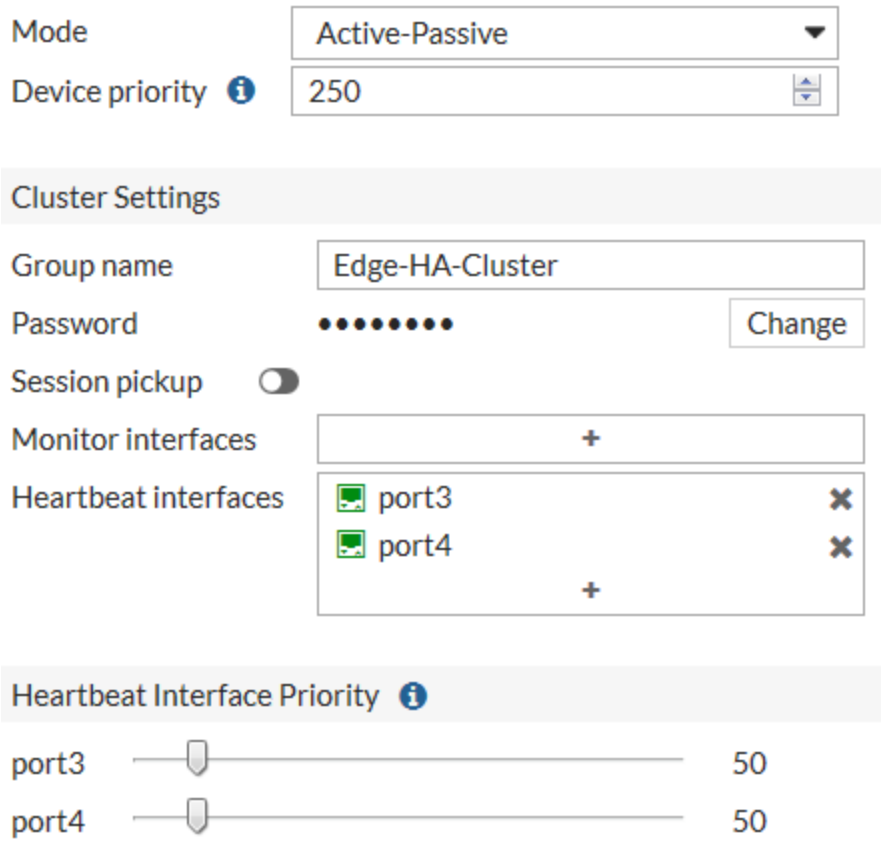
2. You can also install any third-party certificates on the primary FortiGate before you form the cluster. Once the cluster is running, the FGCP synchronizes third-party certificates to the backup FortiGate.

## 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** to **Active-Passive**. Set the **Device priority** to a higher value than the default (in the example, 250) to make sure this FortiGate will always be the primary FortiGate. Also, set a **Group name** and **Password**.

   Make sure you select **Heartbeat interfaces** (in the example, port3 and port4). Set the **Heartbeat Interface Priority** for each interface to 50.




Since the backup FortiGate isn't available, when you save the HA configuration, the primary FortiGate forms a cluster of one FortiGate but keeps operating normally.

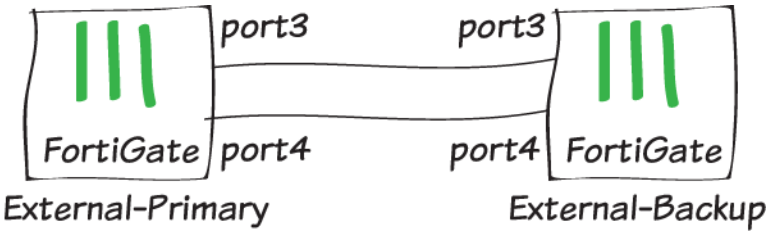
If these steps don't start HA mode, make sure that none of the FortiGate interfaces use DHCP or PPPoE addressing.

If there are other FortiOS HA clusters on your network, you may 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 use case.




Since these connections disrupt traffic, you should make the connections when the network isn't processing a lot of traffic. If possible, make direct Ethernet connections between the heartbeat interfaces of the two FortiGate units.

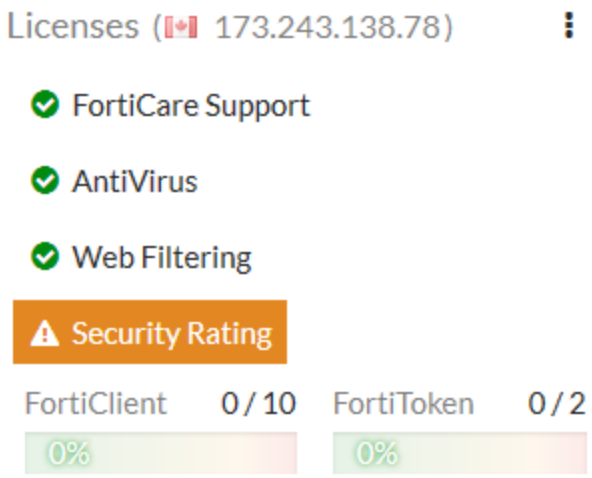
This example uses two FortiGate-600Ds and the default heartbeat interfaces (port3 and port4). You can use any interfaces for HA heartbeat interfaces. A best practice is to use interfaces that don't process traffic, but this is not a requirement. If you are setting up HA between two FortiGates in a VM 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 (called distributed clustering) you must support layer 2 extensions between the remote data centers, using technology such as MPLS or virtual extensible LAN (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 of these connections, as long as you configure the switch to separate traffic from the different networks.

## Configuring the backup FortiGate

1. If required, change the firmware running on the new FortiGate to be the same version as is running on the primary FortiGate.
2. Enter the following command to reset the new backup FortiGate to factory default settings.
   ```
   execute factoryreset
   ```
   You can skip this step if the new FortiGate is fresh from the factory. But if its configuration has been changed at all, it's a best practice to reset your FortiGate to factory defaults to reduce the chance of synchronization problems.
3. Register and apply licenses to the backup FortiGate before configuring it for HA operation. This includes licensing for **FortiCare Support**, **IPS**, **AntiVirus**, **Web Filtering**, **Mobile Malware**, **FortiClient**, **FortiCloud**, **Security Rating**, **Outbreak Prevention**, 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 to all cluster members.

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




4. Click on the **System Information** dashboard widget and select **Configure settings in System > Settings**. Change the FortiGate's **Host name** to identify it as the backup FortiGate.


You can also enter this CLI command:

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

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

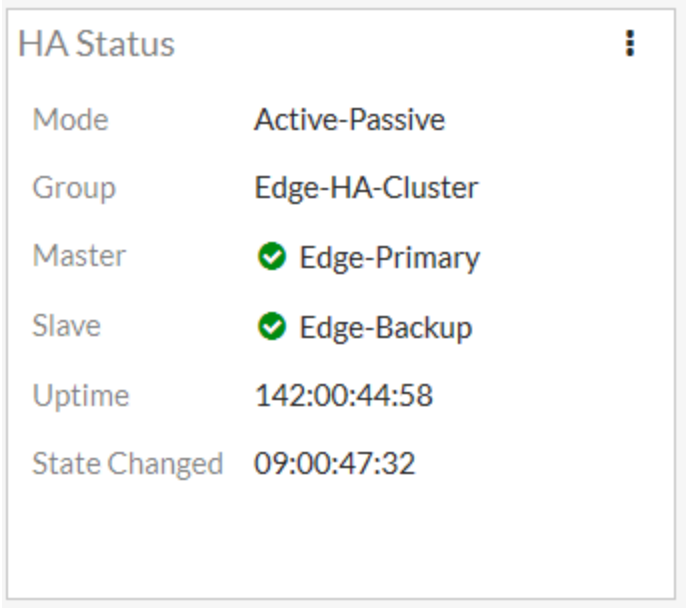
```
config system ha
   set mode a-p
   set group-id 100
   set group-name My-cluster
   set password <password>
   set priority 50
   set hbdev lan4 200 lan5 100
end
```

Similar to when configuring the primary FortiGate, once you enter the CLI command the backup FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity with the FortiGate as FGCP negotiation takes place and the MAC addresses of the FortiGate interfaces are changed 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.

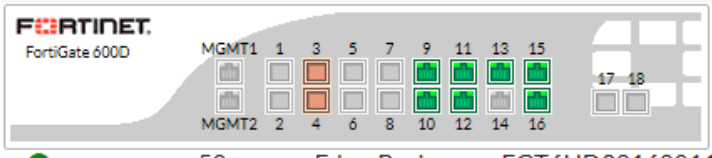
## Viewing the status of the HA cluster

Connect to the GUI of the primary FortiGate. The **HA Status** widget shows the cluster mode (**Mode**) and group name (**Group**).



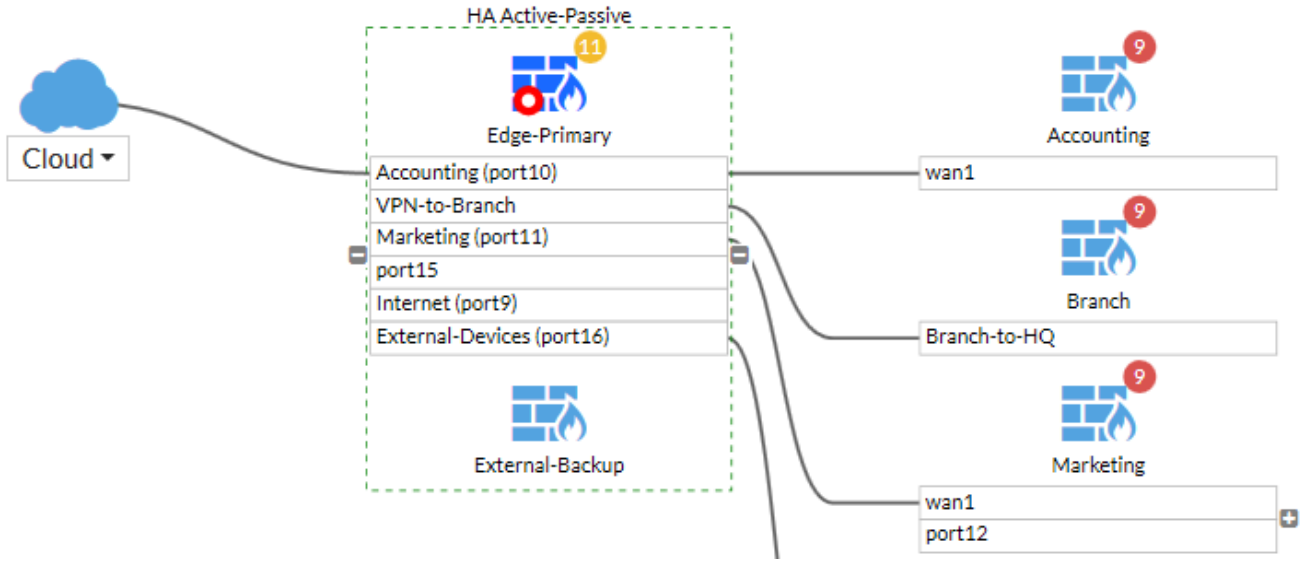

It also shows the host name of the primary FortiGate, which you can hover over to verify that the cluster is synchronized and operating normally. You can click on the widget to change the HA configuration or view a list of recently recorded cluster events, such as members joining or leaving the cluster.

To view the cluster status, click on 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 | Edge-Primary | FGT6HD3916800525 | Master | 9d 22m 33s | 167 | 381.00 kbps |
|  | 50 | Edge-Backup | FGT6HD3916801195 | Slave | 9d 26m 14s | 47 | 72.00 kbps |



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 now be flowing 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 operating 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 will see a momentary pause in the ping results, until traffic diverts to the backup FortiGate, allowing the ping traffic to continue.

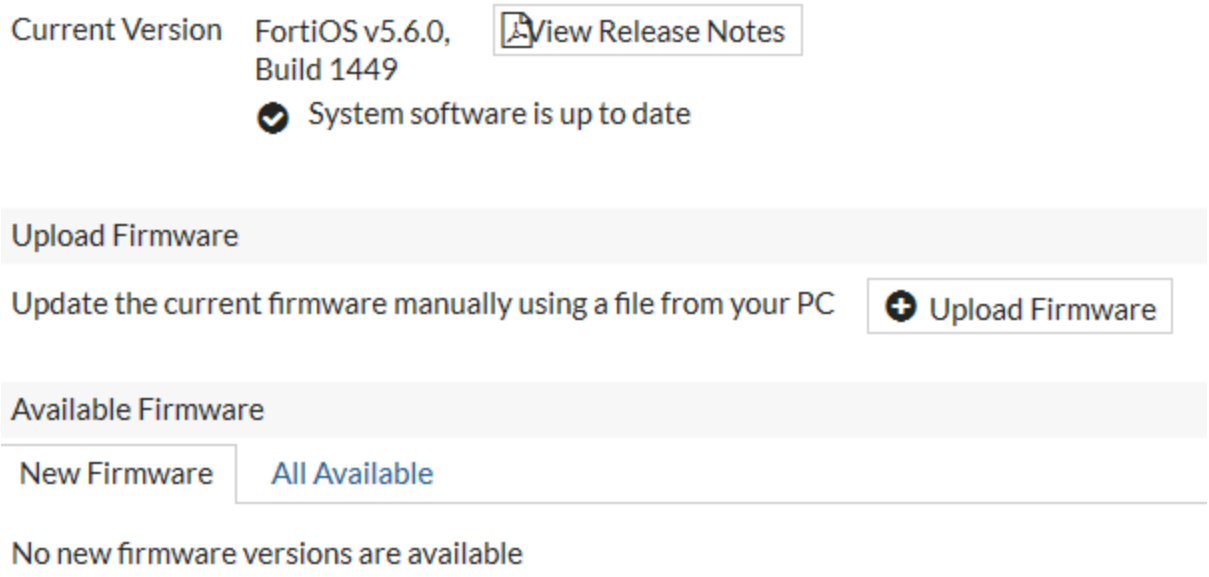
```
64 bytes from 184.25.76.114: icmp_seq=69 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=70 ttl=52 time=8.822 ms\
64 bytes from 184.25.76.114: icmp_seq=71 ttl=52 time=9.034 ms\
64 bytes from 184.25.76.114: icmp_seq=72 ttl=52 time=9.536 ms\
64 bytes from 184.25.76.114: icmp_seq=73 ttl=52 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.

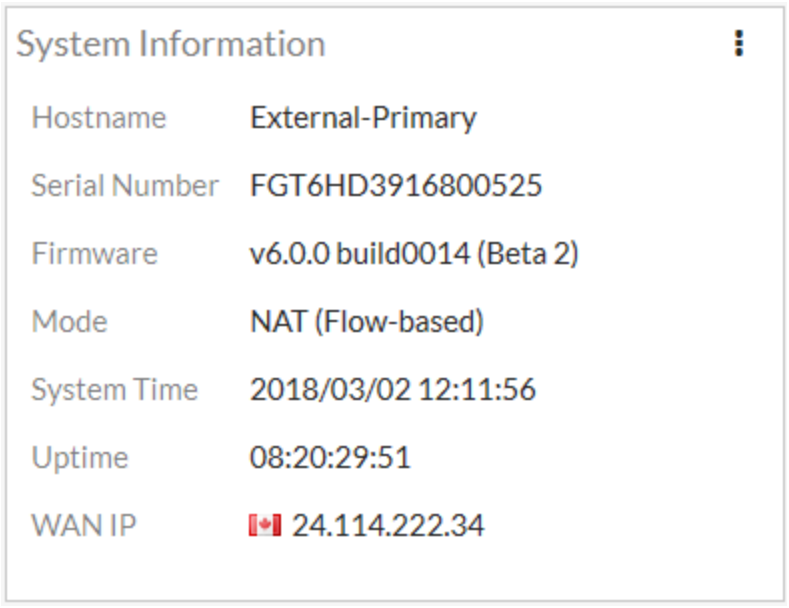
## (Optional) Upgrading the firmware for the HA cluster

Upgrading the firmware on the primary FortiGate automatically upgrades the firmware on the backup FortiGate. Both FortiGates are updated with minimal traffic disruption. Always review the Release Notes before you install new firmware.

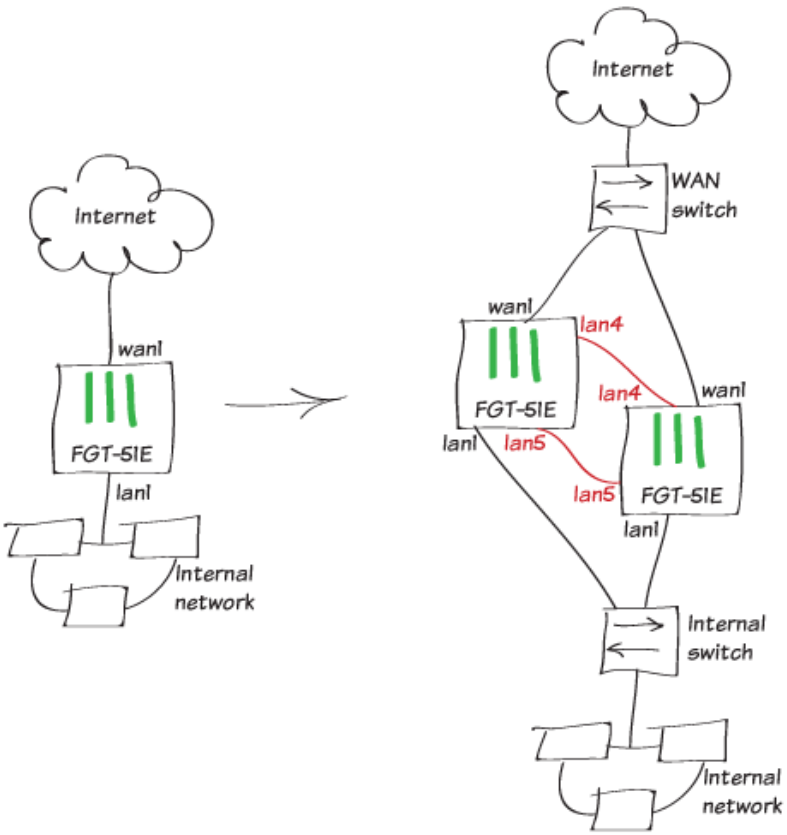
1. Click the **System Information** widget and select **Update firmware in System > Firmware**. Back up the configuration and update the firmware from FortiGuard or upload a firmware image file. The firmware installs onto both the primary and backup FortiGates.




After the upgrade completes, verify that the **System Information** widget shows the new firmware version.




## High Availability with FGCP (expert)




FORTIOS VERSION 6.0

This recipe 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 cluster.

You will configure the FortiGate already on the network to become the primary FortiGate by:

1. Licensing it (if required)
2. Enabling HA
3. Increasing its device priority
4. Enabling override

You will prepare the new FortiGate by:

1. Setting it to factory defaults to wipe any configuration changes
2. Licensing it (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 recipe describes best practices for configuring HA and involves extra steps that are not required for a basic HA setup. If you are looking for a basic HA recipe see High availability with two FortiGates on page 133.

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

This recipe features two FortiGate-51Es. FortiGate-51Es have a 5-port switch lan interface. Before configuring HA, the lan interface was converted to 5 separate interfaces (lan1 to lan5). The lan1 interface connects to the internal network and the wan1 interface connects to the Internet. The lan4 and lan5 interfaces will become the HA heartbeat interfaces.

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 recipe, you can use the wan1 and wan2 interfaces for the HA heartbeat.

## Configuring the primary FortiGate

1. Connect to the primary FortiGate, click on the **System Information** dashboard widget and select **Configure settings in System > Settings**.
2. Change the **Host name** to identify this FortiGate as the primary FortiGate.

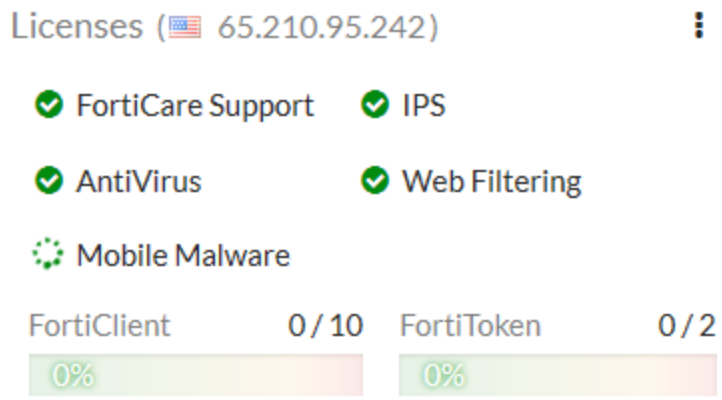
   
   

   You can also enter this CLI command:

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

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**, **Security Rating**, **Outbreak Prevention**, 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 to all cluster members.

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




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 to the backup FortiGate(s).

4. Enter this CLI command to set the HA mode to active-passive, set a group id, group name and password, increase the device priority to a higher value (for example, 250) and enable override.

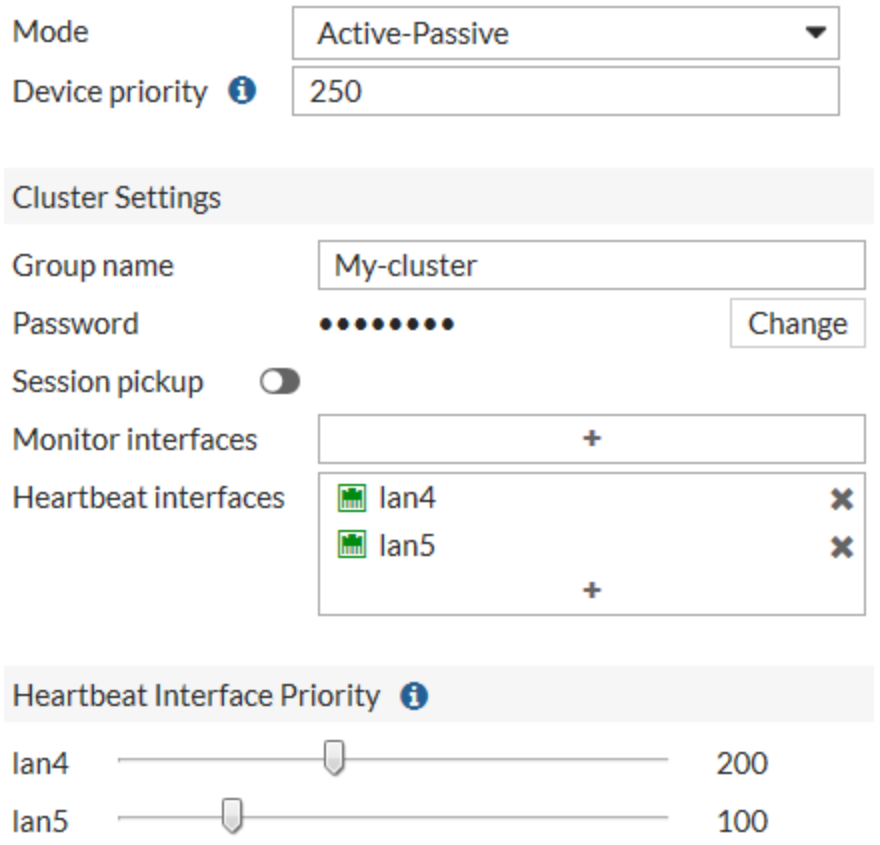
```
config system ha
   set mode a-p
   set group-id 100
   set group-name My-cluster
   set password <password>
   set priority 250
   set override enable
   set hbdev lan4 200 lan5 100
end
```

Enabling override and increasing the device priority means this FortiGate always becomes the primary unit.

This configuration also selects lan4 and lan5 to be the heartbeat interfaces and sets their priorities to 200 and 100 respectively. Its a best practice to set different priorities for the heartbeat interfaces (but not a requirement).

If you have more than one cluster on the same network, each cluster should have a different group id. 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 also configure most of these settings from the GUI (go to **System > HA**).




Override and the group id can only be configured from the CLI.

