FORTINET

The FortiGate Cookbook

Recipes for Success with your FortiGate

FortiOS 5.2

The FortiGate Cookbook 5.2

May-12-15

Fortinet Cookbook - http://cookbook.fortinet.com

Fortinet Knowledge Base - http://kb.fortinet.com

Technical Documentation - http://docs.fortinet.com

Video Tutorials - http://video.fortinet.com

Training Services - http://campus.training.fortinet.com

Technical Support - https://support.fortinet.com

Please report errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.

Table of Contents

Change Log

Date	Change description
May 12, 2015	Initial publication

Introduction

FortiGate is a network security appliance that can apply a number of features to your network traffic, providing a consolidated security solution to match the needs of any network, big or small.

The FortiGate recipes is divided into the following sections:

- Getting Started: recipes to help you start using your FortiGate.
- Security: recipes about using a FortiGate to protect your network.
- WiFi: recipes about managing a wireless network with your FortiGate.
- Authentication: recipes about authenticating users and devices on your network.
- VPNs: recipes about virtual private networks (VPNs), including authentication methods.
- IPv6: recipes about using Internet Protocol version 6 (IPv6).
- Fortinet Integration: recipes about using other Fortinet products alongside a FortiGate.
- Expert: recipes about advanced FortiGate configurations for users with a higher degree of background knowledge.

Some recipes are part of more than one of the above sections. When a recipe is part of multiple sections, it is located in the section that appears first in the Cookbook.

This version of the complete FortiGate cookbook was written using FortiOS 5.2.3.

Tips

Before you get started, here are a few tips about using the FortiGate Cookbook:

Understanding the basics

Some basic steps, such as logging into your FortiGate, are not included in most recipes. This information can be found in the QuickStart guide for your product.

Screenshots vs. text

The FortiGate Cookbook uses both screenshots and text to explain the steps of each example. The screenshots display the entire configuration, while the text highlights key details (i.e. the settings that are strictly necessary for the configuration) and provides additional information. To get the most out of the FortiGate Cookbook, start with the screenshots and then read the text for more details.

Model and firmware

GUI menus, options, and interface names may vary depending on the which model you are using and the firmware build.

For example, some FortiGate models do not have the menu option **Router > Static > Static Routes**.

Ports

The specific ports being used in the documentation are chosen as examples. When you are configuring your unit, you can substitute your own ports, provided that they have the same function.

For example, in most recipes, wan1 is the port used to provide the FortiGate with access to the Internet. If your FortiGate uses a different port for this function, you should use that port in the parts of the configuration that the recipe uses wan1.

IP addresses and object names

IP addresses are sometimes shown in diagrams to make it easier to see the source of the addresses used in the recipe. When you are configuring your product, substitute your own addresses. You should also use your own named for any objects, including user accounts, that are created as part of the recipe. Make names as specific as possible, to make it easier to determine later what the object is used for.

Text elements

Bold text indicates the name of a GUI field or feature. When required, *italic text* indicates information that you must enter.

Selecting OK/Apply

Always select **OK** or **Apply** when you complete a GUI step. Because this must be done frequently, it is an assumed step and is not included in most recipes.

IPv4 vs IPv6 policies

Most recipes in the FortiGate Cookbook use IPv4 security policies. However, the majority of them could also be done using IPv6 policies. If you wish to create an IPv6 policy, go to **Policy & Objects > Policy > IPv6**.

Turning on FortiOS features

Some FortiOS features can be turned off, which means they will not appear in the GUI. If an option required for a recipe does not appear, go to **System > Config > Features** and make sure that option is turned on.

Also, on some FortiGate models, certain features are only available using the CLI. For more information about this, see the Feature/Platform Matrix.

Getting Started

This section contains information about basic tasks to get a FortiGate unit up and running, including installation, as well common roles and configurations a FortiGate unit can have in your network.

Installation

- Choosing your FortiGate's switch mode
- Installing a FortiGate in NAT/Route mode
- Installing a FortiGate in Transparent mode
- Quick installation using DHCP
- Redundant Internet connections
- Troubleshooting your FortiGate installation

Setting up your FortiGate

- FortiGate registration and basic settings
- Updating your FortiGate's firmware
- Setting up FortiGuard services
- FortiGuard troubleshooting
- Logging FortiGate traffic
- Troubleshooting FortiGate logging
- Logging with FortiCloud
- Creating security policies
- Limited access administrator accounts
- Port pairing in Transparent mode

Common configurations

- Port forwarding
- FortiGuard DDNS
- SNMP monitoring
- Packet capture
- VDOM configuration
- High Availability with two FortiGates
- AirPlay for Apple TV
- Protect a web server with DMZ
- Traffic shaping for VoIP

Choosing your FortiGate's switch mode

This section contains information to help you determine which internal switch mode your FortiGate should use, a decision that should be made before the FortiGate is installed.

What is the internal switch mode?

The internal switch mode determines how the FortiGate's physical ports are managed by the FortiGate. The two main modes are Switch mode and Interface mode.

What are Switch mode and Interface mode and why are they used?

In Switch mode, all the internal interfaces are part of the same subnet and treated as a single interface, called either **lan** or **internal** by default, depending on the FortiGate model. Switch mode is used when the network layout is basic, with most users being on the same subnet.

In Interface mode, the physical interfaces of the FortiGate unit are handled individually, with each interface having its own IP address. Interfaces can also be combined by configuring them as part of either hardware or software switches, which allow multiple interfaces to be treated as a single interface. This mode is ideal for complex networks that use different subnets to compartmentalize the network traffic.

Which mode is your FortiGate in by default?

The default mode that a FortiGate starts in varies depending on the model. To determine which mode your FortiGate unit is in, go to **System > Network > Interfaces**. Locate the **lan** or **internal** interface. If the interface is listed as a **Physical Interface** in the **Type** column, then your FortiGate is in Switch mode. If the interface is a **Hardware Switch**, then your FortiGate is in Interface mode.

How do you change the mode?

If you need to change the mode your FortiGate unit is in, first make sure that none of the physical ports that make up the **lan** or **internal** interface are referenced in the FortiGate configuration. Then go to **System > Dashboard > Status** and enter either of the following commands into the **CLI Console**:

1. Command to change the FortiGate to switch mode:
```
config system global
    set internal-switch-mode switch
 exit
```
2. Command to change the FortiGate to interface mode:
```
config system global
    set internal-switch-mode interface
 exit
```

Installing a FortiGate in NAT/Route mode

In this example, you will learn how to connect and configure a new FortiGate unit in NAT/Route mode to securely connect a private network to the Internet.

In NAT/Route mode, a FortiGate unit is installed as a gateway or router between two networks. In most cases, it is used between a private network and the Internet. This allows the FortiGate to hide the IP addresses of the private network using network address translation (NAT).

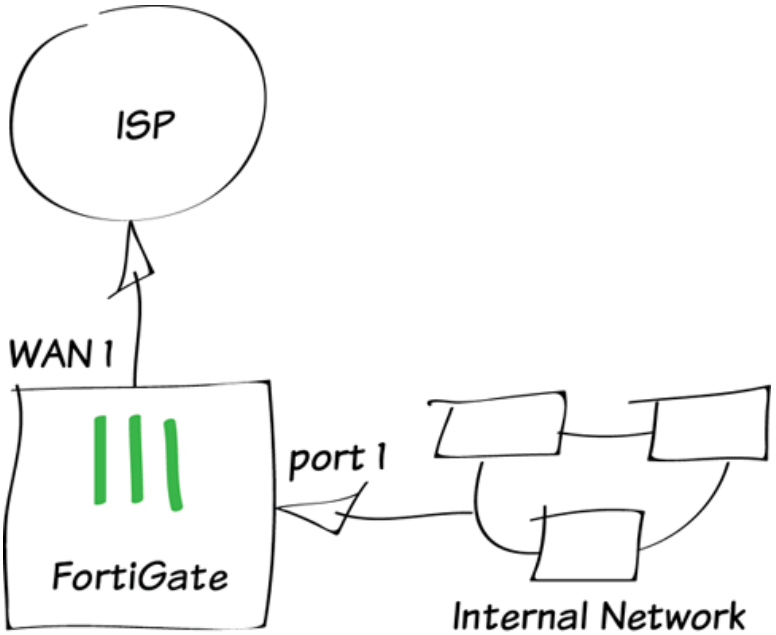
If you have not already done so, ensure that your FortiGate is using the correct internal switch mode. For more information, see Choosing your FortiGate's switch mode.

A video of this recipe is available here.

1. Connecting the network devices and logging onto the FortiGate

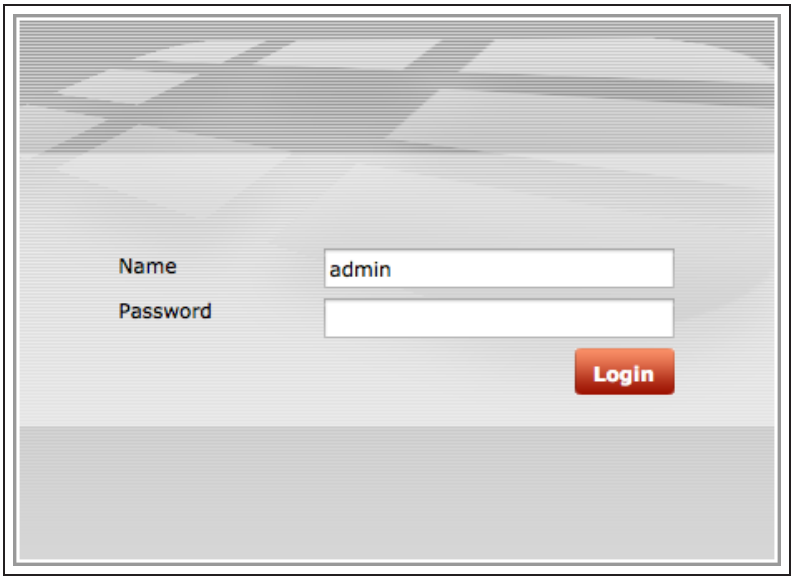
Connect the FortiGate's Internet-facing interface (typically WAN1) to your ISP-supplied equipment and Connect a PC to the FortiGate using an internal port (typically port 1).

Power on the ISP's equipment, the FortiGate unit, and the PC on the internal network.



From the PC on the internal network, connect to the FortiGate's web-based manager using either FortiExplorer or an Internet browser (for information about connecting to the web-based manager, please see your models QuickStart Guide).

Login using an admin account (the default admin account has the username admin and no password).



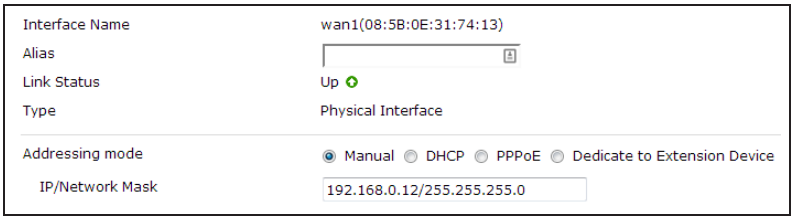
2. Configuring the FortiGate's interfaces

Go to **System > Network > Interfaces** and edit the Internet-facing interface.

If your FortiGate is directly connecting to your ISP, set **Addressing Mode** to **Manual** and set the **IP/Netmask** to the public IP address your ISP has provided you with.

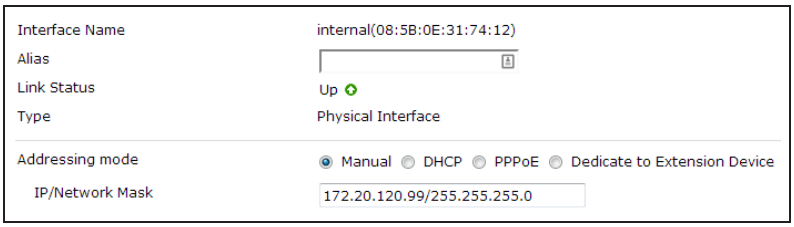
If have some ISP equipment between your FortiGate and the Internet (for example, a router), then the wan1 IP will also use a private IP assigned by the ISP equipment. If this equipment uses DHCP, set **Addressing Mode** to **DHCP** to get an IP assigned to the interface.

If the ISP equipment does not use DHCP, your ISP can provide you with the correct private IP to use for the interface.



Edit the **internal** interface (called **lan** on some FortiGate models).

Set **Addressing Mode** to **Manual** and set the **IP/Netmask** to the private IP address you wish to use for the FortiGate.

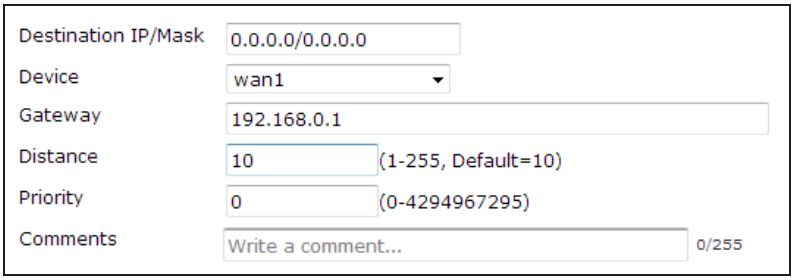


3. Adding a default route

Go to **Router > Static > Static Routes** (or **System > Network > Routing**, depending on your FortiGate model) and create a new route.

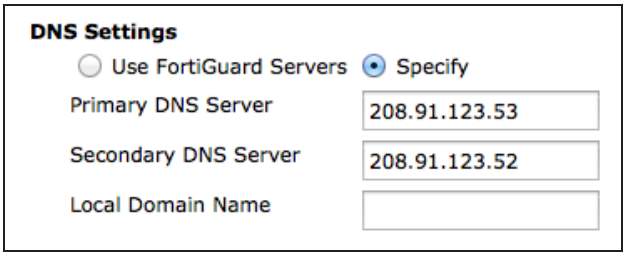
Set the **Destination IP/Mask** to *0.0.0.0/0.0.0.0*, the **Device** to the Internet-facing interface, and the **Gateway** to the gateway (or default route) provided by your ISP or to the next hop router, depending on your network requirements.

A default route always has a Destination IP/Mask of 0.0.0.0/0.0.0.0. Normally, you would have only one default route. If the static route list already contains a default route, you can edit it or delete it and add a new one.



4. (Optional) Setting the FortiGate's DNS servers

The FortiGate unit's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **System > Network > DNS** and add **Primary** and **Secondary** DNS servers.



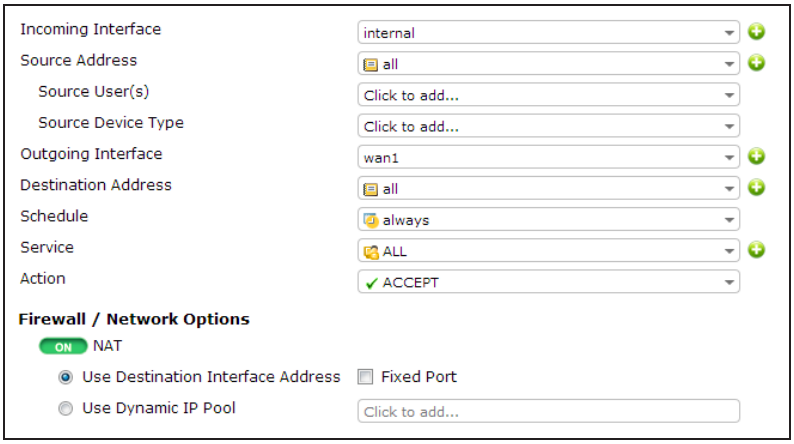
5. Creating a policy to allow traffic from the internal network to the Internet

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.

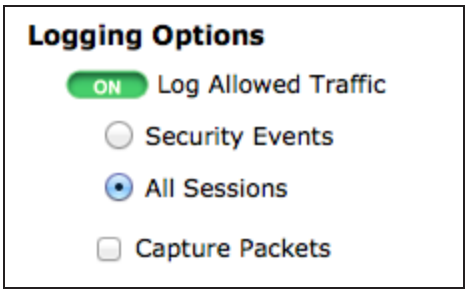
Go to **Policy & Objects > Policy > IPv4** and create a new policy (if your network uses IPv6 addresses, go to **Policy & Objects > Policy > IPv6**).

Set the **Incoming Interface** to the **internal** interface and the **Outgoing Interface** to the Internet-facing interface.

Make sure the **Action** is set to **ACCEPT**. Turn on **NAT** and make sure **Use Destination Interface Address** is selected (later versions of FortiOS 5.2 call this option **Use Outgoing Interface Address**).



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



6. Results

You can now browse the Internet using any computer that connects to the FortiGate's internal interface.

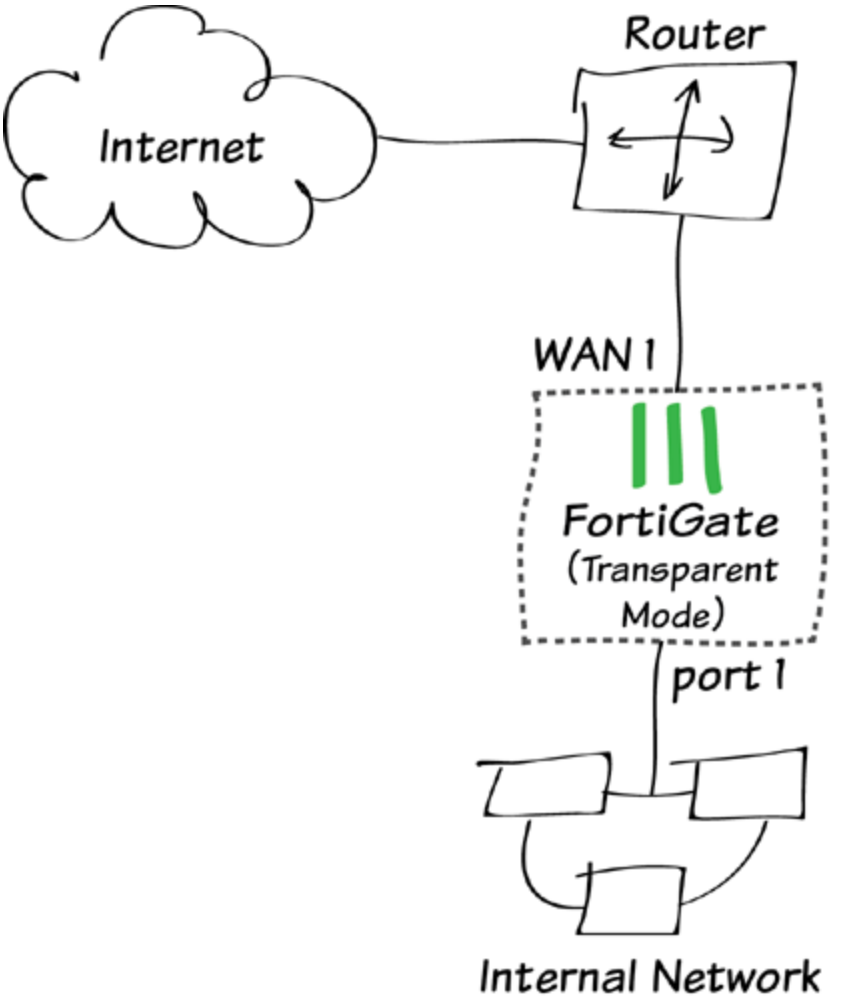
You can view information about the traffic being processed by your FortiGate by going to **System > FortiView > All Sessions** and finding traffic that has the **internal** interface as the **Src Interface** and the Internet-facing interface as the **Dst Interface**.

If these two columns are not shown, right-click on the title row, select **Src Interface** and **Dst Interface** from the dropdown menu, and then select **Apply**.

#		Date/Time	Dst Interfa...	Src Interfa...	Destination	Sent / Received
1		13:10:25	wan1	lan	8.247.14.128 (static.licdn.com)	1.10 KB / 640 B
2		13:10:25	wan1	lan	138.108.6.20 (secure-us.imrworldwide.com)	1.05 KB / 4.29 KB
3		13:10:24	wan1	lan	64.94.107.50 (map-pb.quantserve.com.akadns.net)	967 B / 444 B
4		13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	2.28 KB / 3.81 KB
5		13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	3.34 KB / 5.83 KB
6		13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	3.52 KB / 16.20 KB
7		13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	3.89 KB / 26.95 KB
8		13:10:21	wan1	lan	208.91.114.158 (blog.fortinet.com)	6.03 KB / 32.48 KB
9		13:10:20	wan1	lan	208.91.114.158 (blog.fortinet.com)	1.26 KB / 2.22 KB
10		13:10:19	wan1	lan	8.247.14.128 (static.licdn.com)	1.46 KB / 885 B
11		13:10:19	wan1	lan	64.94.107.50 (map-pb.quantserve.com.akadns.net)	1.58 KB / 710 B
12		13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	5.71 KB / 3.19 KB
13		13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	5.54 KB / 3.19 KB
14		13:10:17	wan1	lan	194.122.82.32 (www.google.ca)	184 B / 92 B
15		13:10:17	wan1	lan	194.122.82.32 (www.google.ca)	184 B / 92 B
16		13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	4.98 KB / 2.80 KB
17		13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	8.01 KB / 4.69 KB
18		13:10:17	wan1	lan	8.247.14.128 (static.licdn.com)	5.96 KB / 3.17 KB
19		13:10:16	wan1	lan	64.94.107.50 (map-pb.quantserve.com.akadns.net)	1.02 KB / 496 B
20		13:10:16	wan1	lan	173.194.43.84 (www.google.com)	272 B / 164 B

For further reading, check out Installing a FortiGate in NAT/Route Mode in the FortiOS 5.2 Handbook.

Installing a FortiGate in Transparent mode



In this example, you will learn how to connect and configure a new FortiGate unit in Transparent mode to securely connect a private network to the Internet. In Transparent mode, the FortiGate applies security scanning to traffic without applying routing or network address translation (NAT).

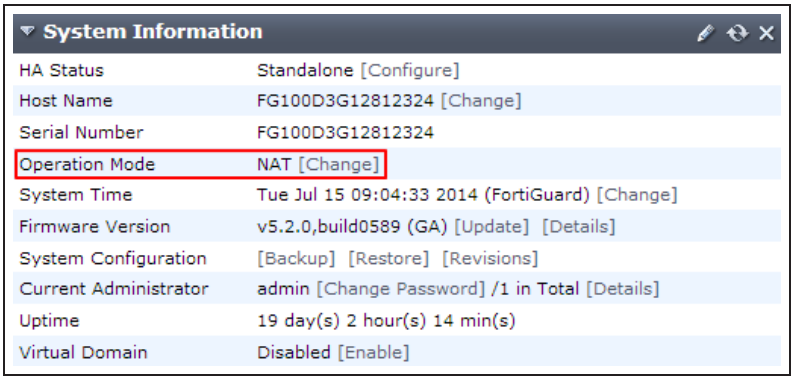
Warning: Changing to Transparent mode removes most configuration changes made in NAT/Route mode. To keep your current NAT/Route mode configuration, backup the configuration using the **System Information** widget, found at **System > Dashboard > Status**.

A video of this recipe is available here.

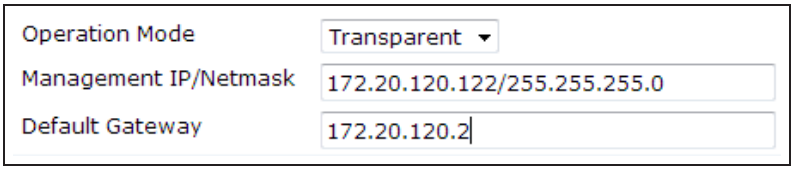
1. Changing the FortiGate's operation mode

Go to **System > Dashboard > Status** and locate the **System Information** widget.

Beside **Operation Mode**, select **Change**.



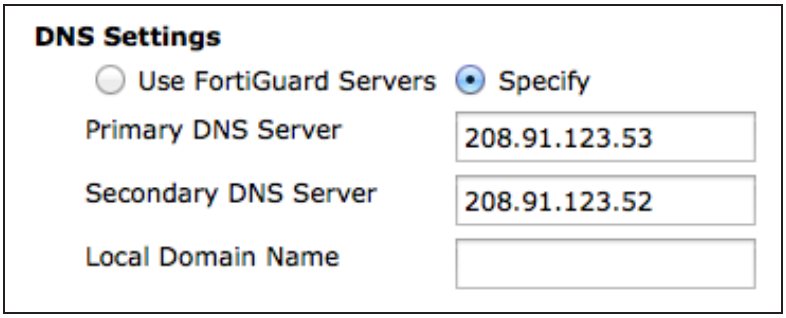
Set the **Operation Mode** to **Transparent**. Set the **Management IP/Netmask** and **Default Gateway** to connect the FortiGate unit to the internal network.



You can now access the GUI by browsing to the Management IP (in the example, you would browse to *http://172.20.120.122*).

2. (Optional) Setting the FortiGate's DNS servers

The FortiGate unit's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **System > Network > DNS** and add **Primary** and **Secondary** DNS servers.

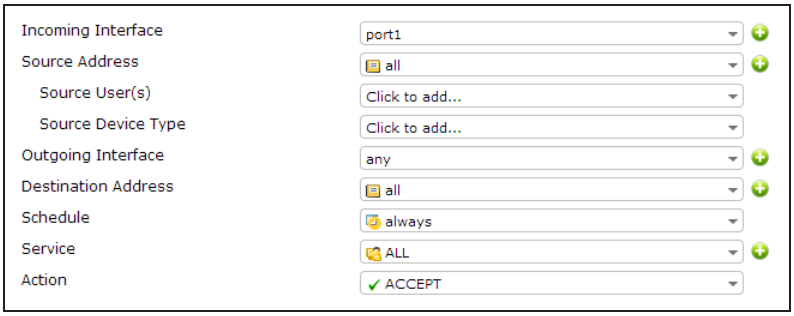


3. Creating a policy to allow traffic from the internal network to the Internet

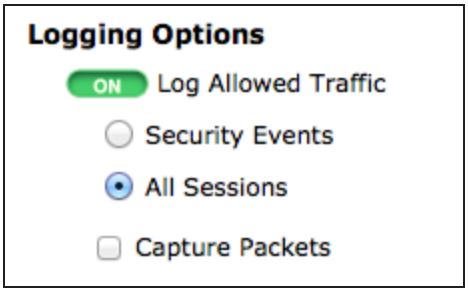
Go to **Policy & Objects > Policy > IPv4** and create a new policy (if your network uses IPv6 addresses, go to **Policy & Objects > Policy > IPv6**).

Set the **Incoming Interface** to the an available external interface (typically port 1) and the **Outgoing Interface** to the Internet-facing interface (typically WAN1).

It is recommended to avoid using any security profiles until after you have successfully installed the FortiGate unit. After the installation is verified, you can apply any required security profiles.

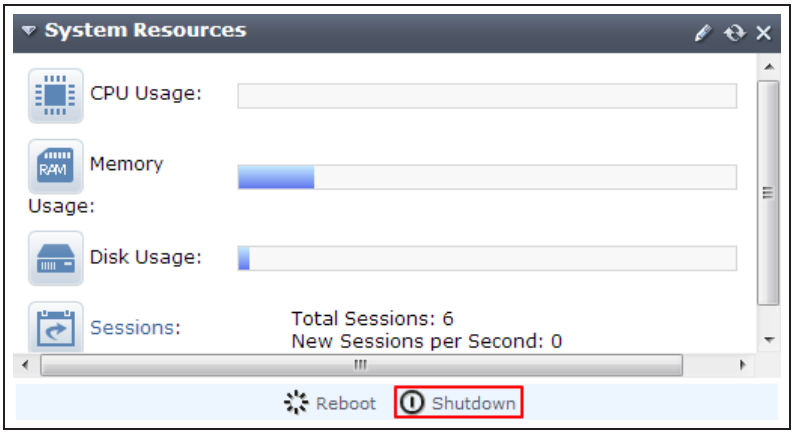


Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.



4. Connecting the network devices

Go to **System > Dashboard > Status** and locate the **System Resources** widget. Select **Shutdown** to power off the FortiGate unit.



Alternatively, you can enter the following command in the **CLI Console** (also found by going to **System > Dashboard > Status**):

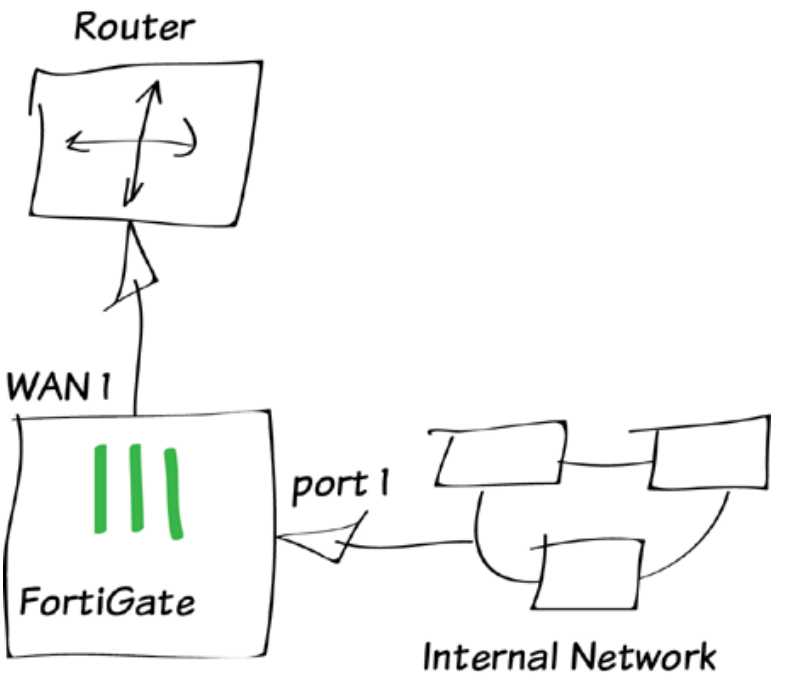
```
execute shutdown
```

Wait until all the lights, except for the power light, on your FortiGate have turned off. If your FortiGate has a power button, use it to turn the unit off. Otherwise, unplug the unit.

You can now connect the FortiGate unit between the internal network and the router.

Connect the wan1 interface to the router internal interface and connect the internal network to the FortiGate internal interface port.

Power on the FortiGate unit.



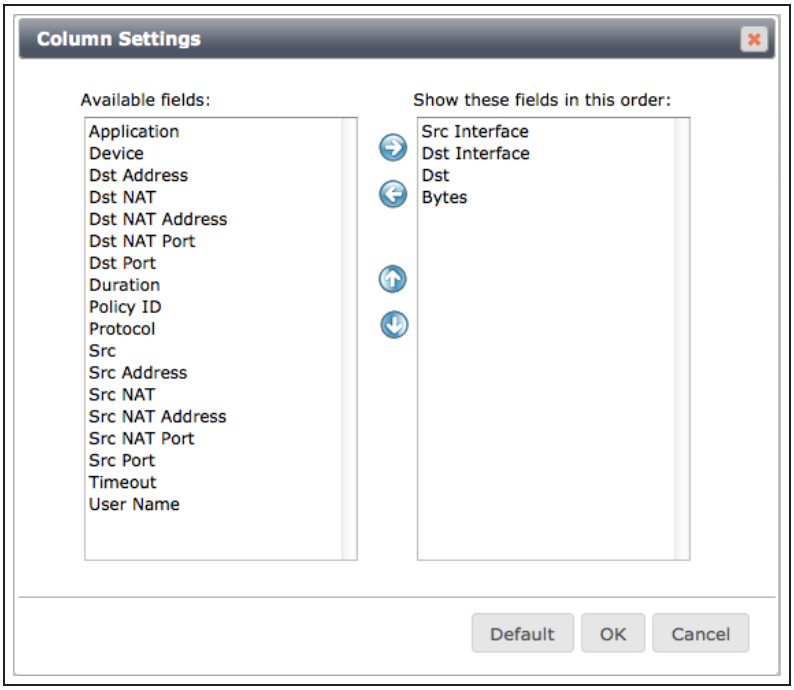
5. Results

You can now browse the Internet using any computer that connects to the FortiGate's internal interface.

You can view information about the traffic being processed by your FortiGate by going to **System > FortiView > All Sessions** and finding traffic that has port 1 as the **Src Interface** and the Internet-facing interface as the Dst Interface.

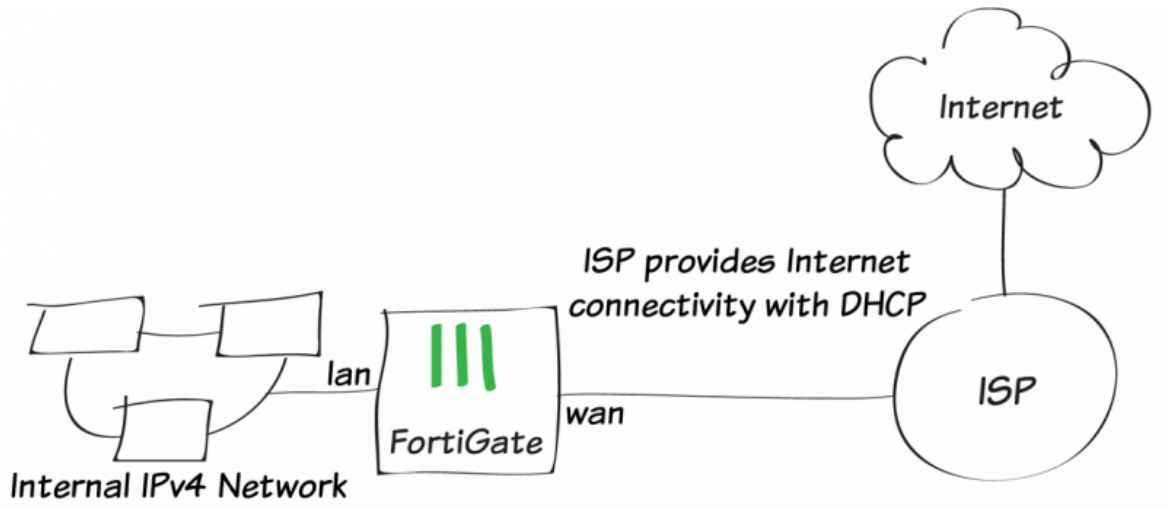
#	Src Interface	Dst Interface	Dst	Bytes (Sent/Received)
1	wan1	wan1	172.20.120.122	6,567
2	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	236
3	port1	wan1	s.yimg.com (68.142.250.160:443)	1,026,162
4	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	262
5	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	291
6	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	178
7	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	204
8	port1	wan1	safebrowsing-cache.google.com (184.150.152.152:443)	10,721
9	port1	wan1	BN1WNS1011410.wns.windows.com (157.56.98.65:443)	7,903
10	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	211
11	port1	wan1	google-public-dns-a.google.com (8.8.8.8:53)	385
12	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	226
13	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	173
14	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	413
15	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	204
16	port1	wan1	safebrowsing-cache.google.com (184.150.152.178:443)	876,026
17	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	184
18	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	441
19	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	212
20	port1	wan1	google-public-dns-b.google.com (8.8.4.4:53)	204

If these two columns are not shown, select **Column Settings** and move **Src Interface** and **Dst Interface** to the list of fields to be shown.



For further reading, check out Installation in the FortiOS 5.2 Handbook.

Quick installation using DHCP



In this example, you will use DHCP and your FortiGate's default configuration to securely connect your internal network to the Internet in two simple steps.

This recipe has the following requirements:

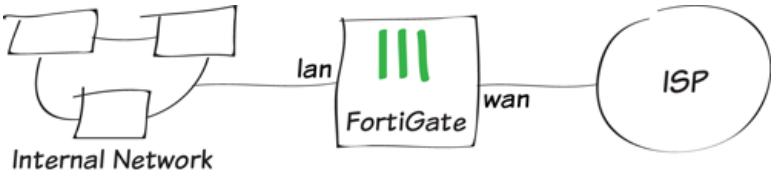
- An ISP that provides connectivity with DHCP and accepts DHCP requests without authentication.
- A FortiGate with a default configuration that includes a DHCP server on the lan (or internal) interface and a security policy that securely allows all sessions from the Internal network to reach the Internet.
- Your network uses IPv4 to connect to the FortiGate and Internet.

1. Connecting the FortiGate to your ISP and the internal network

Connect the FortiGate **wan** interface to your ISP-supplied equipment.

Connect the internal network to the FortiGate's default **lan** or **internal** interface.

Turn on the ISP's equipment, the FortiGate unit, and the PCs on the internal network.