```
config system ha
   set group-id 100
   set override enable
end
```

After you enter the CLI command or make the GUI changes, the FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity with the FortiGate as FGCP negotiation takes place and the MAC addresses of the FortiGate interfaces are changed 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 just 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.

You can verify that the FGCP has set the virtual MAC addresses by viewing the configuration of each FortiGate interface from the GUI (go to **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:09:64:01
Permanent_HWaddr 70:4c:a5:98:11:54
...
```

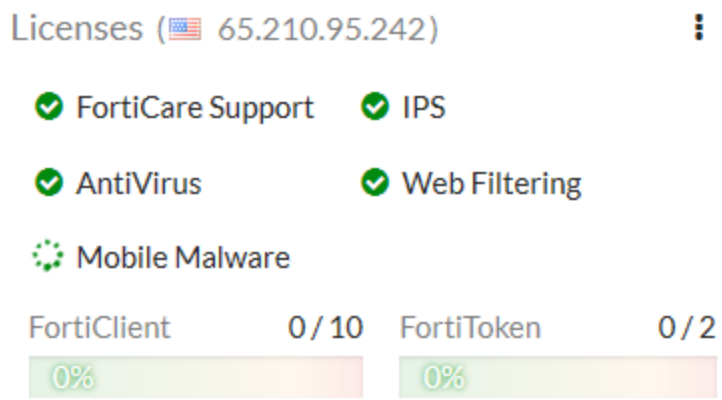
You can also use the `diagnose hardware deviceinfo nic lan2` command to display this information.

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

## Configuring the backup FortiGate

1. If required, change the firmware running on the new FortiGate to be the same version as is running on the primary FortiGate.
2. Enter the following command to reset the new backup FortiGate to factory default settings.
   `execute factoryreset`
   You can skip this step if the new FortiGate is fresh from the factory. But if its configuration has been changed at all, it's a best practice to reset your FortiGate to factory defaults to reduce the chance of synchronization problems.
3. Register and apply licenses to the backup FortiGate before configuring it for HA operation. This includes licensing for **FortiCare Support**, **IPS**, **AntiVirus**, **Web Filtering**, **Mobile Malware**, **FortiClient**, **FortiCloud**, **Security Rating**, **Outbreak Prevention**, 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 to all cluster members.

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




4. Click on the **System Information** dashboard widget and select **Configure settings in System > Settings**. Change the FortiGate's **Host name** to identify it as the backup FortiGate.


   You can also enter this CLI command:

```
config system global
   set hostname Backup
```

```
end
```

1. 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 100
   set group-name My-cluster
   set password <password>
   set priority 50
   set hbdev lan4 200 lan5 100
end
```

Similar to when configuring the primary FortiGate, once you enter the CLI command the backup FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity with the FortiGate as FGCP negotiation takes place and the MAC addresses of the FortiGate interfaces are changed 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 primary and backup FortiGates together and to your network as shown in the network diagram at the start of the use case. Making these connections disrupts network traffic as you disconnect and re-connect cables.

Switches must be used between the cluster and the Internet and between the cluster and the internal network 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 of these connections as long as you configure the switch to separate traffic from the different networks.

The example shows the recommended configuration of direct connections between the lan4 heartbeat interfaces and between the lan5 heartbeat interfaces.

When the heartbeat interfaces are connected, the FortiGates 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 will have the same IP addresses as the primary FortiGate had. 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:

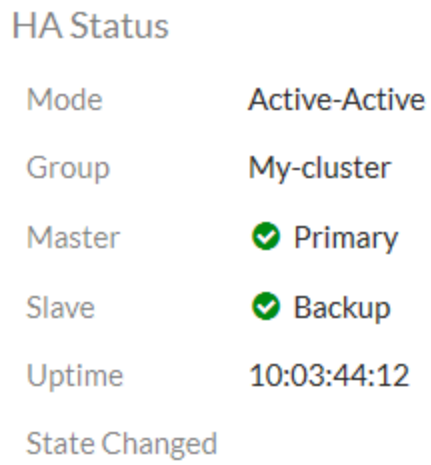
```
diagnose sys ha checksum cluster
```

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

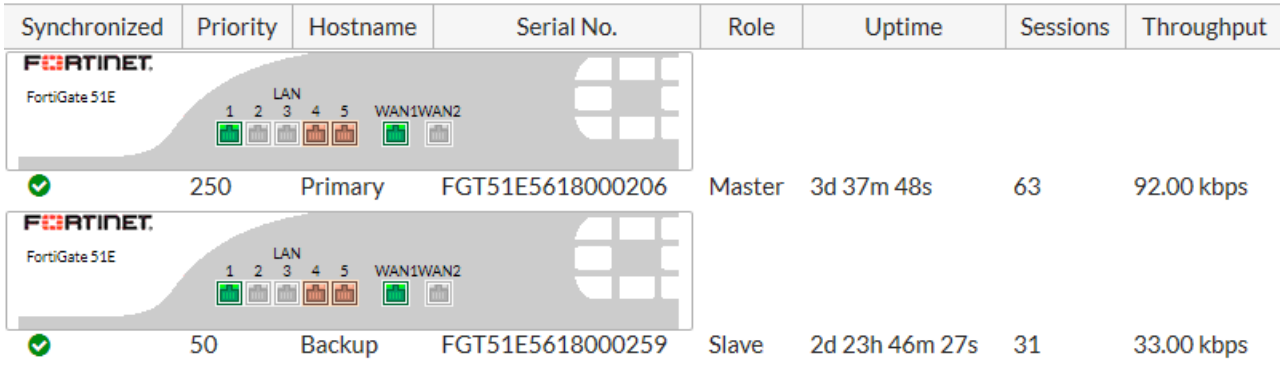
while and enter the command again. Repeat until the checksums are identical. It may take a while for some parts of the configuration to be synchronized.

If the checksums never become identical visit the Fortinet Support website for assistance.

2. The **HA Status** dashboard widget also shows synchronization status. Mouse 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, click on the **HA Status** widget and select **Configure Settings in System > HA** (or go to **System > HA**).




## 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 now be flowing 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 operating 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.

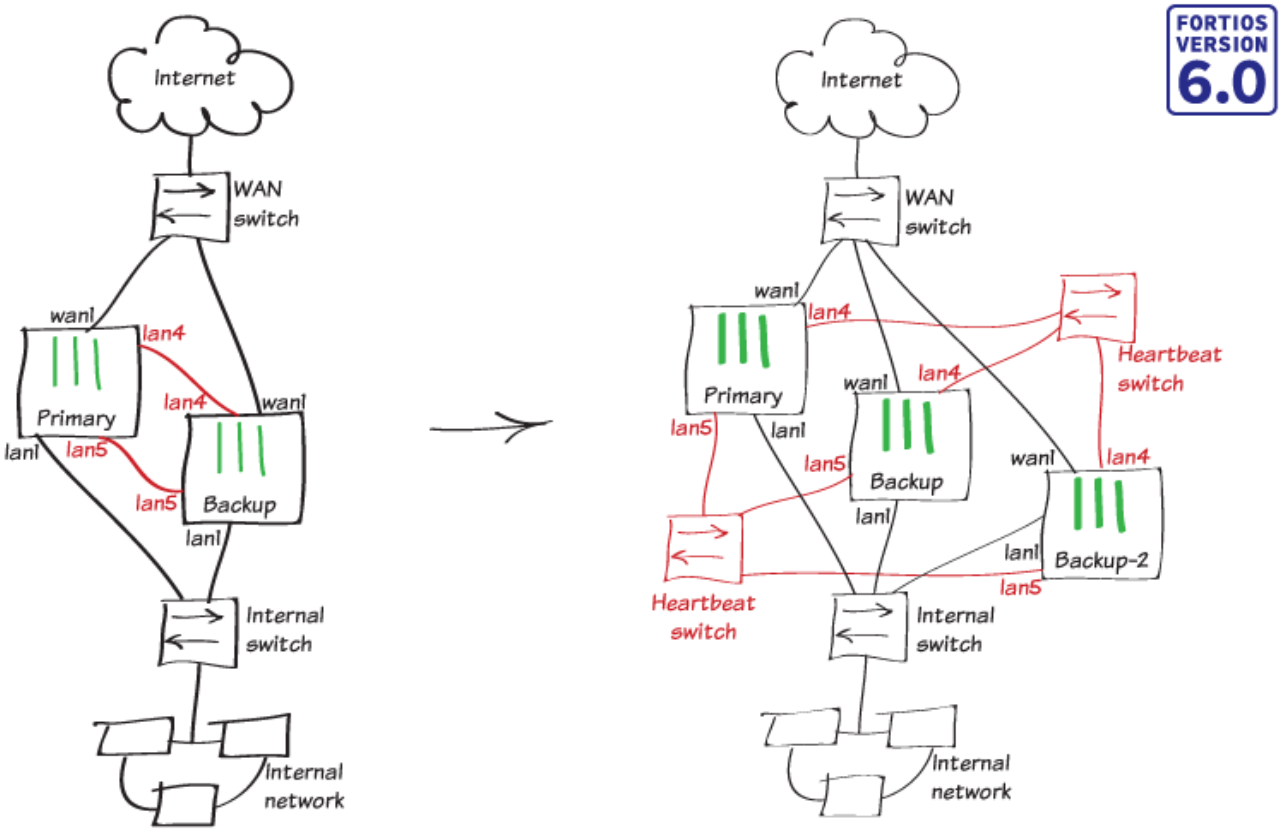
If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover

You will 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.

# Adding a third FortiGate to an FGCP cluster (expert)




This use case describes how to add a third FortiGate to an already established FGCP cluster (the cluster fromHigh Availability with FGCP (expert) on page 141) and configure active-active HA.

You prepare the new FortiGate by:

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

The new FortiGate becomes a second backup FortiGate; its configuration synchronized to match the configuration of the cluster.

Before you start, the new FortiGate should be running the same FortiOS firmware version as the cluster and its interfaces should not be configured to get addresses from DHCP or PPPoE.

After the third FortiGate joins the cluster, this recipe also describes how to switch the cluster to operate in active-active (or a-a) mode. Active-active HA enables proxy-based NGFW/UTM load-balancing to allow the three FortiGates to share proxy-based NGFW/UTM processing. If the cluster handles a large amount of NGFW/UTM traffic, active-active HA with three FortiGates may enhance performance.

This use case features three FortiGate-51Es. These FortiGate models include a 5-port switch lan interface. Before configuring HA, the lan interface was converted to five separate interfaces (lan1 to lan5). The lan1 interface connects to

the internal network and the wan1 interface connects to the Internet. The lan4 and lan5 interfaces become the HA heartbeat interfaces.

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 recipe, you can use the wan1 and wan2 interfaces for the HA heartbeat.

## Enabling override on the primary FortiGate (optional)

Before adding the third FortiGate to the cluster, enable override on the primary FortiGate. In most cases this step would not be necessary but it is a best practice because enabling override makes sure the configuration of the primary FortiGate is not overwritten by the configuration of the new backup FortiGate.

To enable override, log into the primary FortiGate CLI and enter this command:

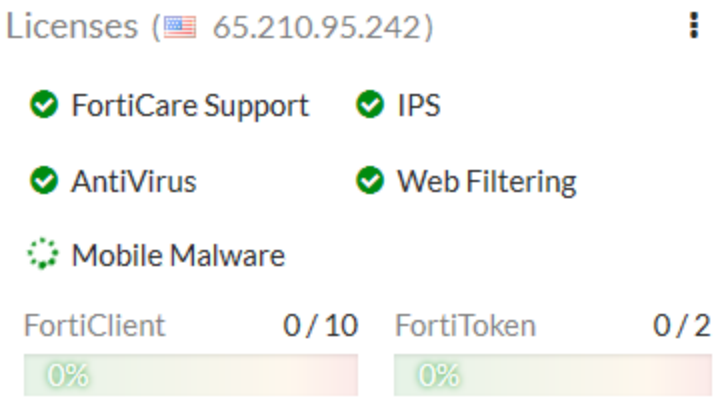
```
config system ha
   set override enable
end
```

## Configuring the new FortiGate

1. Enter this command to reset the new FortiGate to factory default settings:
   `execute factoryreset`
   You can skip this step if the new FortiGate is fresh from the factory. But if its configuration has been changed at all it's recommended to set it back to factory defaults to reduce the chance of synchronization problems.
2. If required, change the firmware running on the new FortiGate to match the cluster firmware version.
3. Register and apply licenses to the new FortiGate before configuring it for HA operation. This includes licensing for **FortiCare Support**, **IPS**, **AntiVirus**, **Web Filtering**, **Mobile Malware**, **FortiClient**, **FortiCloud**, **Security Rating**, **Outbreak Prevention**, 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 to all cluster members.

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




4. Change the host name of the new FortiGate to identify it as **Backup-2** by clicking on the **System Information** dashboard widget and selecting **Configure settings in System > Settings** and changing the **Host name**.


You can also enter this CLI command:

```
config system global
   set hostname Backup-2
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 100
   set group-name My-cluster
   set password <password>
   set priority 50
   set hbdev lan4 200 lan5 100
end
```

Once you enter the CLI command the new FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity with the FortiGate while FGCP negotiation takes place and the FortiGate interface MAC addresses 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.

## Connecting the new FortiGate to the cluster

Connect the new FortiGate to the cluster and your network as shown in the network diagram at the start of this use case. Making these connections disrupts network traffic as you disconnect and re-connect the heartbeat interfaces. If you have already added switches to connect the heartbeat interfaces, you can connect the new FortiGate without disrupting network traffic.

When you add a third FortiGate to a cluster you need to connect the heartbeat interfaces together using switches. You can use separate switches for each heartbeat interface (recommended for redundancy) or you can use the same switch for both heartbeat interfaces as long as you separate the traffic from each heartbeat interface.

When you connect the heartbeat interfaces of the new FortiGate, the cluster re-negotiates. If you have enabled override on the primary FortiGate and set its priority highest, the primary FortiGate synchronizes its configuration to the new FortiGate. The cluster automatically forms with minimal or no additional disruption to network traffic.

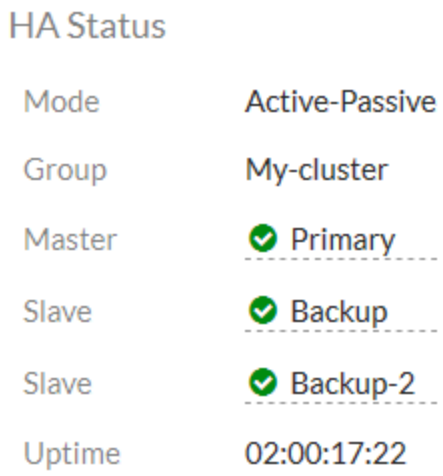
The new cluster will have the same IP addresses as the primary FortiGate. You can log into the cluster by logging into the primary FortiGate CLI or GUI.

## Checking cluster operation

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

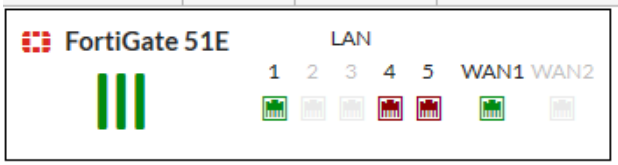
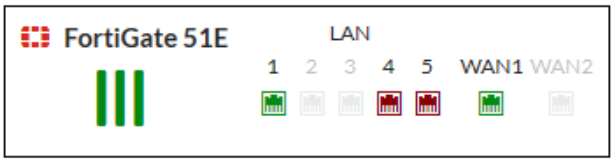
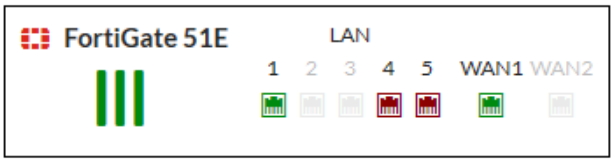
1. Log into the primary FortiGate CLI and enter this command:
   ```
   diagnose sys ha checksum cluster
   ```
   The command output lists all cluster members' configuration checksums. If they all have identical checksums, you can be sure that the configurations are synchronized. If the checksums are 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 visit the Fortinet Support website for assistance.
2. The **HA Status** dashboard widget also shows synchronization status. Mouse 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, click on 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 | Primary | FGT51E5618000086 | Master | 2d 1h 39m 32s | 62 | 49.00 kbps |
|  | | | | | | | |
| ✓ | 50 | Backup | FGT51E5618000259 | Slave | 2d 24m 56s | 25 | 32.00 kbps |
|  | | | | | | | |
| ✓ | 50 | Backup-2 | FGT51E5618000206 | Slave | 2d 1m 36s | 25 | 31.00 kbps |

## 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
```

FGCP clusters dynamically respond to network conditions. If you keep override enabled, the same FortiGate always becomes the primary FortiGate. With override enabled; however, the cluster may negotiate more often to keep the same FortiGate as the primary FortiGate, potentially increasing traffic disruptions.