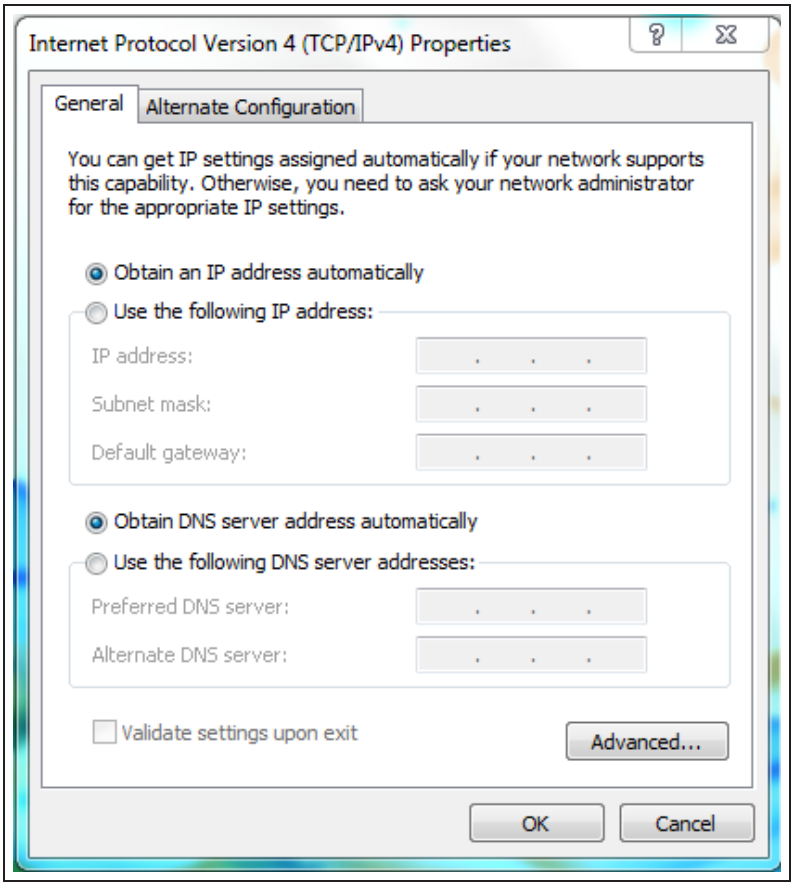
2. Configuring your PCs to use DHCP

Windows Vista/7/8:

Go to **Network and Sharing Center** and select **Local Area Connections**. Select **Properties**.

Select **Internet Protocol Version 4 (TCP/IPv4)**, then select **Properties**.

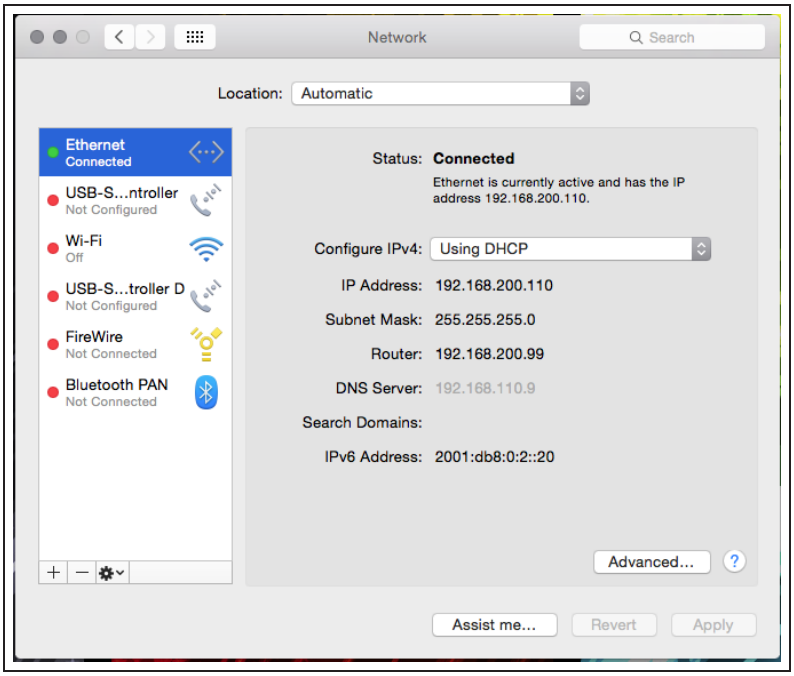
Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



Mac OS X

Go to **Network Preferences** and select **Ethernet**.

Set **Configure IPv4** to **Using DHCP**.



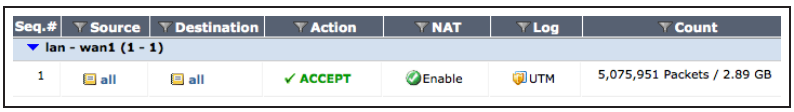
3. Results

From any PC on the internal network, open a web browser and browse to any website. You can successfully connect to the Internet.

Go to **Policy & Objects > IPv4 > Policy**. Your Internet-access policy is at the top of list, in the **lan - wan** section (this section's name varies based on the FortiGate model).

View the **Count** column, which displays the total amount of traffic that has used this policy since the FortiGate's last reboot. The column should display results, showing that the policy is being used for traffic.

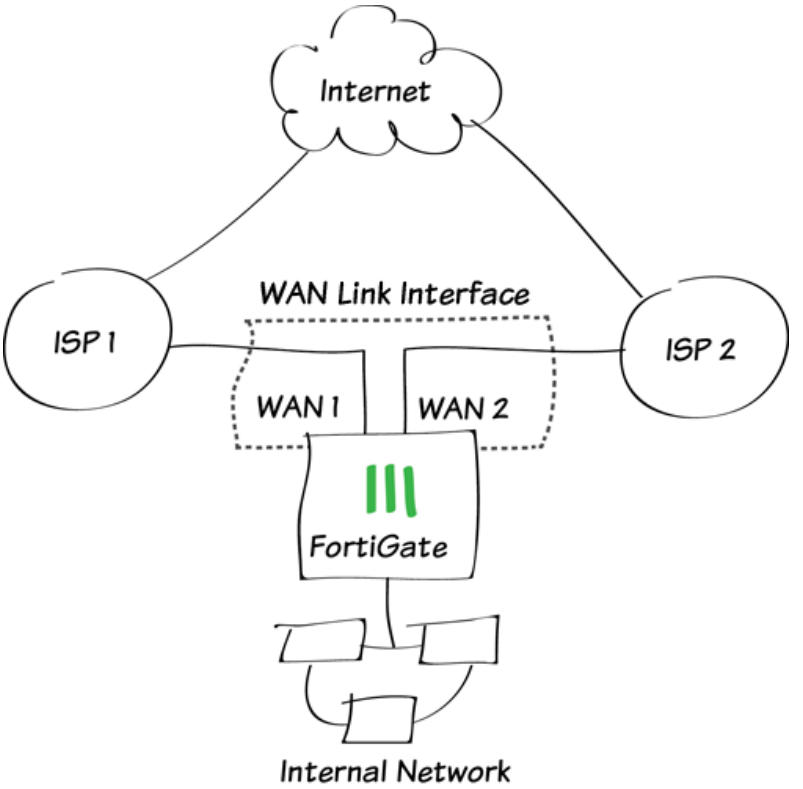
If this column is not visible, right-click on the title row, select **Count**, then **Apply**.



Seq.#	Source	Destination	Action	NAT	Log	Count
lan - wan1 (1 - 1)						
1	all	all	✓ ACCEPT	Enable	UTM	5,075,951 Packets / 2.89 GB

For further reading, check out Installation in the FortiOS 5.2 Handbook.

Redundant Internet connections



In this example, you will create a WAN link interface that provides your FortiGate unit with redundant Internet connections from two Internet service providers (ISPs). The WAN link interface combines these two connections into a single interface.

This example includes weighted load balancing so that most of your Internet traffic is handled by one ISP.

A video of this recipe can be found here.

1. Connecting your ISPs to the FortiGate

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

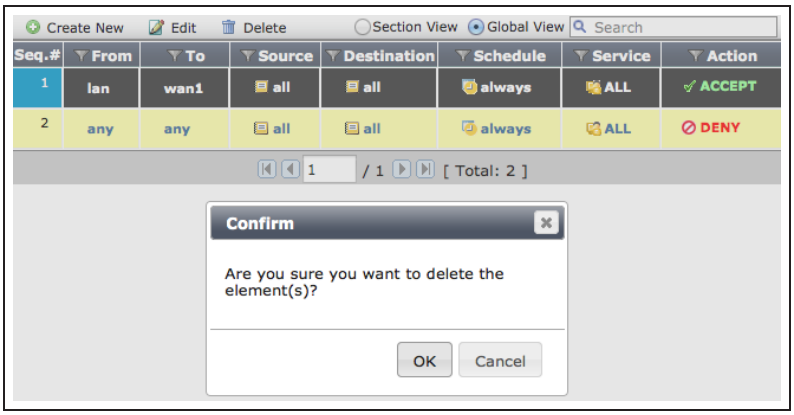
2. Deleting security policies and routes that use WAN1 or WAN2

You will not be able to add an interface to the WAN link interface if it is already used in the FortiGate's configuration, so you must delete any policies or routes that use either WAN1 or WAN2.

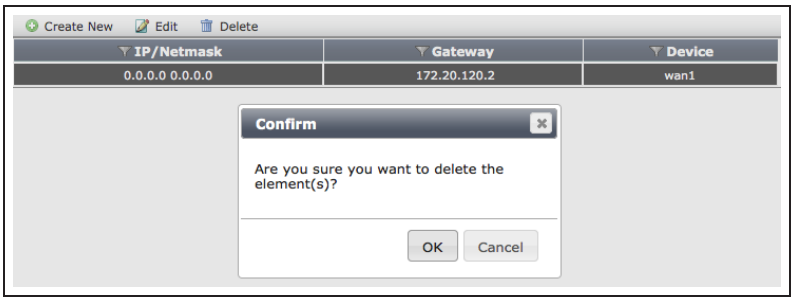
Many FortiGate models include a default Internet access policy that uses WAN1. This policy must also be deleted.

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

After you remove these policies, traffic will no longer be able to reach WAN1 or WAN2 through the FortiGate.



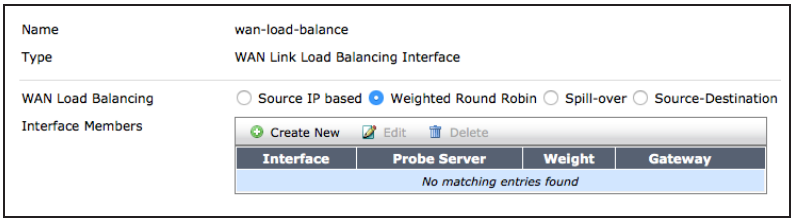
Go to **Router > Static > Static Routes** and delete any routes that use WAN1 or WAN2.



3. Creating a WAN link interface

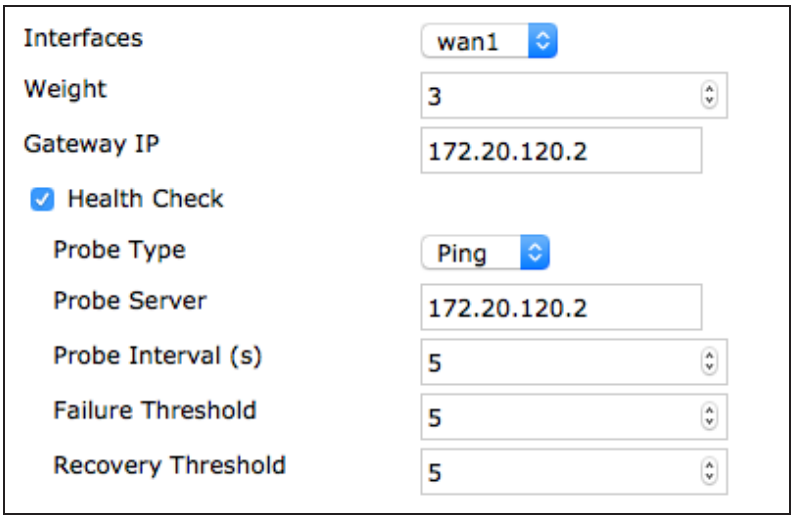
Go to **System > Network > WAN Link Load Balancing**.

Set **WAN Load Balancing** to **Weighted Round Robin**. This will allow you to prioritize the WAN1 interface so that more traffic uses it.



Add WAN1 to the list of **Interface Members**, set **Weight** to 3, and set it to use the **Gateway IP** provided by your ISP.

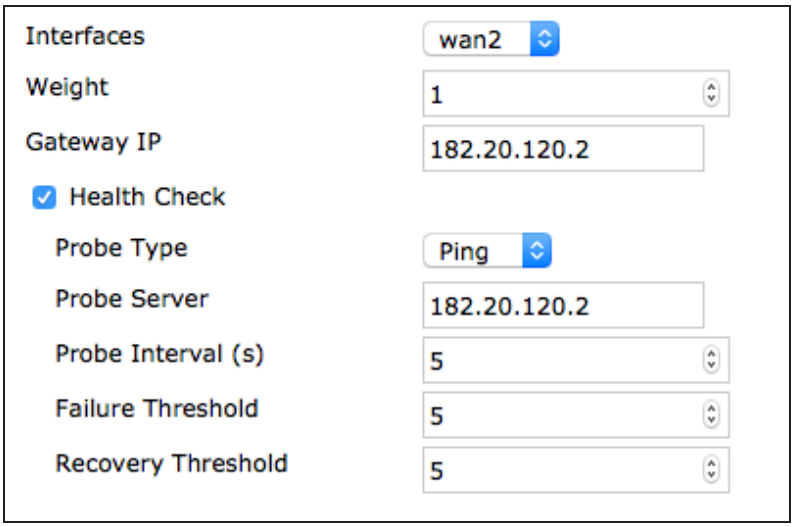
You can optionally configure **Health Check** to verify that WAN1 can connect to the Internet.



Do the same for WAN2, but instead set **Weight** to 1.

You can optionally configure **Health Check** to verify that WAN2 can connect to the Internet.

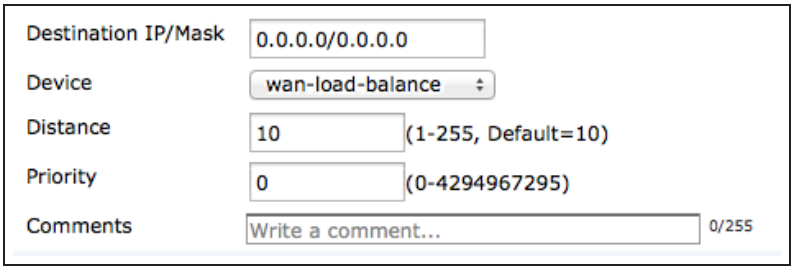
The weight settings will cause 75% of traffic to use WAN1, with the remaining 25% using WAN2.



4. Creating a default route for the WAN link interface

Go to **Router > Static > Static Routes** and create a new default route.

Set **Device** to the WAN link interface.

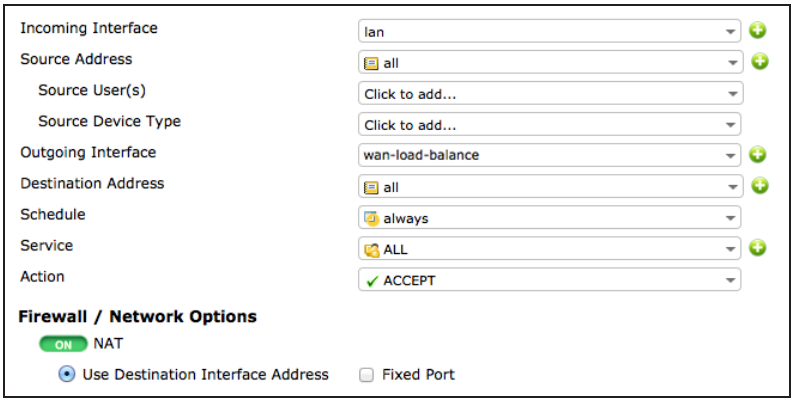


5. Allowing traffic from the internal network to the WAN link interface

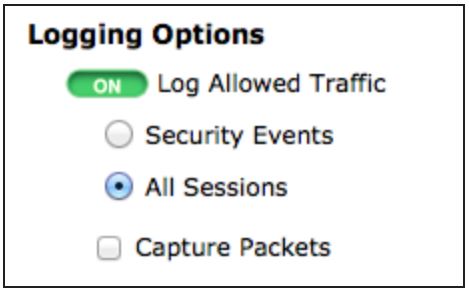
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to your internal network's interface and set **Outgoing Interface** to the WAN link interface.

Turn on **NAT**.



Scroll down to view the Logging Options. To view the results later, turn on Log Allowed Traffic and select All Sessions.



6. Results

Browse the Internet using a PC on the internal network and then go to **System > FortiView > All Sessions**.

Ensure that the **Dst Interface** column is visible in the traffic log. If it is not shown, right-click on the title row and select **Dst Interface** from the dropdown menu. Scroll to the bottom of the menu and select **Apply**.

The log shows traffic flowing through both WAN1 and WAN2.

#	Src Interface	Src	Dst Interface	Bytes (Sent/Received)
1	lan	192.168.200.114:54819	wan2	50,909
2	lan	192.168.200.114:54835	wan1	50,839
3	lan	192.168.200.114:54803	wan2	69,529
4	lan	192.168.200.114:54787	wan1	257,587
5	lan	192.168.200.114:54891	wan1	1,971
6	lan	192.168.200.114:54987	wan2	1,436
7	lan	192.168.200.114:54931	wan1	3,086

Disconnect the WAN1 port, continue to browse the Internet, and refresh the traffic log. All traffic is now flowing through WAN2, until you reconnect WAN1.

#	Src Interface	Src	Dst Interface	Bytes (Sent/Received)
1	lan	192.168.200.114:55491	wan2	286
2	lan	192.168.200.114:63123	wan2	365
3	lan	192.168.200.114:34499	wan2	434
4	lan	192.168.200.114:35923	wan2	362
5	lan	192.168.200.114:37443	wan2	353
6	lan	192.168.200.114:63555	wan2	100

For further reading, check out Installing a FortiGate in NAT/Route Mode in the FortiOS 5.2 Handbook.

Troubleshooting your FortiGate installation

If your FortiGate does not function as desired after completing the installation, try the following troubleshooting methods.

Most methods can be used for both FortiGates in both NAT/Route and Transparent mode. Any exceptions are marked.

1. Use FortiExplorer if you can't connect to the FortiGate over Ethernet.

If you can't connect to the FortiGate GUI or CLI, you may be able to connect using FortiExplorer. See your FortiGate unit's QuickStart Guide for details.

2. Check for equipment issues.

Verify that all network equipment is powered on and operating as expected. Refer to the QuickStart Guide for information about connecting your FortiGate to the network. You will also find detailed information about the FortiGate unit LED indicators.

3. Check the physical network connections.

Check the cables used for all physical connections to ensure that they are fully connected and do not appear damaged, and make sure that each cable connects to the correct device and the correct Ethernet port on that device. Also, check the Unit Operation widget, found at **System > Dashboard > Status**, to make sure the connected interfaces are shown in green.

4. Verify that you can connect to the internal IP address of the FortiGate unit (NAT/Route mode).

Connect to the web-based manager from the FortiGate's internal interface by browsing to its IP address. From the PC, try to ping the internal interface IP address; for example, `ping 192.168.1.99`.

If you cannot connect to the internal interface, verify the IP configuration of the PC. If you can ping the interface but can't connect to the web-based manager, check the settings for administrative access on that interface.

5. Verify that you can connect to the management IP address of the FortiGate unit (Transparent mode).

From the internal network, attempt to ping the management IP address. If you cannot connect to the internal interface, verify the IP configuration of the PC and make sure the cables are connected and all switches and other devices on the network are powered on and operating. Go to the next step when you can connect to the internal interface.

6. Check the FortiGate interface configurations (NAT/Route mode).

Check the configuration of the FortiGate interface connected to the internal network, and check the configuration of the FortiGate interface that connects to the Internet to make sure **Addressing Mode** is set to the correct mode.

7. Verify the security policy configuration.

Go to **Policy & Objects > Policy > IPv4** (or **Policy & Objects > Policy > IPv6**) and verify that the internal interface to Internet-facing interface security policy has been added and is located near the top of the policy list. Check the **Sessions** column to ensure that traffic has been processed (if this column does not appear, right-click on the title row, select **Sessions**, and select **Apply**).

If you are using NAT/Route mode, check the configuration of the policy to make sure that **NAT** is turned on and that **Use Destination Interface Address** is selected (later versions of FortiOS 5.2 call this option **Use Outgoing Interface Address**).

8. Verify that you can connect to the Internet-facing interface's IP address (NAT/Route mode).

Ping the IP address of the FortiGate's Internet-facing interface. If you cannot connect to the interface, the FortiGate unit is not allowing sessions from the internal interface to Internet-facing interface.

9. Verify the static routing configuration (NAT/Route mode).

Go to **Router > Static > Static Routes** (or **System > Network > Routing**) and verify that the default route is correct. View the **Routing Monitor** (found either on the same page or at **Router > Monitor > Routing Monitor**) and verify that the default route appears in the list as a static route. Along with the default route, you should see two routes shown as **Connected**, one for each connected FortiGate interface.

10. Verify that you can connect to the gateway provided by your ISP.

Ping the default gateway IP address from a PC on the internal network. If you cannot reach the gateway, contact your ISP to verify that you are using the correct gateway.

11. Verify that you can communicate from the FortiGate unit to the Internet.

Access the FortiGate CLI and use the command `execute ping 8.8.8.8`. You can also use the `execute traceroute 8.8.8.8` command to troubleshoot connectivity to the Internet.

12. Verify the DNS configurations of the FortiGate unit and the PCs.

Check for DNS errors by pinging or using traceroute to connect to a domain name; for example: `ping www.fortinet.com`. If the name cannot be resolved, the FortiGate unit or PC cannot connect to a DNS server and you should confirm that the DNS server IP addresses are present and correct.

13. Confirm that the FortiGate unit can connect to the FortiGuard network.

Once registered, the FortiGate unit obtains antivirus and application control and other updates from the FortiGuard network. Once the FortiGate unit is on your network, confirm that it can reach FortiGuard.

First, check the License Information widget to make sure that the status of all FortiGuard services matches the services that you have purchased. Go to **System > Config > FortiGuard**. Expand **Web Filtering and Email Filtering Options** and select **Test Availability**. After a minute, the GUI should show a successful connection.

14. Consider changing the MAC address of your external interface (NAT/Route mode).

Some ISPs do not want the MAC address of the device connecting to their network cable to change and so you may have to change the MAC address of the Internet-facing interface using the following CLI command:

Some ISPs do not want the MAC address of the device connecting to their network cable to change and so you may have to change the MAC address of the Internet-facing interface using the following CLI command:

```
config system interface
   edit
      set macaddr
   end
end
```

15. Check the FortiGate bridge table (Transparent mode).

When the FortiGate is in Transparent mode, the unit acts like a bridge sending all incoming traffic out on the other interfaces. The bridge is between interfaces on the FortiGate unit. Each bridge listed is a link between interfaces. Where traffic is flowing between interfaces, you expect to find bridges listed. If you are having connectivity issues, and there are no bridges listed that is a likely cause. Check for the MAC address of the interface or device in question.

To list the existing bridge instances on the FortiGate unit, use the following CLI command:

```
diagnose netlink brctl name host root.b
show bridge control interface root.b host.
fdb: size=2048, used=25, num=25, depth=1
Bridge root.b host table
```

```
port no device devname mac addr ttl attributes
3 4 wan1 00:09:0f:cb:c2:77 88
3 4 wan1 00:26:2d:24:b7:d3 0
3 4 wan1 00:13:72:38:72:21 98
4 3 internal 00:1a:a0:2f:bc:c6 6
1 6 dmz 00:09:0f:dc:90:69 0 Local Static
3 4 wan1 c4:2c:03:0d:3a:38 81
3 4 wan1 00:09:0f:15:05:46 89
3 4 c4:2c:03:1d:1b:10 0
2 5 wan2 00:09:0f:dc:90:68 0 Local Static
```

If your device's MAC address is not listed, the FortiGate unit cannot find the device on the network. Check the device's network connections and make sure they are connected and operational.

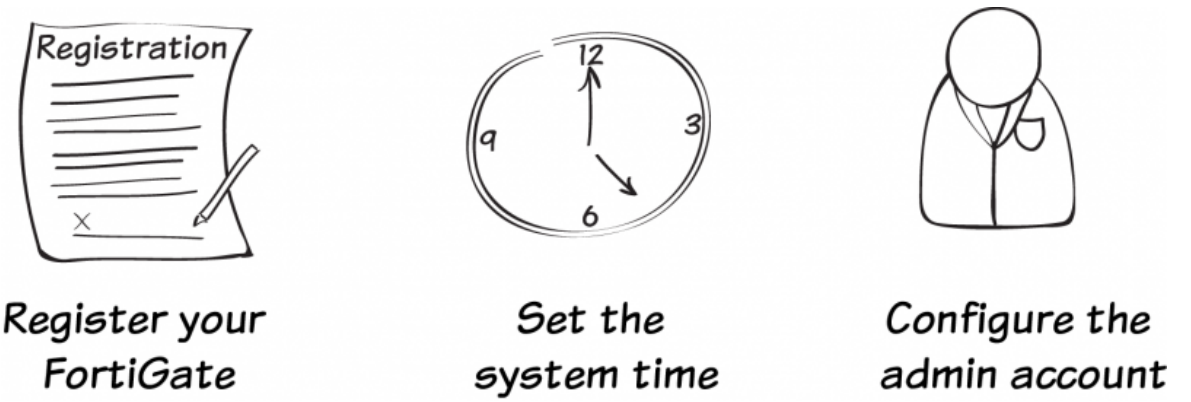
16. Either reset the FortiGate unit to factory defaults or contact the technical assistance center.

If all else fails, reset the FortiGate unit to factory defaults using the CLI command `execute factoryreset`. When prompted, type `y` to confirm the reset.

Resetting the FortiGate unit to factory defaults puts the unit back into NAT/Route mode.

You can also contact the technical assistance center. For contact information, go to support.fortinet.com.

FortiGate registration and basic settings



In this example, you will register your FortiGate unit and set the system time. You will also configure several administrative account settings to prevent unauthorized access.

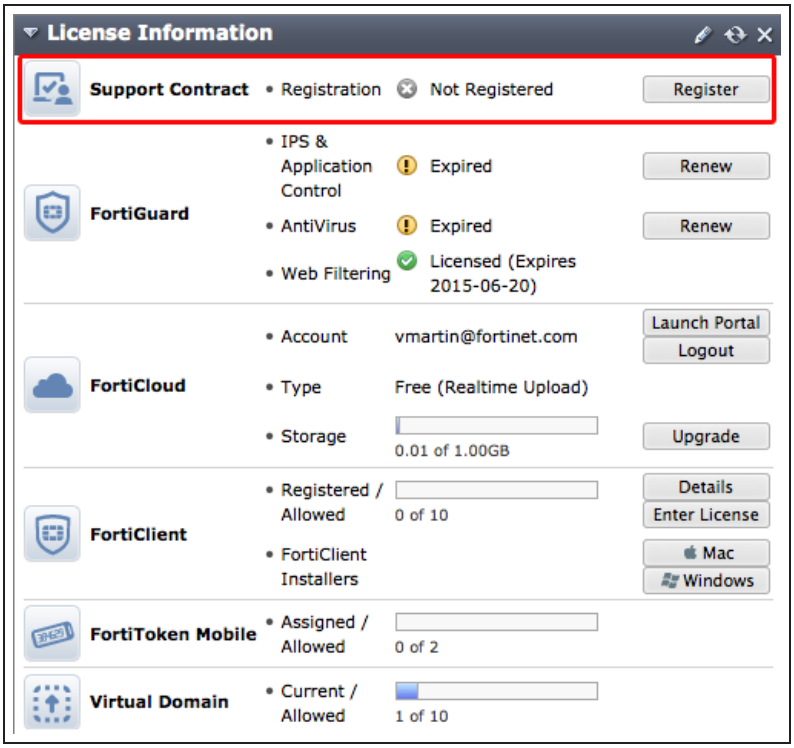
1. Registering your FortiGate

Registering your FortiGate allows you to receive FortiGuard updates and is required for firmware upgrades and access to Fortinet Support.

Before registering your FortiGate unit, it must have Internet connectivity.

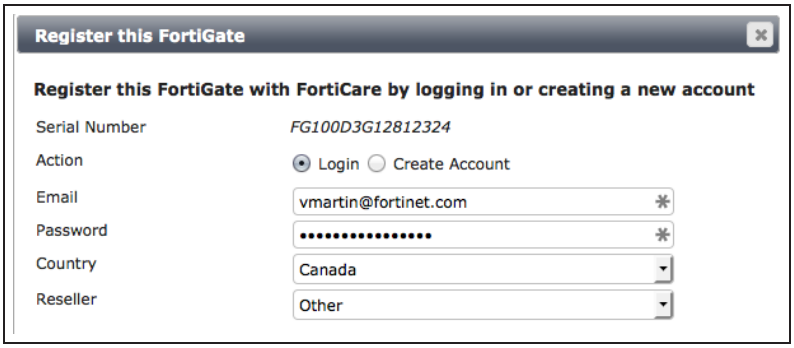
Go to **System > Dashboard > Status** and locate the **License Information** widget.

Next to **Support Contract**, select **Register**.

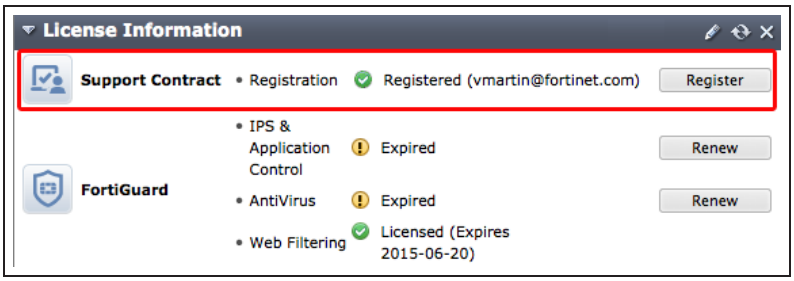


Either use an existing Fortinet Support account or create a new one. Select your **Country** and **Reseller**.

It is recommend to use a common account to register all your Fortinet products, to allow the Support site to keep a complete listing of your devices.



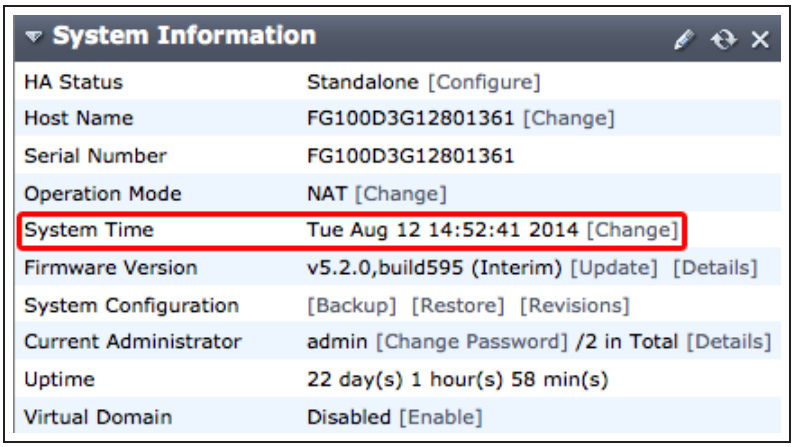
The **License Information** widget now displays the unit as **Registered**.



2. Setting the system time

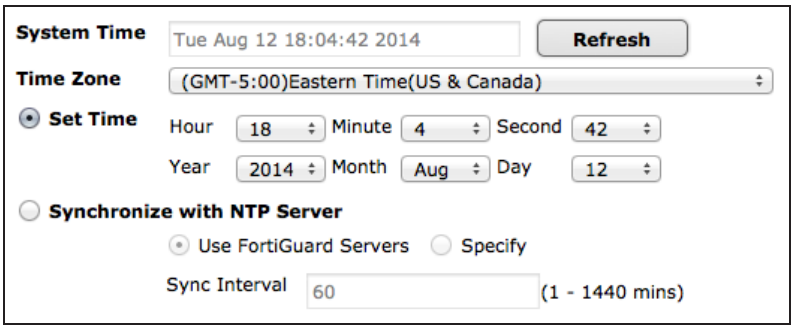
Go to **System > Dashboard > Status** and locate the **System Information** widget.

Next to **System Time**, select **Change**.

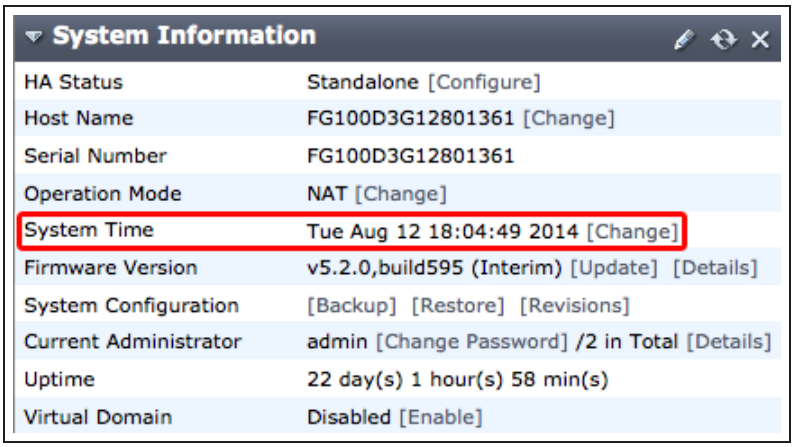


Select your **Time Zone** and either set the time manually or select **Synchronize with NTP Server**.

Since not all time zones have names, you may need to know how many hours ahead (+) or behind (-) you are from Greenwich Mean Time (GMT).



The **System Information** widget now displays the correct time.



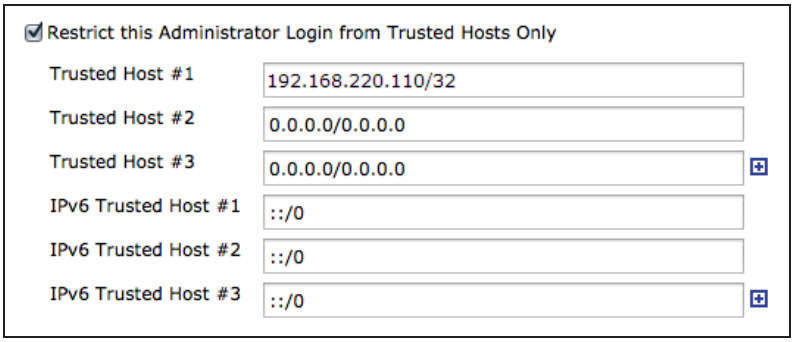
3. (Optional) Restricting administrative access to a trusted host

Go to **System > Admin > Administrators** and edit the default *admin* account.

Enable **Restrict this Administrator Login from Trusted Hosts Only**. Set **Trusted Host #1** to the static IP address of the PC you will use to administer the FortiGate unit, using /32 as the netmask.

You can also set an entire subnet as the trusted host, using /24 as the netmask.

If required, set additional trusted hosts.

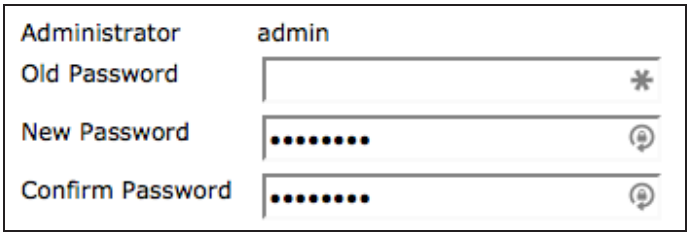


4. Changing the default admin password

Go to **System > Admin > Administrators** and edit the default *admin* account.

Select **Change Password**. Leave **Old Password** blank and enter the **New Password**.

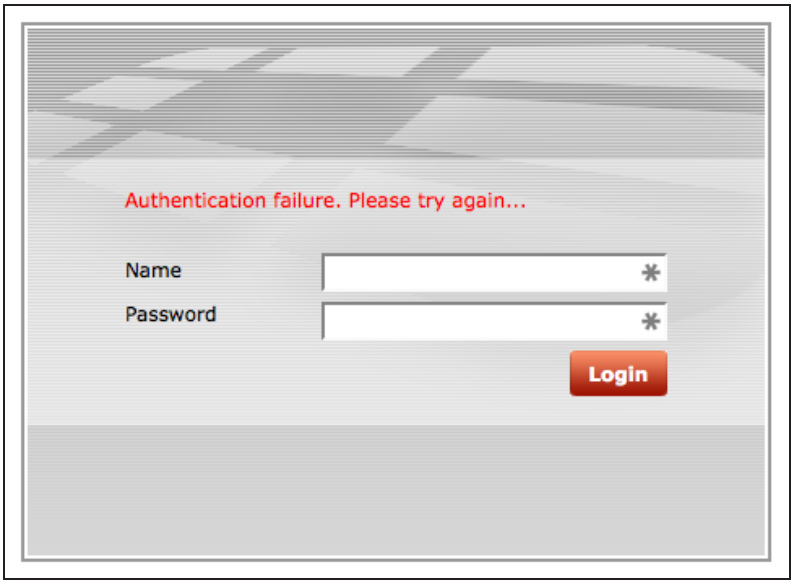
You will be automatically signed out after changing the password.



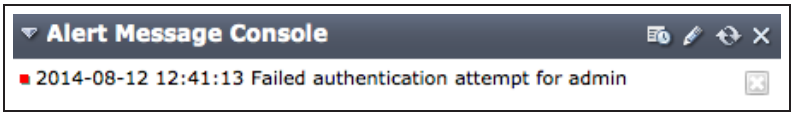
5. Results

Attempt to log in using the admin account without a password. Access is denied.

Log in using the new password to access the FortiGate.



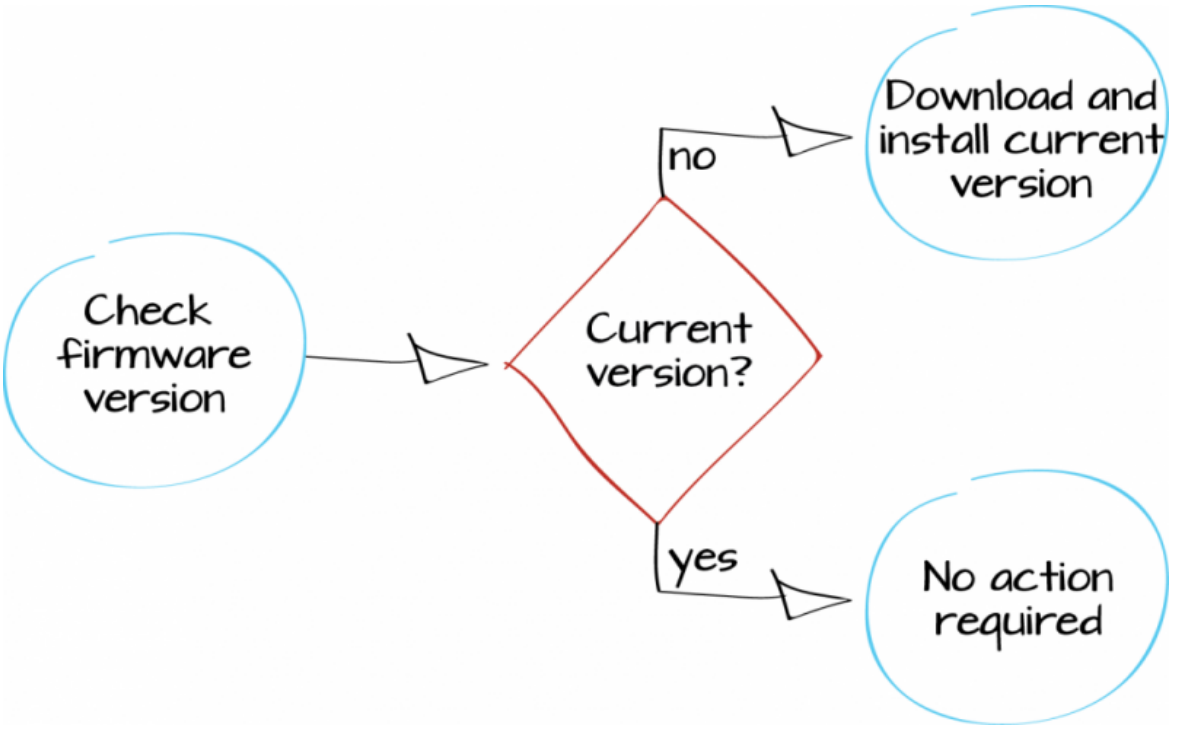
Go to **System > Dashboard > Status** and locate the **Alert Message Console** widget, which indicates the failed authentication attempt.



(Optional) If access has been restricted to a trusted host, attempts to connect from a device that is not trusted will be denied.

For further reading, check out Basic Administration in the FortiOS 5.2 Handbook.

Updating your FortiGate's firmware

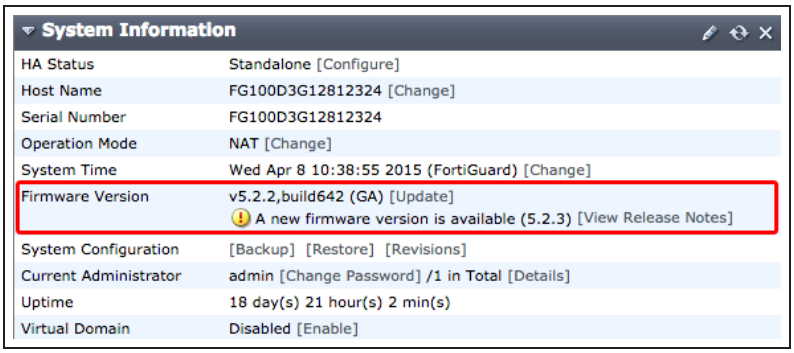


This example verifies the current version of FortiOS firmware and, if necessary, updates it to the latest version.

FortiOS is the operating system used by FortiGate and FortiWiFi units. You can update FortiOS to use the latest tools and security features available.

1. Checking the current FortiOS firmware

Log in to the GUI and go to **System > Dashboard > Status** and view the **System Information** dashboard widget. The **Firmware Version** section shows the firmware that is currently installed and if a new version is available.



2. Reviewing the Release Notes

If a new version is available, select **View Release Notes** to access the Release Notes for that version. Review the release notes to determine if you want to upgrade to this version.

Pay extra attention to the **Upgrade Information** section, to find out if you can upgrade directly from your current firmware to the latest version. You should also check the **Supported Upgrade Paths** document, found at the Fortinet Documentation Library.

3. Updating to the latest firmware

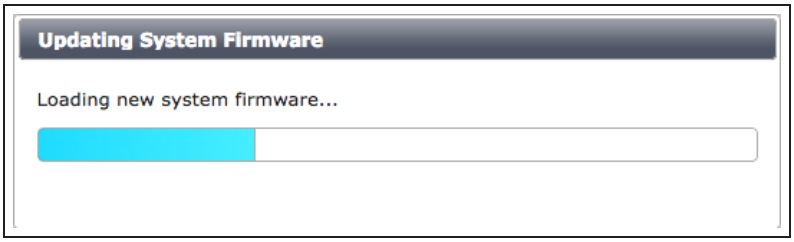
If you wish to upgrade to the latest FortiOS version, select **Update**.

Under **Available Firmware**, select the **Recommended** tab, then select **Backup Config and Upgrade**.

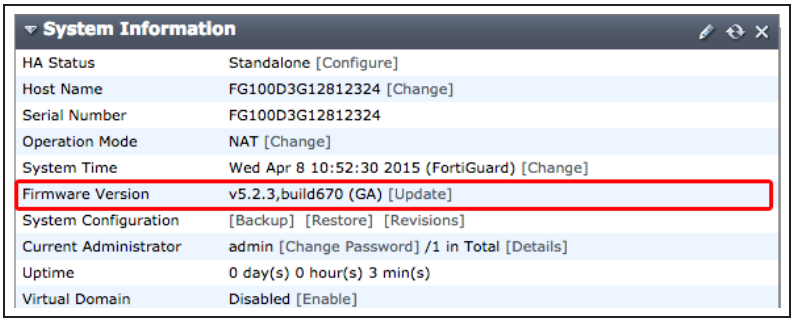
4. Results

The FortiGate unit uploads the firmware image file, updates to the new firmware version, restarts, and displays the FortiGate login. This process takes a few minutes.

You may have to refresh your browser to see the FortiGate login.

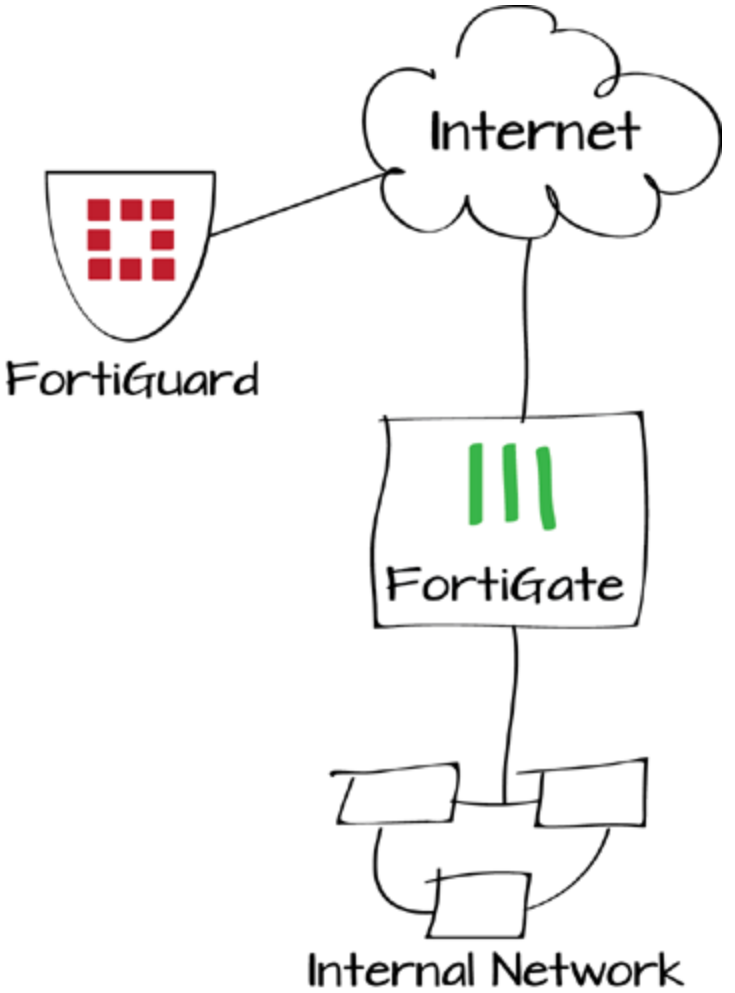


Go to **System > Dashboard > Status**. In the **System Information** dashboard widget, the **Firmware Version** will show the updated version of FortiOS.



For further reading, check out Firmware in the FortiOS 5.2 Handbook.

Setting up FortiGuard services



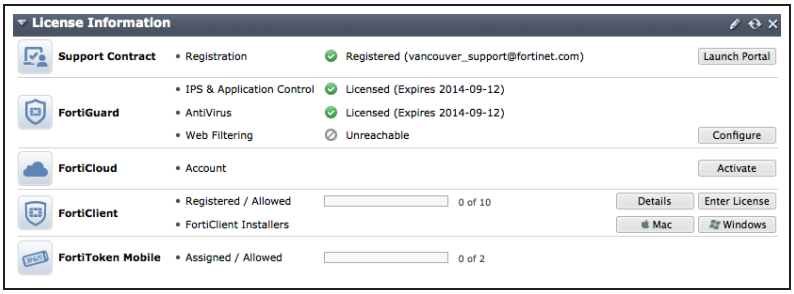
If you have purchased FortiGuard services and registered your FortiGate unit, the FortiGate should automatically connect to FortiGuard and display license information about your FortiGuard services. In this example, you will verify whether the FortiGate unit is communicating with the FortiGuard Distribution Network (FDN) by checking the **License Information** dashboard widget.

1. Verifying the connection

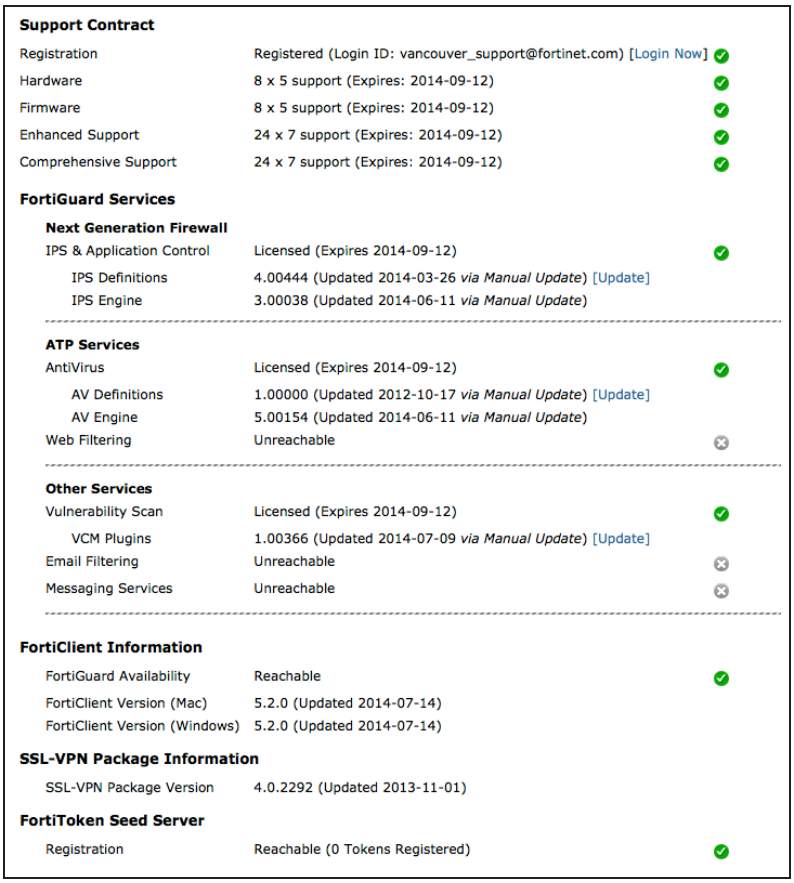
Go to **System > Dashboard > Status** and go to the **License Information** widget. Any subscribed services should have a green checkmark, indicating that connections are successful.

A gray X indicates that the FortiGate unit cannot connect to the FortiGuard network, or that the FortiGate unit is not registered.

A red X indicates that the FortiGate unit was able to connect but that a subscription has expired or has not been activated.



You can also view the FortiGuard connection status by going to **System > Config > FortiGuard**.

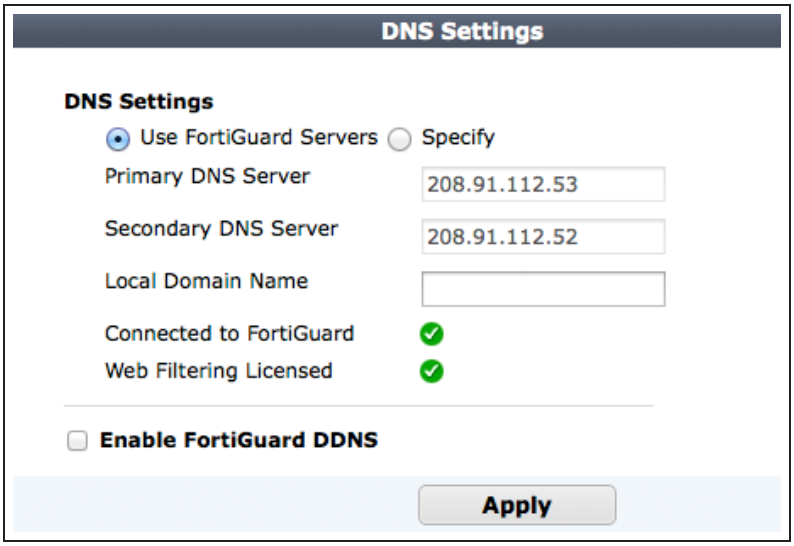


Support Contract		
Registration	Registered (Login ID: vancouver_support@fortinet.com) [Login Now]	✓
Hardware	8 x 5 support (Expires: 2014-09-12)	✓
Firmware	8 x 5 support (Expires: 2014-09-12)	✓
Enhanced Support	24 x 7 support (Expires: 2014-09-12)	✓
Comprehensive Support	24 x 7 support (Expires: 2014-09-12)	✓
FortiGuard Services		
Next Generation Firewall		
IPS & Application Control	Licensed (Expires 2014-09-12)	✓
IPS Definitions	4.00444 (Updated 2014-03-26 *via Manual Update*) [Update]	
IPS Engine	3.00038 (Updated 2014-06-11 *via Manual Update*)	
ATP Services		
AntiVirus	Licensed (Expires 2014-09-12)	✓
AV Definitions	1.00000 (Updated 2012-10-17 *via Manual Update*) [Update]	
AV Engine	5.00154 (Updated 2014-06-11 *via Manual Update*)	
Web Filtering	Unreachable	⊗
Other Services		
Vulnerability Scan	Licensed (Expires 2014-09-12)	✓
VCM Plugins	1.00366 (Updated 2014-07-09 *via Manual Update*) [Update]	
Email Filtering	Unreachable	⊗
Messaging Services	Unreachable	⊗
FortiClient Information		
FortiGuard Availability	Reachable	✓
FortiClient Version (Mac)	5.2.0 (Updated 2014-07-14)	
FortiClient Version (Windows)	5.2.0 (Updated 2014-07-14)	
SSL-VPN Package Information		
SSL-VPN Package Version	4.0.2292 (Updated 2013-11-01)	
FortiToken Seed Server		
Registration	Reachable (0 Tokens Registered)	✓

2. Troubleshooting communication errors

Go to **System > Network > DNS** and ensure that the primary and secondary DNS servers are correct.

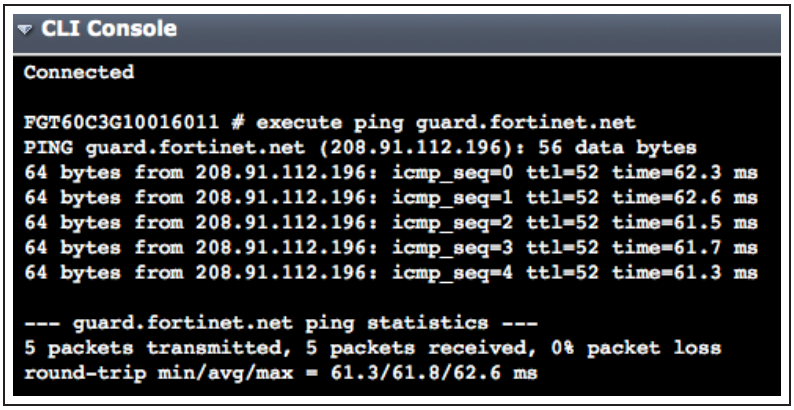
In this screenshot, the FortiGate has been successfully tested already.



To test if you are connected to the correct DNS server, go to **System > Dashboard > Status** and enter the following command into the CLI Console:

```
execute ping guard.fortinet.net
```

If the connection the is successful, the CLI Console should display a similar output as the example.

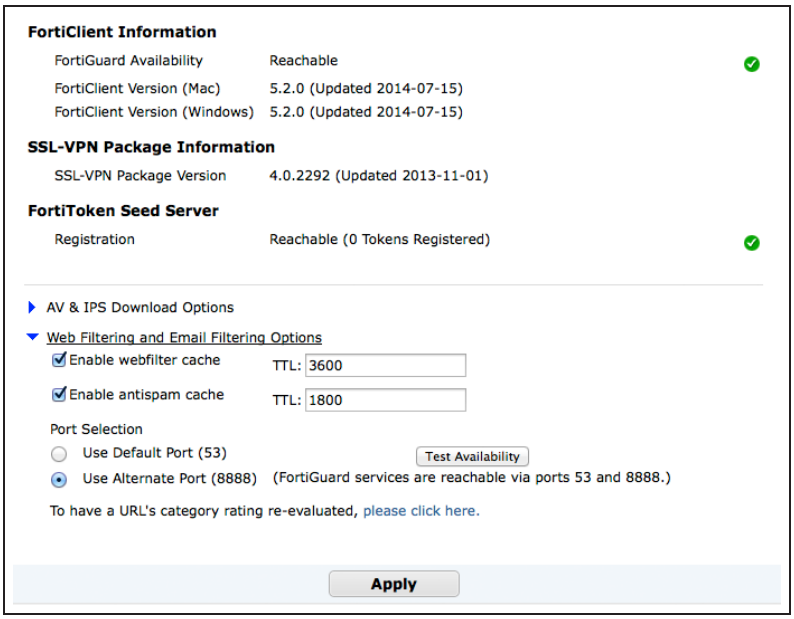


To test if the FortiGuard services are reachable, go to **System > Config > FortiGuard**.

Under the **Web Filtering and Email Filtering Options**, select **Test Availability**. This will indicate which ports are open.If the FortiGate default port (53) cannot be unblocked, go to **System > Config > FortiGuard**. Under the **Web Filtering and Email Filtering Options** choose **Use Alternate Port (8888)**.

If you are updating FortiGuard using a FortiManager, the FortiGate can also use port 80.

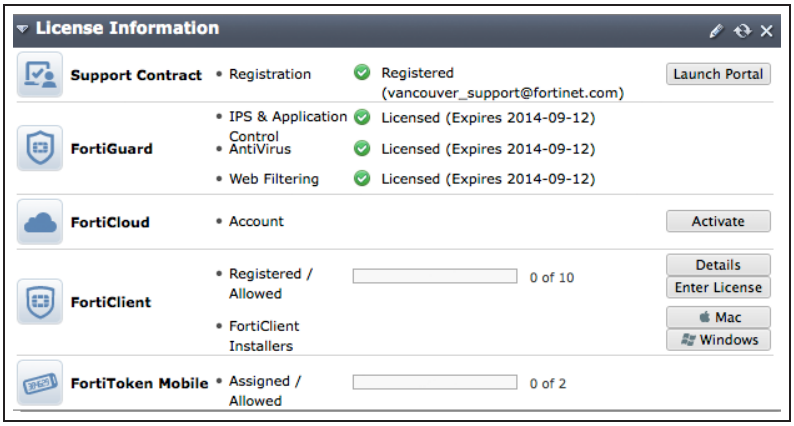
If further problems occur, you may have to unblock ports using the CLI. See the CLI Reference for FortiOS 5.2 for more information.



3. Results

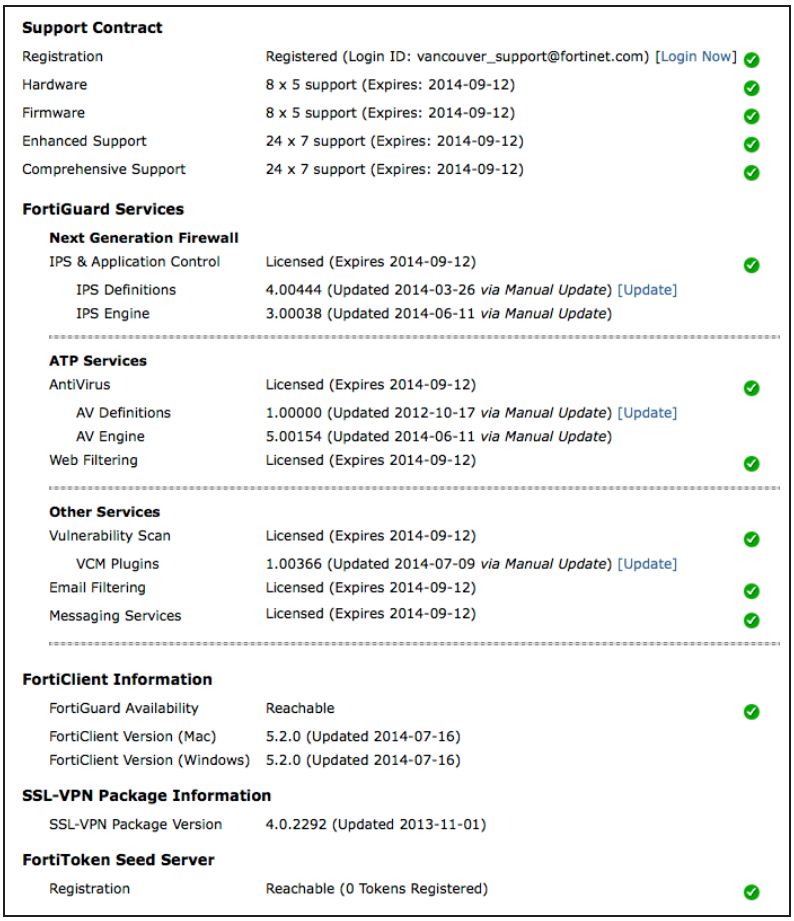
Go to **System > Dashboard > Status** and go to the **License Information** widget.

Any subscribed services should have a green checkmark, indicating that connections have been established and that the licenses have been verified.



Go to **System > Config > FortiGuard**.

Features and services you are subscribed to should have a green checkmark, indicating that connections are successful.



Support Contract

Registration	Registered (Login ID: vancouver_support@fortinet.com) [Login Now]
Hardware	8 x 5 support (Expires: 2014-09-12)
Firmware	8 x 5 support (Expires: 2014-09-12)
Enhanced Support	24 x 7 support (Expires: 2014-09-12)
Comprehensive Support	24 x 7 support (Expires: 2014-09-12)

FortiGuard Services

Next Generation Firewall

IPS & Application Control	Licensed (Expires 2014-09-12)
IPS Definitions	4.00444 (Updated 2014-03-26 *via Manual Update*) [Update]
IPS Engine	3.00038 (Updated 2014-06-11 *via Manual Update*)

ATP Services

AntiVirus	Licensed (Expires 2014-09-12)
AV Definitions	1.00000 (Updated 2012-10-17 *via Manual Update*) [Update]
AV Engine	5.00154 (Updated 2014-06-11 *via Manual Update*)
Web Filtering	Licensed (Expires 2014-09-12)

Other Services

Vulnerability Scan	Licensed (Expires 2014-09-12)
VCM Plugins	1.00366 (Updated 2014-07-09 *via Manual Update*) [Update]
Email Filtering	Licensed (Expires 2014-09-12)
Messaging Services	Licensed (Expires 2014-09-12)

FortiClient Information

FortiGuard Availability	Reachable
FortiClient Version (Mac)	5.2.0 (Updated 2014-07-16)
FortiClient Version (Windows)	5.2.0 (Updated 2014-07-16)

SSL-VPN Package Information

SSL-VPN Package Version	4.0.2292 (Updated 2013-11-01)

FortiToken Seed Server

Registration	Reachable (0 Tokens Registered)

For further reading, check out FortiGuard in the FortiOS 5.2 Handbook.

FortiGuard troubleshooting

This section contains tips to help you with some common challenges of using FortiGuard.

FortiGuard services appear as expired/unreachable.

Verify that you have registered your FortiGate unit, purchased FortiGuard services and that the services have not expired at support.fortinet.com.

Services are active but still appear as expired/unreachable.

Verify that the FortiGate unit can communicate with the Internet by accessing FortiGate CLI and using the command `execute ping 8.8.8.8`. You can also use the `execute traceroute 8.8.8.8` command to troubleshoot connectivity to the Internet.

The FortiGate is connected to the Internet but can't communicate with FortiGuard.

If you have not done so already, verify your DNS settings and ensure that an unblocked port is being used for FortiGuard traffic.

If the FortiGate interface connected to the Internet gets its IP address using DHCP, go to **System > Network > Interfaces** and edit the Internet-facing interface. Ensure that
Override internal DNS is selected.

Communication errors remain.

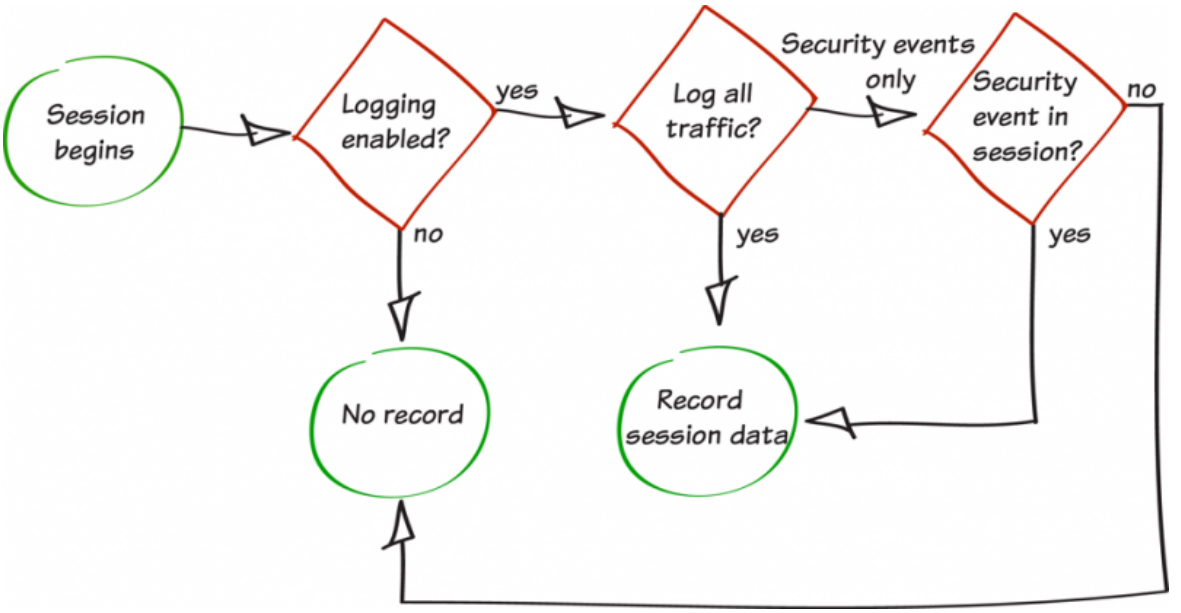
FortiGate units contact the FortiGuard Network by sending UDP packets with typical source ports of 1027 or 1031, and destination ports of 53 or 8888. The FDN reply packets would then have a destination port of 1027 or 1031. If your ISP blocks UDP packets in this port range, the FortiGate unit cannot receive the FDN reply packets.

In effort to avoid port blocking, You can configure your FortiGate unit to use higher-numbered ports, such as 2048-20000, using the following CLI command:

```
config system global
 set ip-src-port-range 2048-20000
end
```

Trial and error may be required to select the best source port range. You can also contact your ISP to determine the best range to use.

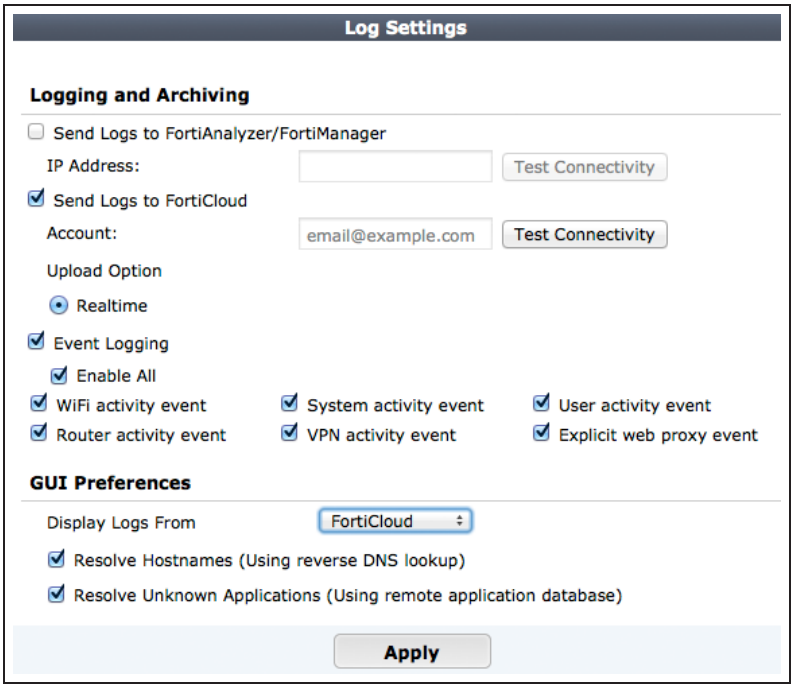
Logging FortiGate traffic



In this example, you will enable logging to capture the details of the network traffic processed by your FortiGate unit. Capturing log details will provide you with detailed traffic information that you can use to asses any network issues.

1. Recording log messages and enabling event logging

Go to **Log & Report > Log Config > Log Settings**.Select where log messages will be recorded. You can save log messages to disk if it is supported by your FortiGate unit, to a FortiAnalyzer or FortiManager unit if you have one, or to FortiCloud if you have a subscription. Each of these options allow you to record and view log messages and to create reports based on them.In most cases, it is recommended to **Send Logs to FortiCloud**, as shown in the example.



Next, enable **Event Logging**. You can choose to Enable All types of logging, or specific types, such as WiFi activity events, depending on your needs.

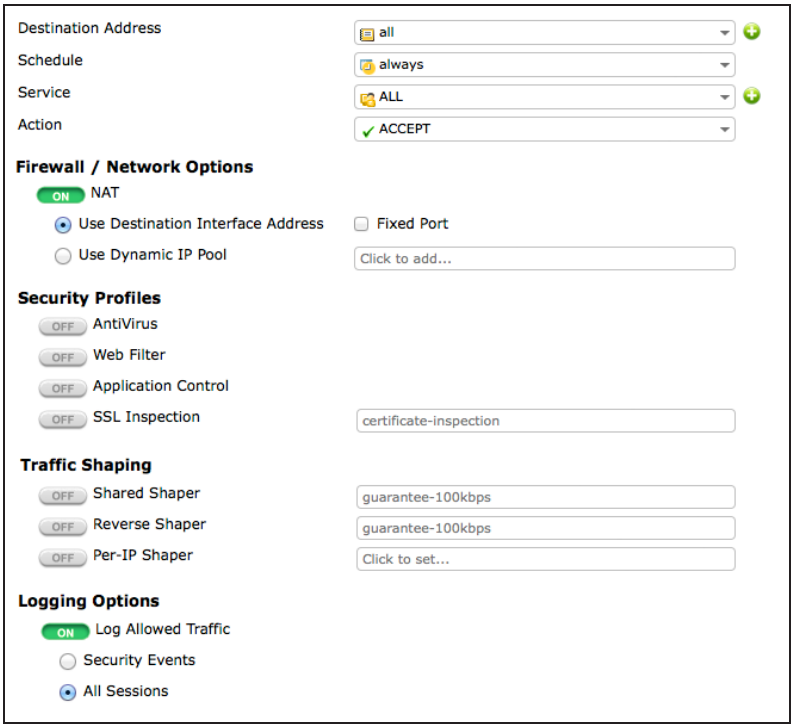
Under the **GUI Preferences**, ensure that the **Display Logs From** is set to the same location where the log messages are recorded (in the example, **FortiCloud**).

2. Enabling logging in the security policies

Go to **Policy & Objects > Policy > IPv4**. Edit the policies controlling the traffic you wish to log.

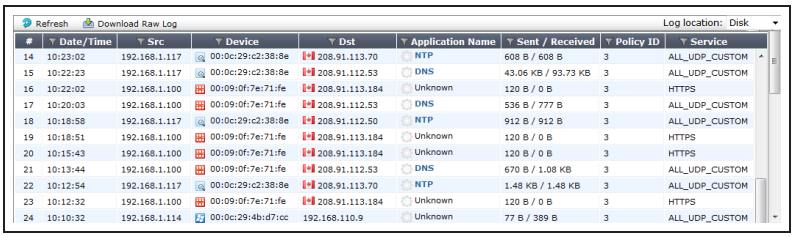
Under **Logging Options**, select **All Sessions**.

In most cases, you should select Security Events, as All Sessions requires more system resources and storage space. For now, however, All Sessions will be used to verify that logging has been set up successfully.



3. Results

View traffic logs by going to **Log & Report > Traffic Log > Forward Traffic**. The logs display a variety of information about your traffic, including date/time, source, device, and destination.To change the information shown, right-click on any column title and select **Column Settings** to enable or disable different columns.



#	Date/Time	Src	Device	Dst	Application Name	Sent / Received	Policy ID	Service
14	10:23:02	192.168.1.117	00:0c:29:c2:38:8e	208.91.113.70	NTP	608 B / 608 B	3	ALL_UDP_CUSTOM
15	10:22:23	192.168.1.117	00:0c:29:c2:38:8e	208.91.112.53	DNS	43.06 KB / 93.73 KB	3	ALL_UDP_CUSTOM
16	10:22:02	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184	Unknown	120 B / 0 B	3	HTTPS
17	10:20:03	192.168.1.100	00:09:0f:7e:71:fe	208.91.112.53	DNS	536 B / 777 B	3	ALL_UDP_CUSTOM
18	10:18:58	192.168.1.117	00:0c:29:c2:38:8e	208.91.112.50	NTP	912 B / 912 B	3	ALL_UDP_CUSTOM
19	10:18:51	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184	Unknown	120 B / 0 B	3	HTTPS
20	10:15:43	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184	Unknown	120 B / 0 B	3	HTTPS
21	10:13:44	192.168.1.100	00:09:0f:7e:71:fe	208.91.112.53	DNS	670 B / 1.08 KB	3	ALL_UDP_CUSTOM
22	10:12:54	192.168.1.117	00:0c:29:c2:38:8e	208.91.113.70	NTP	1.48 KB / 1.48 KB	3	ALL_UDP_CUSTOM
23	10:12:32	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184	Unknown	120 B / 0 B	3	HTTPS
24	10:10:32	192.168.1.114	00:0c:29:4b:d7:cc	192.168.110.9	Unknown	77 B / 389 B	3	ALL_UDP_CUSTOM

For further reading, check out Logging and reporting overview in the FortiOS 5.2 Handbook.