If you disable override it is more likely that the backup FortiGate could become the primary FortiGate. Disabling override is recommended unless its important that the same FortiGate remains the primary FortiGate

To see how enabling override can cause minor traffic disruptions, with override enabled set up a continuous ping through the cluster. Then disconnect power to the backup unit. You will most likely notice a brief disruption in the ping traffic. Try the same thing with override disabled and you shouldn't see this traffic disruption.

With override enabled, the disruption is minor and shouldn't be noticed by most users. For smoother operation, the best practice is to disable override.

## Converting to an active-active cluster

Log into the primary FortiGate CLI and enter this command to convert the cluster from an active-passive to an active-active cluster. The cluster changes modes without any traffic interruption.

```
config system ha
   set mode a-a
```

```
end
```

Active-active HA load-balancing distributes proxy-based NGFW/UTM processing to all cluster members. Proxy-based NGFW/UTM processing is CPU and memory-intensive. Distributing NGFW/UTM processing in this way may result in higher throughput.

## Results

Most traffic should now be flowing through the primary FortiGate with proxy-based NGFW/UTM sessions distributed to all three FortiGates in the cluster. 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 operating 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.

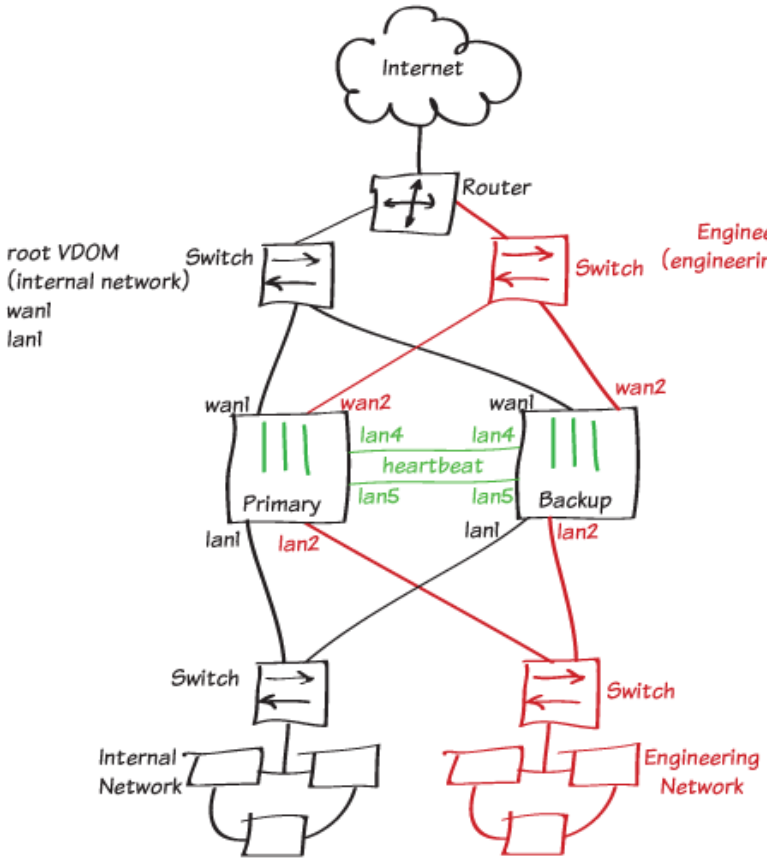
If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover.

You will 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)




FORTIOS VERSION 6.0

In this use case you 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 use case describes a very simple two-VDOM configuration. However, the same principles described in this example 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 in the virtual cluster.

This use case describes the recommended steps for setting up a virtual cluster of two FortiGates. You can follow the procedure described in High Availability with FGCP (expert) on page 141 to configure virtual clustering by converting a FortiGate with VDOMs to HA mode and then adding another FortiGate to form a cluster. However, taking this approach with virtual clustering is not as foolproof as a normal HA configuration. If you accidentally add the management VDOM to virtual cluster 2 before adding the backup FortiGate, the configuration of the primary FortiGate can be overwritten by the backup FortiGate. If want to experiment with this approach, make sure you don't add the management VDOM to virtual cluster 2 until all of the FortiGates have joined the cluster.

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

This user case features two FortiGate-51Es. FortiGate-51Es have a 5-port switch lan interface. Before configuring HA, the lan interface was converted to 5 separate interfaces (lan1 to lan5).

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 recipe, you can use the wan1 and wan2 interfaces for the HA heartbeat.

## Preparing the FortiGates

1. If required, upgrade the firmware running on the FortiGates. Both FortiGates should be running the same version of FortiOS.
2. On each FortiGate, enter the following command to reset them factory default settings.
   ```
   execute factoryreset
   ```
   You can skip this step if the FortiGates are fresh from the factory. But if their configurations have changed at all, it's a best practice to reset them to factory defaults to reduce the chance of synchronization problems.

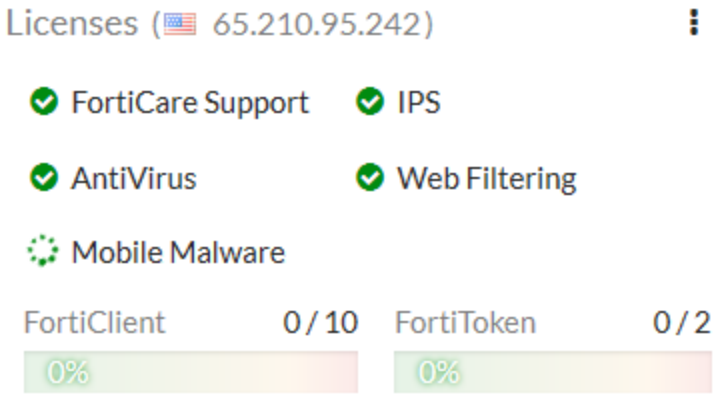
   In some cases, after resetting to factory defaults you may want to make some initial configuration changes to connect the FortiGates to the network or for other reasons. To write this recipe, the lan switch on the FortiGate-51Es was converted to separate lan1 to lan5 interfaces.
3. Change the primary FortiGate **Host name** to identify it as the primary FortiGate by going to **System > Settings**.

4. Change the backup FortiGate **Host name** to identify it as the backup FortiGate by going to **System > Settings**.

   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
   ```
5. Register and apply licenses to the FortiGates before configuring the cluster. This includes licensing for **FortiCare Support**, **IPS**, **AntiVirus**, **Web Filtering**, **Mobile Malware**, **FortiClient**, **FortiCloud**, **Security Rating**, **Outbreak Prevention**, and additional **virtual domains** (VDOMs).

Both 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 to all cluster members.

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

## Configuring clustering

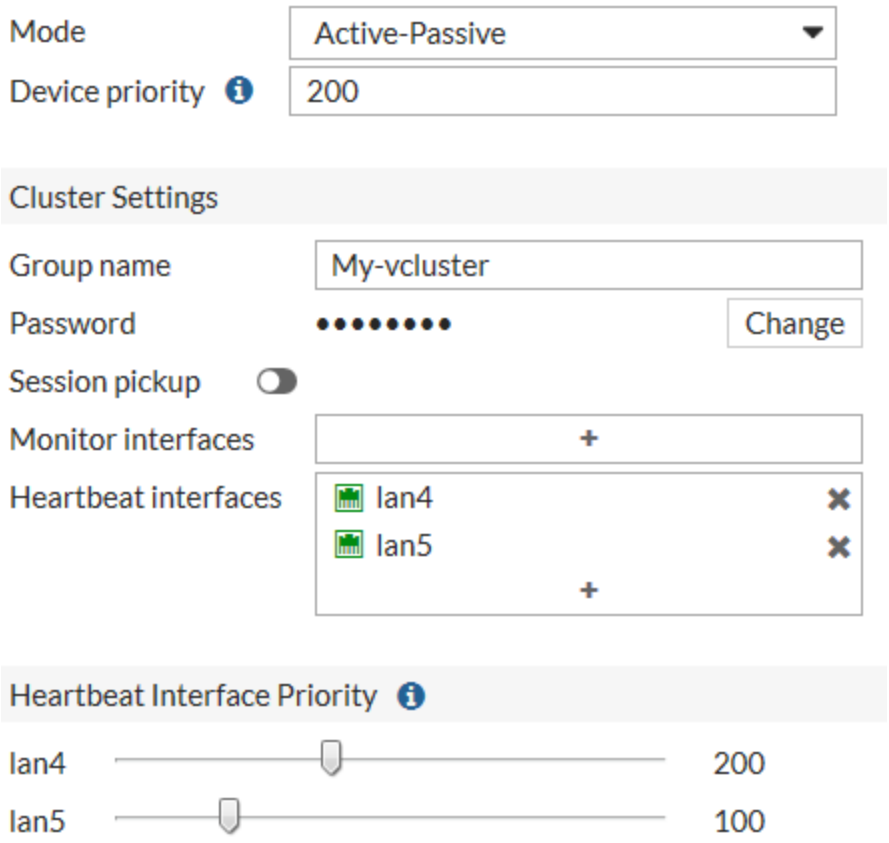
1. On the primary FortiGate, enter the following CLI command to set the HA mode to active-passive, set a group-id, group name, and password, increase the device priority to 200, enable override, and configure the heartbeat interfaces (lan4 and lan5 in this example).

```
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
```

If you have more than one cluster on the same network, each cluster should have a different group id. 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.

Enabling override is optional; but it makes sure the FortiGate with the highest device priority becomes the primary unit.

You can also configure most of these settings from the GUI (go to **Global > System > HA**). The group-id and override can only be configured from 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
```

After you enable HA, each FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity as FGCP negotiation takes place 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 (or just 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 (go to 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 the use case. Making these connections disrupts network traffic as you disconnect and re-connect cables.

Switches must be used between the cluster and the Internet, between the cluster and the internal network, and between the cluster and the Engineering network as shown in the diagram. You can use any good quality switches to make these connections.

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

You can also use fewer switches for all of these connections as long as you configure the switches to separate traffic from the different networks.

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.

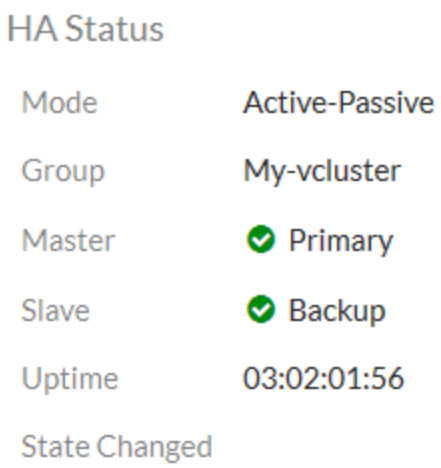
Check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration. Log into the primary FortiGate CLI and enter this command:

```
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.

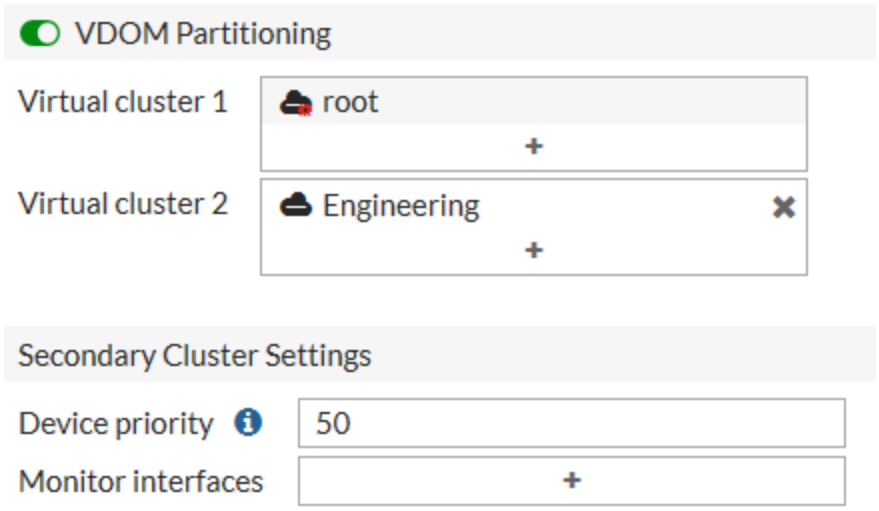
You can also use the `get system ha status` command to display detailed information about the cluster. .

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. Enable VDOMs by going to **System > Settings > System Operation Settings** and enabling **Virtual Domains**. Or enter the following CLI command.
```
config system global
   set vdom-admin enable
end
```
2. Add VDOMs as required. Go to **Global > System > VDOM** and select **Create New**. Or enter the following CLI command to add the Engineering VDOM.
```
config global
   edit Engineering
end
```
3. Configure virtual clustering and VDOM partitioning on the primary FortiGate. The following command enables virtual cluster 2, adds the Engineering VDOM to virtual cluster 2, and sets 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
   end
```
You can also configure virtual clustering and VDOM partitioning from the GUI by going to **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 can only configure the virtual cluster 2 priority of the backup FortiGate from the CLI. Use `execute ha manage` to access the backup FortiGate CLI.

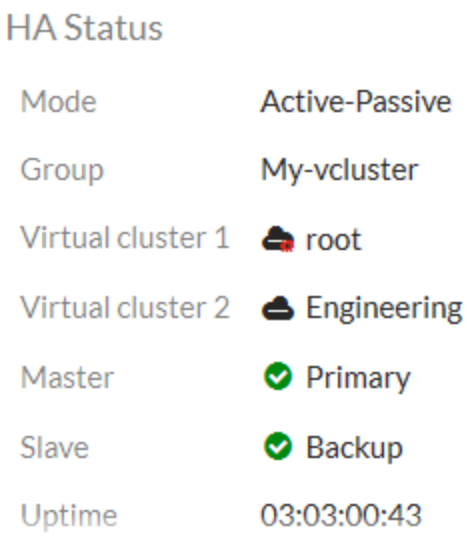
```
config global
  config system ha
    config secondary-vcluster
      set priority 200
    end
  end
```

The root VDOM can only be associated with virtual cluster 1.

The VDOM that is assigned as the management VDOM can also only be associated with virtual cluster 1.

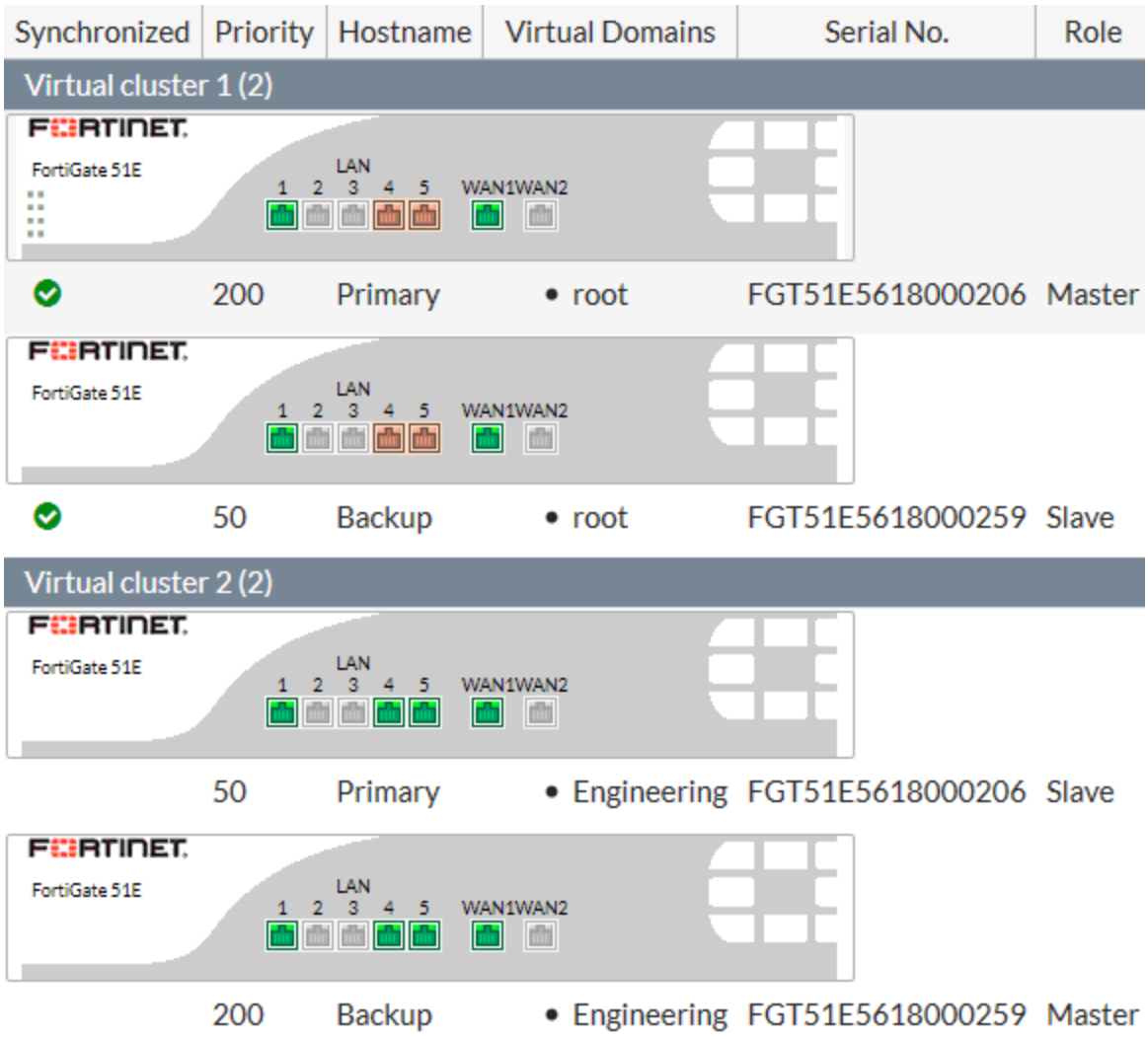
## Checking virtual cluster operation

1. Once again use the `diagnose sys ha checksum` cluster command and the `get system ha status` command to check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration.
   The **HA Status** dashboard widget shows the VDOMs in the virtual clusters. You can hover over the VDOM names to see status information for the VDOMs. You can hover over the host names of each FortiGate to verify that they are synchronized and both have the same checksum.




2. To view more information about the cluster status, click on 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 FortiGate for the root VDOM (so the primary FortiGate processes all root VDOM traffic). The page also shows that Backup is the primary FortiGate for the Engineering VDOM (so the backup FortiGate processes all Engineering VDOM traffic).




## Results

All traffic should now be flowing 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 operating 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

---

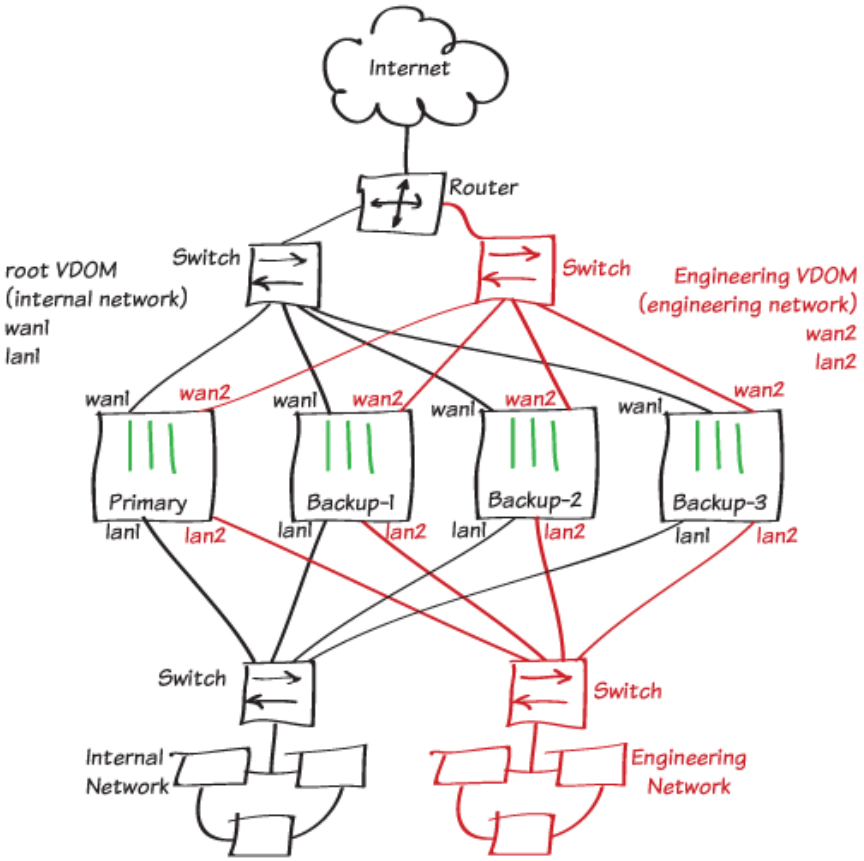
You will see a momentary pause in the ping results, until traffic diverts to the backup FortiGate, allowing the ping traffic to continue.

```
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.

When 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.

# FGCP Virtual Clustering with four FortiGates (expert)




FORTIOS VERSION 6.0

In this use case you set up a FortiGate Clustering Protocol (FGCP) virtual clustering configuration with four 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 recipe describes a very simple two-VDOM configuration. However, the same principles described in this example 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 in the virtual cluster.

The third FortiGate (the recipe 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, which 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, which becomes the new backup FortiGate.

This recipe describes the recommended steps for setting up a virtual cluster of four FortiGates. You can follow the procedure described in High Availability with FGCP (expert) on page 141 to configure virtual clustering by converting a FortiGate with VDOMs to HA mode and then adding another FortiGate to form a cluster. However, taking this approach with virtual clustering is not as foolproof as a normal HA configuration. If you accidentally add the management VDOM to virtual cluster 2 before adding the backup FortiGate, the configuration of the primary FortiGate can be overwritten by the

backup FortiGate. If want to experiment with this approach, make sure you don't add the management VDOM to virtual cluster 2 until all of the FortiGates have joined the cluster.

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

This recipe features four FortiGate-51Es. FortiGate-51Es have a 5-port switch lan interface. Before configuring HA, the lan interface was converted to 5 separate interfaces (lan1 to lan5).

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 recipe, you can use the wan1 and wan2 interfaces for the HA heartbeat.

## Preparing the FortiGates

1. If required, upgrade the firmware running on the FortiGates. All of the FortiGates should be running the same version of FortiOS.
2. On each FortiGate, enter the following command to reset them factory default settings.
   ```
   execute factoryreset
   ```
   You can skip this step if the FortiGates are fresh from the factory. But if their configurations have changed at all, it's a best practice to reset them to factory defaults to reduce the chance of synchronization problems.

   In some cases, after resetting to factory defaults you may want to make some initial configuration changes to connect the FortiGates to the network or for other reasons. To write this recipe, the lan switch on the FortiGate-51Es was converted to separate lan1 to lan5 interfaces.
3. Change the primary FortiGate **Host name** to identify it as the primary FortiGate by going to **System > Settings**.

   
   
4. Change the backup FortiGate **Host name** to identify it as Backup-1 by going to **System > Settings**.

   
   
5. Change the third FortiGate **Host name** to identify it as Backup-2 by going to **System > Settings**.

   
   
6. Change the fourth FortiGate **Host name** to identify it as Backup-3 by going to **System > Settings**.

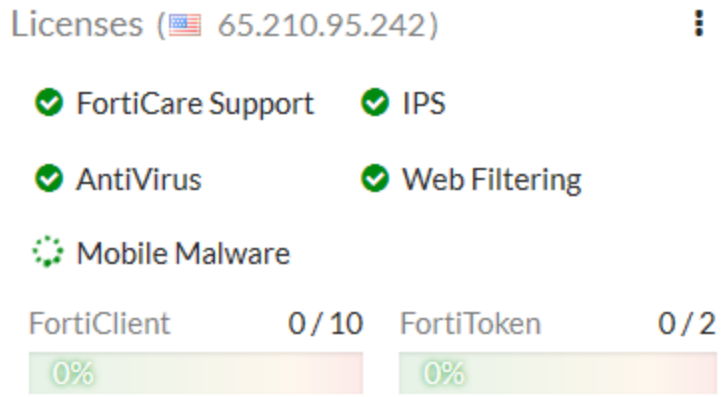
   You can also use the CLI to change the host name. From the Primary FortiGate:
   ```
   config system global
      set hostname Primary
   end
   ```
   From the Backup-1 FortiGate:
   ```
   config system global
      set hostname Backup-1
   end
   ```
   From the Backup-2 FortiGate:
   ```
   config system global
   ```

```
    set hostname Backup-2
  end
```

From the Backup-3 FortiGate:

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

7. Register and apply licenses to the FortiGates before configuring the cluster. This includes licensing for **FortiCare Support**, **IPS**, **AntiVirus**, **Web Filtering**, **Mobile Malware**, **FortiClient**, **FortiCloud**, **Security Rating**, **Outbreak Prevention**, 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 to all cluster members.

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

## Configuring clustering

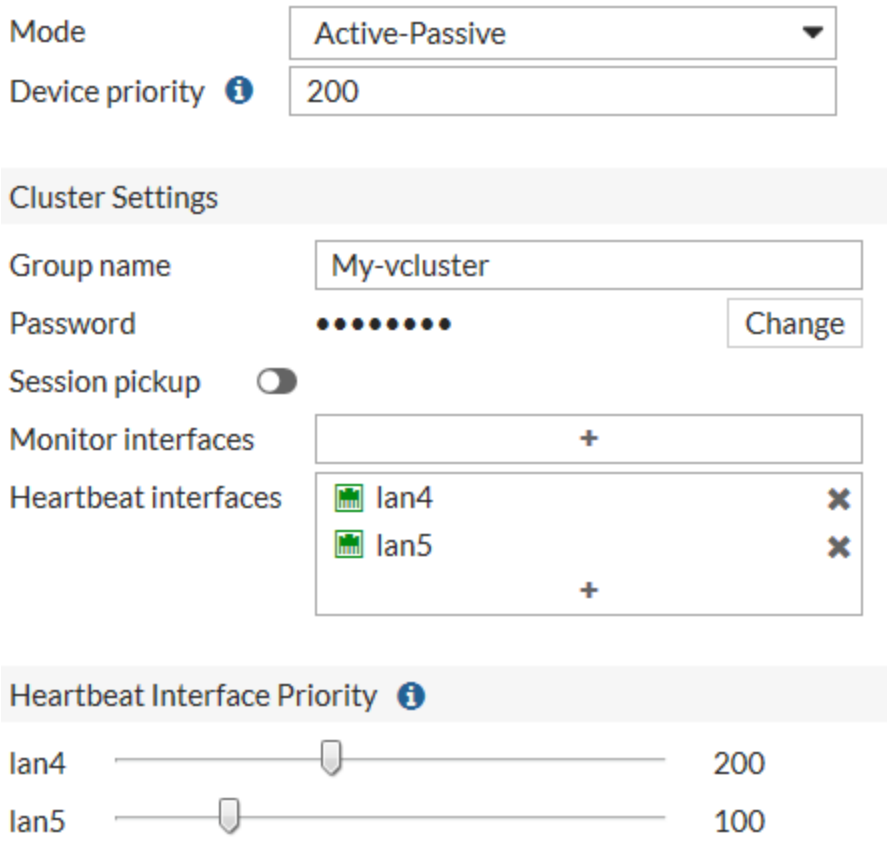
1. On the primary FortiGate, enter the following CLI command to set the HA mode to active-passive, set a group-id, group name, and password, increase the device priority to 200, enable override, and configure the heartbeat interfaces (lan4 and lan5 in this example).

```
  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
```

If you have more than one cluster on the same network, each cluster should have a different group id. 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.

Enabling override is optional; but it makes sure the FortiGate with the highest device priority becomes the primary unit.

You can also configure most of these settings from the GUI (go to **Global > System > HA**). The group-id and override can only be configured from 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 relatively low value means the Backup-1 FortiGate will most likely always become 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
```

After you enable HA, each FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity as FGCP negotiation takes place 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 (or just 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 (go to 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 the use case. Making these connections disrupts network traffic as you disconnect and re-connect cables.

Switches must be used between the cluster and the Internet, between the cluster and the internal network, and between the cluster and the Engineering network as shown in the diagram. You can use any good quality switches to make these connections.

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

You can also use fewer switches for all of these connections as long as you configure the switches to separate traffic from the different networks.

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.

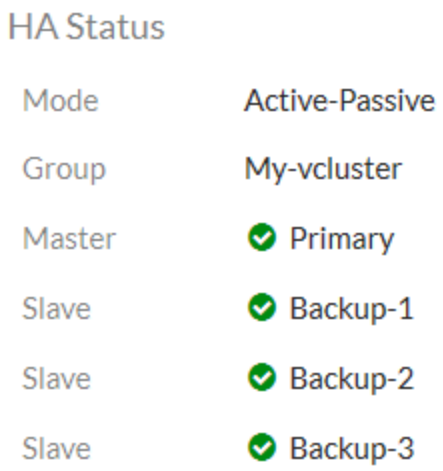
Check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration. Log into the primary FortiGate CLI and enter this command:

```
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. .

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

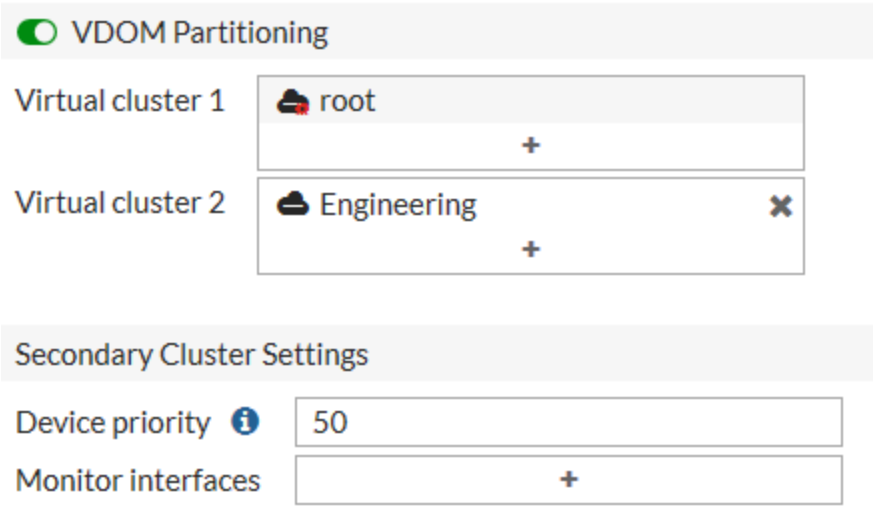
1. Enable VDOMs by going to **System > Settings > System Operation Settings** and enabling **Virtual Domains**. Or enter the following CLI command.
   ```
   config system global
      set vdom-admin enable
   end
   ```
2. Add VDOMs as required. Go to **Global > System > VDOM** and select **Create New**. Or enter the following CLI command to add the Engineering VDOM.

```
config global
   edit Engineering
end
```

3. Configure virtual clustering and VDOM partitioning on the primary FortiGate. The following command enables virtual cluster 2, adds the Engineering VDOM to virtual cluster 2, and sets 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 by going to **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 can only configure the virtual cluster 2 priority of the backup FortiGate from the CLI. 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 can only configure the virtual cluster 2 priority of the Backup-2 FortiGate from the CLI. Use execute ha manage to access the backup FortiGate CLI.

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

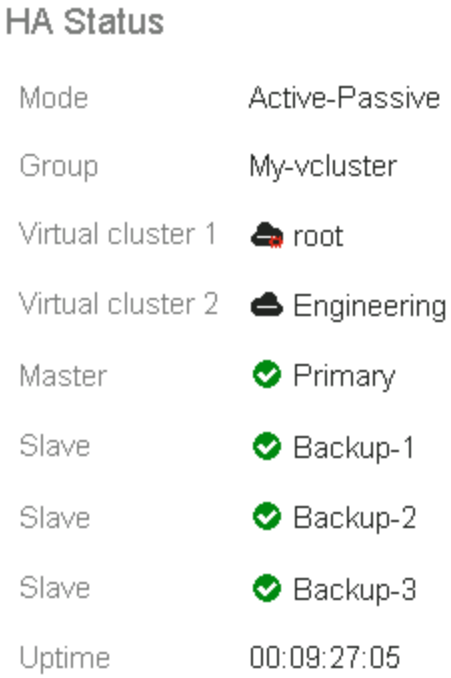
6. Set the virtual cluster 2 priority of the Backup-3 FortiGate to 150 so that if the backup FortiGate fails, Backup-3 will have the highest virtual cluster 2 device priority. The FGCP synchronizes all other HA settings from the primary

FortiGate.
You can only configure the virtual cluster 2 priority of the backup FortiGate from the CLI. 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. Once again use the `diagnose sys ha checksum` cluster command and the `get system ha status` command to check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration.
   The **HA Status** dashboard widget shows the VDOMs in the virtual clusters. You can hover over the VDOM names to see status information for the VDOMs. You can hover over the host names of each FortiGate to verify that they are synchronized and both have the same checksum.




2. To view more information about the cluster status, click on 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 FortiGate for the root VDOM (so the primary FortiGate processes all root VDOM traffic). The page also shows that Backup-1 is the primary 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 now be flowing through the primary FortiGate and Engineering VDOM traffic should be flowing 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.

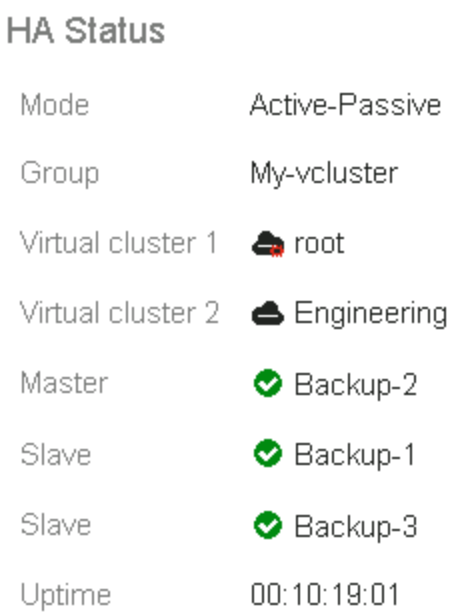
If you are using port monitoring, you can also unplug the primary FortiGate's Internet-facing interface to test failover.

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

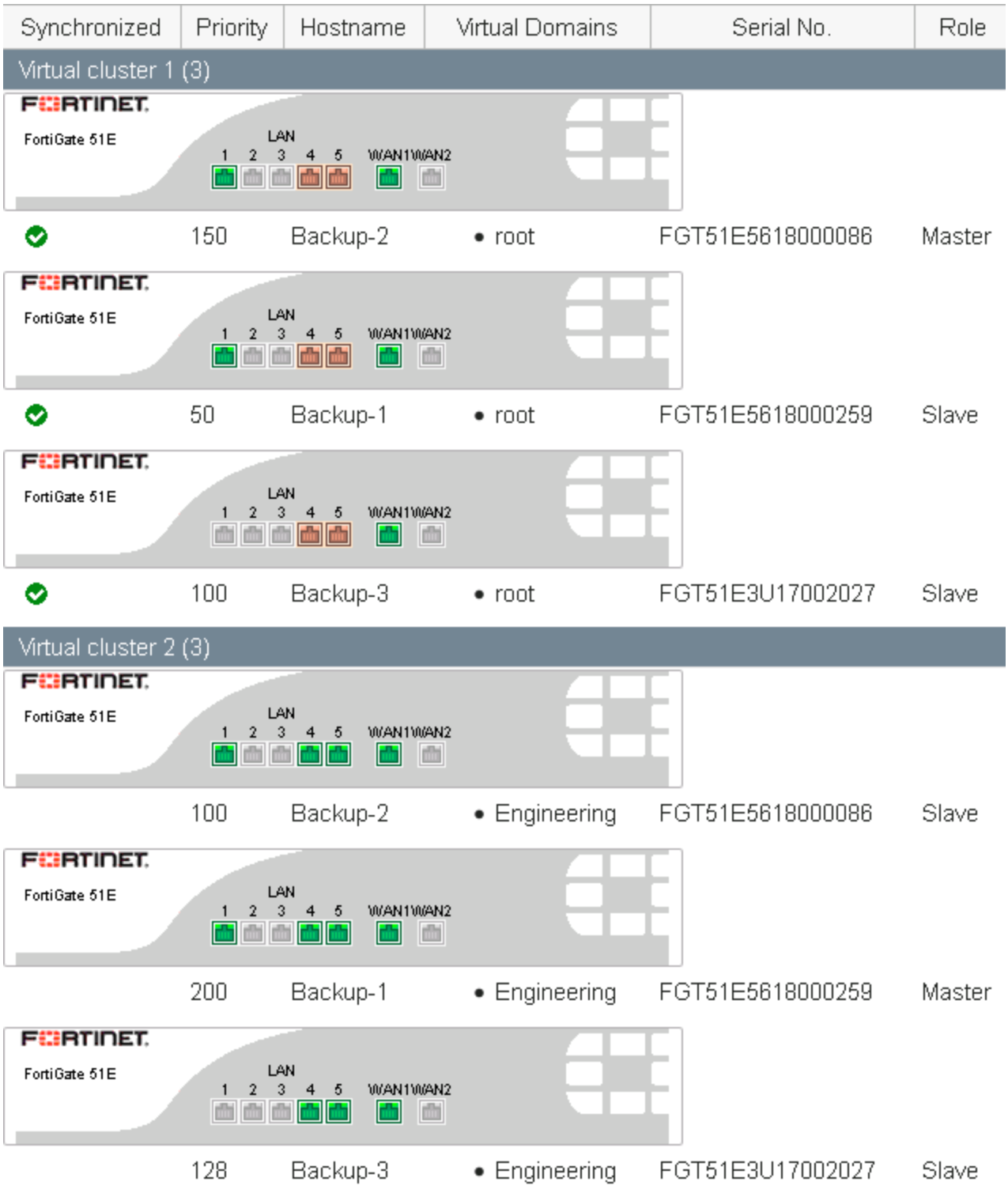
```
64 bytes from 184.25.76.114: icmp_seq=69 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=70 ttl=52 time=8.822 ms\
64 bytes from 184.25.76.114: icmp_seq=71 ttl=52 time=9.034 ms\
64 bytes from 184.25.76.114: icmp_seq=72 ttl=52 time=9.536 ms\
64 bytes from 184.25.76.114: icmp_seq=73 ttl=52 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 FortiGate.