Troubleshooting FortiGate logging

This section contains tips to help you with some common challenges of FortiGate logging.

No log messages appear.

Ensure that logging is enabled in both the **Log Settings** and the policy used for the traffic you wish to log, as logging will not function unless it is enabled in both places.

If logging is enabled in both places, check that the policy in which logging is enabled is the policy being used for your traffic. Also make sure that the policy is getting traffic by going to the policy list and adding the **Sessions** column to the list.

Logs from a FortiAnalyzer, FortiManager, or from FortiCloud do not appear in the GUI.

Ensure that the correct log source has been selected in the **Log Settings**, under **GUI Preferences**.

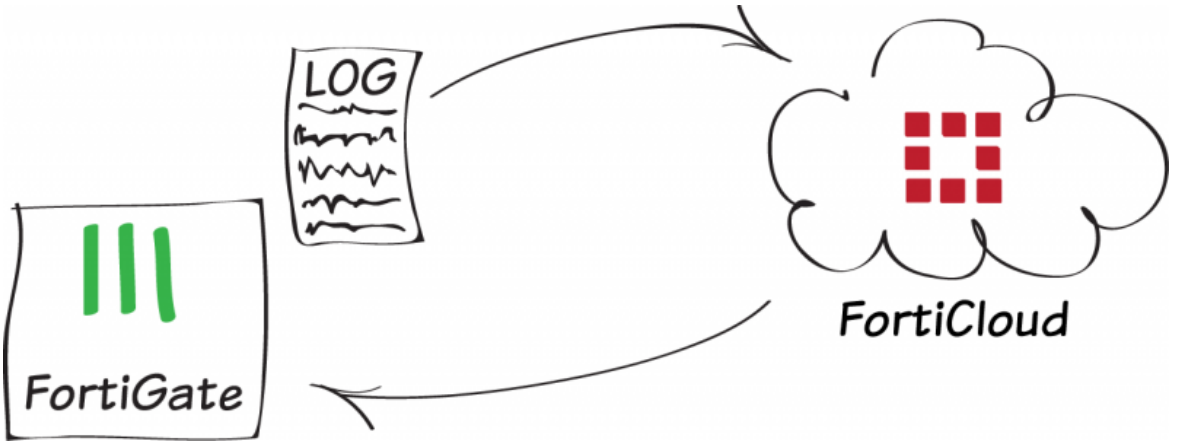
The FortiGate unit's performance level has decreased since enabling disk logging.

If enabling disk logging has impacted overall performance, change the log settings to either send logs to a FortiAnalyzer unit, a FortiManager unit, or to FortiCloud.

Logging to a FortiAnalyzer unit is not working as expected.

The firmware for the FortiGate and FortiAnalyzer units may not be compatible. Check the firmware release notes, found at support.fortinet.com, to see if this is the case.

Logging with FortiCloud

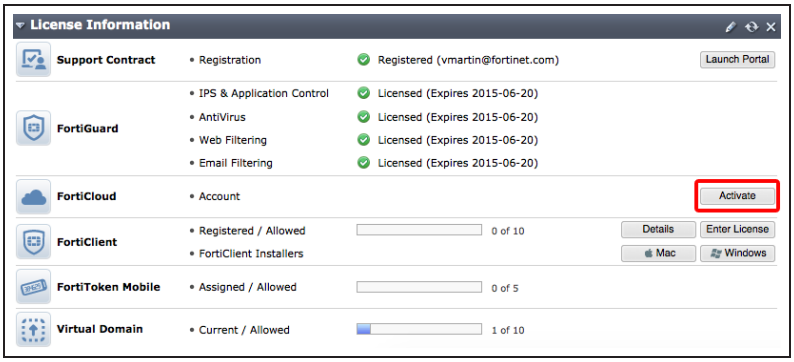


In this example, you will use FortiCloud, an online logging service provided by Fortinet, to store the logs of your FortiGate unit's traffic. You will also access logs using the FortiCloud website.

Before you can use FortiCloud, you must register your FortiGate. For more information, see FortiGate registration and basic settings.

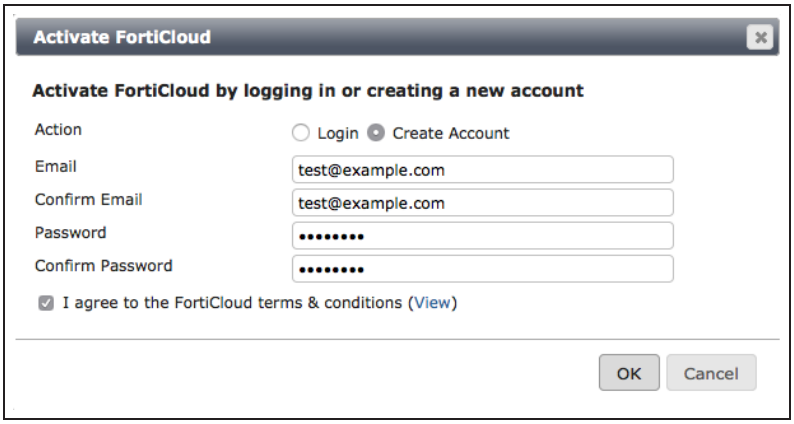
1. Activating FortiCloud

Go to **System > Dashboard > Status** and locate the **License Information** widget. In the **FortiCloud** section, select **Activate**.

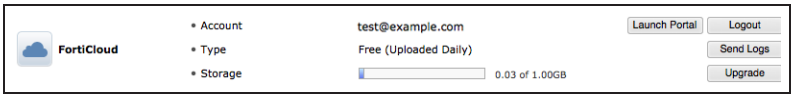


Either use an existing FortiCloud account or create a new one.

It is recommend to use a common FortiCloud account for all your Fortinet logs.



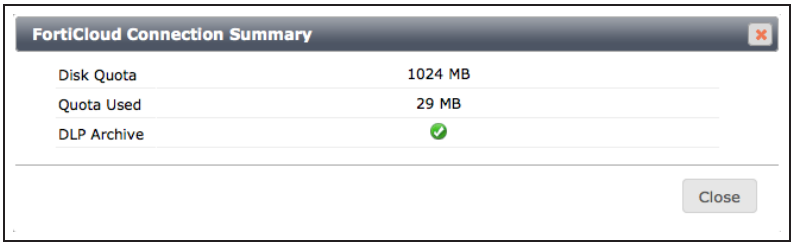
Information about your FortiCloud account now appears in the **License Information** widget.



2. Sending logs to FortiCloud

Go to **Log & Report > Log Config > Log Settings**. Enable **Send Logs to FortiCloud** and ensure that **Upload Option** is set to **Realtime.**

Select **Test Connectivity** to verify the connection between your FortiGate and FortiCloud.

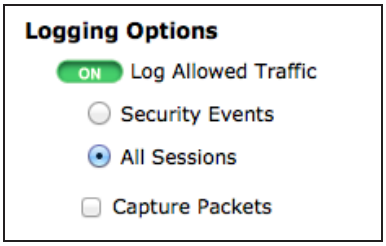


Adjust the **Event Logging** settings as required and set the GUI Preferences to **Display Logs from FortiCloud**.

3. Enabling logging in your Internet access security policy

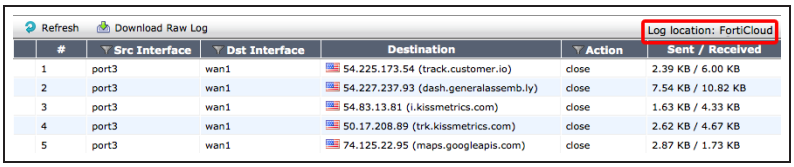
Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

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



4. Results

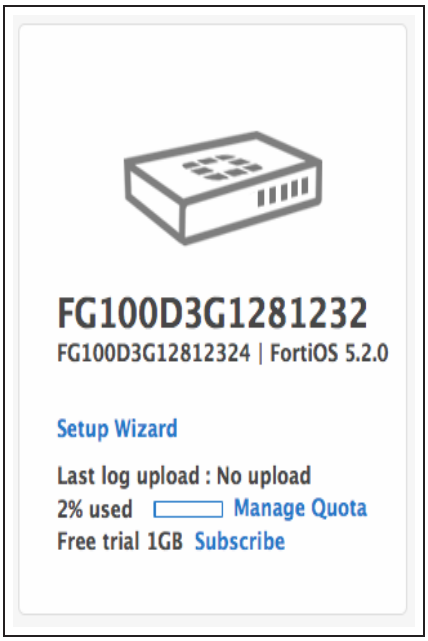
Browse the Internet.Go to **Log & Report > Traffic Log > Forward Traffic**. In the top right corner of the screen, the **Log location** is shown as **FortiCloud**.



#	Src Interface	Dst Interface	Destination	Action	Sent / Received
1	port3	wan1	54.225.173.54 (track.customer.io)	close	2.39 KB / 6.00 KB
2	port3	wan1	54.227.237.93 (dash.generalassemb.ly)	close	7.54 KB / 10.82 KB
3	port3	wan1	54.83.13.81 (i.kissmetrics.com)	close	1.63 KB / 4.33 KB
4	port3	wan1	50.17.208.89 (trk.kissmetrics.com)	close	2.62 KB / 4.67 KB
5	port3	wan1	74.125.22.95 (maps.googleapis.com)	close	2.87 KB / 1.73 KB

Go to **System > Dashboard > Status**. In the **FortiCloud** section of the **License Information** widget, select **Launch Portal**.A screen will open in your browser, showing all the devices that are linked with your FortiGate account. Select the appropriate unit.

You can also access your FortiCloud account by going to www.forticloud.com

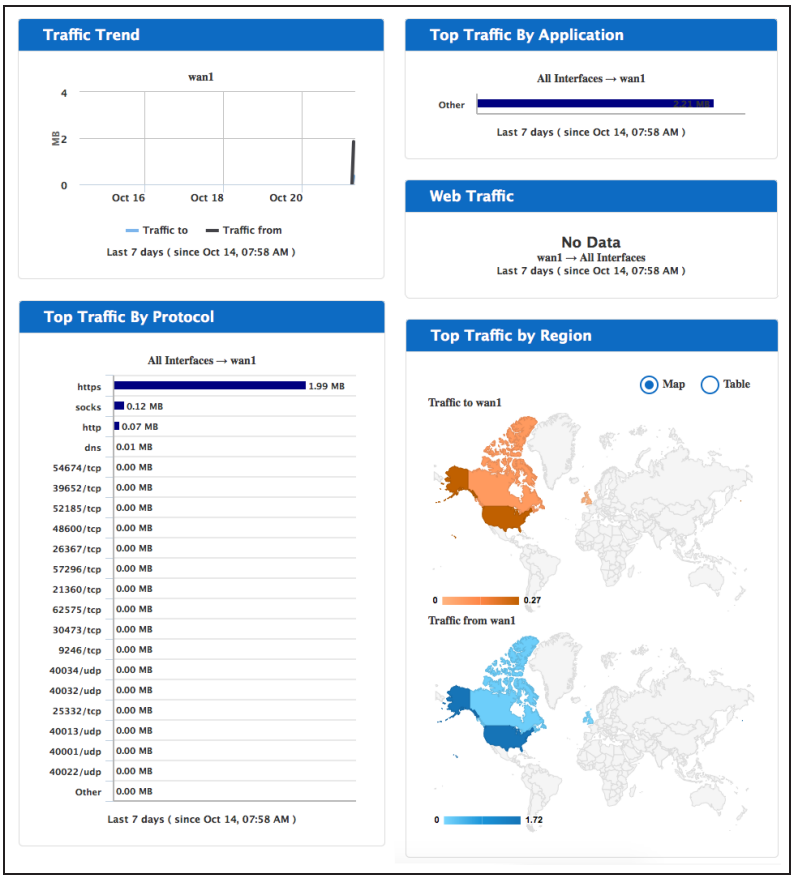


After selecting your device, the FortiCloud Dashboard appears, showing a variety of information about your traffic.

If traffic does not appear in FortiCloud right away, wait 10-15 minutes and try again.

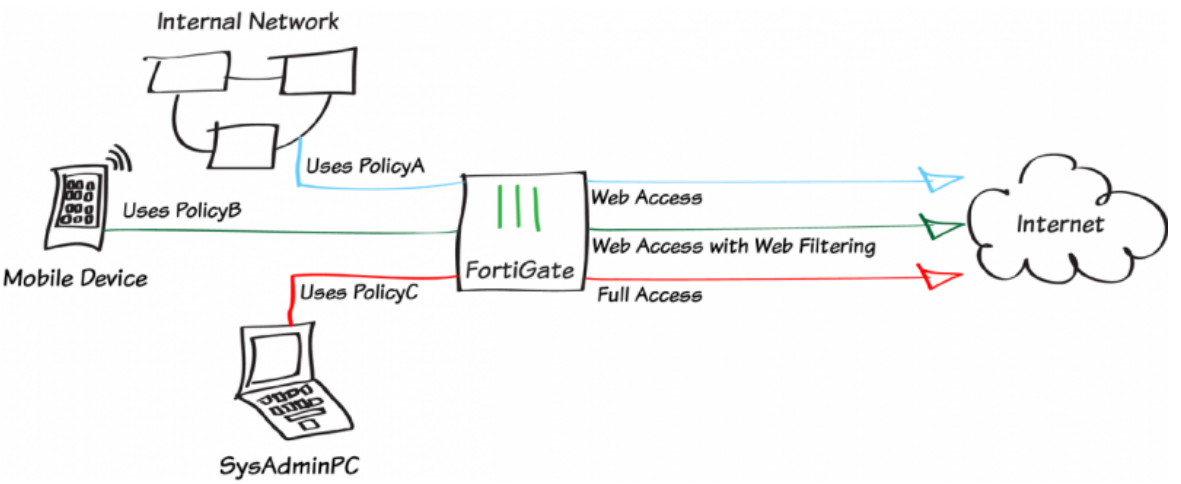
From the portal, you can also access options for **FortiView**, **Drilldown**, **Reports**, and **Management**.

For more information about using FortiCloud, see the FortiCloud FAQ



For further reading, check out FortiCloud in the FortiOS 5.2 Handbook.

Creating security policies



This example shows how to create and order multiple security policies in the policy table, in order to apply the appropriate policy to various types of network traffic.

In the example, three IPv4 policies will be configured. PolicyA will be a general policy allowing Internet access to the LAN. PolicyB will allow Internet access while applying web filtering for specific mobile devices connecting through the LAN. PolicyC will allow the system administrator's PC (named SysAdminPC) to have full access

In this example, a wireless network has already been configured that is in the same subnet as the wired LAN. For information about this configuration, seeSetting up a WiFi bridge with a FortiAP.

A fourth policy, the default "deny" policy, will also be used.

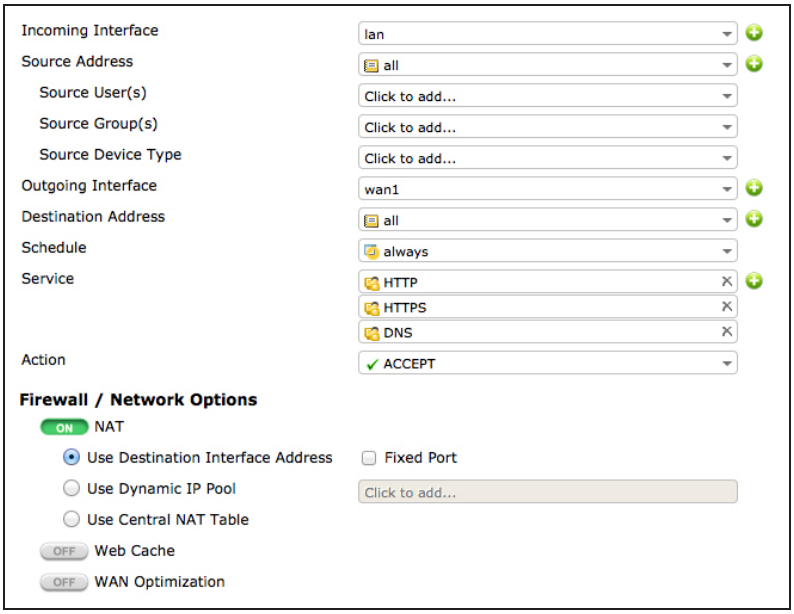
A video of this recipe can be found here.

1. Configuring PolicyA to allow general web access

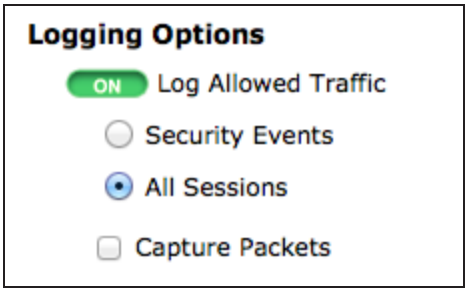
Go to **Policy & Objects > Policy > IPv4** and edit the policy allowing outgoing traffic.

Set **Service** to **HTTP**, **HTTPS**, and **DNS**.

Ensure that you have enabled **NAT**.



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



2. Creating PolicyB to allow access for mobile devices

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

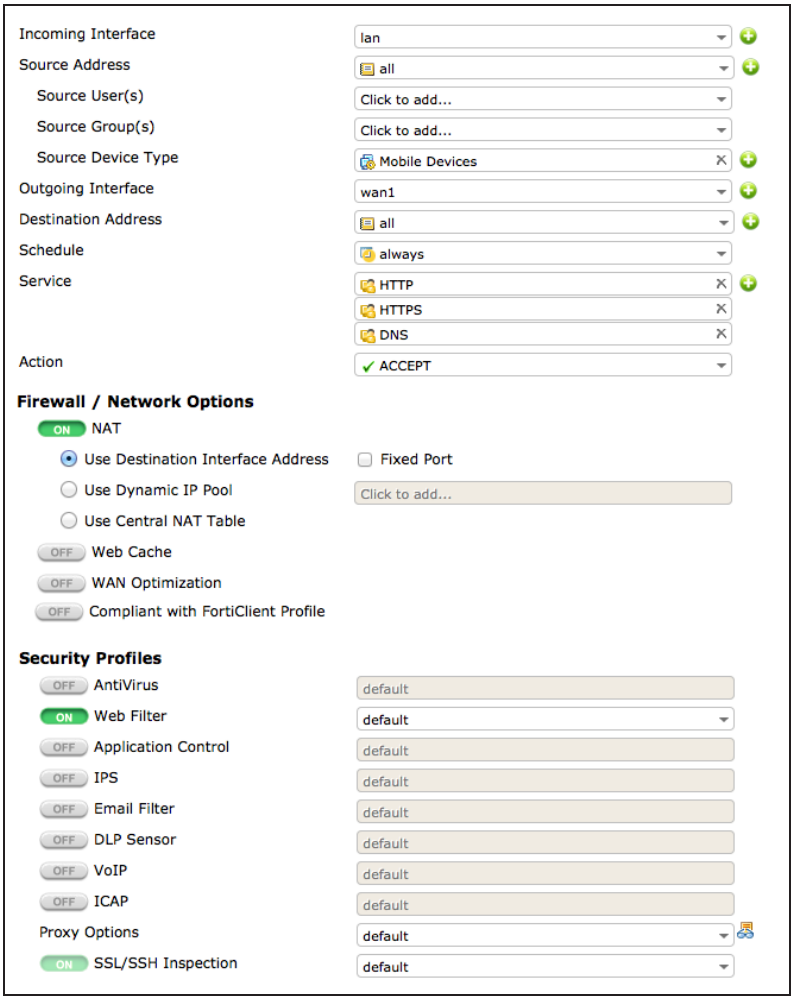
Set **Incoming Interface** to **lan**, **Source Device Type** to **Mobile Devices** (a default device group that includes tablets and mobile phones).

Using a device group will automatically enable device identification on the lan interface.

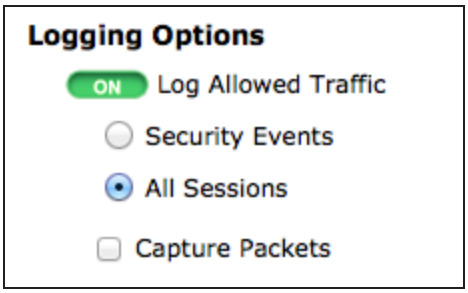
Outgoing Interface to your Internet-facing interface, and **Service** to **HTTP**, **HTTPS**, and **DNS**.

Enable **NAT**.

Under **Security Profiles**, enable **Web Filter** and set it to use the **default** profile. This action will enable **Proxy Options** and **SSL Inspection**. Use the **default** profile for **Proxy Options** and set **SSL Inspection** to **certificate-inspection** to allow HTTPS traffic to be inspected.



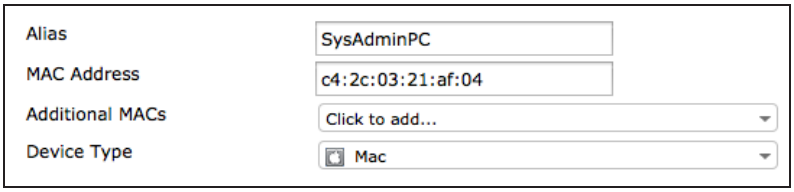
Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.



3. Defining SysAdminPC

Go to **User & Device > Device > Device Definitions** and create a new definition for the system administrator's PC.

Select an approprate **Alias**, then set the **MAC Address**. Set the appropriate **Device Type**.

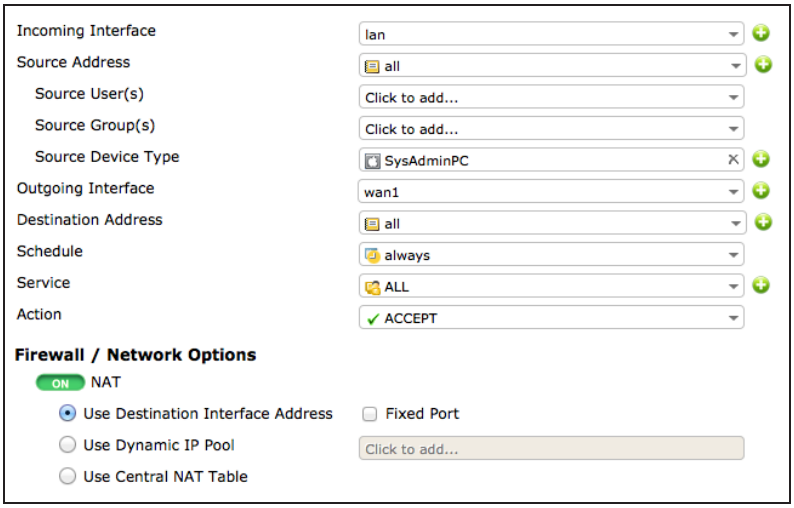


4. Configuring PolicyC to allow access for SysAdminPC

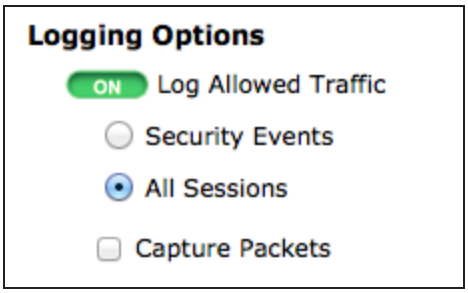
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to **lan**, **Source Device Type** to SysAdminPC, **Outgoing Interface** to your Internet-facing interface, and **Service** to **ALL**.

Enable **NAT**.

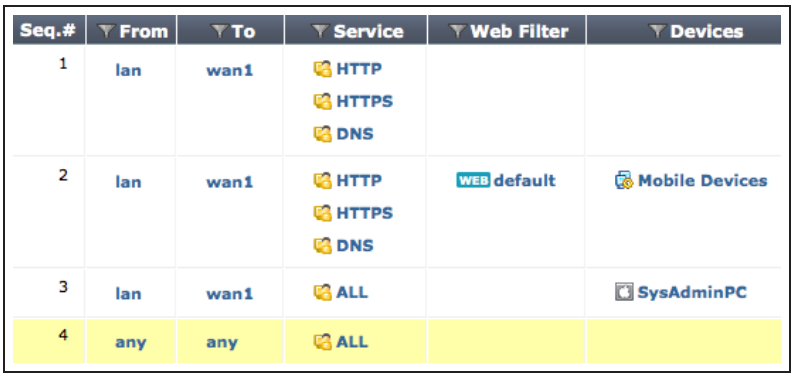


Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.



5. Ordering the policy table

Go to **Policy & Objects > Policy > IPv4** to view the policy table. Currently, the policies are arranged in the order they were created: PolicyA is at the top, followed by PolicyB, PolicyC, and the default deny policy.

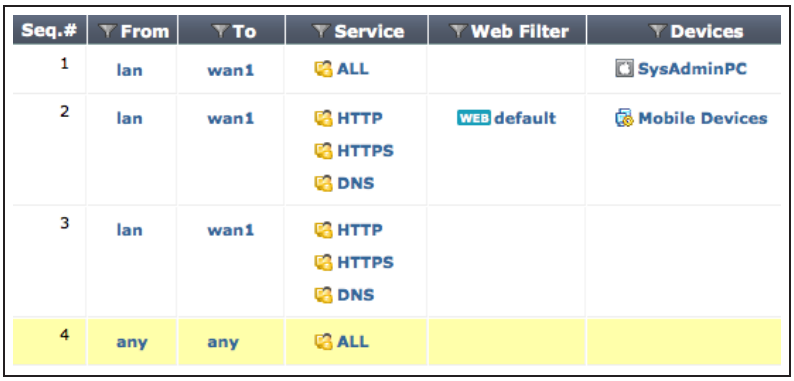


Seq.#	From	To	Service	Web Filter	Devices
1	lan	wan1	HTTP HTTPS DNS		
2	lan	wan1	HTTP HTTPS DNS	WEB default	Mobile Devices
3	lan	wan1	ALL		SysAdminPC
4	any	any	ALL		

In order to have the correct traffic flowing through each policy, they must be arranged so that the more specific policies are located at the top.

In the example, the policy table has been set to show only the columns that best display the differences between the policies. To do this, right-click on the top of the table, select or deselect columns as necessary, then select ***Apply****.*

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



Seq.#	From	To	Service	Web Filter	Devices
1	lan	wan1	ALL		SysAdminPC
2	lan	wan1	HTTP HTTPS DNS	WEB default	Mobile Devices
3	lan	wan1	HTTP HTTPS DNS		
4	any	any	ALL		

6. Results

Browse the Internet using the system administrator's PC, a different PC, and a mobile device.

Go to **Log & Report > Traffic Log > Forward Traffic**.

You can see that traffic from the three devices flows through different policies. In the example, the SysAdmin PC (IP 10.10.11.10), a Windows PC (IP 10.10.11.14), and an iPad (IP 10.10.11.13) were used to generate traffic.

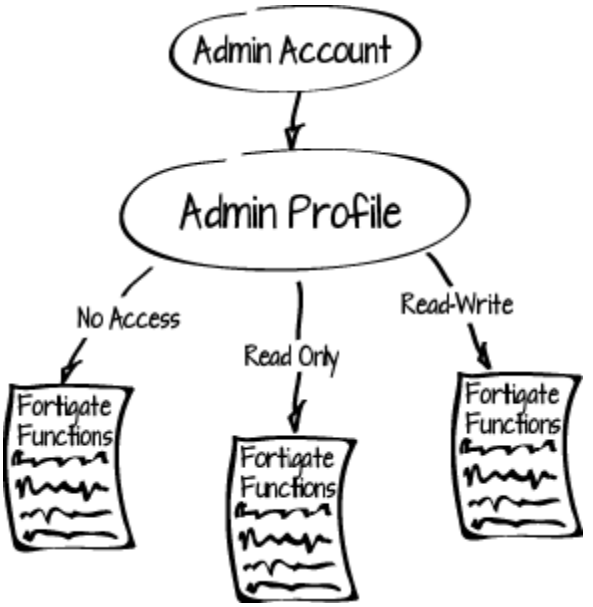
Policy ID is automatically assigned to a policy when it is created, and so, in the example, the ID for PolicyA is 1, PolicyB is 2, and PolicyC is 3.

#	Policy ID	Date/Ti...	Source	Destination	Device
1	3	13:42:18	10.10.11.10	72.167.239.239 (ocsp.godaddy.com.akadns.net)	SysAdminPC
2	3	13:42:18	10.10.11.10	208.91.114.193	SysAdminPC
3	3	13:42:18	10.10.11.10	192.0.65.242 (polldaddy.com)	SysAdminPC
4	3	13:42:18	10.10.11.10	208.91.114.193	SysAdminPC
5	3	13:42:18	10.10.11.10	192.0.65.242 (polldaddy.com)	SysAdminPC
6	3	13:42:18	10.10.11.10	208.91.114.193	SysAdminPC
7	1	13:41:55	10.10.11.14	74.125.226.133 (safebrowsing-cache.google.com)	00:26:22:6c:be:d6
8	1	13:41:55	10.10.11.14	74.125.226.133 (safebrowsing-cache.google.com)	00:26:22:6c:be:d6
9	1	13:41:55	10.10.11.14	74.125.226.133 (safebrowsing-cache.google.com)	00:26:22:6c:be:d6
10	1	13:41:55	10.10.11.14	74.125.226.133 (safebrowsing-cache.google.com)	00:26:22:6c:be:d6
11	1	13:41:55	10.10.11.14	74.125.226.133 (safebrowsing-cache.google.com)	00:26:22:6c:be:d6
12	1	13:41:55	10.10.11.14	74.125.226.133 (safebrowsing-cache.google.com)	00:26:22:6c:be:d6
13	2	13:39:51	10.10.11.13	17.134.126.129 (gs-loc.ls-apple.com.akadns.net)	d8:a2:5e:1d:b1:a6
14	2	13:39:34	10.10.11.13	66.235.138.194 (metrics.apple.com)	d8:a2:5e:1d:b1:a6
15	2	13:39:34	10.10.11.13	184.87.13.15 (e3191.dscc.akamaiedge.net)	d8:a2:5e:1d:b1:a6
16	2	13:39:34	10.10.11.13	23.0.160.208 (images.apple.com)	d8:a2:5e:1d:b1:a6

(Optional) Attempt to make an SSL connection to a web server with all three devices. Only the system administrator's PC will be able to connect.

For further reading, check out Firewall policies in the FortiOS 5.2 Handbook.

Limited access administrator accounts



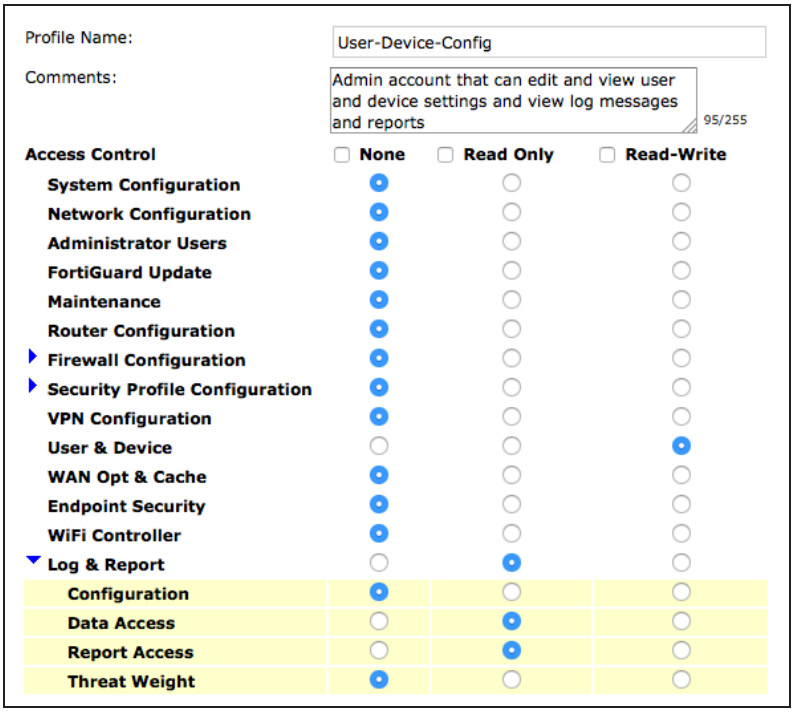
In this recipe you will create a FortiGate administrator account that is limited to read and write access for user and device authentication and read access for logging and reporting. In addition you will use the Trusted Hosts feature to control the IP address that the administrator can log in from.

The administrator account will have the same access limitations for both the GUI and CLI.

1. Creating a new administrator profile

Go to **System > Admin > Admin Profiles.**

Create a new administer profile that limits administrators with this profile to read and write access to **User and Devices** and read only access to **Log & Report** data and report access.

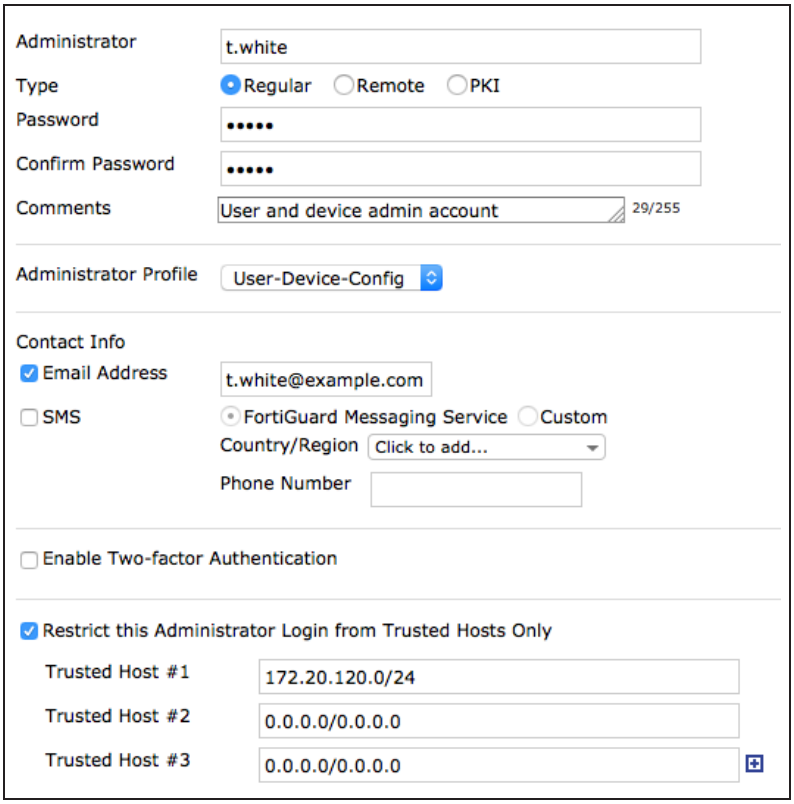


2. Adding a new administrator and assigning the profile

Go to **System > Admin > Administrators**.

Create a new administrator account and assign it to the **Administrator Profile** that you just created.

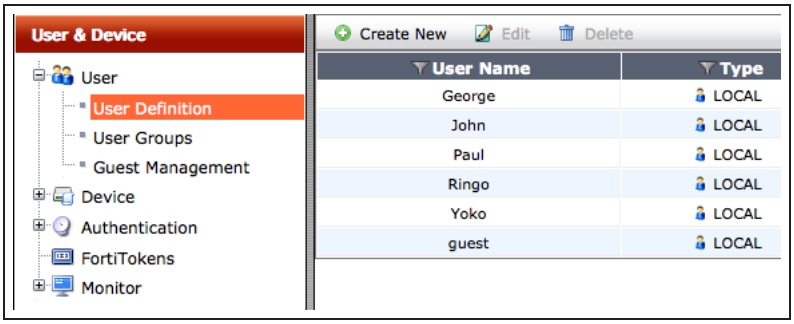
Add an IP address to at least one of the **Trusted Host** fields to control where the administrator can log in from. In the example the administrator can log in only from the 172.20.120.0 network.



3. Results

Log into the FortiGate unit with the t.white. administrator account. t.white should only see the **User & Device** and the **Log & Report** menus.

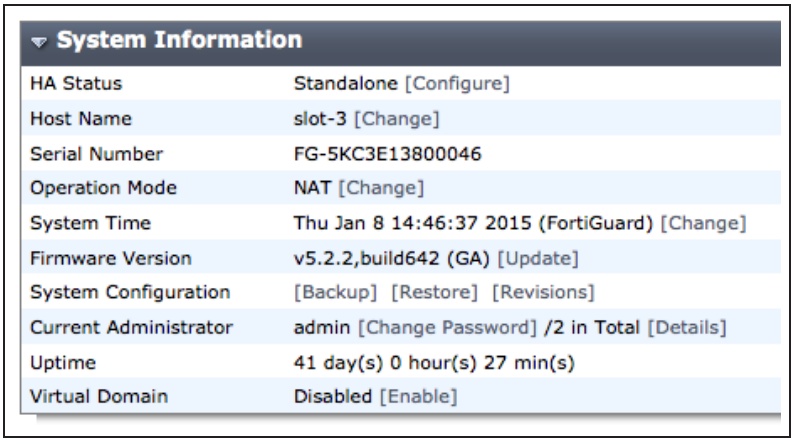
t.white should be able to change user and device authentication settings and view log messages and reports.

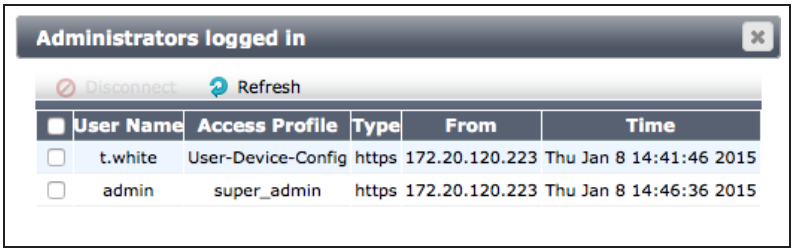


Log in from another browser window with the admin account.

Go to **System > Dashboard > Status**, and view the **System Information** widget. It should show two administrators.

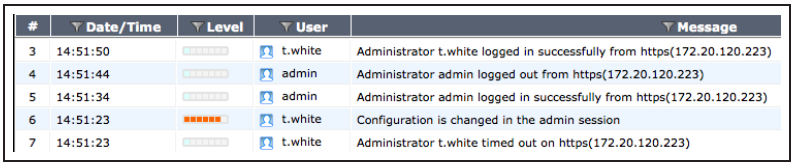
Select **Details** to view the list of logged in administrators.





Using the admin or t.white account, go to **Log & Report > Event Log > System**.

Log messages should show activity for both administrators. Select a log entry to view details. Log entries for t.white should show the source address that t.white logged in from. This address

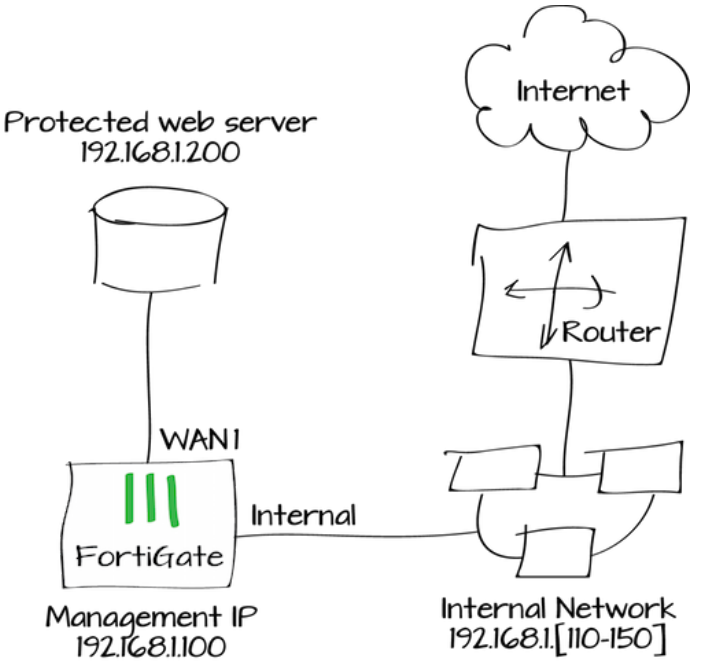


should be within the Trusted Hosts network address.

#	1	**Action**	login
Date/Time	14:57:11	**Level**	
Log Description	Admin logged in successfully	**Log ID**	32001
Message	Administrator t.white logged in successfully from https(172.20.120.223)	**Profile Name**	User-Device-Config
Reason	none	**Status**	success
Sub Type	system	**Timestamp**	1/8/2015, 2:57:11 PM
User	t.white	**User Interface**	https(172.20.120.223)
Virtual Domain	root		

For further reading, check out Administrators in the FortiOS 5.2 Handbook.

Port pairing in Transparent mode



When you create a port pair, all traffic accepted by one of the paired interfaces can only exit out the other interface. Restricting traffic in this way simplifies your FortiGate configuration because security policies between these interfaces are pre-configured.

In this example you will create a wan1 to Internal port pair to make it easier to allow access to a web server protected by a FortiGate in Transparent mode. In this unusual configuration, the web server is connected to the FortiGate's wan1 interface and the FortiGate's Internal interface is connected to an internal network. Users on the internal network access the web server through the FortiGate.

Traffic between port-paired interfaces does not check the bridge table and MAC addresses are not learned. Instead traffic received by one interface in a port pair is forwarded out the other (if allowed by a firewall policy). This makes port pairing useful for unusual topologies where MAC addresses do not behave normally. For example, port paring can be used in a Direct Server Return (DSR) topology where the response MAC address pair may not match the request's MAC address pair.

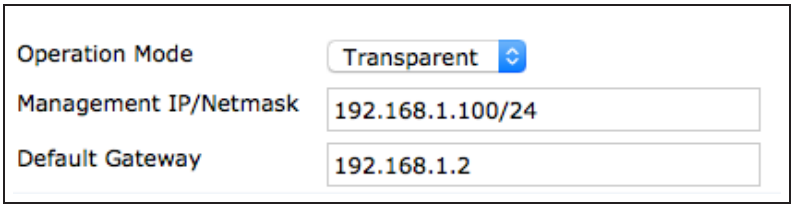
1. Switching the FortiGate unit to transparent mode and adding a static route

Go to **System > Dashboard > Status**.

In the **System Information** widget, select **Change** beside **Operation Mode**.

Change the **Operation Mode** to **Transparent**. Add a **Management IP/Netmask**. Also add a **Default Gateway** for your network so that the FortiGate unit can connect to the Internet.

If the Management IP is the same as the IP address that you logged into the FortiGate unit with, you will remain logged in after the operation mode has changed. Otherwise, log into the FortiGate unit using the management IP (in the example, 172.20.120.142).

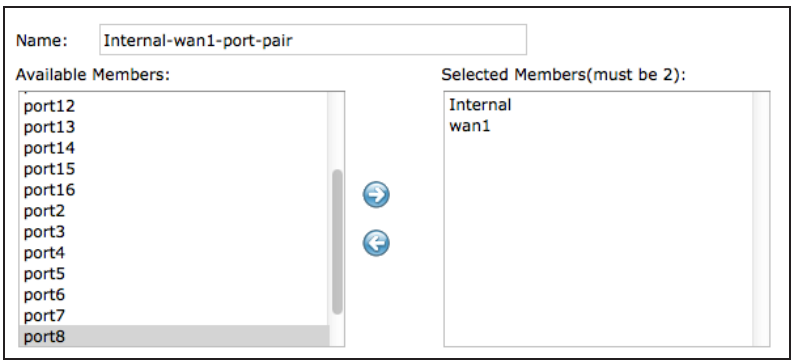


2. Creating an internal and wan1 port pair

Go to **System > Network > Interfaces**.

Select **Create New > Port Pair**. Create a port pair that includes the internal and wan1 interfaces.

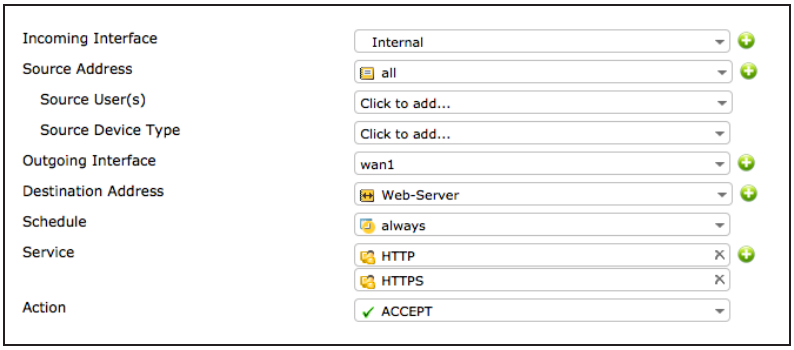
All traffic accepted by the internal interface can only exit out of the wan1 interface.



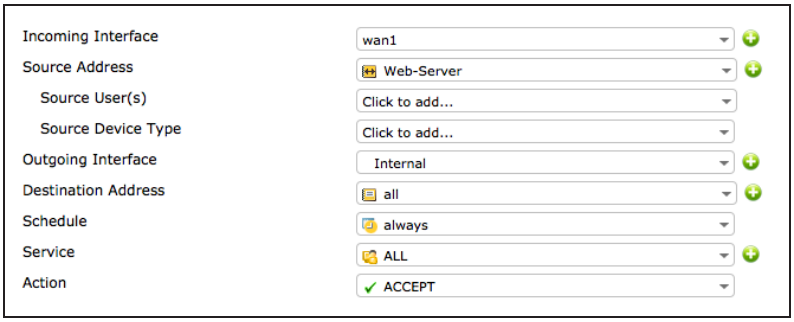
3. Creating security policies

Go to **Policy & Objects > Policy > IPv4**.

Create a security policy that allows internal users to access the protected web server using HTTP and HTTPS.



Create a second security policy that allows connections from the web server to the internal network and to the Internet using any service.



4. Results

Connect to the web server from the internal network and surf the Internet from the server itself.

Go to **Log & Report > Traffic Log > Forward Traffic** to verify that there is traffic from the internal to wan1 interface.

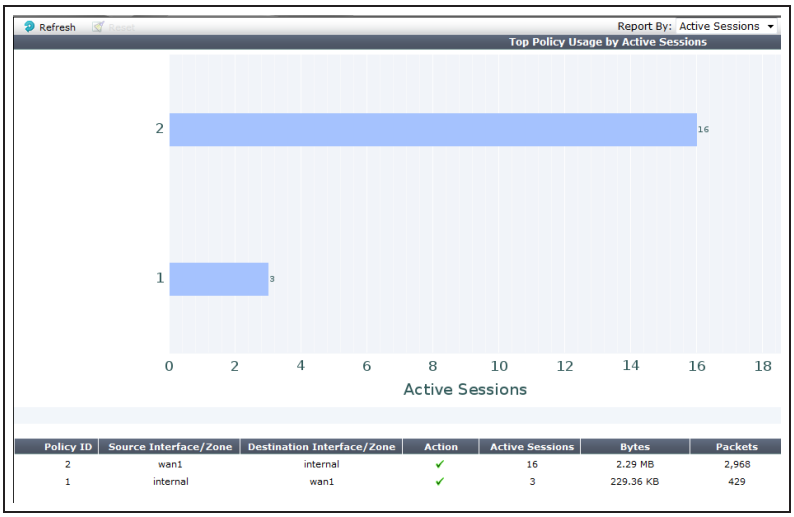
Select an entry for details.

Refresh | Download Raw Log | Log location: Disk

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received	Policy ID	Service
1	11:05:11	wan1	internal	192.168.1.200	8.8.8.8	75 B / 286 B	2	DNS
2	11:05:11	wan1	internal	192.168.1.200	8.8.8.8	77 B / 277 B	2	DNS
3	11:05:11	wan1	internal	192.168.1.200	74.125.225.223	1.04 KB / 9.08 KB	2	HTTPS
4	11:05:06	wan1	internal	192.168.1.200	74.125.226.79	728 B / 2.62 KB	2	HTTPS
5	11:05:02	wan1	internal	192.168.1.200	192.168.1.99	0 B / 1.72 KB	2	8010/tcp
6	11:04:46	internal	wan1	192.168.1.111	192.168.1.200	164 B / 132 B	1	HTTP
7	11:04:46	internal	wan1	192.168.1.111	192.168.1.200	164 B / 132 B	1	HTTP
8	11:04:46	internal	wan1	192.168.1.111	192.168.1.200	164 B / 132 B	1	HTTP
9	11:04:42	wan1	internal	192.168.1.200	192.168.1.99	0 B / 1.72 KB	2	8010/tcp
10	11:04:27	internal	wan1	192.168.1.111	192.168.1.200	1.46 KB / 2.92 KB	1	HTTPS
11	11:04:27	internal	wan1	192.168.1.111	192.168.1.200	1.33 KB / 2.70 KB	1	HTTPS
12	11:04:27	internal	wan1	192.168.1.111	192.168.1.200	1.33 KB / 2.75 KB	1	HTTPS
13	11:04:22	wan1	internal	192.168.1.200	192.168.1.99	0 B / 1.72 KB	2	8010/tcp
14	11:04:21	wan1	internal	192.168.1.200	74.125.226.67	58.96 KB / 2.06 MB	2	HTTP

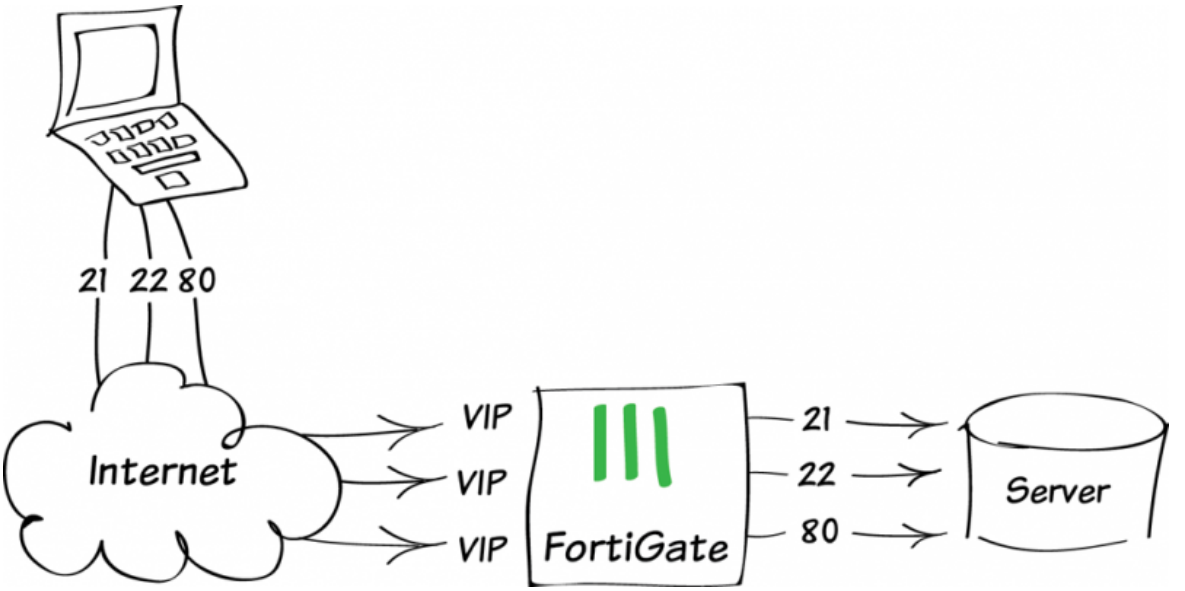
Dst	74.125.225.223	**Virtual Domain**	root
Received	9296	**Source Country**	Reserved
Application Name	SSL	**Sent / Received**	1.04 KB / 9.08 KB
Duration	17	**Sent**	1067
Application Details		**Service**	HTTPS
Protocol	6	**Destination Country**	United States
Application Control List	default	**Dst Port**	443
roll	65531	**Status**	close
Timestamp	Wed Mar 13 11:05:11 2013	**Tran Display**	noop
Sequence Number	700150	**Policy ID**	2
Src Interface	wan1	**Src**	192.168.1.200
Sent Packets	15	**Level**	notice
Application Category	Web.Surfing	**Application ID**	15895
Src Port	51218	**Application Control Action**	detected
Log ID	13	**Sub Type**	forward
Threat		**Received Packets**	13
Date/Time	11:05:11 (Wed Mar 13 11:05:11 2013)	**Dst Interface**	internal

Go to **Policy & Objects > Monitor > Policy Monitor** to view the active sessions.



For further reading, check out Interfaces in the FortiOS 5.2 Handbook.

Port forwarding



This example illustrates how to use virtual IPs to configure port forwarding on a FortiGate unit. In this example, TCP ports 80 (HTTP), 21 (FTP), and 22 (SSH) are opened, allowing remote connections to communicate with a server behind the firewall.

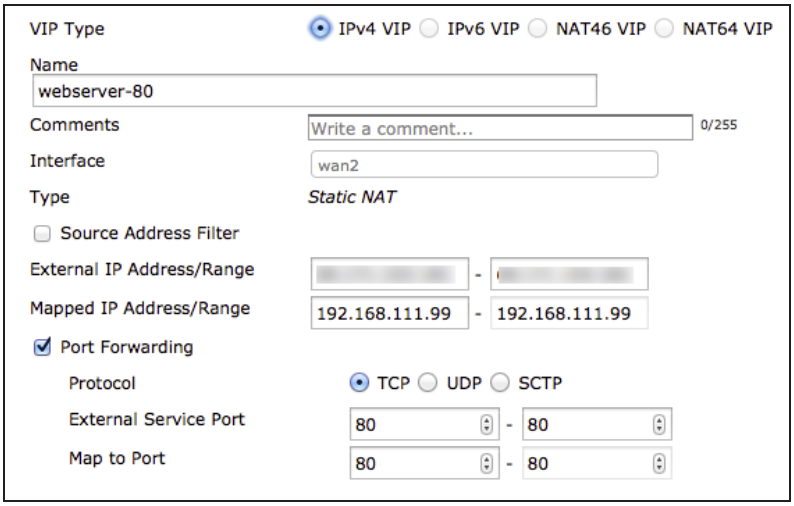
A video of this recipe can be found here.

1. Creating three virtual IPs

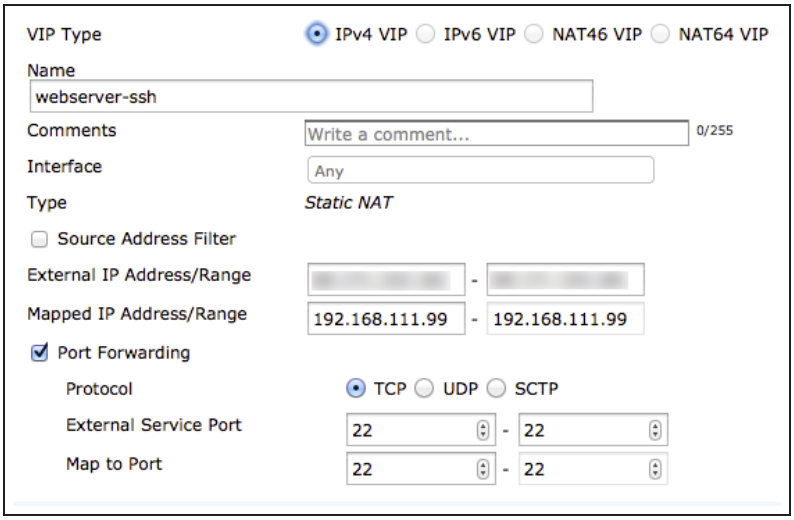
Go to **Policy & Objects > Objects > Virtual IPs > Create New > Virtual IP**.

Enable **Port Forwarding** and add a virtual IP for TCP port 80. Label this VIP *webserver-80*.

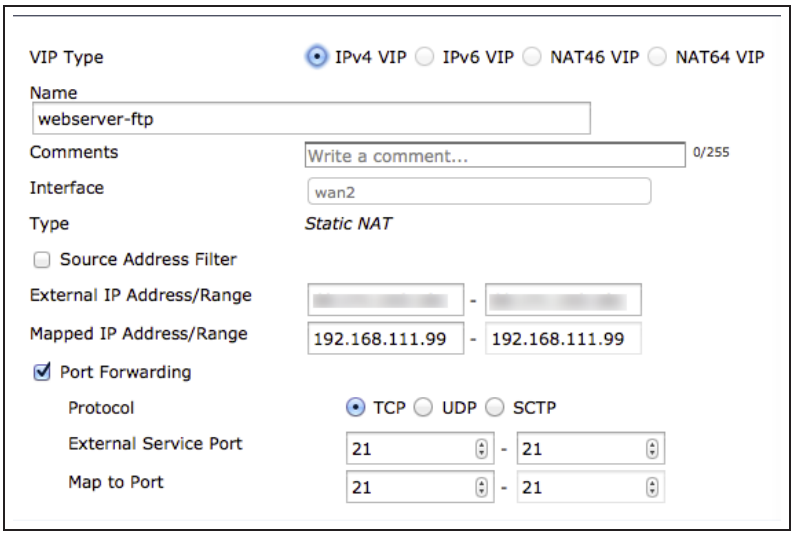
While this example maps port 80 to port 80, any valid External Service port can be mapped to any listening port on the destination computer.



Create a second virtual IP for TCP port 22. Label this VIP *webserver-ssh*.



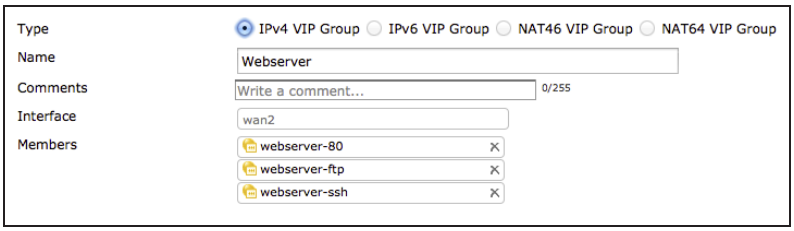
Create a third a virtual IP for TCP port 21. Label this VIP *webserver-ftp*.



2. Adding virtual IPs to a VIP group

Go to **Policy & Objects > Objects > Virtual IPs > Create New > Virtual IP Group**.

Create a VIP group. Under **Members**, include all three virtual IPs previously created.

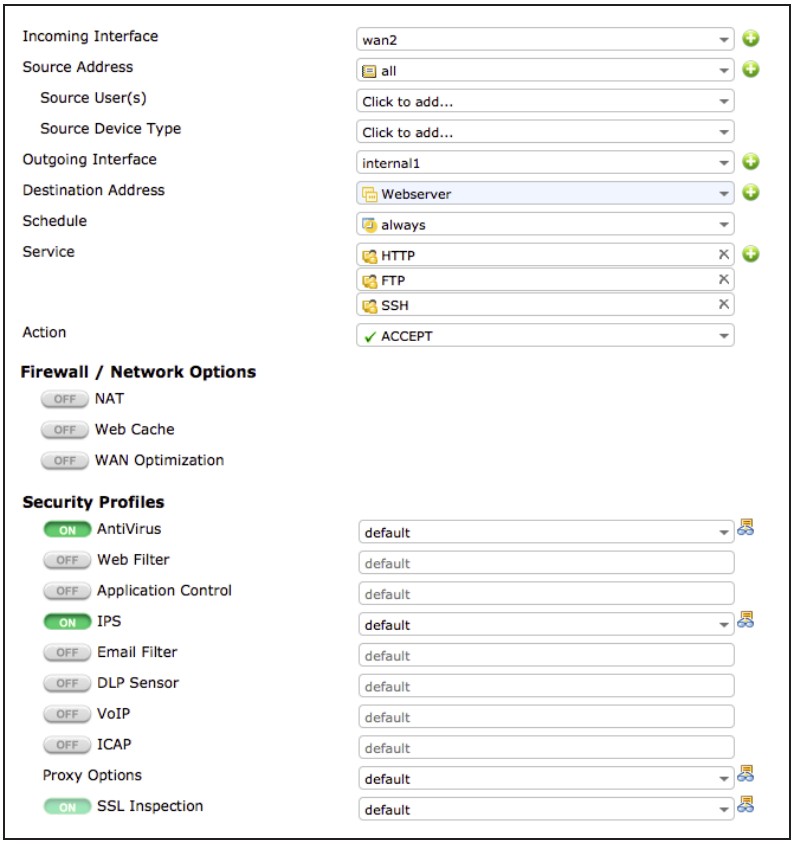


3. Creating a security policy

Go to **Policy & Objects > Policy > IPv4** and create a security policy allowing access to a server behind the firewall.

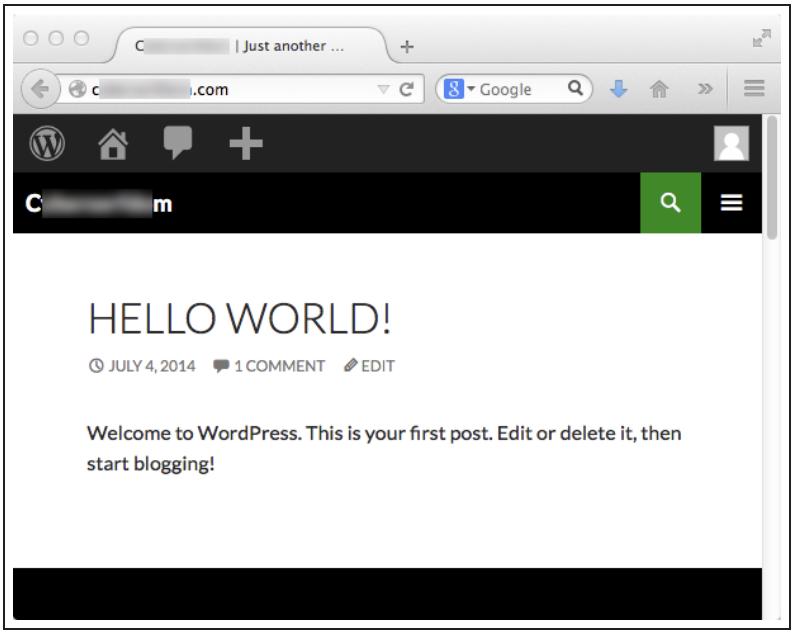
Set **Incoming Interface** to your Internet-facing interface, **Outgoing Interface** to the interface connected to the server, and **Destination Address** to the VIP group. Set **Service** to allow **HTTP**, **FTP**, and **SSH** traffic.

Use the appropriate **Security Profiles** to protect the servers.

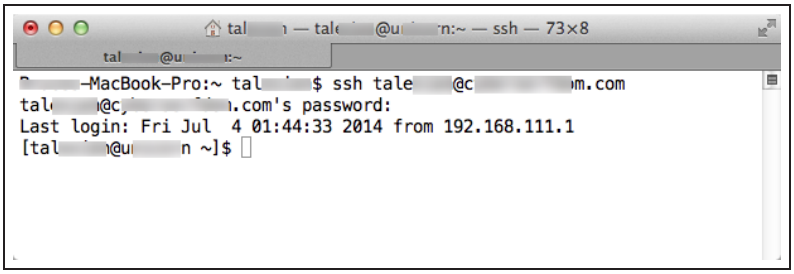


4. Results

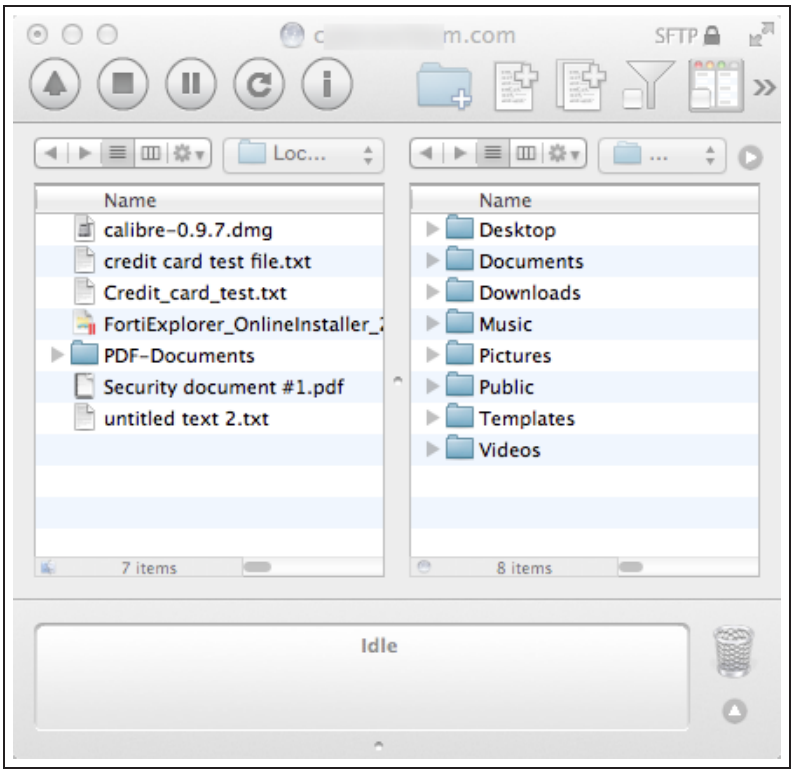
To ensure that TCP port 80 is open, connect to the web server on the other side of the firewall.



To ensure that TCP port 22 is open, connect to the SSH server on the other side of the firewall.

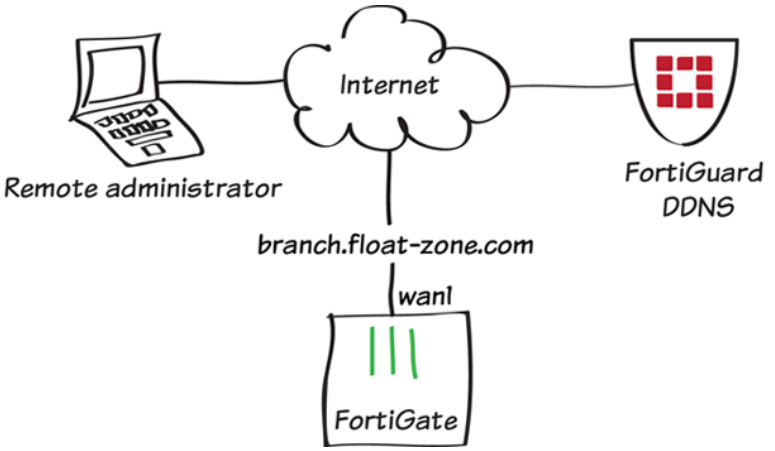


To ensure that TCP port 21 is open, use an FTP client to connect to the FTP server on the other side of the firewall.



For further reading, check out Virtual IPs in the FortiOS 5.2 Handbook.

FortiGuard DDNS



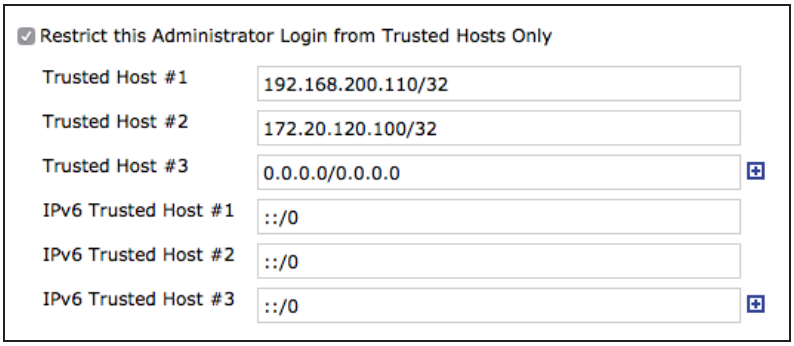
In this example, you will use FortiGuard Dynamic Domain Name Service (DDNS) to allow a remote administrator to access your FortiGate's Internet-facing interface using a domain name that remains constant, even when its IP address changes.

An active FortiCare Support Contract is required to use FortiGuard DDNS.

1. Limited administrative access to trusted hosts

Go to **System > Admin > Administrators** and edit the default *admin* account.

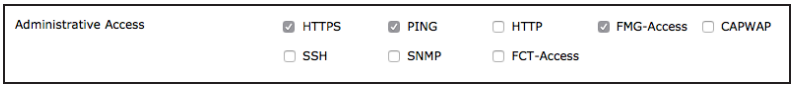
Enable **Restrict this Administrator Login from Trusted Hosts Only**. Add the required internal or remote devices as Trusted Hosts. You can also set an entire subnet as the trusted host, using /24 as the netmask.



2. Enabling HTTP/HTTPS access on the Internet-facing interface

Go to **System > Network > Interfaces** and edit the Internet-facing interface (typically **wan1**).

Make sure that **Administrative Access** is allowed for HTTPS.



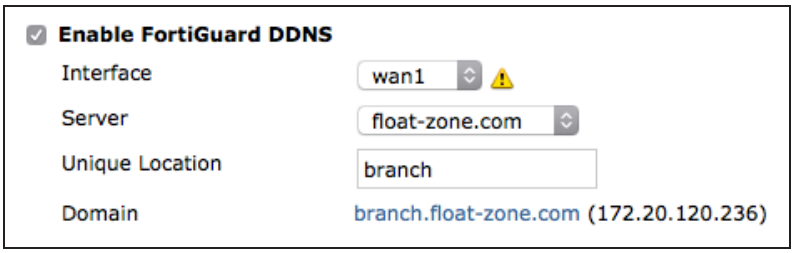
2. Setting up FortiGuard DDNS

Go to **System > Network > DNS** and enable **FortiGuard DDNS**.

Set **Interface** to your Internet-facing interface, select a **Server**, and select a **Unique Location** that will be used in the domain name.

The FortiGuard DDNS service will verify that the resulting domain name is unique and valid. If it is valid, select **Apply**. The domain name is now displayed, with the current IP address of the interface.

You can click the domain name to browse to the address with a web server.



You can also configure FortiGuard

```
config system ddns
```

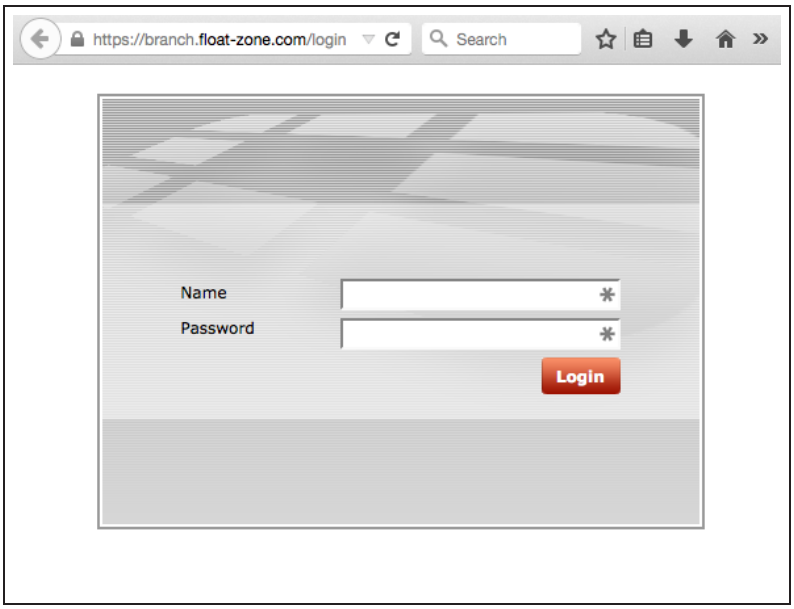
DDNS by using the following CLI commands:

```
  edit 0
    set ddns-server FortiGuardDDNS
    set ddns-domain "branch.float-zone.com"
    set monitor-interface wan1
  end
end
```

3. Results

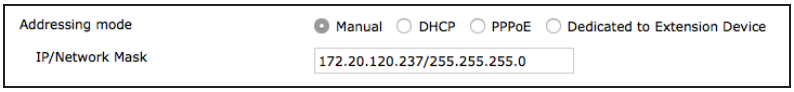
Browse to the domain name assigned to the interface, using HTTPS (in the example, https://branch.float-zone.com).

The FortiGate login screen will appear.



Go to **System > Network > Interfaces** and edit the Internet-facing interface.