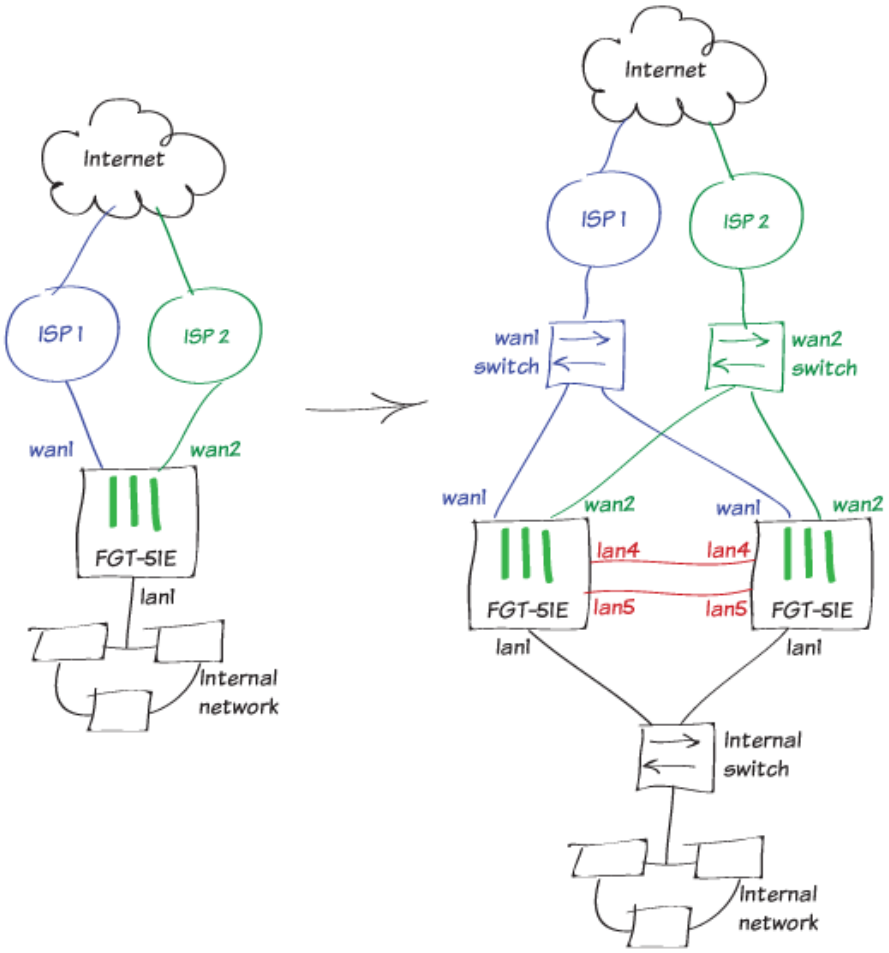

The **System > HA** page shows that the Backup-2 FortiGate has become the primary FortiGate for virtual cluster 1. This page also shows that the Backup-1 FortiGate continues to process virtual cluster 2 traffic.




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 will be distributed between them.

## SD-WAN with FGCP HA (expert)



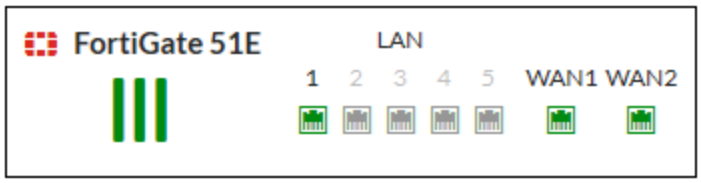

FORTIOS VERSION 6.0

This use case provides an example of how to set up a FortiGate for redundant Internet connectivity using SD-WAN and then convert this single FortiGate into an FGCP HA cluster of two FortiGates. This SD-WAN HA configuration allows you to load balance your Internet traffic between multiple ISP links and provides redundancy for your network's Internet connection if your primary ISP is unavailable or if one of the FortiGates in the HA cluster fails.

This use case features two FortiGate-51Es, which have a 5-port switch lan interface. Before starting the steps in this recipe, we converted the lan interface to 5 separate interfaces (lan1 to lan5). The lan1 interface connects to the internal network, the wan1 interface connects to one Internet service provider (ISP) and the wan2 to a second ISP. For the FGCP HA configuration, the lan4 and lan5 interfaces become HA heartbeat interfaces.

## Connecting the FortiGate to your ISPs

Connect the Internet-facing ports (WAN ports) on the FortiGate to your ISP devices. Connect WAN1 to the ISP that you want to use for most traffic. Connect WAN2 to the other ISP.




## Removing existing configuration references to interfaces

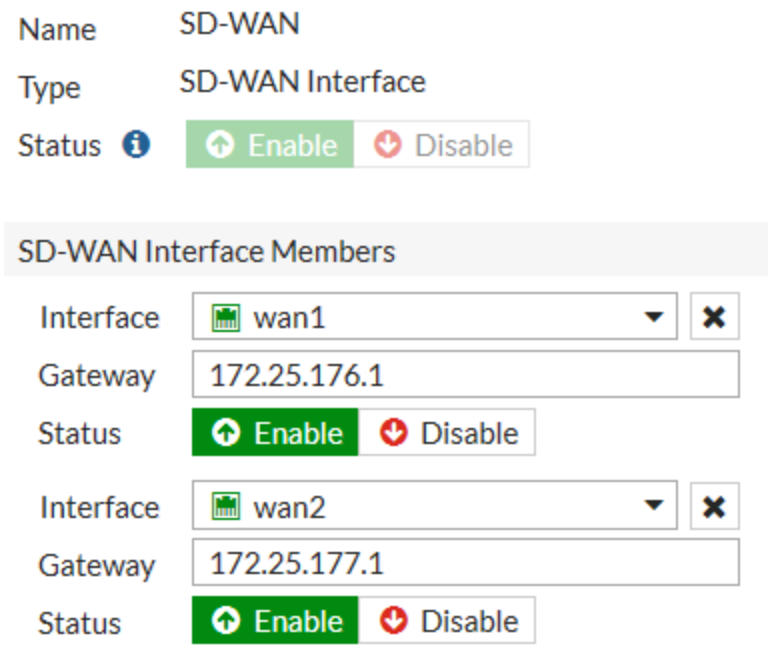
Before you can configure FortiGate interfaces as SD-WAN members, you must remove or redirect existing configuration references to those interfaces in routes and security policies. This includes the default Internet access policy that's included with many FortiGate models. Note that after you remove the routes and security policies, traffic can't reach the WAN ports through the FortiGate.

Redirecting the routes and policies to reference other interfaces avoids your having to create them again later. After you configure SD-WAN, you can reconfigure the routes and policies to reference the SD-WAN interface.

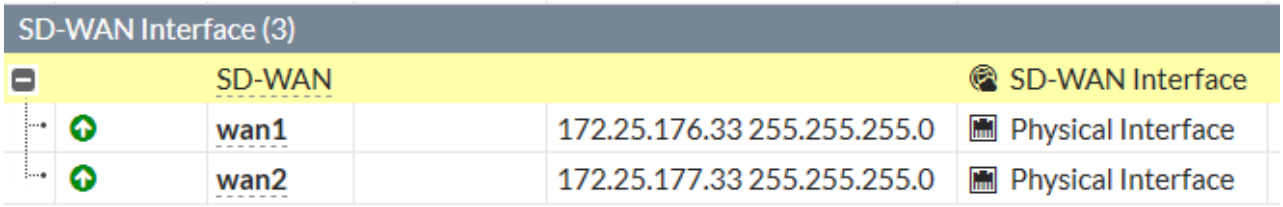
1. Go to **Network > Static Routes** and delete any routes that use WAN1 or WAN2.
2. Go to **Policy & Objects >IPv4 Policy** and delete any policies that use WAN1 or WAN2.

## Creating the SD-WAN interface

1. Go to **Network > SD-WAN** and set **Status** to **Enable**.
   Under SD-WAN Interface Members, select + and select wan1. Set the Gateway to the default gateway for this interface. This is usually the default gateway IP address of the ISP that this interface is connected to. Repeat these steps to add wan2.

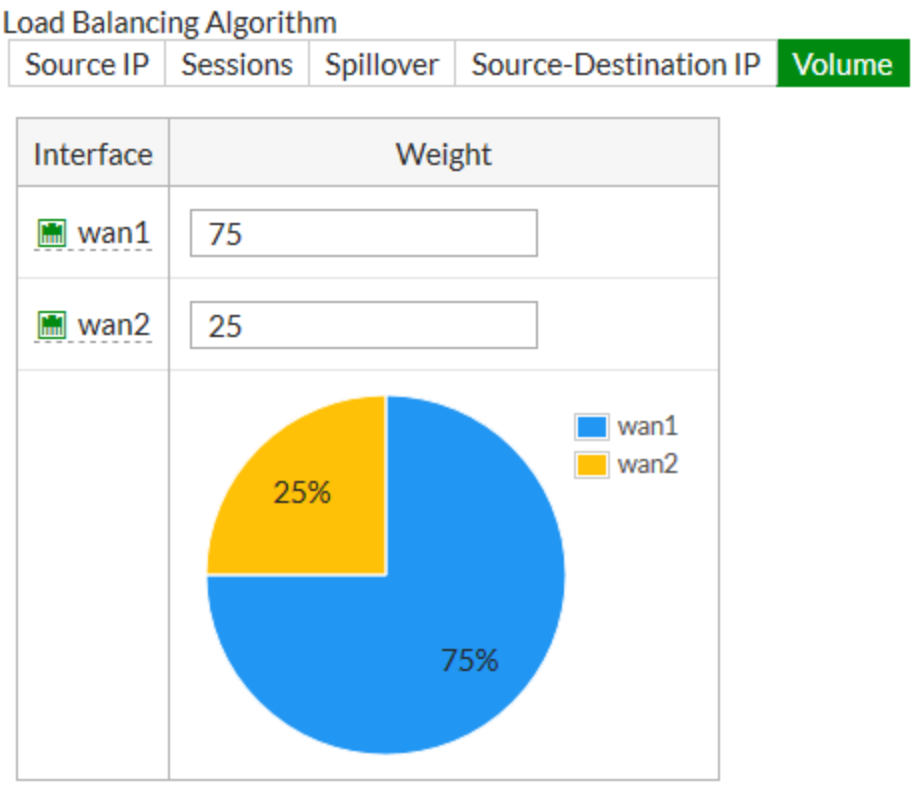



2. Go to **Network > Interfaces** and verify that the virtual interface for SD-WAN appears in the interface list. You can expand SD-WAN to view the ports that are included in the SD-WAN interface.



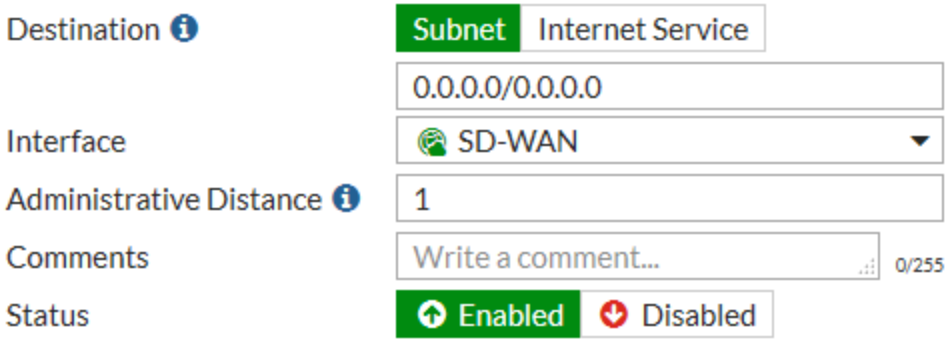

## Configuring SD-WAN load balancing

1. Go to **Network > SD-WAN Rules** and edit the rule named **sd-wan**.
2. In the **Load Balancing Algorithm** field, select **Volume**, and prioritize WAN1 to serve more traffic.
   In the 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.




## Creating a static route for the SD-WAN interface

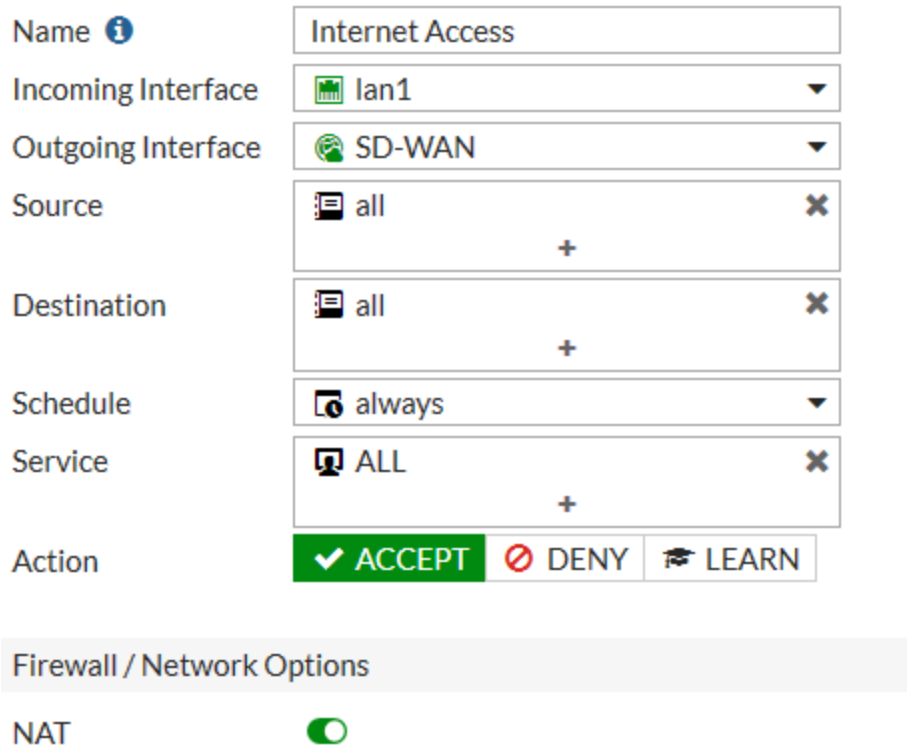
1. Go to **Network > Static Routes** and create a route.
2. In the **Destination** field, select **Subnet**, and leave the destination IP address and subnet mask as 0.0.0.0/0.0.0.0.
3. In the Interface field, select the SD-WAN interface from the drop-down menu.
4. Ensure that **Status** is set to **Enable**.




5. If you previously removed or redirected existing references in routes to interfaces that you wanted to add as SD-WAN interface members, you can now reconfigure those routes to reference the SD-WAN interface.

## Configuring a security policy for SD-WAN

1. Configure a security policy that allows traffic from your organization's internal network to the SD-WAN interface.
2. Go to **Policy & Objects >IPv4 Policy** and create a policy.
3. Set **Incoming Interface** to the interface that connects to your organization's internal network, and set **Outgoing Interface** to the SD-WAN interface.
4. Enable **NAT** and apply **Security Profiles** as required.
5. Configure other policy options as required.



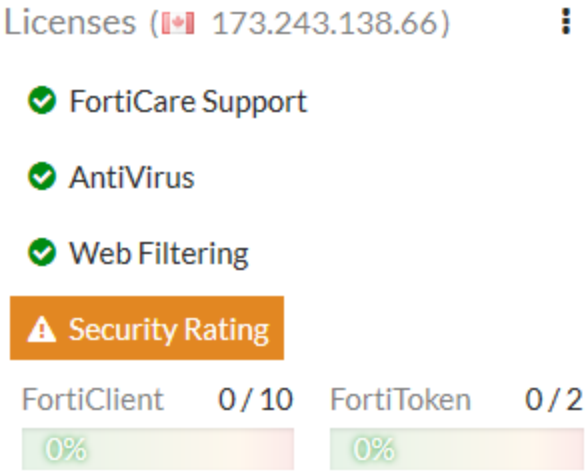

## Configuring the FortiGate for HA

1. Change the **Host name** to identify this FortiGate as the primary FortiGate. From the **System Information** dashboard widget, select **Configure settings in System > Settings**.


You can also enter this CLI command:

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

2. Register and apply licenses to the primary FortiGate before configuring it for HA operation.




3. Enter this CLI command to set the HA mode to active-passive; set a group ID, group name and password; increase the device priority to a higher value (for example, 250); and enable override.

```
config system ha
set mode a-p
   set group-id 100
   set group-name My-cluster
   set password <password>
   set priority 250
   set override enable
   set hbdev lan4 200 lan5 100
end
```

Enabling override and increasing the device priority means this FortiGate always becomes the primary unit.

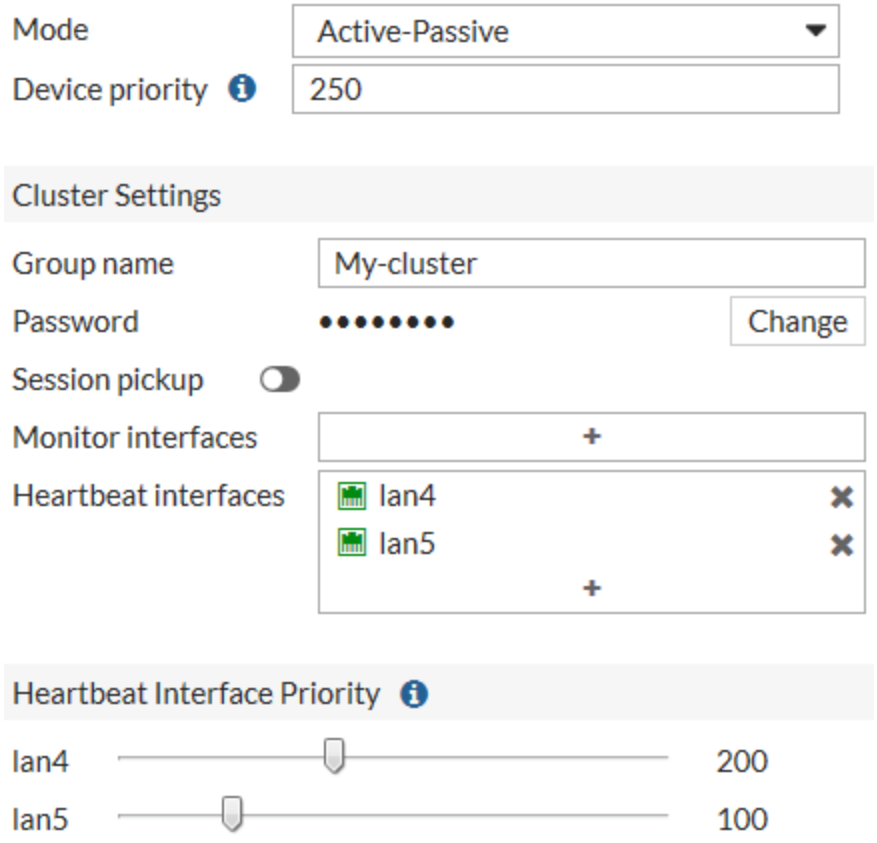
This configuration also selects lan4 and lan5 to be the heartbeat interfaces and sets their priorities to 200 and 100 respectively. It's a best practice to set different priorities for the heartbeat interfaces (but not a requirement).