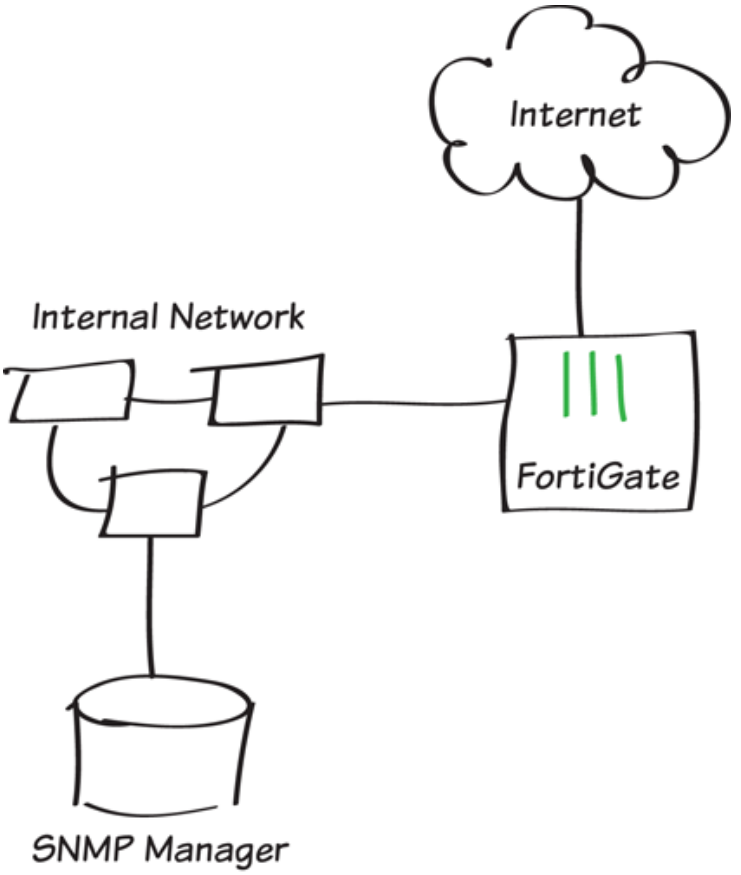
Change the interface's **IP Address/Netmask**.



You will still be able to access the interface using the domain name.

For further reading, check out Dynamic DNS configuration in the FortiOS 5.2 Handbook.

SNMP monitoring

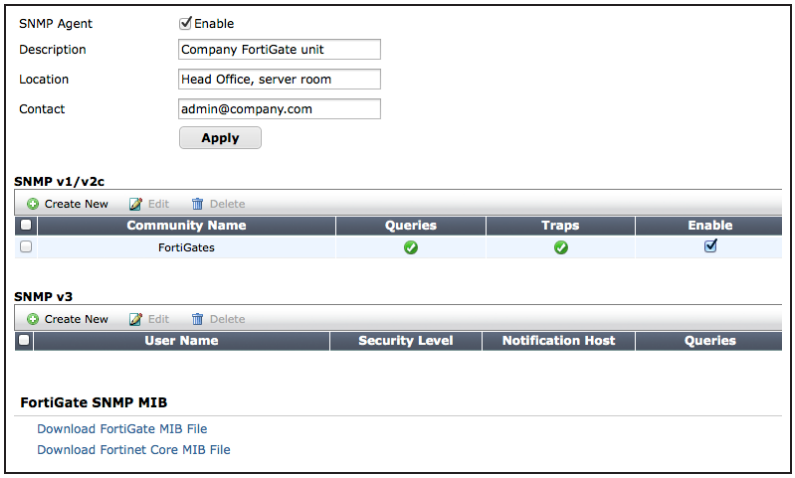


In this example, you configure the FortiGate SNMP agent and an example SNMP manager so that the SNMP manager can get status information from the FortiGate unit and so that the FortiGate unit can send traps to the SNMP manager.

The Simple Network Management Protocol (SNMP) enables you to monitor hardware on your network. You configure the hardware, such as the FortiGate SNMP agent, to report system information and send traps (alarms or event messages) to SNMP managers.

1. Configuring the FortiGate SNMP agent

Go to **System > Config > SNMP**. Enable the **SNMP Agent** and add any necessary information.

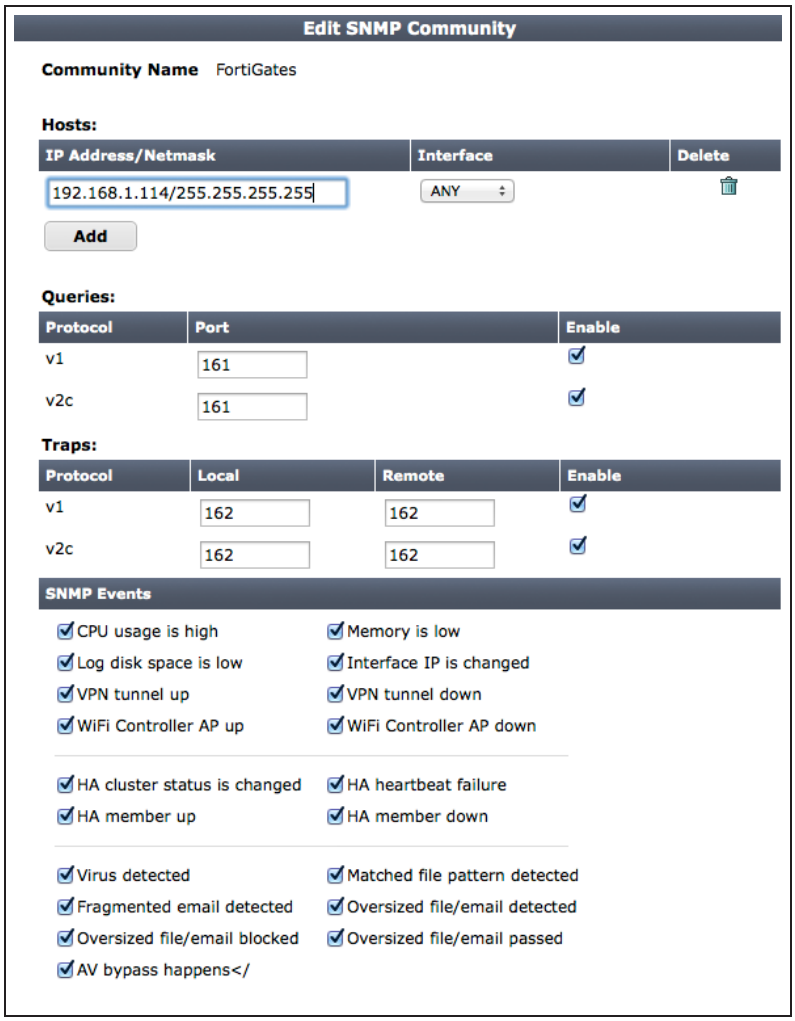


Under SNMP v1/v2c, create a new community.

Add the IP address of SNMP manager (in the example, *192.168.1.114/32*). If required, change the query and trap ports to match the SNMP manager.

You can add multiple SNMP managers, or set the **IP address/Netmask** to *0.0.0.0/0.0.0.0* and the **Interface** to **ANY**, so that any SNMP manager on any network connected to the FortiGate unit can use this SNMP community and receive traps from the FortiGate unit.

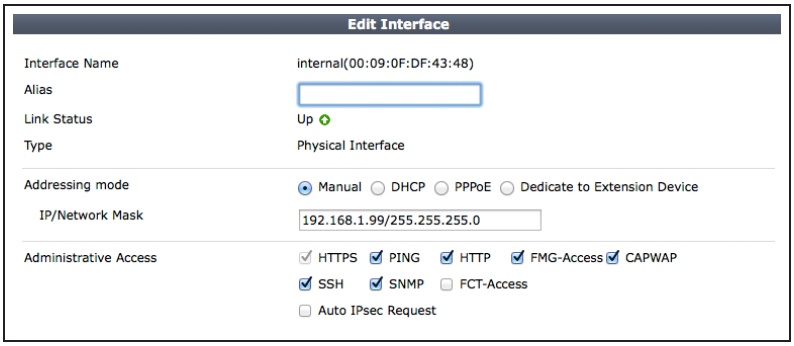
Enable the **SNMP Events** (traps) that you need. In most cases, leave them all enabled.



2. Enabling SNMP on a FortiGate interface

Go to **System > Network > Interfaces** and edit the interface connected to the same network as the SNMP manager.

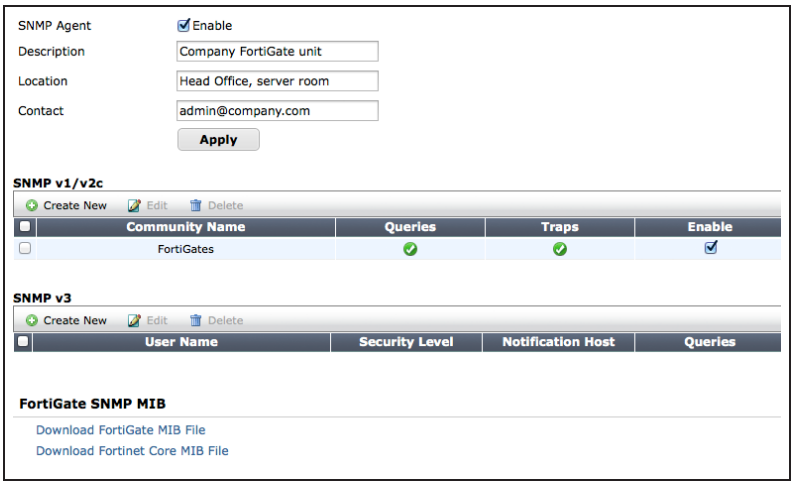
Enable **SNMP** for **Administrative Access**.



3. Downloading the Fortinet MIB files to and configuring an example SNMP manage

Two types of MIB files are available for FortiGate units: the Fortinet MIB and the FortiGate MIB. The Fortinet MIB contains traps, fields, and information that is common to all Fortinet products. The FortiGate MIB contains traps, fields, and information that is specific to FortiGate units.

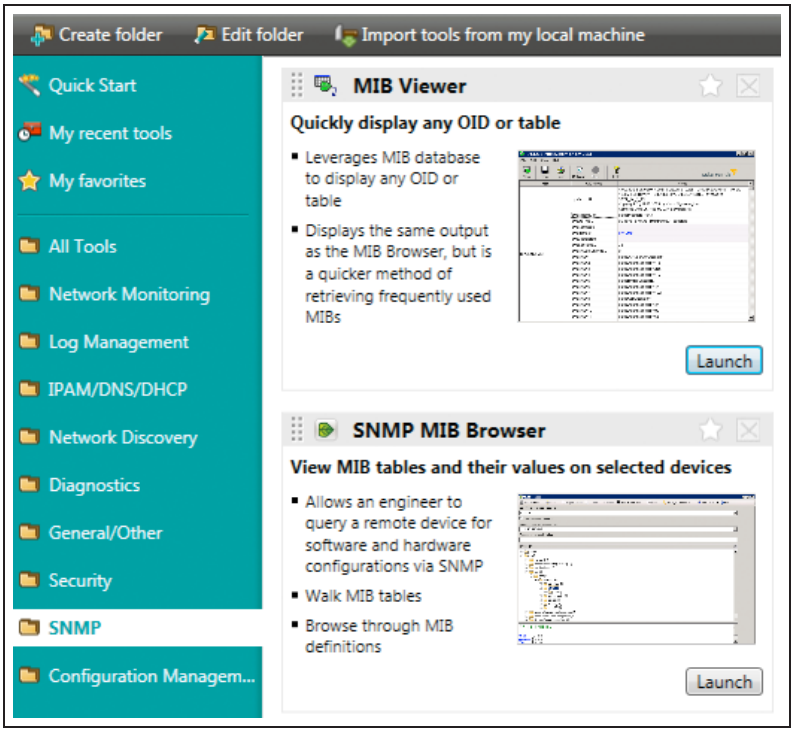
Go to **System > Config > SNMP** and select **Download FortiGate SNMP MIB File** and **Download Fortinet Core MIB File**.Configure the SNMP manager to receive traps from the FortiGate unit. Install the FortiGate and Fortinet MIBs.



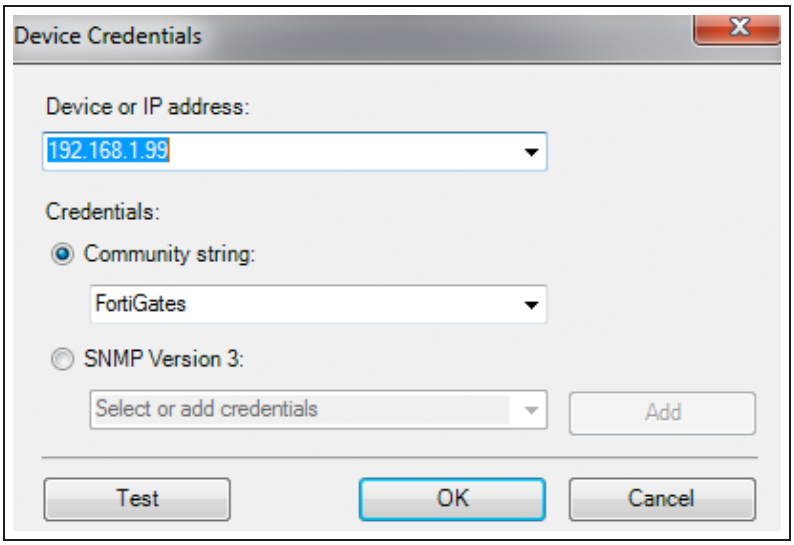
4. Results

This example uses the SolarWinds SNMP trap viewer.

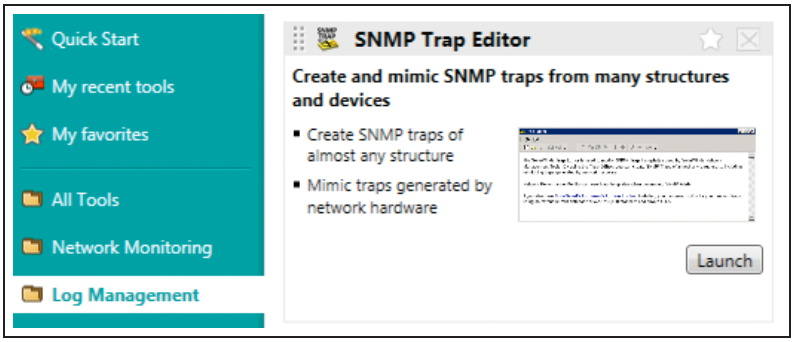
In the SolarWinds Toolset Launch Pad, go to **SNMP > MIB Viewer** and select **Launch**.



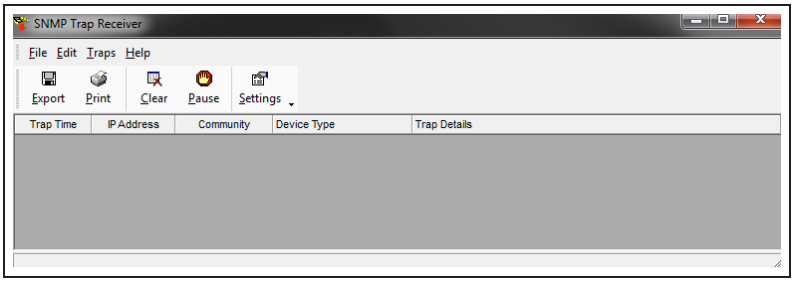
Choose **Select Device**, enter the IP address of the FortiGate unit, and choose the appropriate community string credentials.



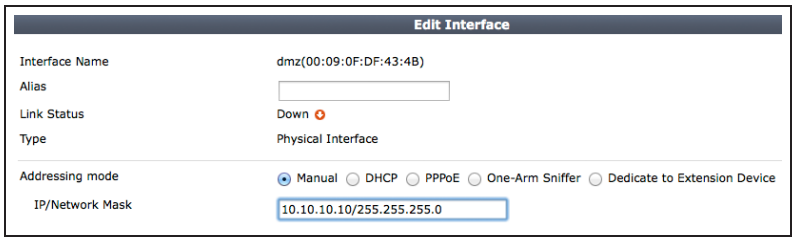
Open the **SNMP Trap Receiver** and select **Launch**.



The SNMP Trap Receiver will appear.



On the FortiGate unit, perform an action to trigger a trap (for example, change the IP address of the DMZ interface).

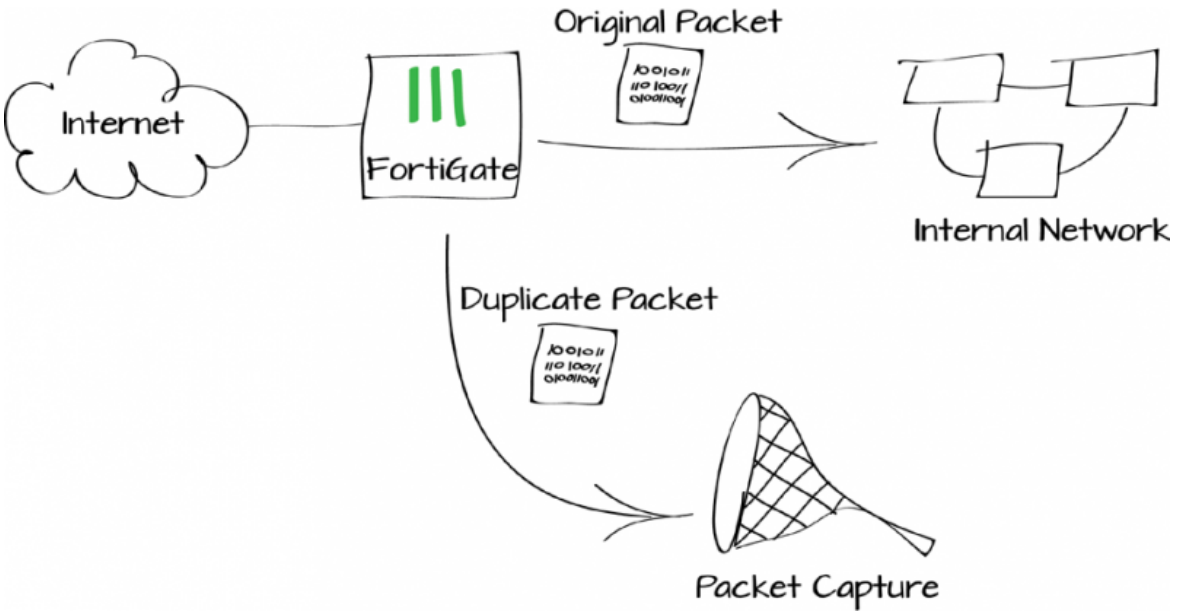


Verify that the SNMP manager receives the trap.

Trap Time	IP Address	Community	Device Type	Trap Details
08-Mar-13 10:49 AM	192.168.1.99	FortiGates		sysUpTime = 6976332 snmpTrapOID = fnTrapInfChg.1.3.0.201 fnTrapInfChg.1.1.1 = FG100D3G12801361 sysName = FG100D3G12801361 ifIndex = 2
08-Mar-13 10:49 AM	192.168.1.99	FortiGates	fnTrapSystem.1.1004	sysUpTime = 6976332 snmpTrapOID = fnTrapSystem.1.1004.0.201 fnTrapInfChg.1.1.1 = FG100D3G12801361 sysName = FG100D3G12801361 ifIndex = 2 experimental.1057.1 = 192.168.1.99
08-Mar-13 10:49 AM	192.168.1.99	FortiGates		sysUpTime = 6976332 snmpTrapOID = fnTrapSystem.6.0.1004 fnTrapInfChg.1.1.1 = FG100D3G12801361 ifName.2 = dmz fnTrapSystem.6.2.1 = 10.10.10.1 fnTrapSystem.6.2.2 = 255.255.255.0
08-Mar-13 10:49 AM	192.168.1.99	FortiGates	fnTrapSystem.1.1004	sysUpTime = 6976332 snmpTrapOID = fnTrapSystem.1.1004.0.1004 fnTrapInfChg.1.1.1 = FG100D3G12801361 ifName.2 = dmz fnTrapSystem.6.2.1 = 10.10.10.1 fnTrapSystem.6.2.2 = 255.255.255.0 experimental.1057.1 = 192.168.1.99

For further reading, check out SNMP in the FortiOS 5.2 Handbook.

Packet capture



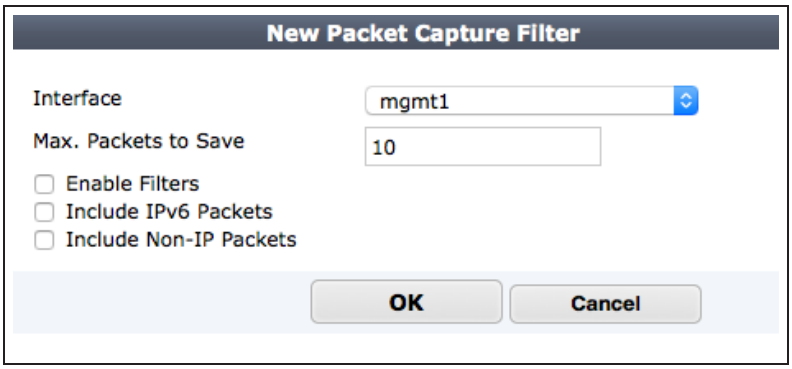
In this example, you will set up and run some basic packet capture filters on your FortiGate and download and view the resulting .pcap file.

You can use packet capturing to learn about network activity seen by your FortiGate by creating and saving packet capture filters that define the packets to capture. You can then run these filters at any time, download the resulting .pcap (packet capture) file, and use a tool like Wireshark to analyze the results.

1. Creating packet capture filters

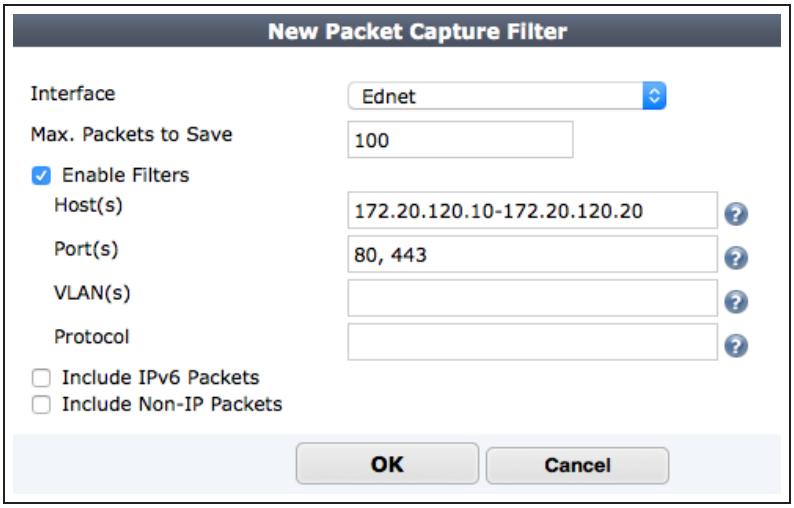
Go to **System > Network > Packet Capture** and create a new filter. Below are a few examples of different filters you can use.

The simplest filter just captures all of the packets received by an interface. This example captures 10 packets received by the mgmt1 interface.



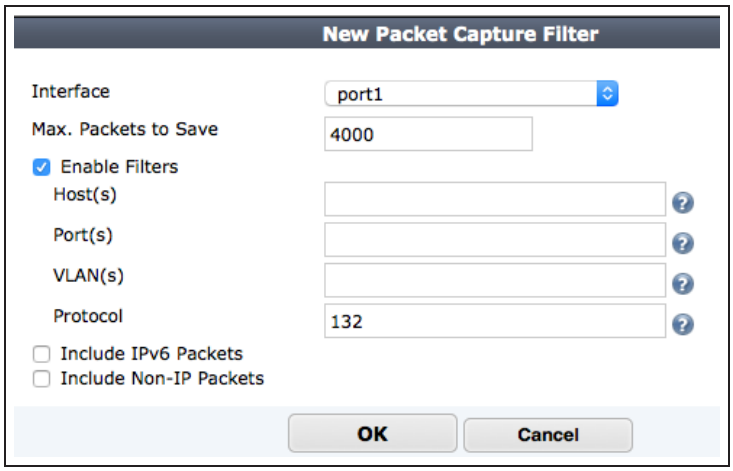
You can select **Enable Filters** to restrict the packets to capture.

This filter captures 100 HTTP and HTTPS packets (port 80 and 443) received by the Ednet wireless interface that have a source or destination address in the range 172.20.120.10 to 172.20.120.20.

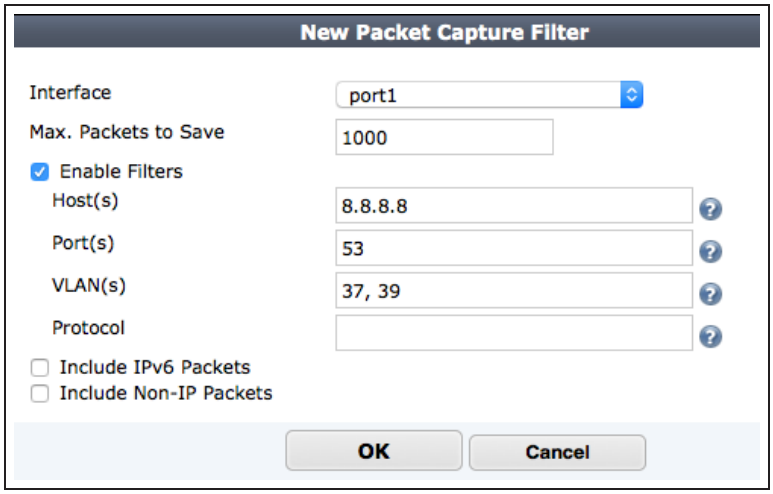


This filter captures the first 4000 Stream Control Transmission Protocol (SCTP) packets received by the port1 interface.

Protocols are identified using IP protocol numbers; for example, SCTP is protocol 132.



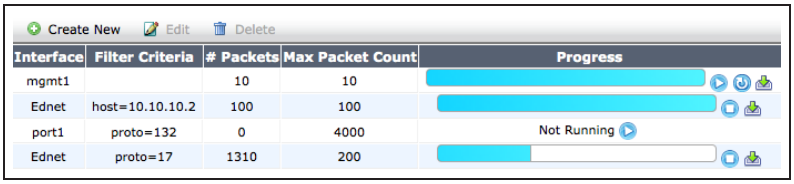
This filter captures the first 1000 DNS packets querying the Google DNS server (IP address 8.8.8.8) with VLAN IDs 37 or 39.



2. Results

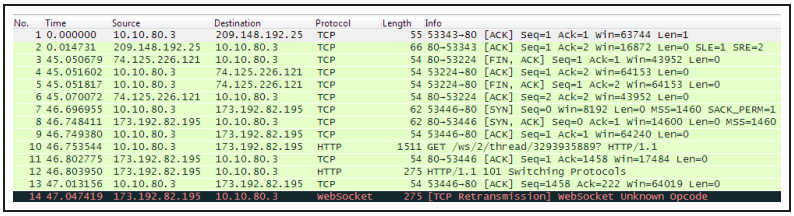
Running packet capture filters may affect FortiGate performance.

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



You can stop and restart multiple filters at any time.

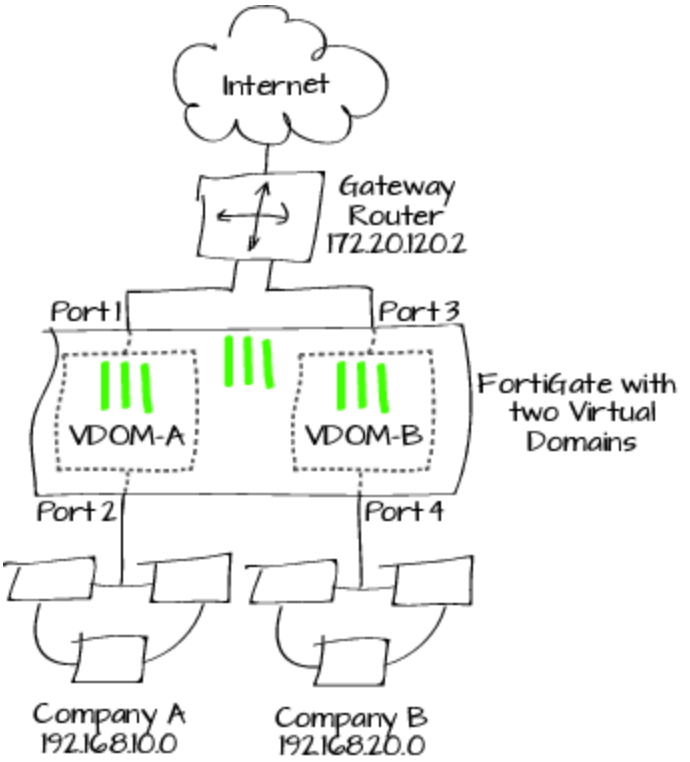
Download any saved .pcap file to your computer. You can open the file with a .pcap file viewer like Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.80.3	209.148.192.25	TCP	55	53343→80 [ACK] Seq=1 Ack=1 Win=63744 Len=1
2	0.014731	209.148.192.25	10.10.80.3	TCP	66	80→53343 [ACK] Seq=1 Ack=2 Win=16872 Len=0 SLE=1 SRE=2
3	45.050679	74.125.226.121	10.10.80.3	TCP	54	80→53224 [FIN, ACK] Seq=1 Ack=1 Win=43952 Len=0
4	45.051602	10.10.80.3	74.125.226.121	TCP	54	53224→80 [ACK] Seq=1 Ack=2 Win=64153 Len=0
5	45.051817	10.10.80.3	74.125.226.121	TCP	54	53224→80 [FIN, ACK] Seq=1 Ack=2 Win=64153 Len=0
6	45.070072	74.125.226.121	10.10.80.3	TCP	54	80→53224 [ACK] Seq=2 Ack=2 Win=43952 Len=0
7	46.696955	10.10.80.3	173.192.82.195	TCP	62	53446→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
8	46.748411	173.192.82.195	10.10.80.3	TCP	62	80→53446 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
9	46.749380	10.10.80.3	173.192.82.195	TCP	54	53446→80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	46.753544	10.10.80.3	173.192.82.195	HTTP	1511	GET /ws/2/thread/3293935889? HTTP/1.1
11	46.802775	173.192.82.195	10.10.80.3	TCP	54	80→53446 [ACK] Seq=1 Ack=1458 Win=17484 Len=0
12	46.803950	173.192.82.195	10.10.80.3	HTTP	275	HTTP/1.1 101 Switching Protocols
13	47.013156	10.10.80.3	173.192.82.195	TCP	54	53446→80 [ACK] Seq=1458 Ack=222 Win=64019 Len=0
14	47.047419	173.192.82.195	10.10.80.3	WebSocket	275	[TCP Retransmission] WebSocket Unknown Opcode

For further reading, check out Monitoring in the FortiOS 5.2 Handbook.

VDOM configuration



This example illustrates how to use VDOMs to host two FortiOS instances on a single FortiGate unit.

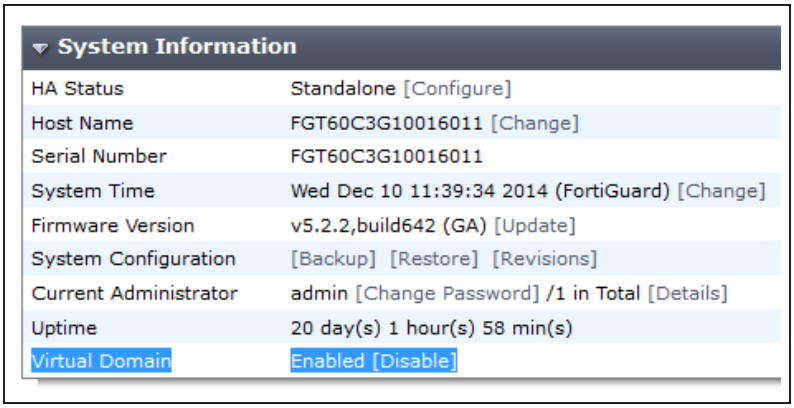
Virtual Domains (VDOMs) can be used to divide a single FortiGate unit into two or more virtual instances of FortiOS that function as independent FortiGate units. This example simulates an ISP that provides Company A and Company B with distinct Internet services. Each company has its own VDOM, IP address, and internal network.

1. Switching to VDOM mode and creating two VDOMS

Go to **System > Dashboard > Status**.

In the **System Information** widget, find **Virtual Domain** and select **Enable**.

You will be required to re-login after enabling **Virtual Domain** due to the GUI menu options changing.



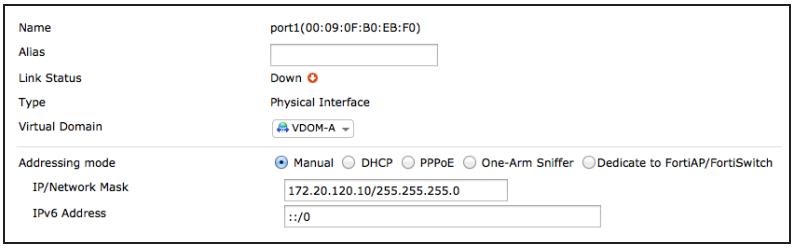
Go to **Global > VDOM > VDOM**.

Create two VDOMS: *VDOM-A* and *VDOM-B*. Leave both VDOMs as **Enabled**, with **Operation Mode** set to **NAT**.

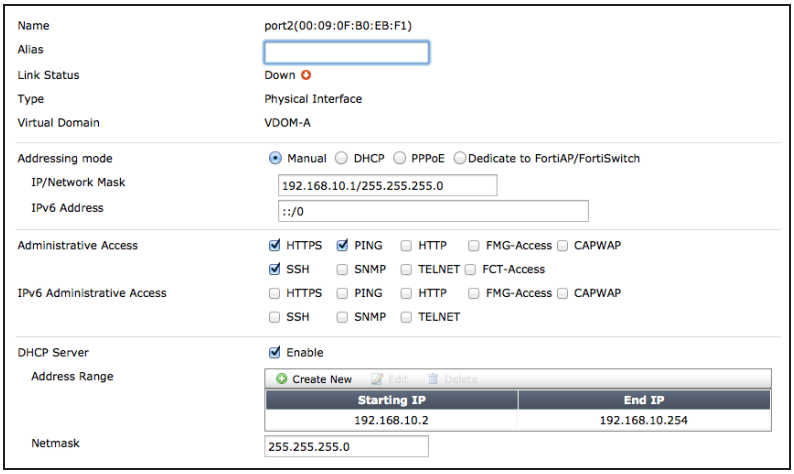
2. Assigning interfaces to each VDOM

Go to **Global > Network > Interfaces**.

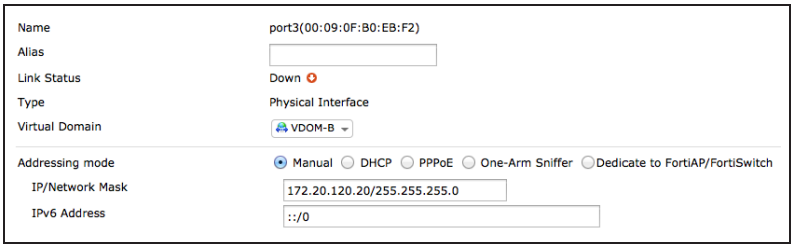
Edit **port1** and add it to VDOM-A. Set **Addressing Mode** to **Manual** and assign an **IP/Network Mask** to the interface (in the example, *172.20.120.10/255.255.255.0*).



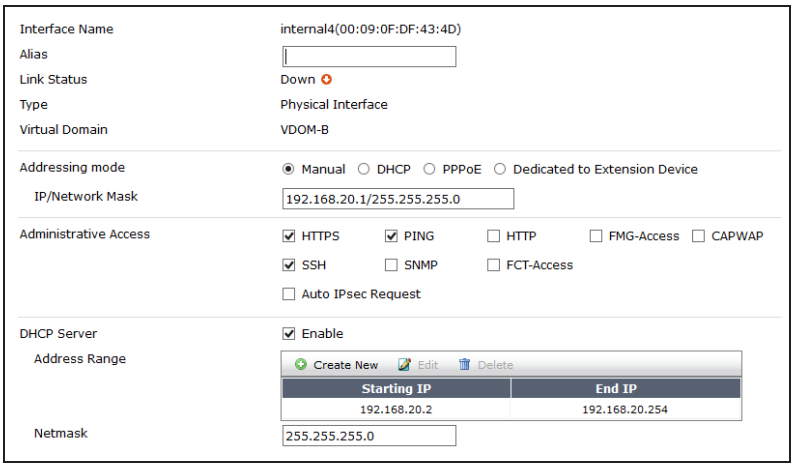
Edit **port2** and add it to VDOM-A. Set **Addressing Mode** to **Manual**, assign an **IP/Network Mask** to the interface (in the example, *192.168.10.1/255.255.255.0*), and set **Administrative Access** to **HTTPS**, **PING**, and **SSH**. Enable **DHCP Server**.



Edit **port3** and add it to VDOM-B. Set **Addressing Mode** to **Manual** and assign an **IP/Network Mask** to the interface (in the example, *172.20.120.20/255.255.255.0*).