If you have more than one cluster on the same network, each cluster should have a different group ID. 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.

Override and the group ID can only be configured from the CLI.

```
config system ha
   set group-id 100
   set override enable
end
```

4. You can also configure most of these settings from the GUI (go to **System > HA**).




After you enter the CLI command or make changes from the GUI, the FortiGate negotiates to establish an HA cluster. You may temporarily lose connectivity with the FortiGate as FGCP negotiation takes place and the MAC addresses of the FortiGate interfaces are changed 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 just deleting all ARP table entries). You can usually delete the ARP table from a command prompt using a command similar to `arp -d`.

## Configuring the backup FortiGate

If required, change the firmware running on the new FortiGate to the same version as is running on the primary FortiGate.

Enter the following command to reset the new backup FortiGate to factory default settings.

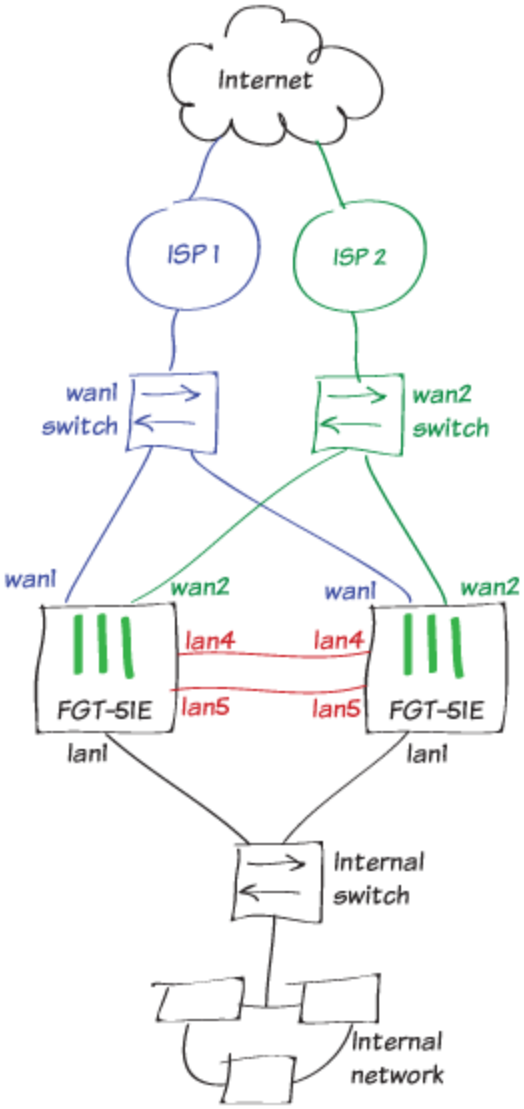
execute factoryreset

You can skip this step if the new FortiGate is fresh from the factory. But if its configuration has been changed at all, it's a best practice to reset your FortiGate to factory defaults to reduce the chance of synchronization problems.

## Connecting the primary and backup FortiGates

Connect the primary and backup FortiGates to each other and to your network as shown. Making these connections disrupts network traffic as you disconnect and re-connect cables.

Switches must be used between the cluster and the ISPs and between the cluster and the internal network 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 of these connections as long as you configure the switch to separate traffic from the different networks.




The example shows the recommended configuration of direct connections between the lan4 heartbeat interfaces and between the lan5 heartbeat interfaces.

When the heartbeat interfaces are connected, the FortiGates 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.

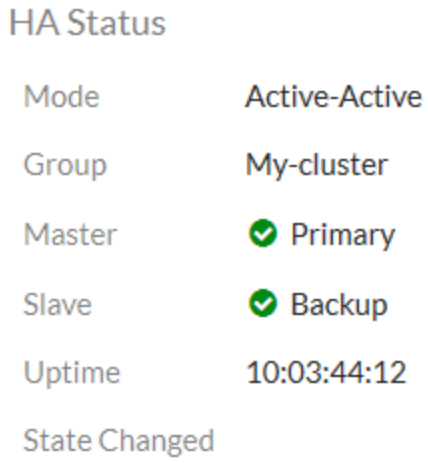
The cluster will have the same IP addresses as the primary FortiGate had. You can log into the cluster by logging into the primary FortiGate CLI or GUI using one of the original IP addresses of the primary FortiGate.

## Checking cluster operation

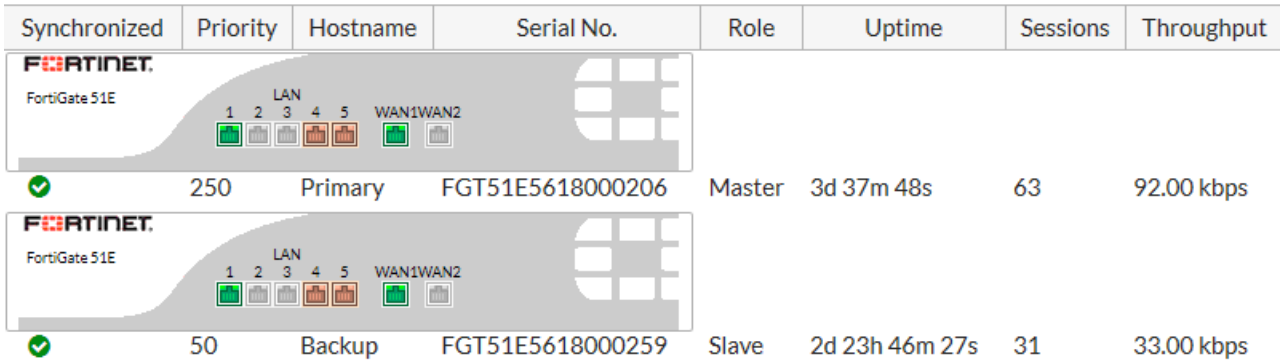
Check the cluster synchronization status to make sure the primary and backup FortiGates both have the same configuration.

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 some parts of the configuration to be synchronized.

   If the checksums never become identical visit the Fortinet Support website for assistance.
2. The **HA Status** dashboard widget also shows synchronization status. Mouse 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, click on the **HA Status** widget and select **Configure Settings in System > HA** (or go to **System > HA**).



## 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
```

FGCP clusters dynamically respond to network conditions. If you keep override enabled, the same FortiGate always becomes the primary FortiGate. With override enabled; however, the cluster may negotiate more often to keep the same FortiGate as the primary FortiGate, potentially increasing traffic disruptions.

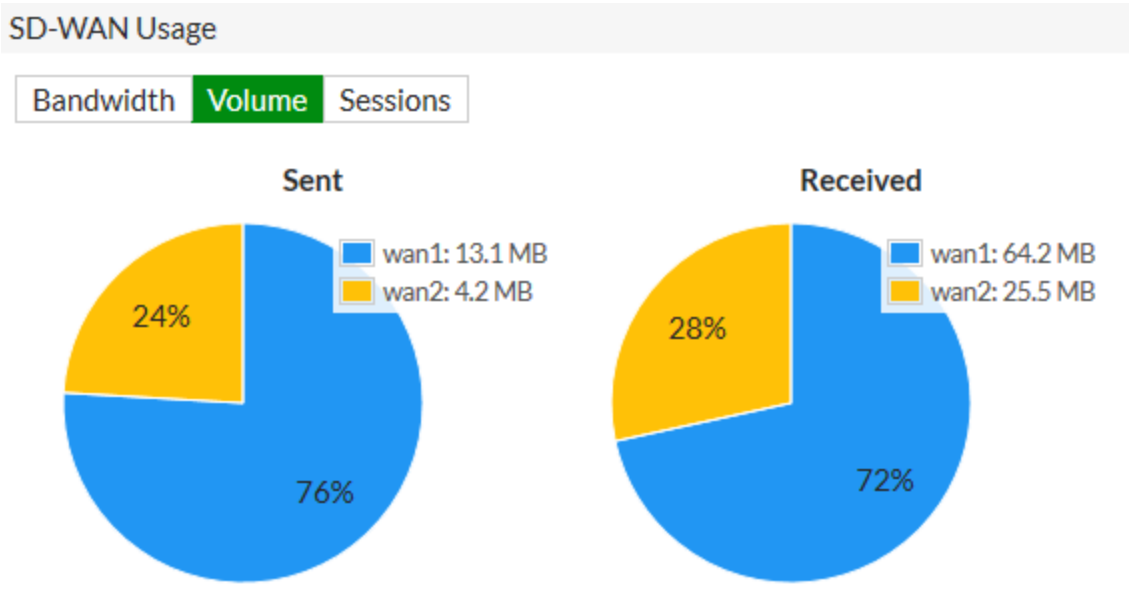
If you disable override it is more likely that the backup FortiGate could become the primary FortiGate. Disabling override is recommended unless its important that the same FortiGate remains the primary FortiGate

To see how enabling override can cause minor traffic disruptions, with override enabled set up a continuous ping through the cluster. Then disconnect power to the backup unit. You will most likely notice a brief disruption in the ping traffic. Try the same thing with override disabled and you shouldn't see this traffic disruption.

With override enabled, the disruption is minor and shouldn't be noticed by most users. For smoother operation, the best practice is to disable override.

## Results

1. Browse the Internet using a computer on your internal network.
2. Go to **Network > SD-WAN**.
   In the **SD-WAN Usage** section, you can see the bandwidth, volume, and sessions for traffic on the SD-WAN interfaces.




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

interface.

| + | 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 HA failover

All traffic should now be flowing 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 operating 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 will see a momentary pause in the ping results, until traffic diverts to the backup FortiGate, allowing the ping traffic to continue.

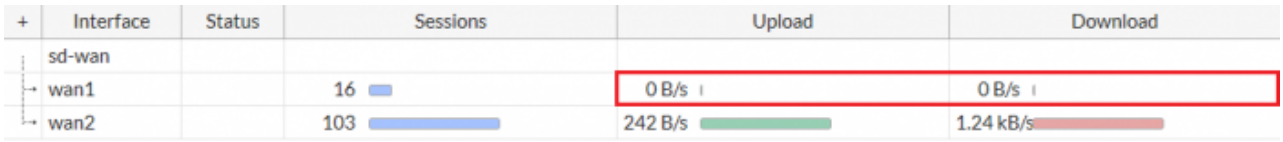
```
64 bytes from 184.25.76.114: icmp_seq=69 ttl=52 time=8.719 ms\
64 bytes from 184.25.76.114: icmp_seq=70 ttl=52 time=8.822 ms\
64 bytes from 184.25.76.114: icmp_seq=71 ttl=52 time=9.034 ms\
64 bytes from 184.25.76.114: icmp_seq=72 ttl=52 time=9.536 ms\
64 bytes from 184.25.76.114: icmp_seq=73 ttl=52 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.

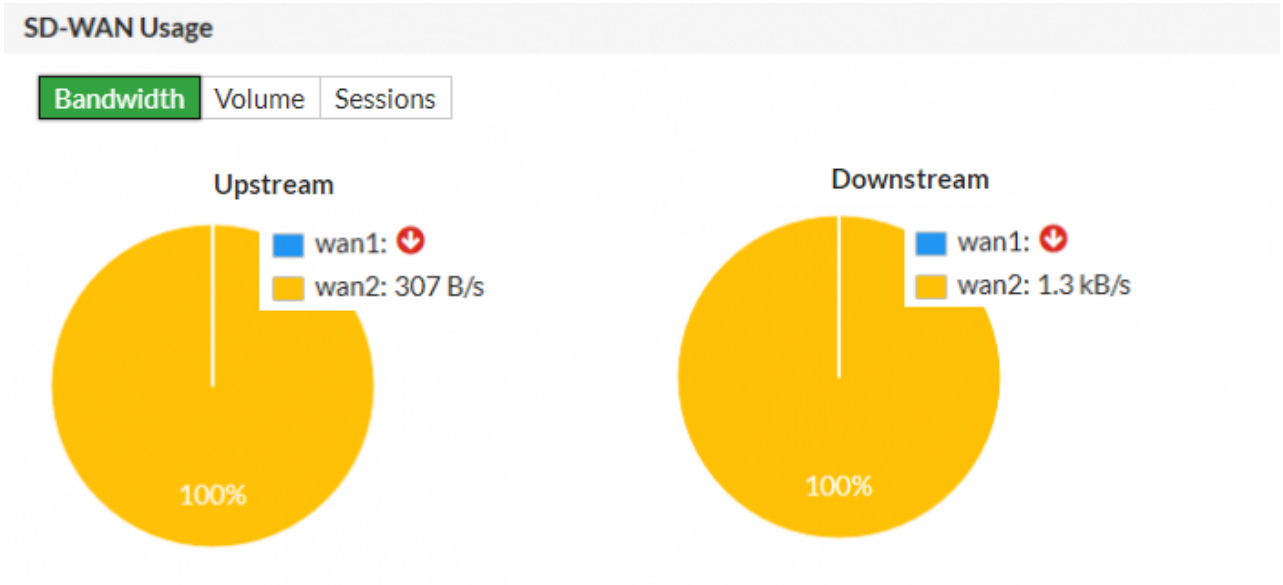
## Testing ISP failover

1. To test failover of the redundant Internet configuration, you must simulate a failed Internet connection to one of the ports. You can do so by disconnecting power from the wan1 switch or otherwise disconnecting the wan1 interfaces of both FortiGates from ISP 1.

2. Verify that users still have Internet access by navigating to **Monitor > SD-WAN Monitor.** The **Upload** and **Download** values for WAN1 show that traffic isn't going through that interface.




3. Go to **Network > SD-WAN**. In the **SD-WAN Usage** section, you can see that bandwidth, volume, and sessions have diverted entirely through WAN2.



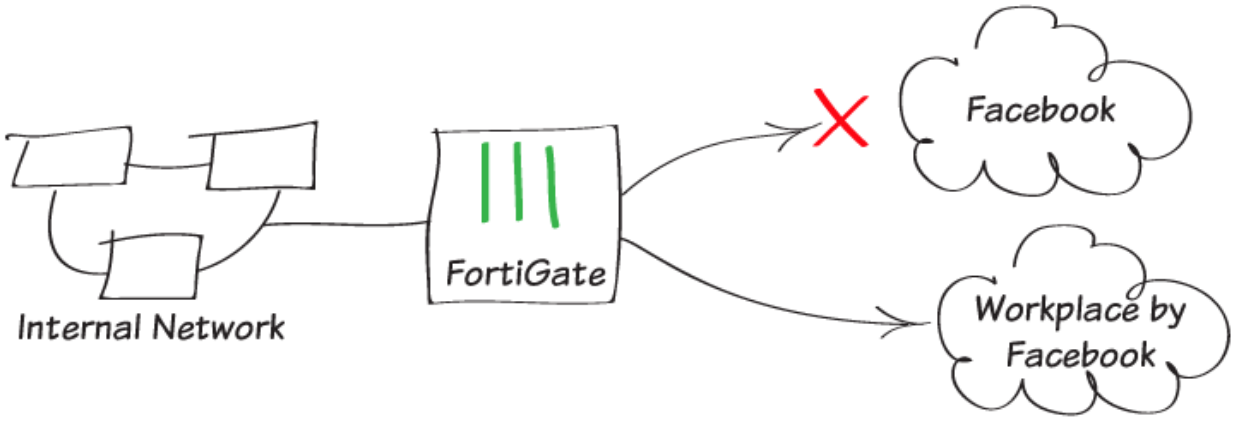

Users on the internal network shouldn't notice the WAN1 failure. Likewise, if you're using the WAN1 gateway IP address to connect to the admin dashboard, nothing should change from your perspective. It appears as though you're still connecting through WAN1.

4. After you verify successful failover, re-establish the connection to ISP 1.

# Security profiles

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

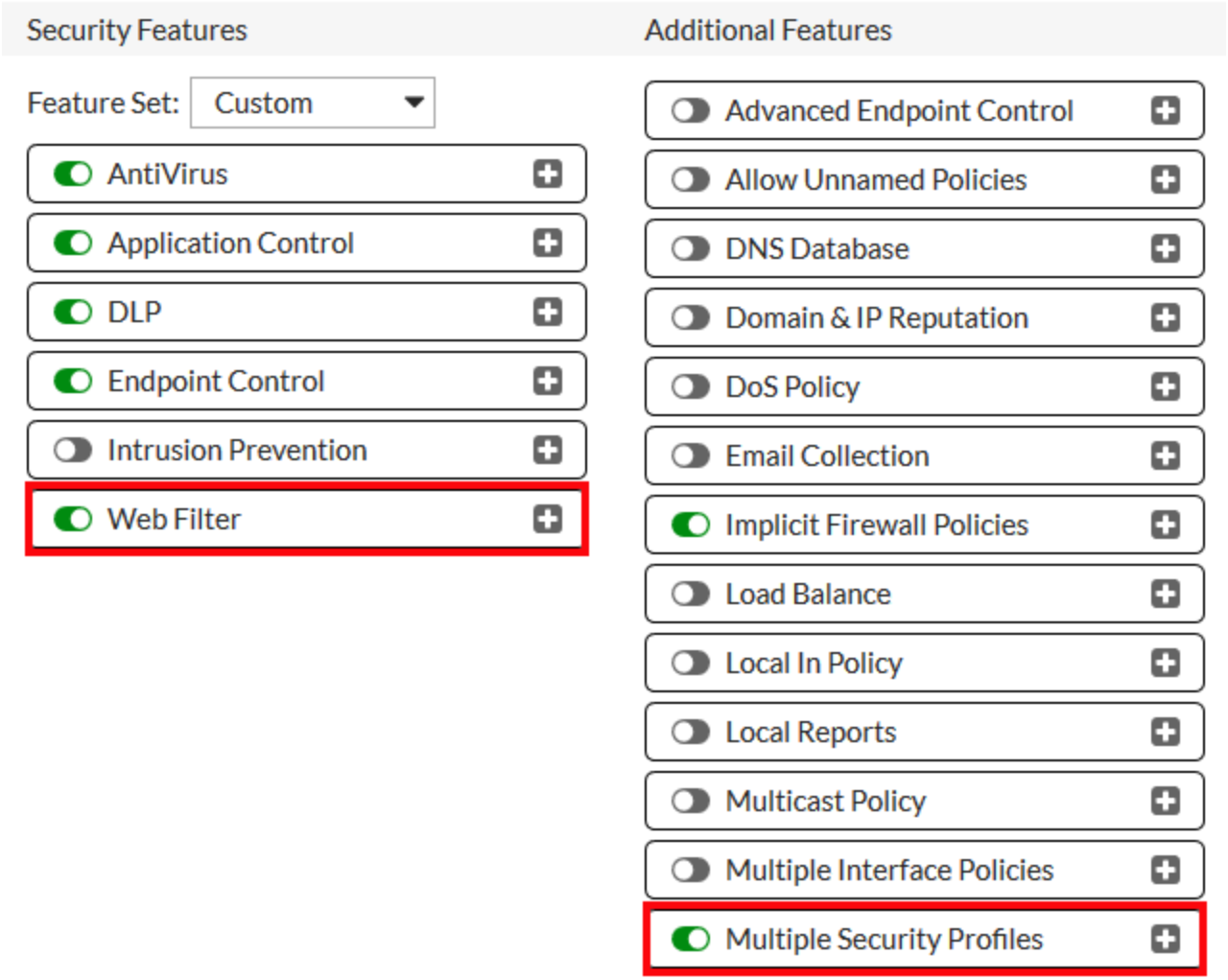
## Blocking Facebook while allowing Workplace by Facebook



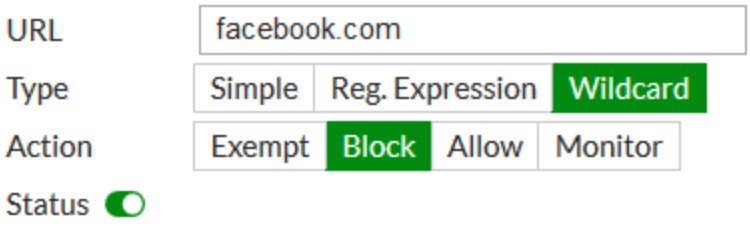

In this recipe, you block access to Facebook using web filtering, while making an exception to allow access to Workplace by Facebook.