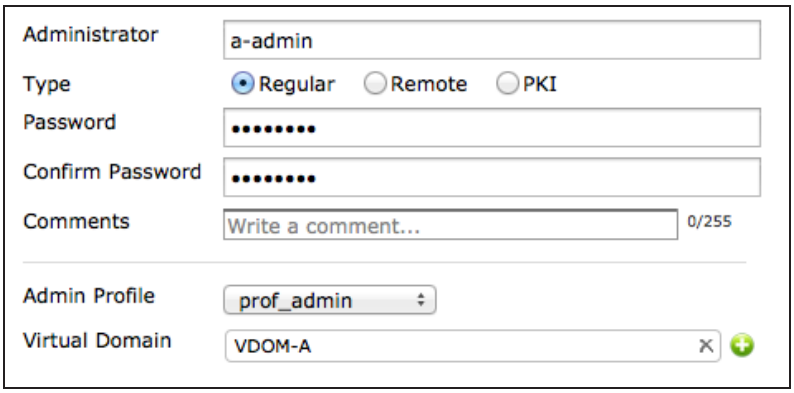
Edit **port4** and add it to VDOM-B. Set **Addressing Mode** to **Manual**, assign an **IP/Network Mask** to the interface (in the example, *192.168.20.1/255.255.255.0*), and set **Administrative Access** to **HTTPS**, **PING**, and **SSH**. Enable *DHCP Server*.



3. Creating administrators for each VDOM

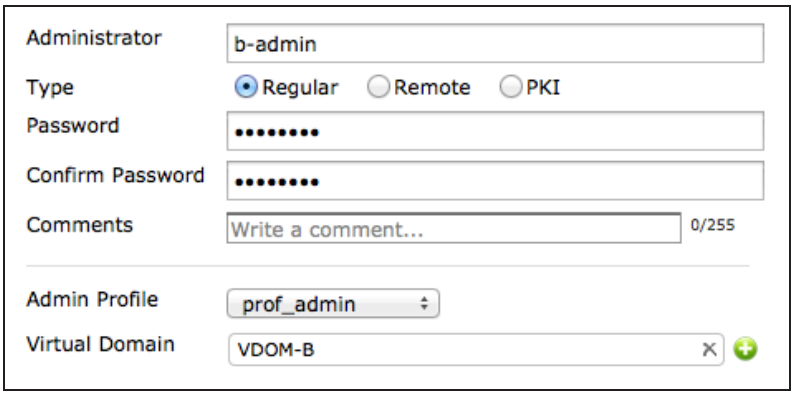
Go to **Global > Admin > Administrators**.

Create an administrators for VDOM-A, called *a-admin*. Set **Type** to **Regular**, set a password, and set **Admin Profile** to **prof_admin**.



Create an administrators for VDOM-B, called *b-admin*. Set **Type** to **Regular**, set a password, and set **Admin Profile** to **prof_admin**.

Make sure to remove the **root** VDOM from both administrator accounts.

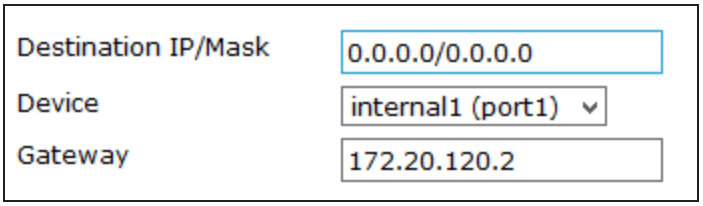


4. Creating a basic configuration for VDOM-A

Go to **Virtual Domains** and select **VDOM-A**.

Go to **System > Network > Routing**.

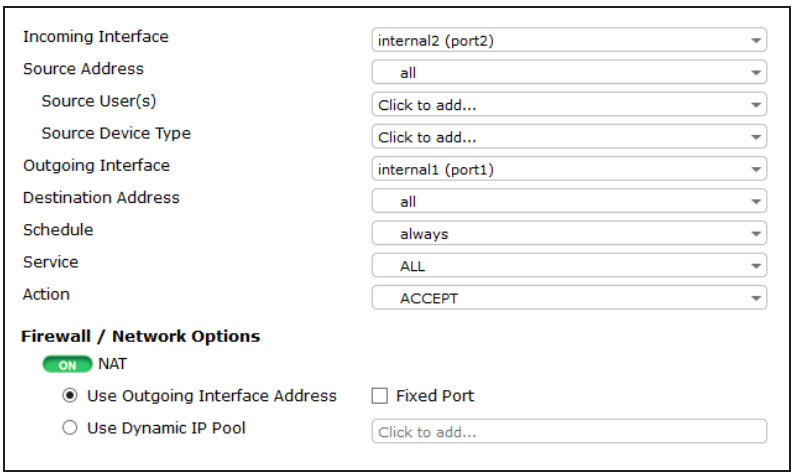
Create a default route for the VDOM. Set **Destination IP/Mask** to *0.0.0.0/0.0.0.0*, set **Device** to **port1**, and set **Gateway** to the IP of the gateway router (in the example, *172.20.120.2*).



Connect a PC to port2. Using HTTPS protocol, browse to the IP set for port2 and log into VDOM-A using the a-admin account (in the example, *192.168.10.1*).

Go to **Policy & Objects > Policy > IPv4**

Create a policy to allow Internet access. Set **Incoming Interface** to **port2** and **Outgoing Interface** to **port1**. Ensure **NAT** is turned **On**.



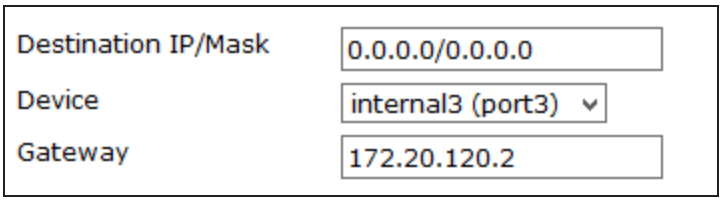
5. Creating a basic configuration for VDOM-B

If you have logged out of the FortiGate unit, log back in.

Go to **Virtual Domains** and select **VDOM-B**.

Go to **System > Network > Routing**

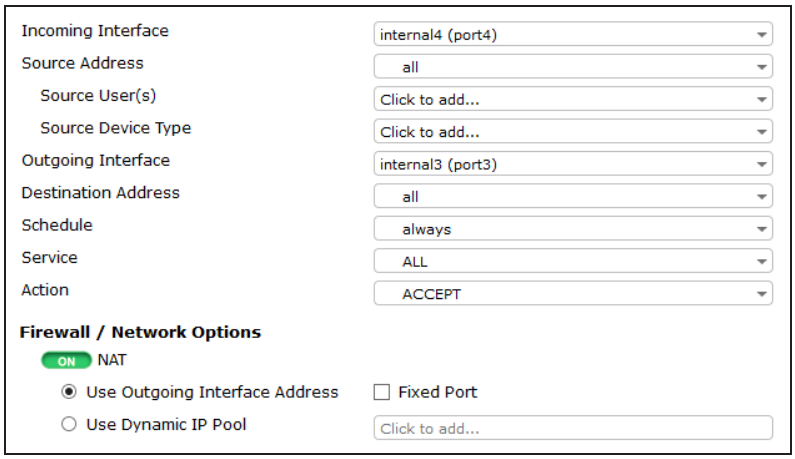
Create a default route for the VDOM. Set **Destination IP/Mask** to *0.0.0.0/0.0.0.0*, set **Device** to **port3**, and set **Gateway** to the IP of the gateway router (in the example, *172.20.120.2*).



Connect a PC to port4. Using HTTPS protocol, browse to the IP set for port4 and log into VDOM-B using the a-admin account (in the example, *https://192.168.10.1*).

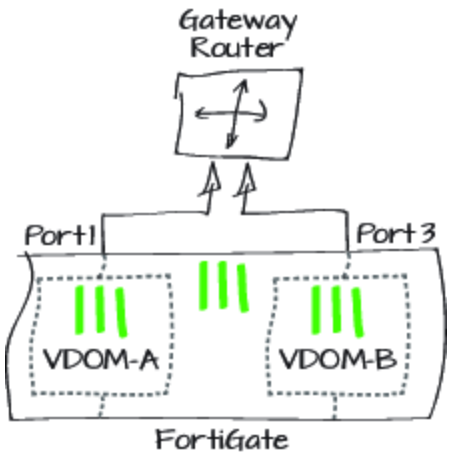
Go to **Policy & Objects > Policy > IPv4**

Create a policy to allow Internet access. Set **Incoming Interface** to **port4** and **Outgoing Interface** to **port3**. Ensure **NAT** is turned **On**.



6. Connecting the gateway router

Connect port 1 and port3 of the FortiGate unit to the gateway router to allow Internet traffic to flow.

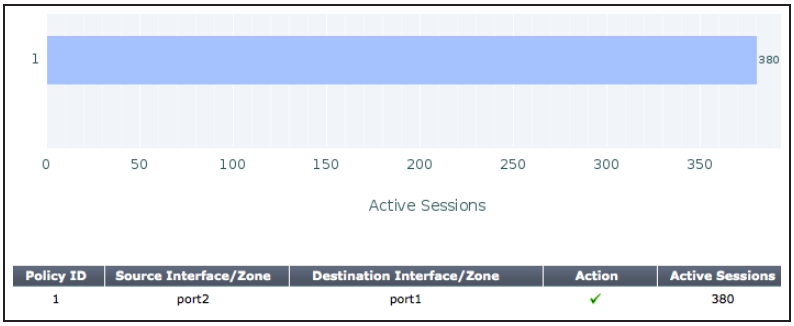


7. Results

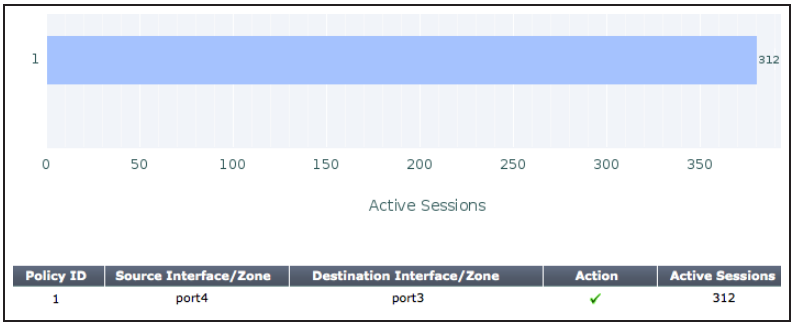
Connect to the Internet from the company A and company B networks and then log into the FortiGate unit

Go to **Virtual Domains** and select **VDOM-A**.

Go to **Policy & Objects > Monitor > Policy Monitor** to view the sessions being processed on VDOM-A.

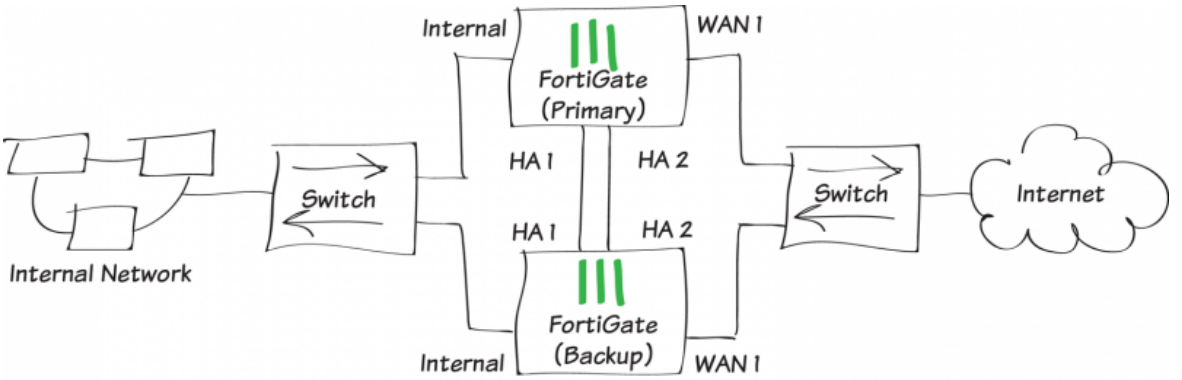


Go to **Policy & Objects > Monitor > Policy Monitor** to view the sessions being processed on VDOM-B.



For further reading, check out Virtual Domains in the FortiOS 5.2 Handbook.

High Availability with two FortiGates



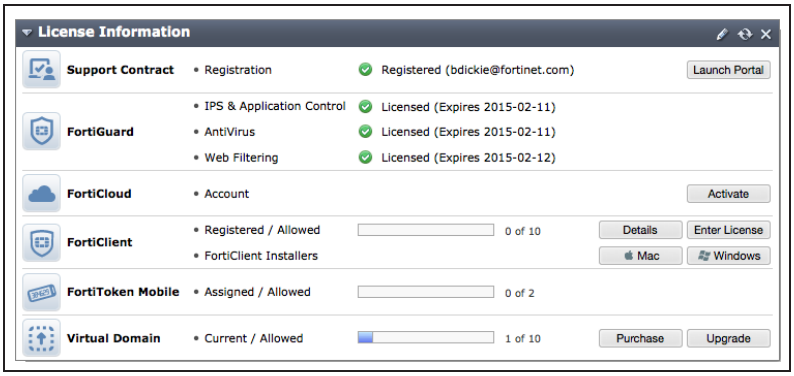
In this recipe, a backup FortiGate unit will be installed and connected to a FortiGate unit that has previously been installed to provide redundancy if the primary FortiGate unit fails. This set up, called High Availability (HA), improves network reliability.

If you have not already installed a FortiGate, see Installing a FortiGate in NAT/Route mode.

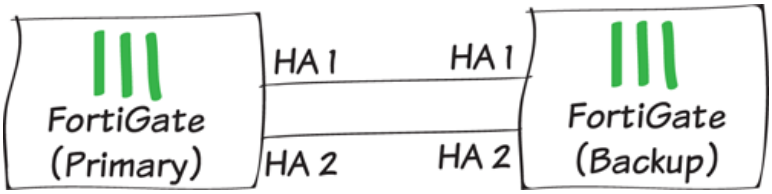
A video of this recipe is available here.

1. Adding the backup FortiGate unit and configuring HA

Make sure both FortiGates are running the same FortiOS firmware version. Register and apply licenses to the new FortiGate unit before adding it to the cluster. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**.



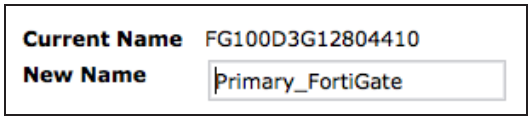
Connect your network as shown in the initial diagram, with Ethernet cables connecting the **HA** heartbeat interfaces of the two FortiGate units. If your FortiGate unit does not have dedicated HA heartbeat interfaces, you can use different interfaces, provided they are not used for any other function.



A switch must be used between the FortiGates and Internet, and another is required between the FortiGates and the internal network, as shown in the network diagram for this recipe.

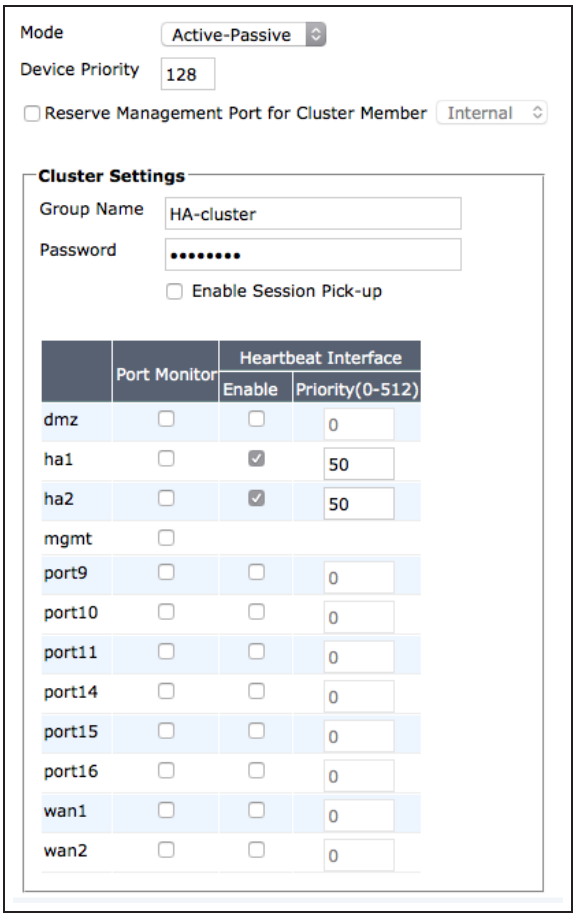
Connect to the primary FortiGate and go to **System > Dashboard > Status** and locate the **System Information** widget.

Change the unit's **Host Name** to identify it as the primary FortiGate.



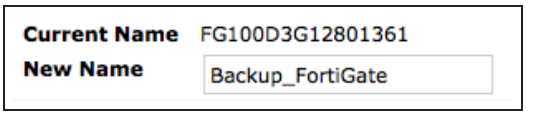
In the **System Information** widget, configure **HA Status**. Set the **Mode** to **Active-Passive** and set a **Group Name** and **Password**.

Ensure that the two **Heartbeat Interfaces** are selected and their priorities are both set to 50.



Connect to the backup FortiGate and go to **System > Dashboard > Status**.

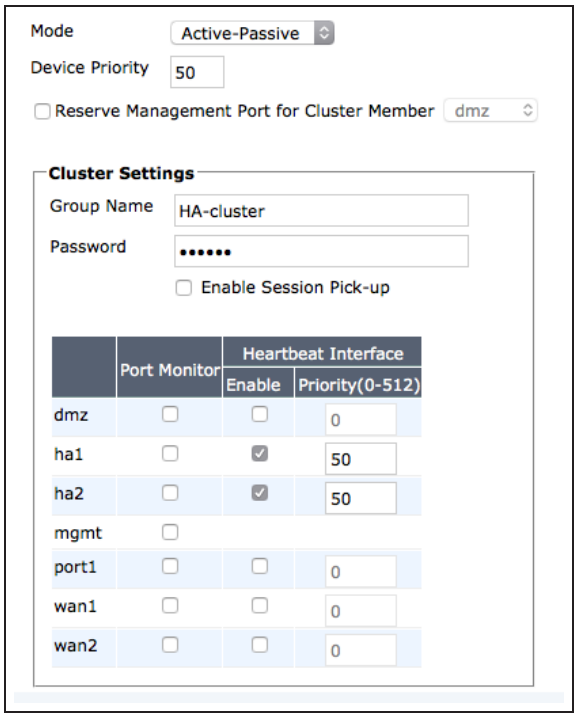
Change the unit's **Host Name** to identify it as the backup FortiGate.



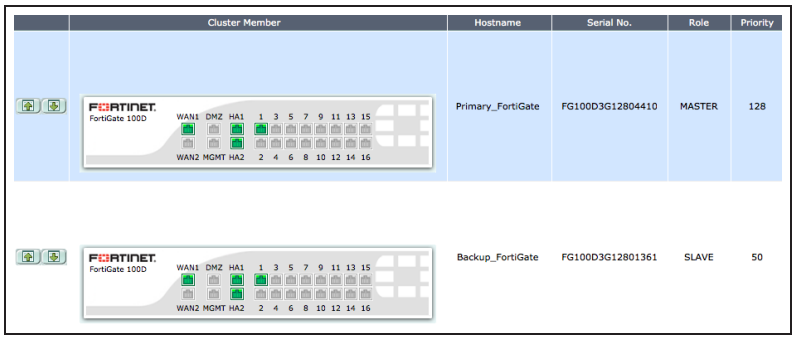
Configure **HA Status** and set the **Mode** to **Active-Passive**.

Set the **Device Priority** to be lower than the primary FortiGate. Ensure that the **Group Name** and **Password** match those on the primary FortiGate.

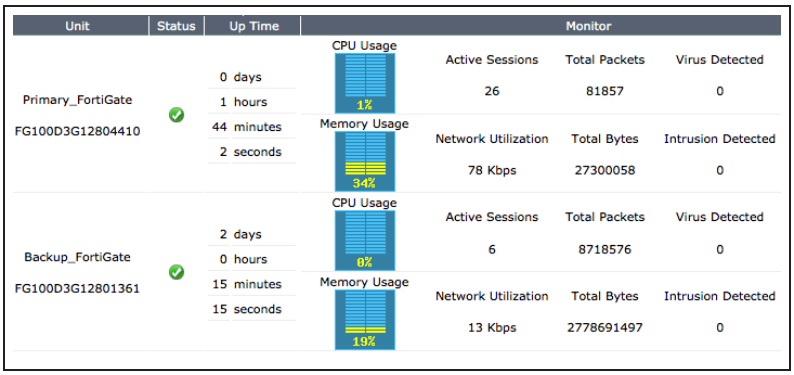
Ensure that the two **Heartbeat Interfaces** are selected and their priorities are both set to 50.



Connect to the primary FortiGate and go to **System > Config > HA** to view the cluster information.



Select **View HA Statistics** for more information on how the cluster is operating and processing traffic.



2. Results

Normally, traffic should now be flowing through the primary FortiGate. However, if the primary FortiGate is unavailable, traffic should failover and the backup FortiGate will be used. Failover will also cause the primary and backup FortiGates to reverse roles, even when both FortiGates are available again.

To test this, ping the IP address 8.8.8.8 using 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.

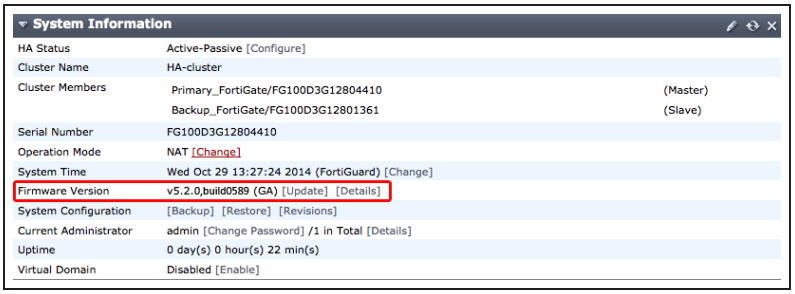
```
Reply from 8.8.8.8: bytes=32 time=50ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Request timed out.
Reply from 8.8.8.8: bytes=32 time=482ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
```

3. (Optional) Upgrading the firmware for the HA cluster

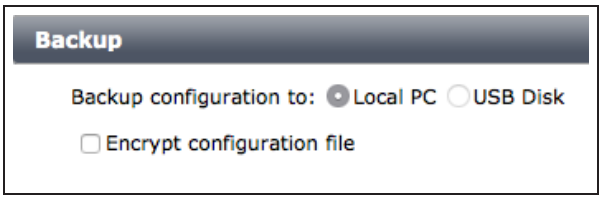
For information about accessing firmware images, see Updating your FortiGate's firmware.

When a new version of the FortiOS firmware becomes available, upgrading the firmware on the primary FortiGate will automatically upgrade the backup FortiGate's firmware as well.

Always review the Release Notes and Supported Upgrade Paths documentation before installing new firmware. These documents can be found at the Fortinet Document Library.

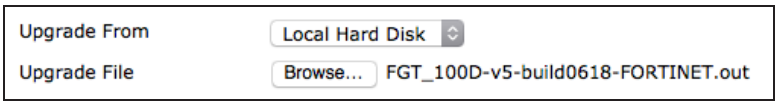


Go to **System > Dashboard > Status** and view the **System Information** widget. Now that the FortiGates are in HA mode, their configuration is synchronized and the **System Information** widget displays information for both units.



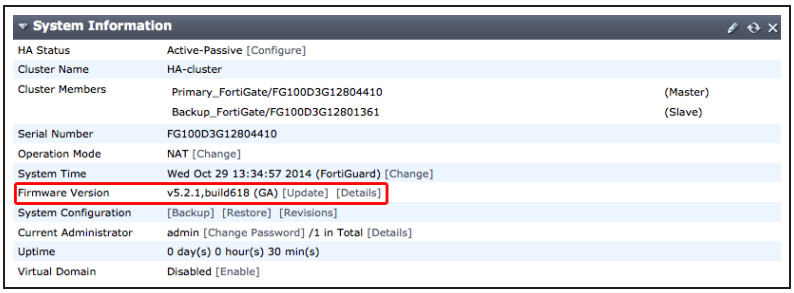
Select **Backup** beside **System Configuration**. Always remember to back up your configuration before doing any firmware upgrades.

Go to **System > Dashboard > Status** and view the **System Information** widget. Select **Upgrade** beside **Firmware Version**. Find the firmware image file that you downloaded and select **OK** to upload and install the firmware build.



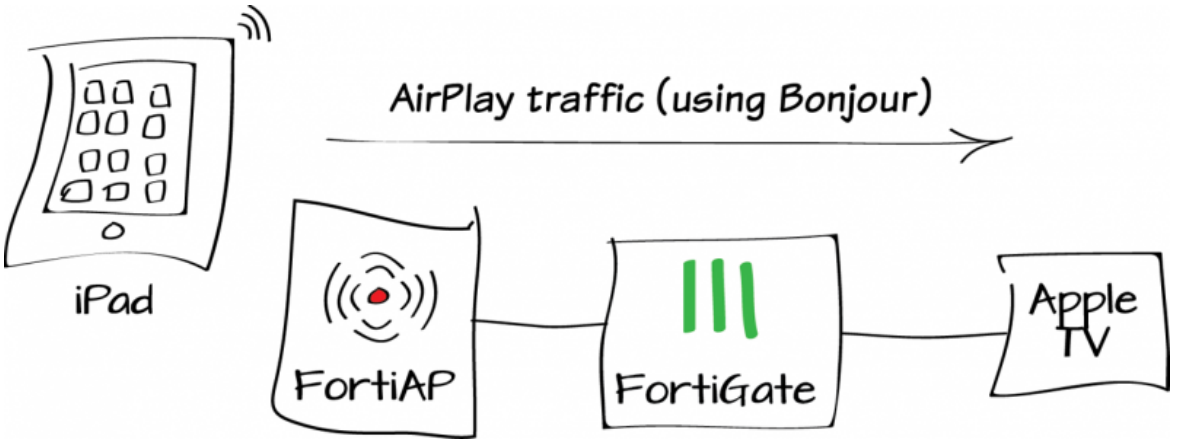
The firmware will load onto both the primary FortiGate unit and the backup unit.

Go to **System > Dashboard > Status** and verify that the **System Information** widget shows the new firmware version.



For further reading, check out Configuring and connecting HA clusters in the FortiOS 5.2 Handbook.

AirPlay for Apple TV



In this example, you will create multicast security policies to allow AirPlay communication between an iOS device and an Apple TV through a FortiGate unit.

Apple TV can also be connected to the Internet wirelessly. AirPlay will function from any iOS device connected to the same SSID as the Apple TV, without any configuration required on the FortiGate.

This recipe uses a FortiAP in Tunnel mode. For more information, see Setting up WiFi with FortiAP.

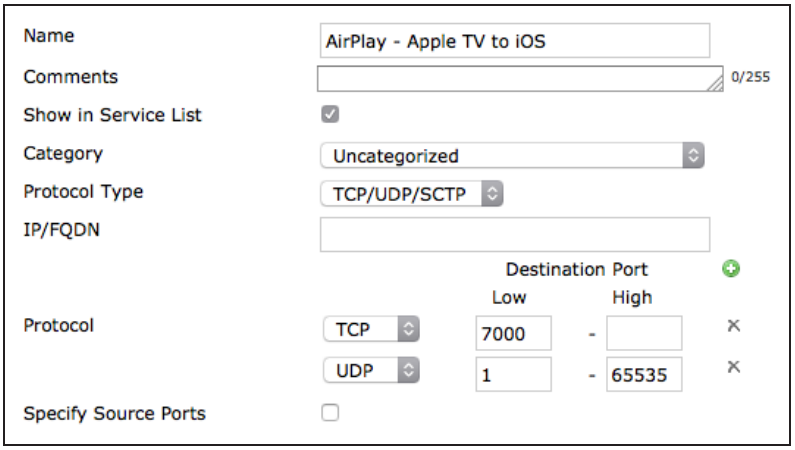
1. Enabling multicast policies

Go to **System > Config > Features**.

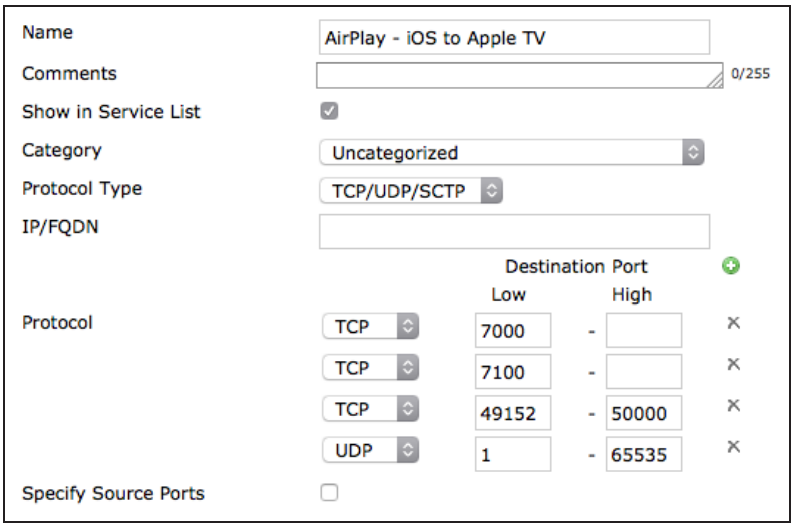
Select **Show More** and enable **Multicast Policy**. **Apply** the changes.

2. Creating AirPlay services

Go to **Policy & Objects > Objects > Services** and create a service as shown for the connection from the Apple TV to the iOS device.



Go to **Policy & Objects > Objects > Services** and create a service as shown for the connection from the iOS device to the Apple TV.

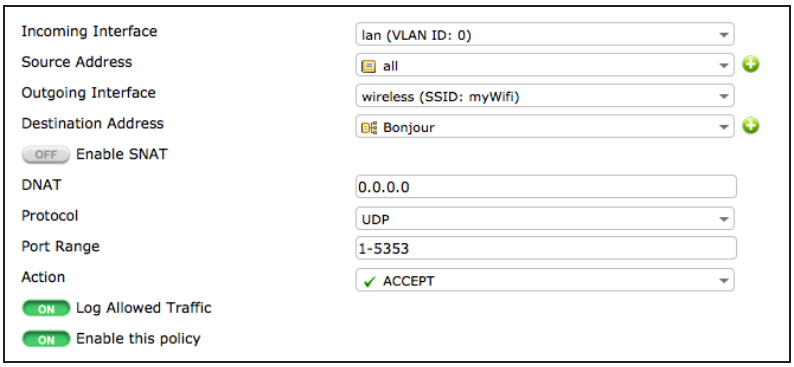


3. Allowing multicast between the wireless and internal networks

Go to **Policy & Objects > Policy > Multicast** and create a policy allowing local network traffic to reach the wireless network.

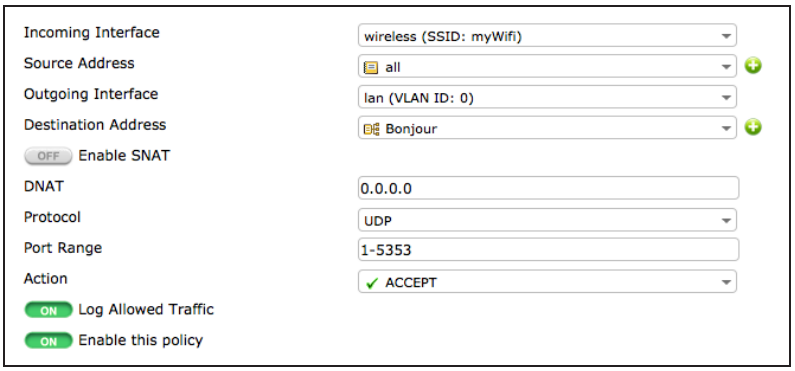
Set **Incoming Interface** to **lan**, **Outgoing Interface** to the wireless interface, and **Destination Address** to **Bonjour**.

Bonjour is a default multicast address that is used by Apple devices to discover shared services on the local network. Using it in the multicast policies will allow the iOS device and Apple TV to connect to each other through the FortiGate.



Create a second policy allowing wireless traffic to reach the internal network.

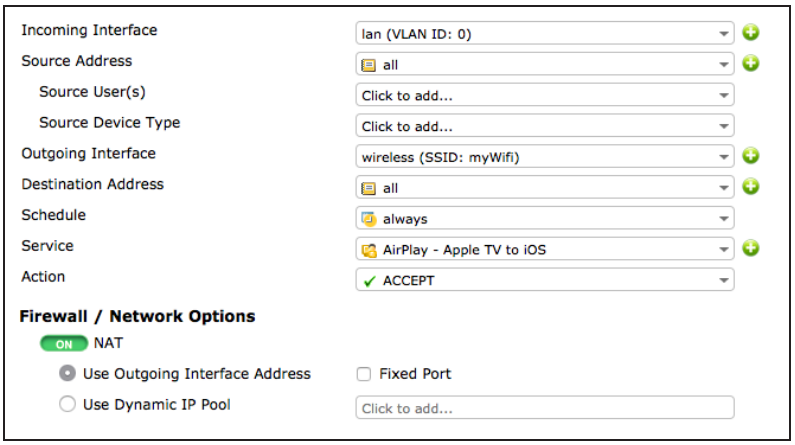
Set **Incoming Interface** to the wireless interface, **Outgoing Interface** to **lan**, and **Destination Address** to **Bonjour**.



4. Allowing airplay between the wireless and internal networks

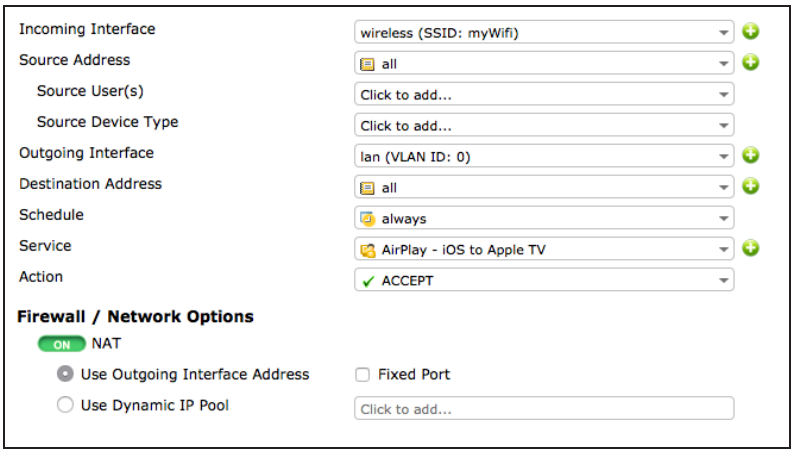
Go to **Policy & Objects > Policy > IPv4** and create a policy allowing traffic from the Apple TV to the iOS device.

Set **Incoming Interface** to **lan**,**Outgoing Interface** to the SSID, and **Service** to allow connections from the Apple TV to the iOS device.



Create a second policy allowing traffic from the iOS device to the Apple TV.

Set **Incoming Interface** to the SSID, **Outgoing Interface** to **lan**, and **Service** to allow connections from the iOS device to the Apple TV.



5. Results

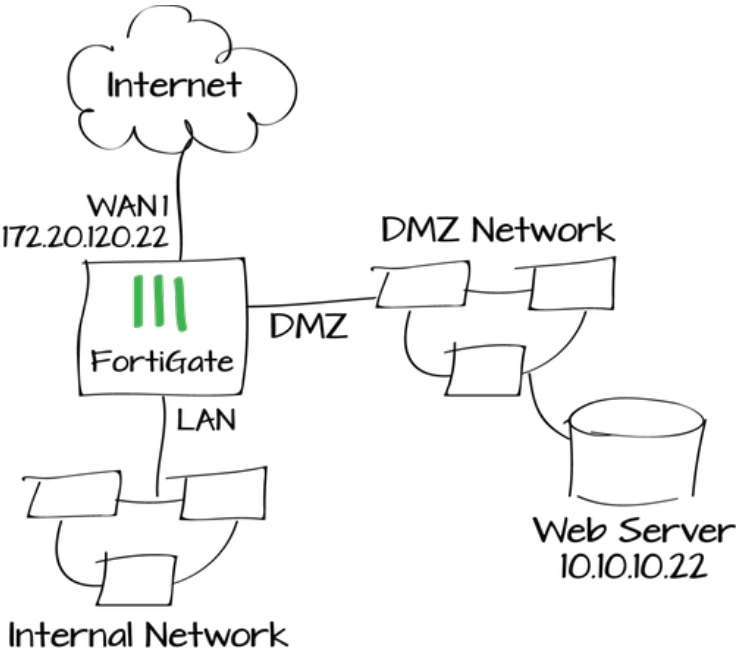
Use AirPlay to stream audio or video from an iOS device to the Apple TV.