### Creating a web filter profile

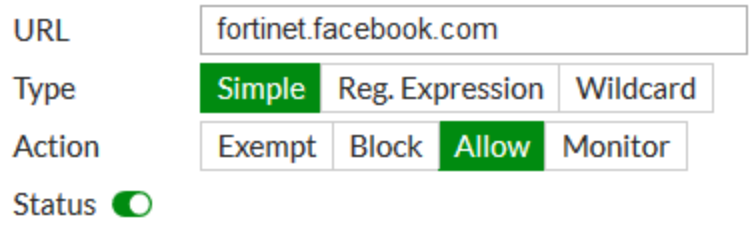
1. To make sure the features you need are available in the GUI, go to **System > Feature Visibility**. Under **Security Features**, enable **Web Filter**. Under **Additional Features**, enable **Multiple Security Profiles**.



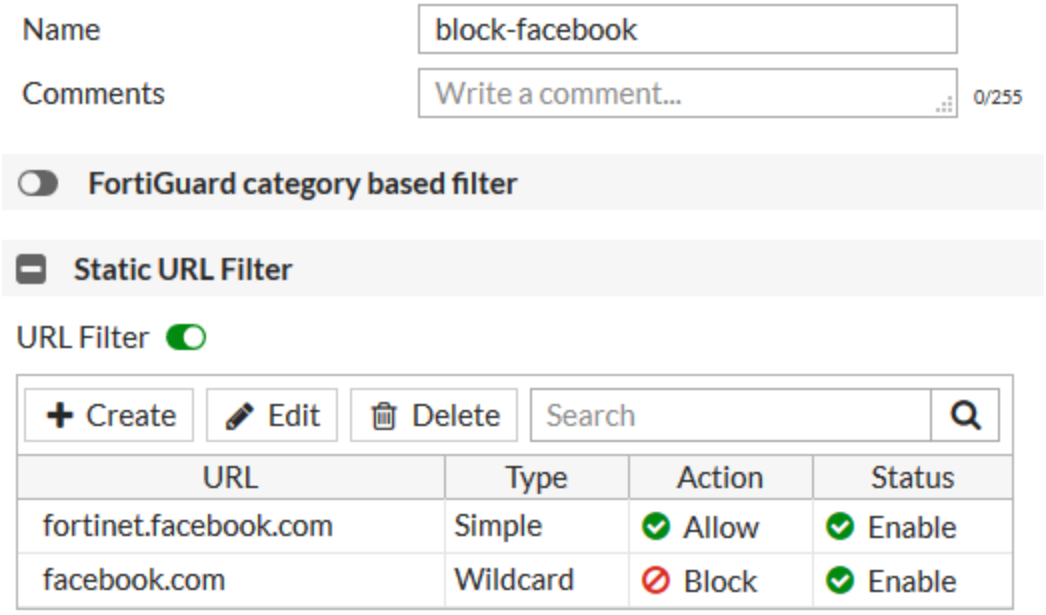

2. To create a web filter profile, go to **Security Profiles > Web Filter** and select ⊕.
3. Enter a **Name** for the profile. Under **Static URL Filter**, enable **URL Filter**. Create a new URL filter to block Facebook. Set **URL** to *facebook.com*, **Type** to **Wildcard**, and **Action** to **Block**.




4. Create a **URL** filter to allow Workplace by Facebook. Set URL to your Workplace by Facebook site (in the example, *fortinet.facebook.com*), **Type** to **Simple**, and **Action** to **Allow**.

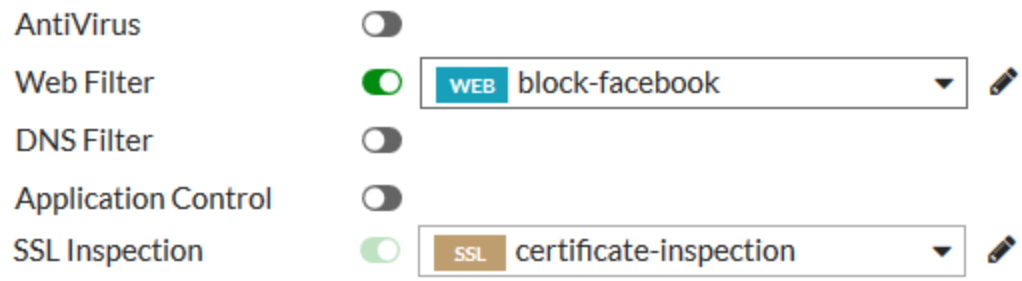



URL filters are applied in the order that they are listed. Make sure the filter allowing Workplace by Facebook is located above the filter blocking Facebook.




## Applying the security profiles

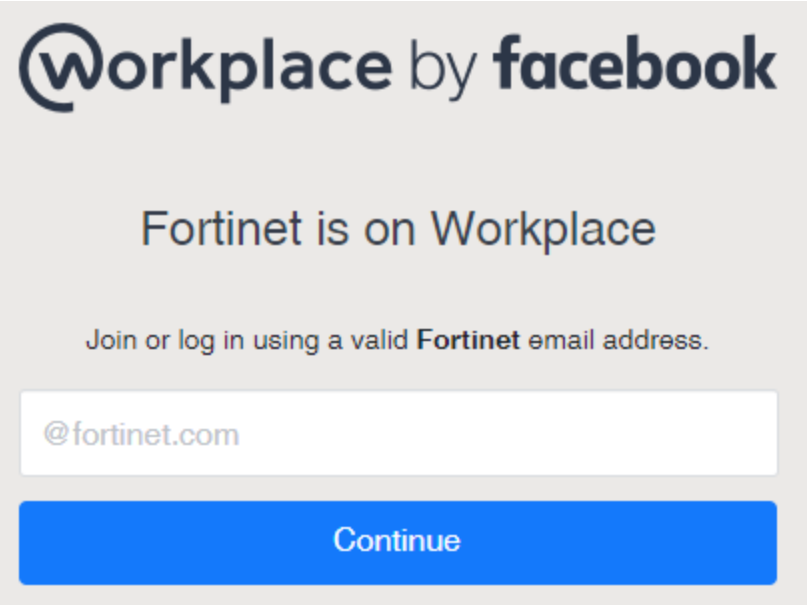
1. To apply the security profiles to traffic, go to **Policy > IPv4 Policy** and edit the policy allowing Internet access.
2. Under **Security Profiles**, enable **Web Filter** and set it to use the new profiles.
3. Set **SSL Inspection** to **certificate-inspection**.



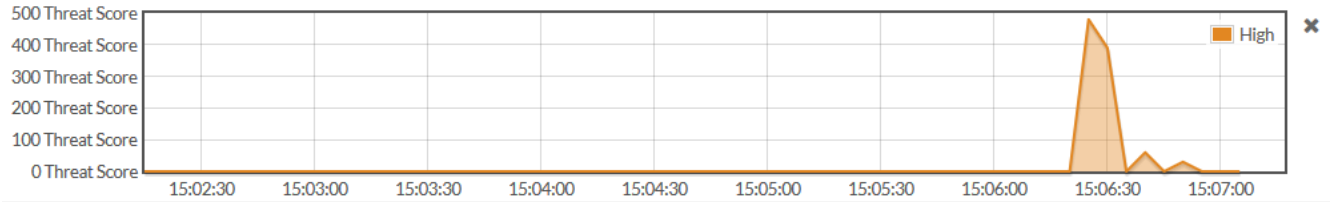
## Results

Attempt to access www.facebook.com. Access is blocked. Access is also blocked for the Facebook app.

Browse to your Workplace by Facebook site. Access is allowed.

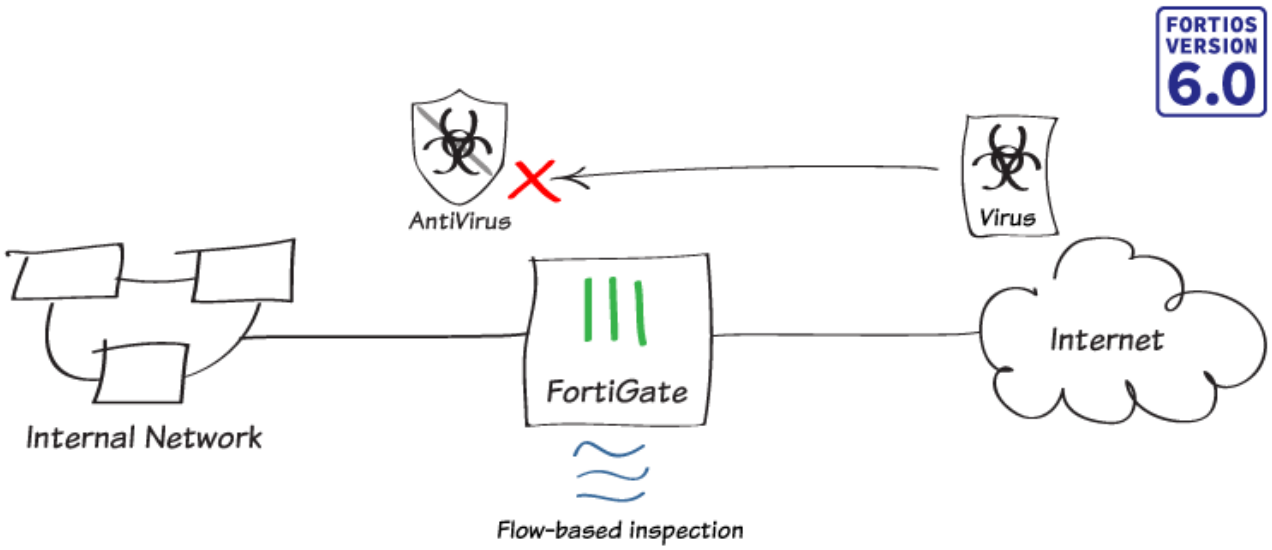



To view information about the blocked traffic, go to **FortiView > Threats**. The page shows the blocked attempts to access Facebook.




| Threat | Category | Threat Level | Threat Score (Blocked/Allowed) | Sessions (Blocked/Allowed) |
|---|---|---|---|---|
| www.facebook.com | N/A - Static URL Filter | High | 480 | 16 |
| facebook.com | N/A - Static URL Filter | High | 360 | 12 |
| edge-chat.facebook.com | N/A - Static URL Filter | High | 60 | 2 |
| 1-edge-chat.facebook.com | N/A - Static URL Filter | High | 30 | 1 |

# Antivirus scanning using flow-based inspection

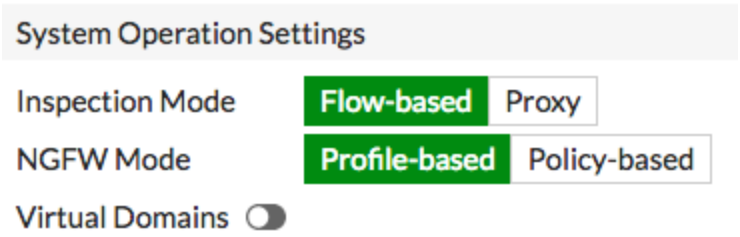



In this recipe, you will turn on flow-based inspection on your FortiGate and apply flow-based antivirus scanning to network traffic.

For more information about the different antivirus inspection modes available in FortiOS, see FortiOS antivirus inspection modes.

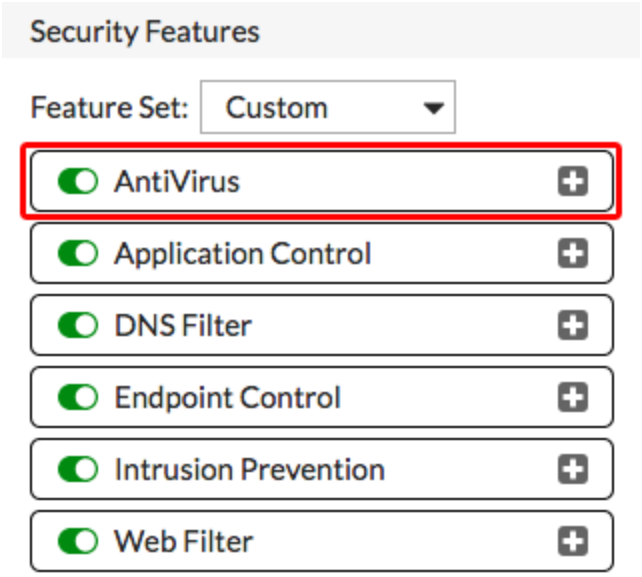
## Verifying the inspection mode

1. Flow-based is the default inspection mode for FortiOS. To verify that your FortiGate is in this mode, go to **System > Settings** and locate **System Operations Settings**.
2. Verify that **Inspection Mode** is set to **Flow-based** and **NGFW Mode** is set to **Profile-based**.

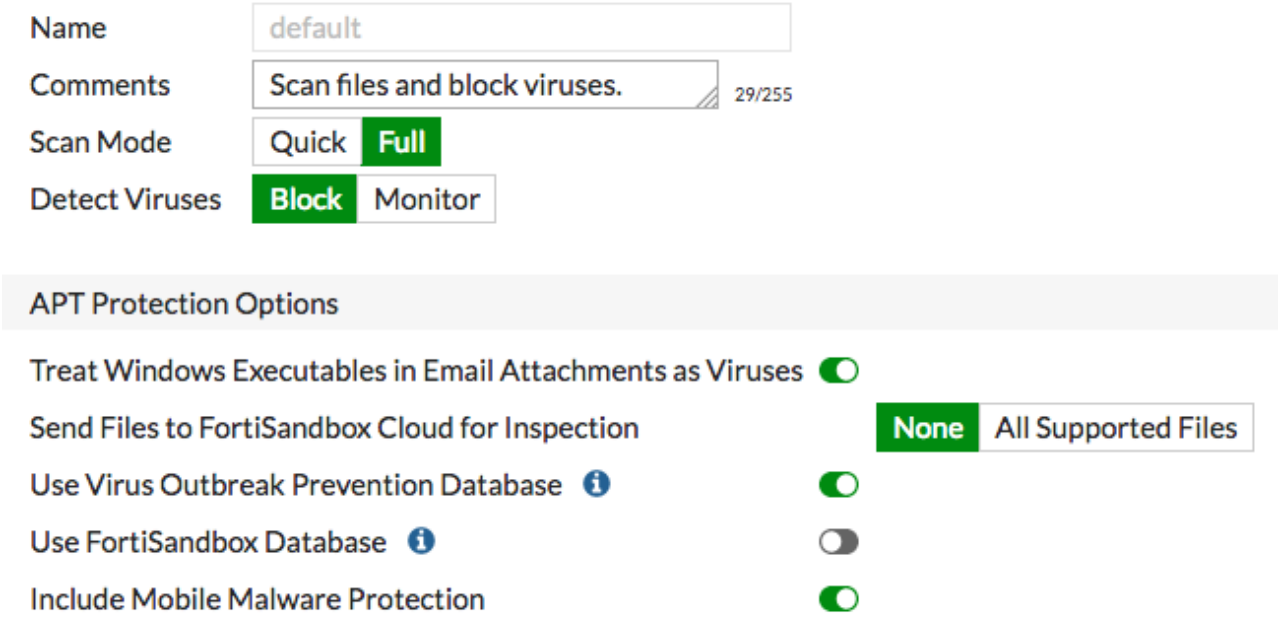


## Configuring the AntiVirus profile

1. Go to **System > Feature Visibility** and verify that **AntiVirus** is enabled under **Security Features**.



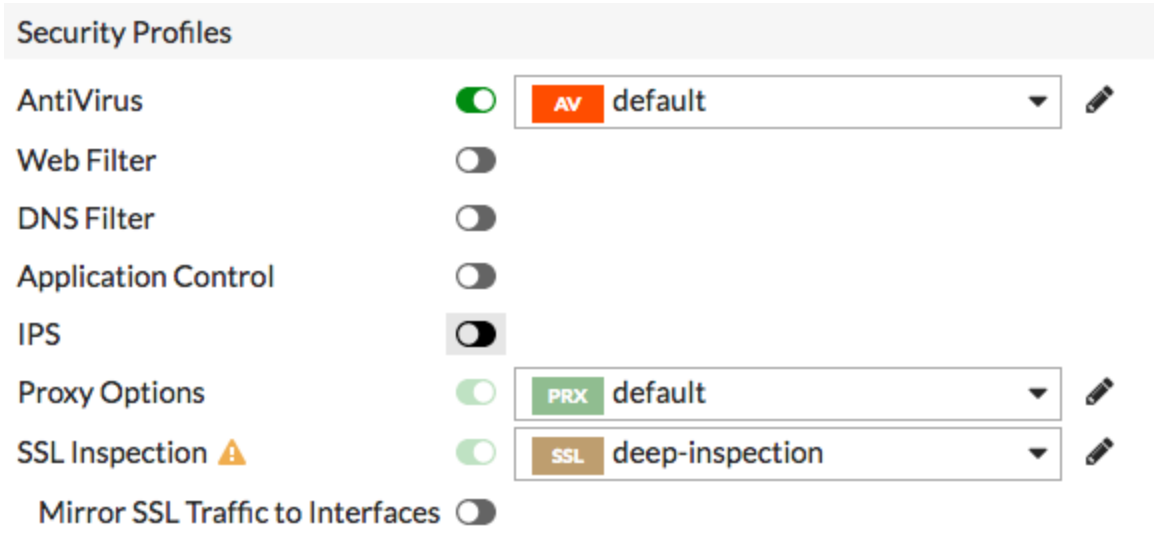

2. To edit the default antivirus profile, go to **Security > Profiles AntiVirus**.
3. Set **Scan Mode** to **Full** and **Detect Viruses** to **Block**.
4. Under **APT Protection Options**, enable **Use Virus Outbreak Prevention Database** to provide an additional layer of protection from early stage virus outbreaks.




## Enabling antivirus in a policy

Delete this text and replace it with your own content.

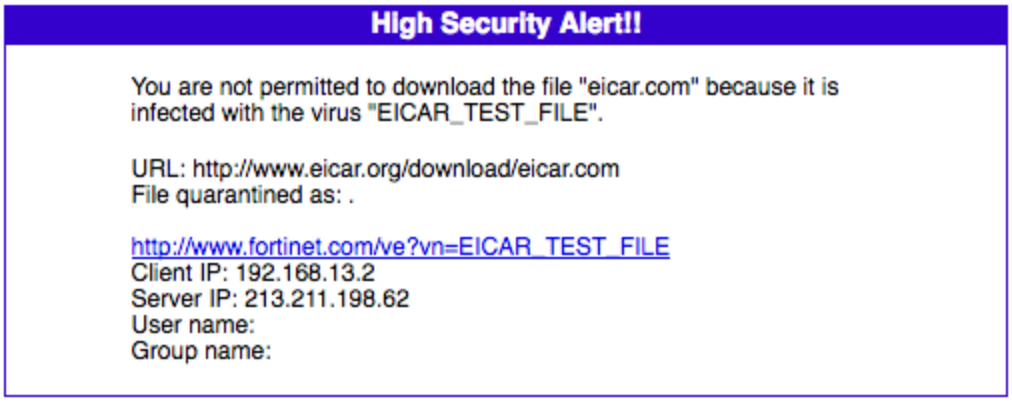
1. To edit your Internet access policy, go to **Policy & Objects > IPv4 Policy**.
2. Under **Security Profiles**, enable **AntiVirus** and select the **default** profile.
3. **SSL Inspection** is enabled by default. Select **deep-inspection**.



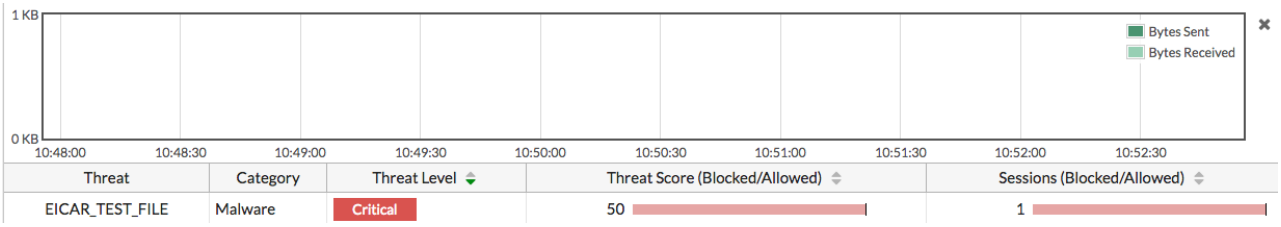

Using the deep-inspection profile may cause certificate errors. See **Preventing certification warnings** for more information.

## Results

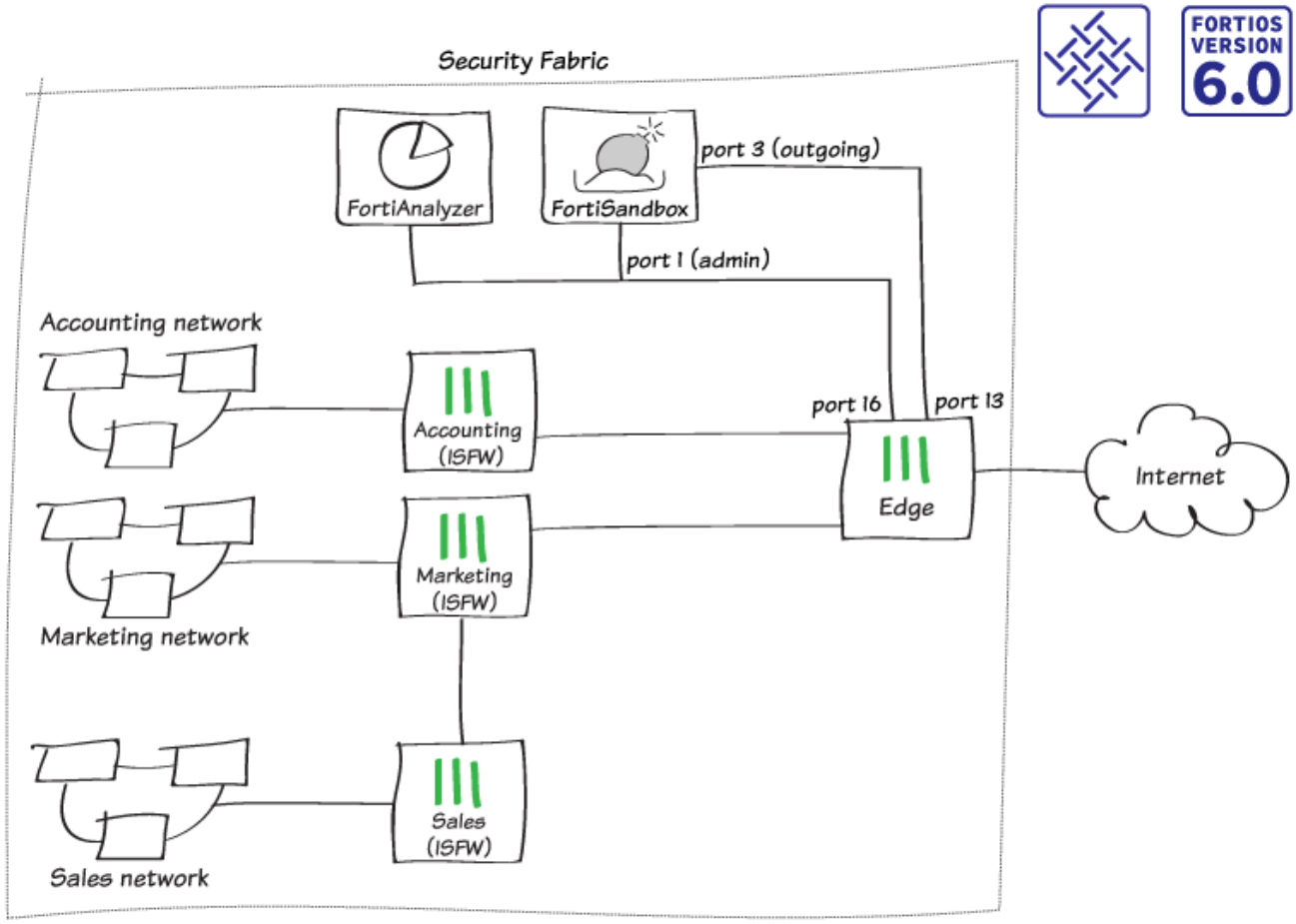
1. To test the antivirus scanning, go to www.eicar.org and attempt to download a test file. The browser will display a message denying permission to download the file.



2. To view information about the blocked file, go to **FortiView > Traffic from LAN/DMZ > Threats**.




# FortiSandbox in the Fortinet Security Fabric




In this recipe, you will add a FortiSandbox to the Fortinet Security Fabric and configure each FortiGate in the network to send suspicious files to FortiSandbox for sandbox inspection. The FortiSandbox scans and tests these files in isolation from your network.

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

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

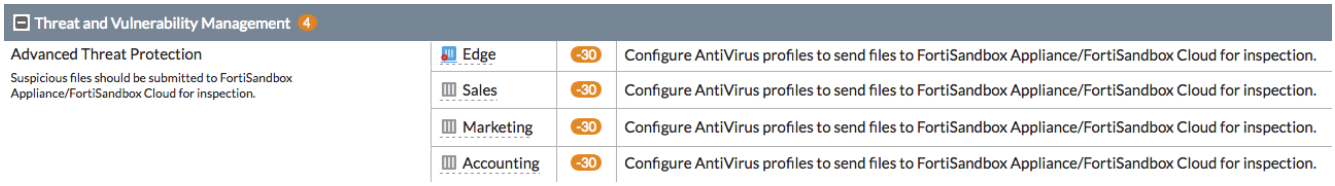
If possible, you can also use a separate Internet connection for FortiSandbox port 3, rather than connecting through the Edge FortiGate to use your main Internet connection. This configuration avoids having IP addresses from your main network blacklisted if malware that's tested on the FortiSandbox generates an attack. If you use this configuration, you can skip the steps listed for FortiSandbox port 3.

## Checking the Security Rating

On Edge (the root FortiGate in the Security Fabric), go to **Security Fabric > Security Rating**.

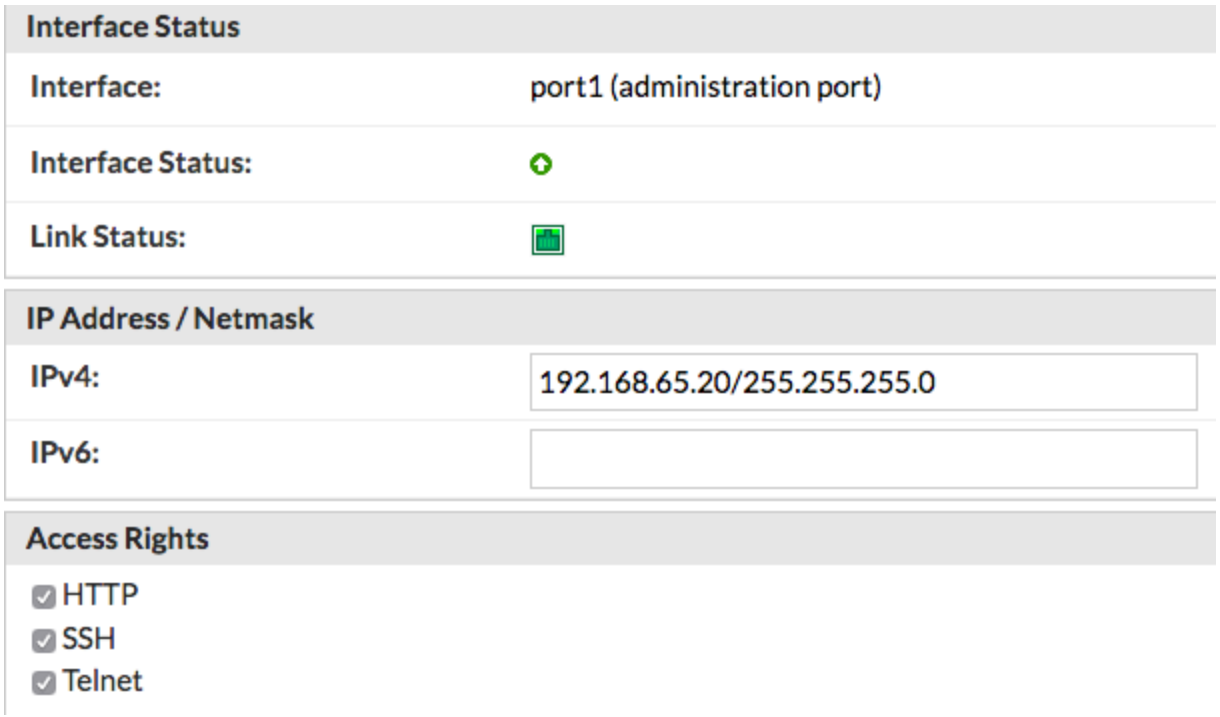
Since you haven't yet installed a FortiSandbox in your network, the Security Fabric fails the **Advanced Threat Protection** check.

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

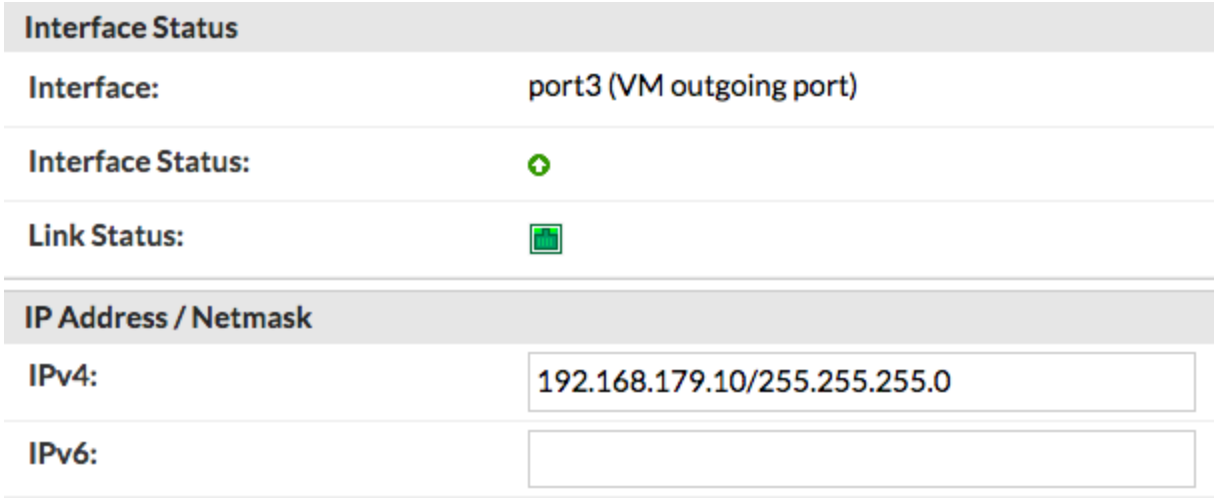



## Connecting the FortiSandbox and Edge

1. Connect to the FortiSandbox.
2. To edit **port1**, which is used for communication between the FortiSandbox and the rest of the Security Fabric, go to **Network > Interfaces**.
3. Set **IP Address/Netmask** to an internal IP address.
   In this example, the FortiSandbox connects to the same subnet as the FortiAnalyzer that you installed previously, using the IP address 192.168.65.20.

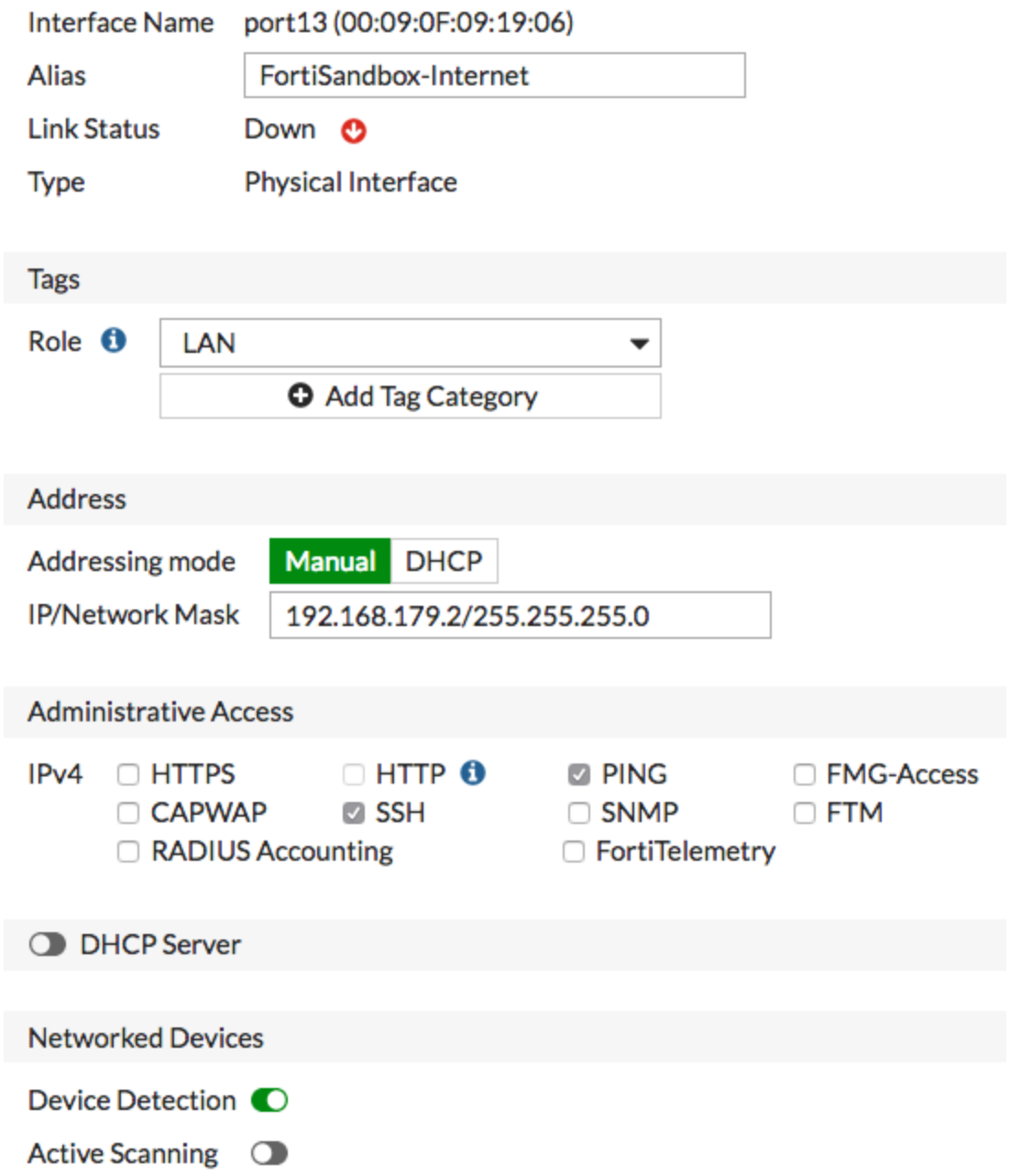



4. Edit **port3**.
   This port is used for outgoing communication by the virtual machines (VMs) running on the FortiSandbox. It's recommended that you connect this port to a dedicated interface on your FortiGate to protect the rest of the network from threats that the FortiSandbox is currently investigating.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




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

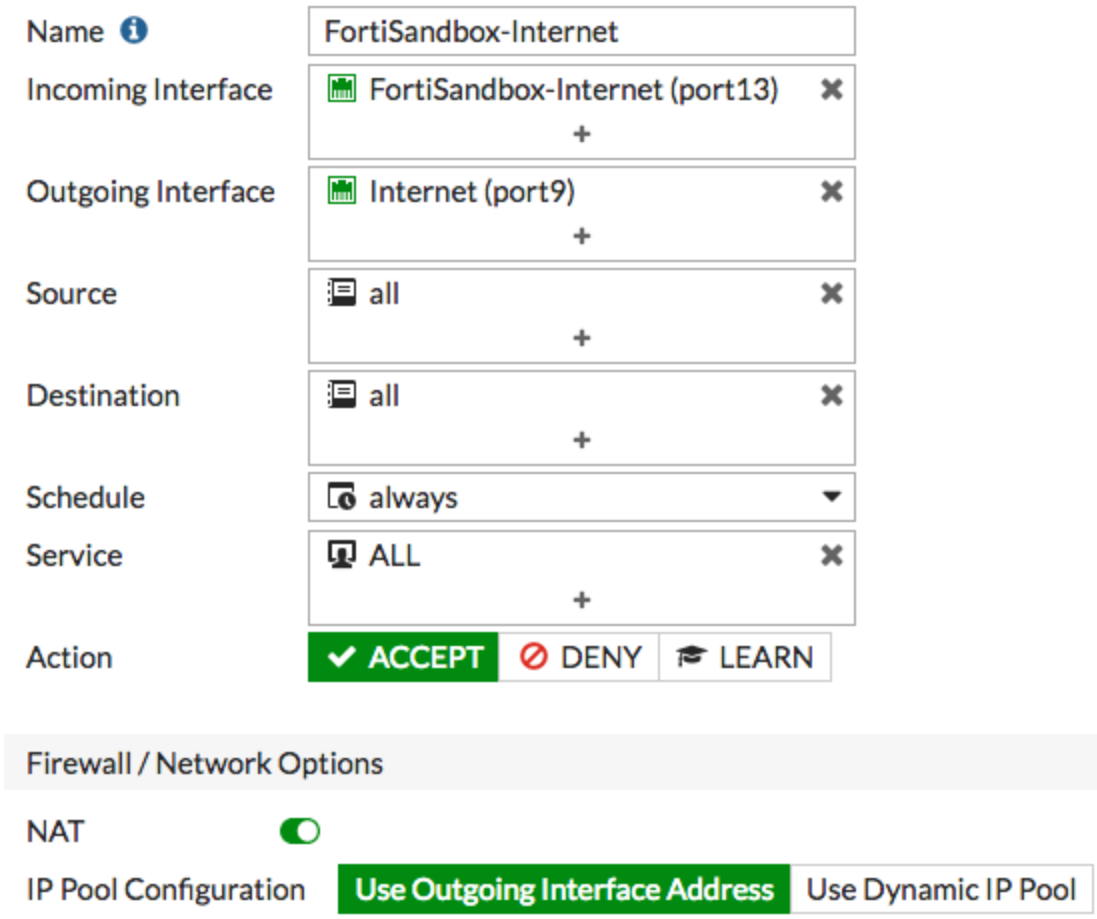
7. Connect to Edge.
8. To configure the port that connects to port3 on the FortiSandbox (in the example, **port13**), go to **Network > Interfaces**. Set **IP/Network Mask** to an address on the same subnet as port 3 on the FortiSandbox (in the example, 192.168.179.2/255.255.255.0)




9. Connect the FortiSandbox to the Security Fabric.

## Allowing VM Internet access

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




3. Connect to FortiSandbox.
4. 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.