Go to **Log & Report > Traffic Log > Multicast**. You will see traffic flowing between the two devices, using both multicast policies.

#		Date/Time	Source	Destination	Sent / Received	Policy ID
1		14:31:40	192.168.77.2	224.0.0.251	69 B / 0 B	1
2		14:31:40	10.10.20.3	224.0.0.251	118 B / 0 B	2
3		14:31:31	192.168.77.2	224.0.0.251	81 B / 0 B	1
4		14:31:30	10.10.20.3	224.0.0.251	59 B / 0 B	2
5		14:29:59	192.168.77.2	224.0.0.251	138 B / 0 B	1
6		14:29:58	10.10.20.3	224.0.0.251	118 B / 0 B	2
7		14:29:48	192.168.77.2	224.0.0.251	81 B / 0 B	1
8		14:29:48	10.10.20.3	224.0.0.251	59 B / 0 B	2
9		14:29:14	192.168.77.2	224.0.0.251	511 B / 0 B	1
10		14:29:05	192.168.77.2	224.0.0.251	4.90 KB / 0 B	1

For further reading, check out Multicast forwarding in the FortiOS 5.2 Handbook.

Protect a web server with DMZ



In the following example, you will protect a web server by connecting it using your FortiGate's DMZ network.

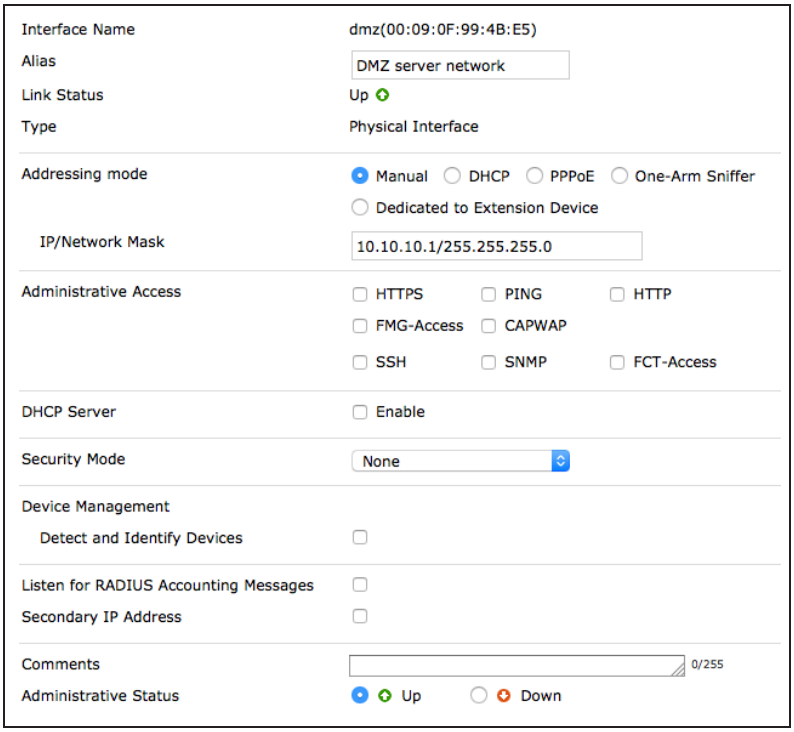
An internal to DMZ security policy with a virtual IP (VIP) allows internal users to access the web server using an internal IP address (10.10.10.22). A WAN-to-DMZ security policy also with a VIP hides the internal address, allowing external users to access the web server using a public IP address (172.20.120.22).

1. Configuring the FortiGate's DMZ interface

Go to **System > Network > Interfaces**. Edit the **DMZ** interface.

The DMZ Network (from the term 'demilitarized zone') is a secure network connected to the FortiGate that only grants access if it has been explicitly allowed. Using the DMZ interface is recommended but not required.

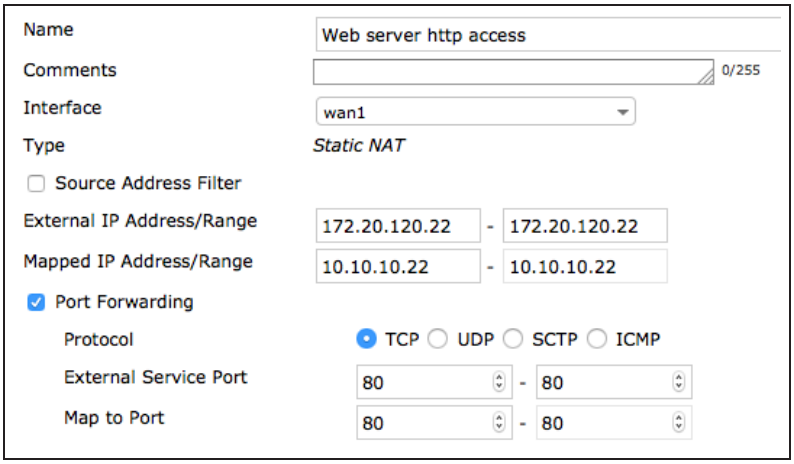
For enhanced security, disable all **Administrative Access** options.

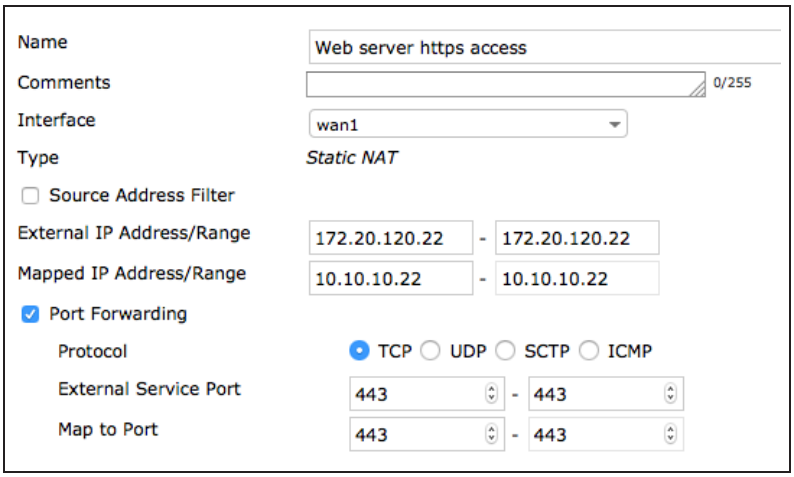


2. Creating virtual IPs (VIPs)

Go to **Policy & Objects > Objects > Virtual IPs**. Create two virtual IPs: one for HTTP access and one for HTTPS access.

Each virtual IP has the same address, mapping from the public-facing interface to the DMZ interface. The difference is the port for each traffic type: port 80 for HTTP and port 443 for HTTPS.

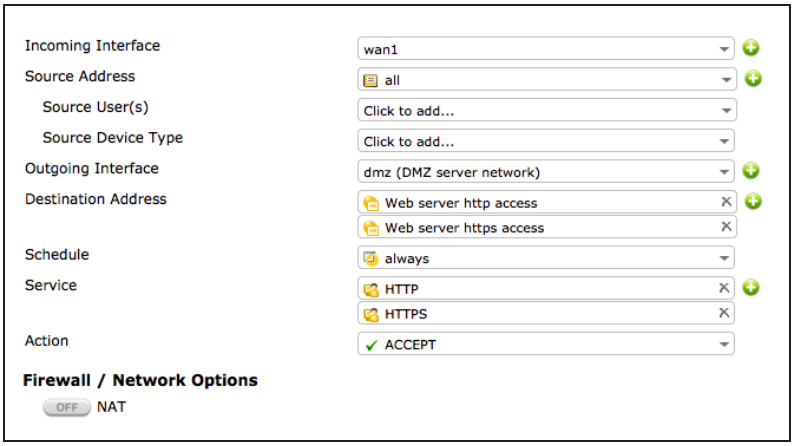




3. Creating security policies

Go to **Policy & Objects > Policy > IPv4**. Create a security policy to allow HTTP and HTTPS traffic from the Internet to the DMZ interface and the web server.

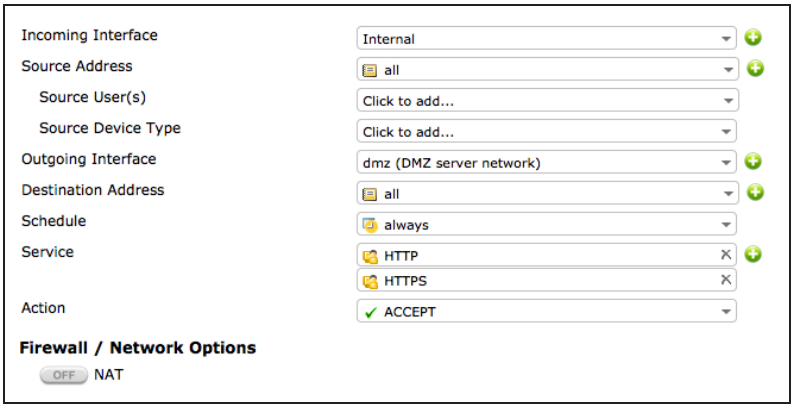
Do not enable NAT and, for testing purposes, enable logging for all sessions.



Create a second security policy to allow HTTP and HTTPS traffic from the internal network to the DMZ interface and the web server.

Adding this policy allows traffic to pass directly from the internal interface to the DMZ interface.

Do not enable NAT and, for testing purposes, enabe logging for all sessions.

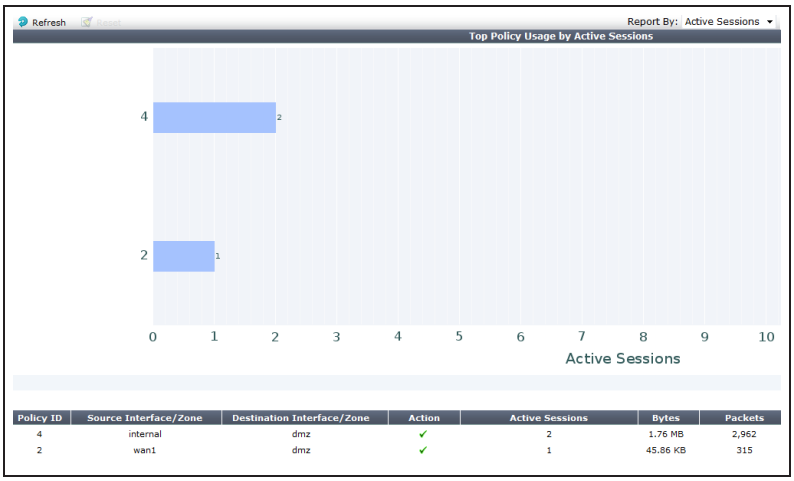


4. Results

External users can access the web server on the DMZ network from the Internet using its Internet address (in this example, http://172.20.120.22 and https://172.20.120.22). Internal users can access the web server using its DMZ address (in this example. and https://10.10.10.22).

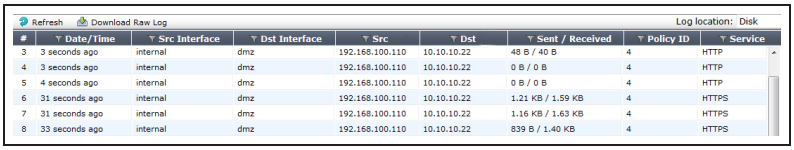
Go to **Policy & Objects > Monitor > Policy Monitor**.

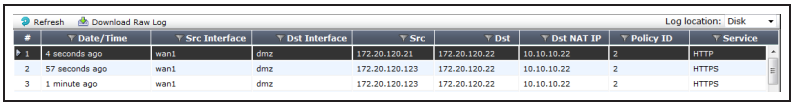
Use the policy monitor to verify that traffic from the Internet and from the internal network is allowed to access the web server. This verifies that the policies are configured correctly.



Go to **Log & Report > Traffic Log > Forward Traffic**.

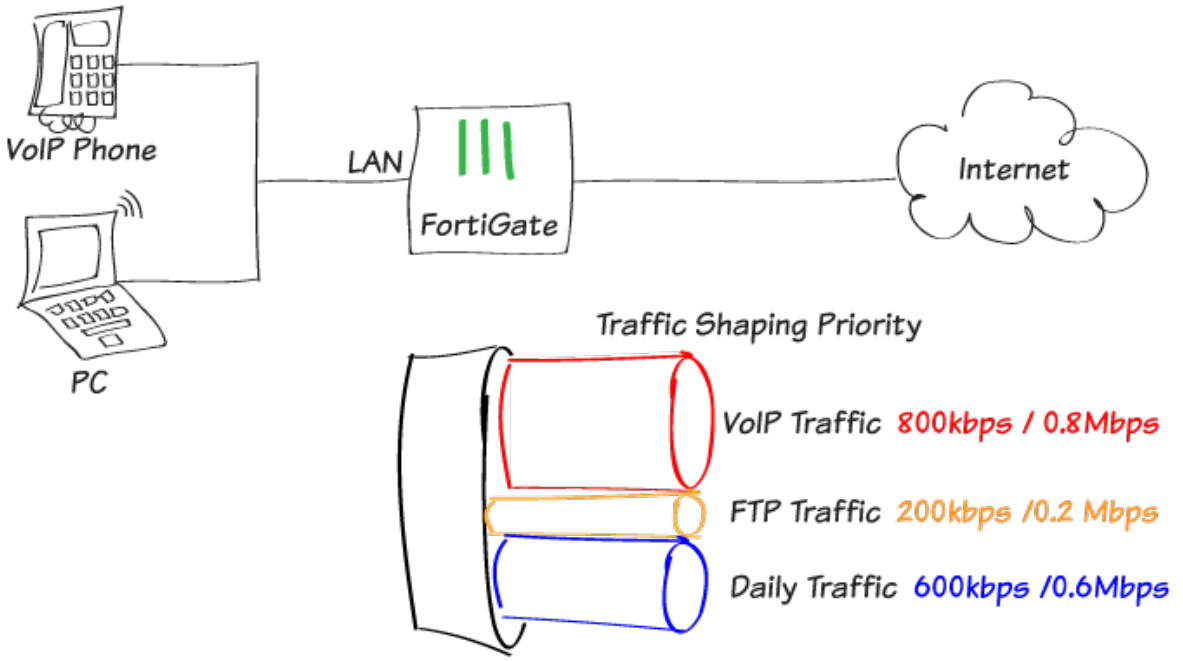
The traffic log shows sessions from the internal network and from the Internet accessing the web server on the DMZ network.





For further reading, check out Firewall in the FortiOS 5.2 Handbook.

Traffic shaping for VoIP



The quality of VoIP phone calls through a firewall often suffers when the firewall is busy and the amount of bandwidth available for the VoIP traffic fluctuates. This can be irritating, leading to unpredictable results and caller frustration. This recipe describes how to add traffic shaping to guarantee that enough bandwidth is available for VoIP traffic, regardless of any other activity on the network.

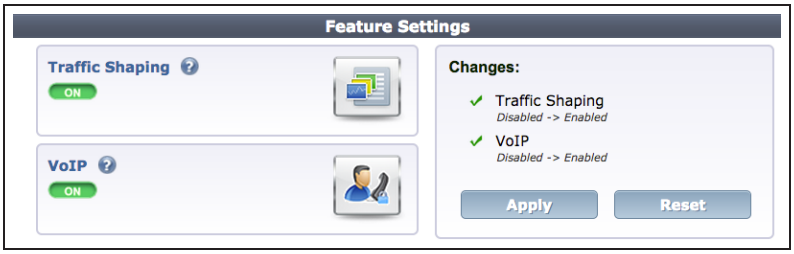
To achieve high quality real-time voice transmissions, VoIP traffic requires priority over other types of traffic, minimal packet loss, and jitter buffers. You will limit bandwidth consuming services, like FTP, while providing a consistent bandwidth for day-to-day email and web-based traffic. First,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

Before you apply QoS measures, ensure you have enough network bandwidth to support real-time voice traffic.

1. Enabling Traffic Shaping and VoIP features

Go to **System > Config > Features** and click the **Show More** button to view additional features. If necessary, select **ON** to enable both **Traffic Shaping** and **VoIP**. Apply your changes.

Traffic shaping rules and VoIP profiles can now be applied to firewall policies.



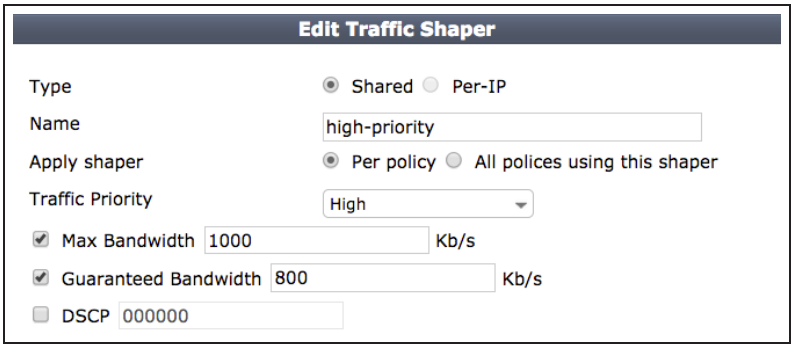
2. Configuring a high priority VoIP traffic shaper

Go to **Policy & Objects > Objects > Traffic Shapers** and edit the existing **high-priority** traffic shaper.

Set **Type** to **Shared**. Set **Apply shaper** to **Per Policy**.

*Select **Per Policy** when you want each security policy for day-to-day business traffic to have the same distribution of bandwidth, regardless of the number of policies using the shaper. In this example, 800kb/s (0.8Mbps) each.*

Set **Traffic Priority** to **High**. Select **Max Bandwidth** and enter `1000` kb/s (1 Mbps). Select **Guaranteed Bandwidth** and enter `800` kb/s (0.8 Mbps).



3. Configuring a low priority FTP traffic shaper

Go to **Policy & Objects > Objects > Traffic Shapers** and edit the existing **low-priority** traffic shaper.

Set **Type** to **Shared**. Set **Apply shaper** to **All policies using this shaper**.

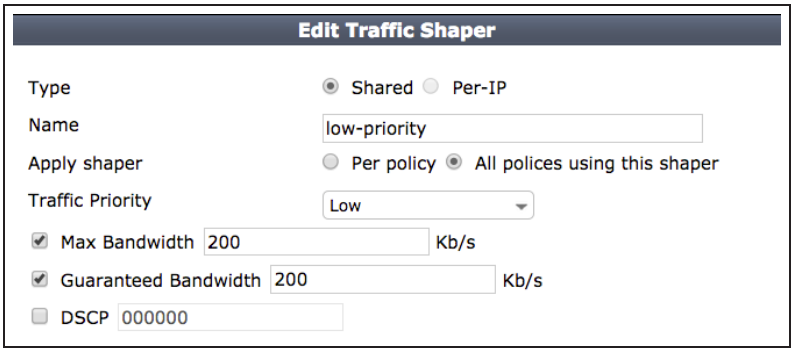
*Select **All policies using this shaper** to ensure that **all** policies using your shaper will be restricted to share a set amount of bandwidth. In this example, 200kb/s (0.2 Mbps) total.*

Set **Traffic Priority** to **Low.**

*If you are creating a new traffic shaper, the **Traffic Priority** is set to **High** by default. A failure to set different shaper priorities will result in a lack of prioritized traffic.*

Set **Max Bandwidth** and **Guaranteed Bandwidth** to 200 kb/s (0.2 Mbps).

Setting a low maximum bandwidth will prevent sudden spikes in traffic caused by large FTP file uploads and downloads.

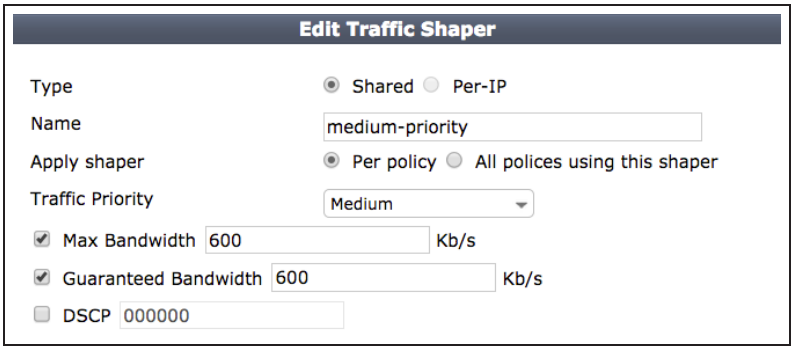


4. Configuring a medium priority daily traffic shaper

Go to **Policy & Objects > Objects > Traffic Shapers** and edit the existing **medium-priority** traffic shaper.

Set **Type** to **Shared**. Set **Apply shaper** to **Per Policy**. Select **Max Bandwidth** and enter 600 kb/s (0.6 Mbps). Set **Traffic Priority** to **Medium**. Select **Guaranteed Bandwidth** and enter 600 kb/s (0.6 Mbps).

*This shaper should be set to a moderate value and set to **per policy** so that day-to-day traffic has the same distribution of bandwidth.*



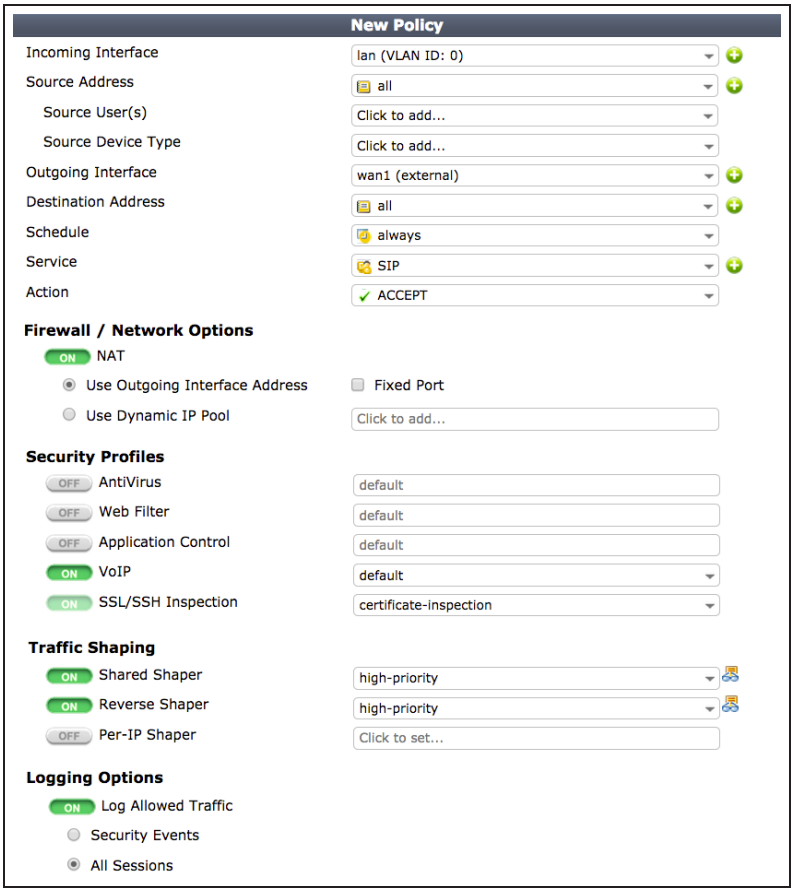
5. Applying each shaper to a device-based policy

Go to **Policy & Objects > Policy > IPv4** and create a new security policy for SIP traffic.

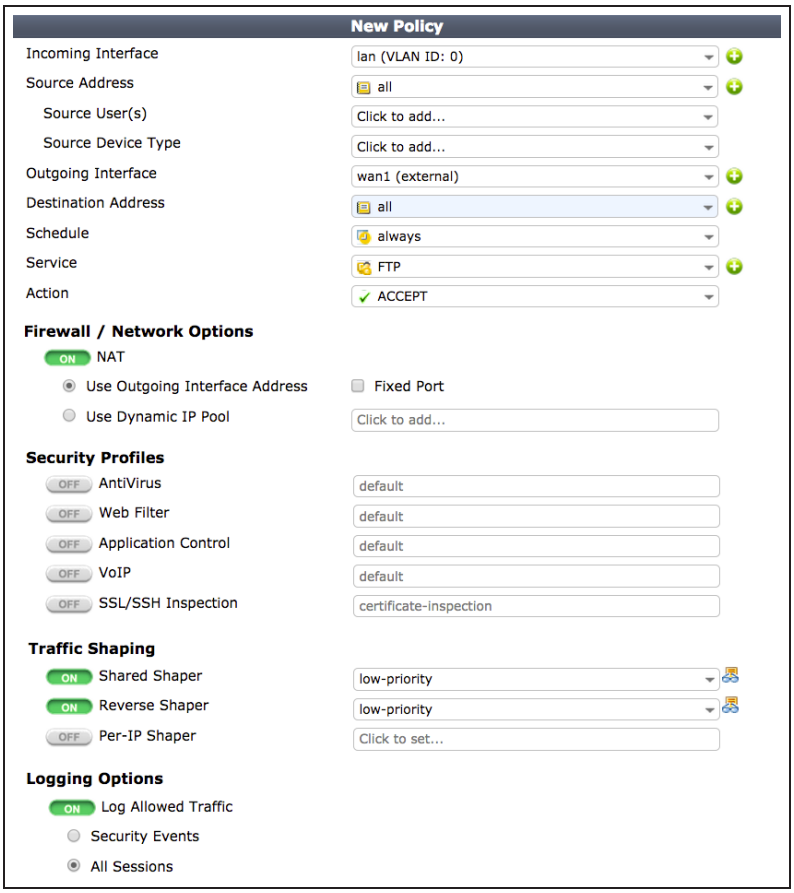
Enable **Shared Shaper** and **Reverse Shaper** and select **high-priority**.

*Make sure that you include a **Reverse Shaper** so that return traffic for a VoIP call has the same guaranteed bandwidth as an outgoing call.*

For **Logging Options**, select **All Sessions** for testing purposes.

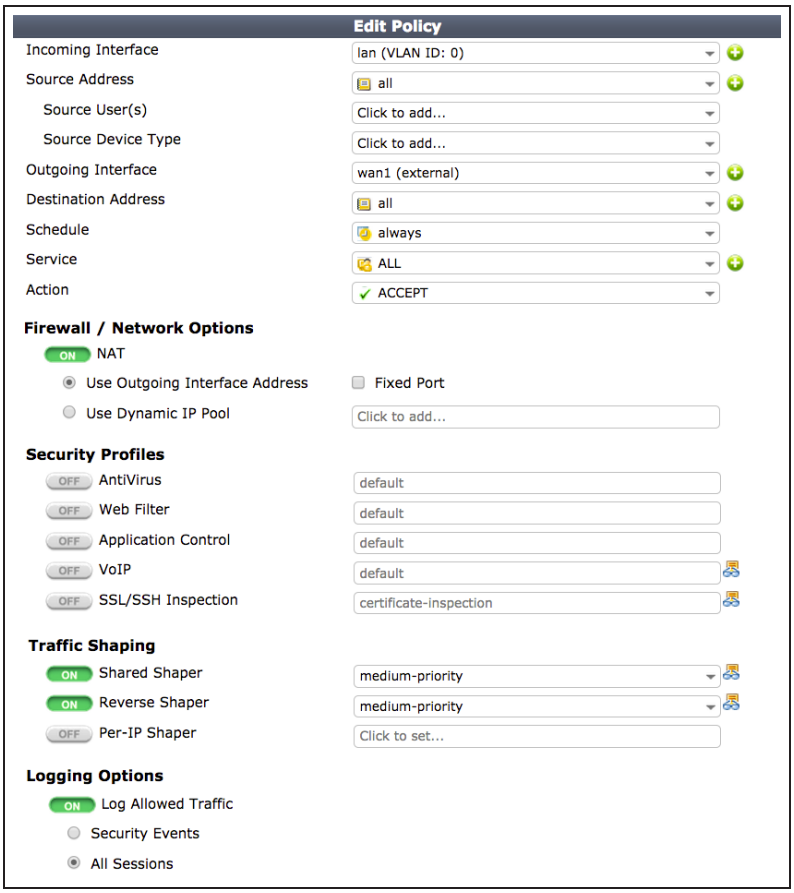


Go to **Policy & Objects > Policy > IPv4** and create a security policy for FTP traffic.



Go to **Policy & Objects > Policy > IPv4** and create a security policy for daily web-based, email traffic, and other traffic.

You can also edit your existing general access security policy.

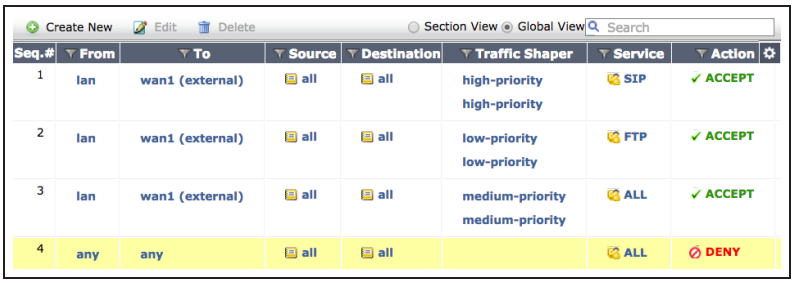


Arrange your policies are in the following order:

Click on the far left of the column you want to move and drag it up or down to arrange it.

1. High-priority (SIP/VoIP traffic)
2. Low-priority (FTP traffic)
3. Medium-priority (Day-to-day traffic)

More specific restrictive policies, like the SIP and FTP policies, should always be placed at the top of the list, above the unrestricted general access policy that allows "all".

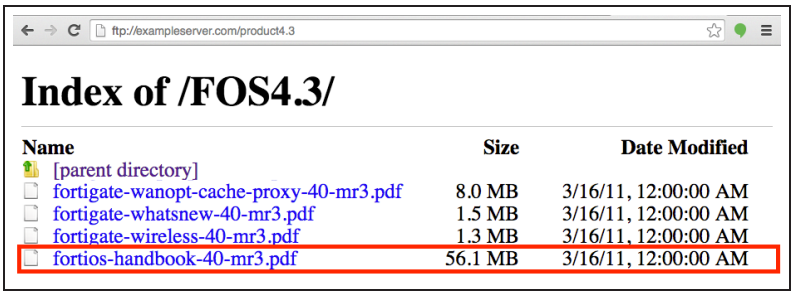


6. Results

Browse the Internet using a PC on your internal network to generate daily web traffic. Then, generate FTP traffic.

In this example, a 56.1 MB file was downloaded from an FTP server.

The FTP download or upload should occur slowly.



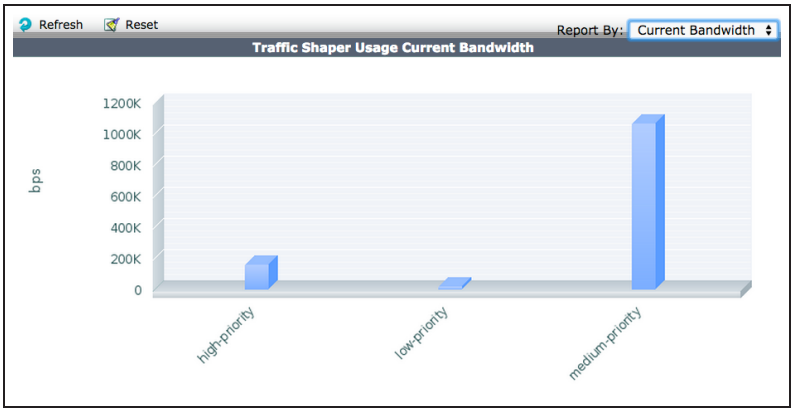
Finally, generate SIP traffic.

In this example, SIP traffic was generated by placing a call with a VoIP FortiFone connected to the internal interface of the FortiGate.

Go to **Policy & Objects > Monitor > Traffic Shaper Monitor** and report by the **Current Bandwidth**. You can see how much of your current bandwidth is being used by active traffic shapers. If the standard traffic volume is high enough, it will top out at the maximum bandwidth defined by each shaper.

In the screenshot, the SIP traffic is only using a small part of the allocated bandwidth.

You will have normal voice quality on your VoIP call, even with daily traffic and FTP downloads running.



Go to **Log & Report > Log & Archive**

Access > Traffic Log and filter the **Service** by **SIP** to see your VoIP traffic. Select an individual log message to view the shaper name in the **Sent Shaper Name** field.

For further reading, check out Traffic Shaping in the FortiOS 5.2 Handbook.

Security

This section contains information about using a FortiGate's security features, including antivirus, web filtering, application control, intrusion protection (IPS), email filtering, and data leak prevention (DLP). This section also includes information about using SSL inspection to inspect encrypted traffic.

Application Control

- Blocking P2P traffic and YouTube applications
- Blocking Windows XP traffic
- Blocking and monitoring Tor traffic
- Controlling access to Apple's App Store
- Restricting online gaming to evenings

Data Leak Prevention

- Preventing data leaks
- Prevent credit card numbers from being leaked

Intrusion Protection

- Protecting a web server
- Logging DNS domain lookups

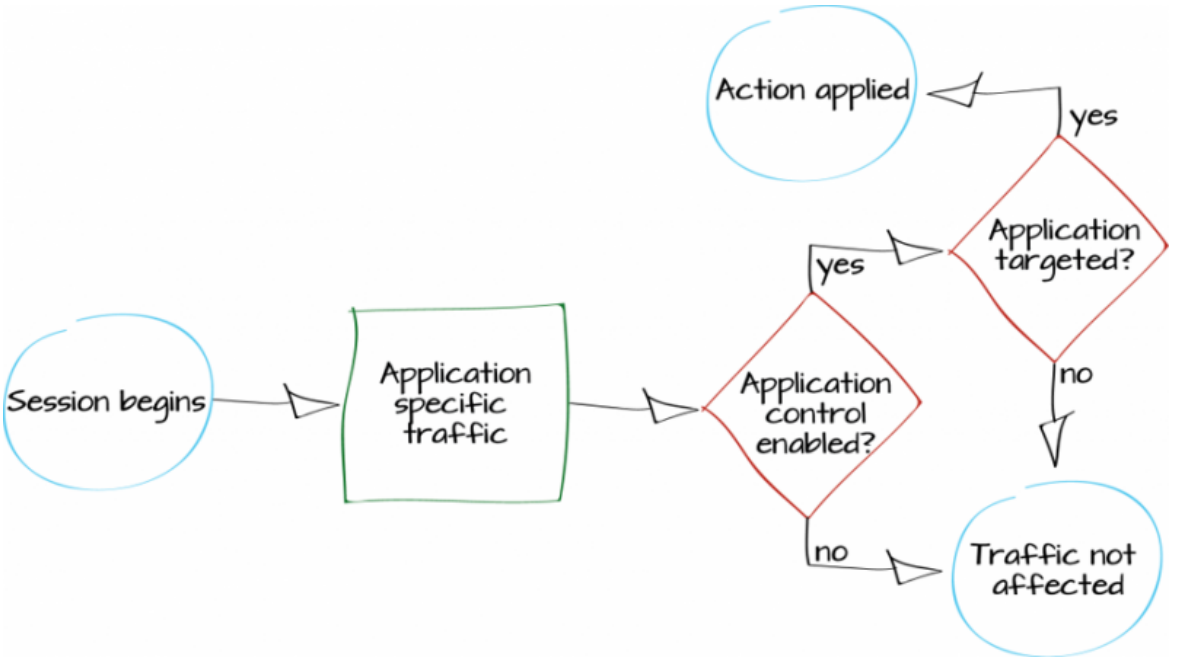
SSL Inspection

- Why you should use SSL inspection
- Preventing certificate warnings

Web Filtering

- Blocking Facebook
- Web rating overrides
- Web filtering using quotas
- Blocking Google access for consumer accounts
- Overriding a web filter profile
- Restricting online gaming to evenings
- Troubleshooting web filtering

Blocking P2P traffic and YouTube applications

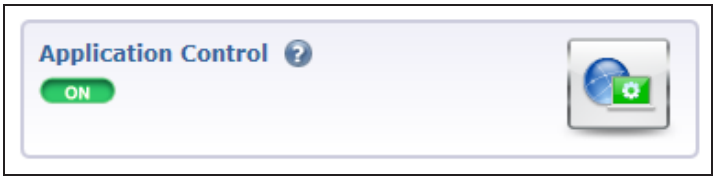


In this example, you will learn how to use Application Control to monitor traffic and determine if there are any applications currently in use that should not have network access. If you discover any applications that you wish to block, application control will then be used to ensure that these applications cannot access the network.

A video of this recipe is available here.

1. Enabling Application Control and multiple security profiles

Go to **System > Config > Features** and ensure that **Application Control** is turned **ON**.



Select **Show More** and enable **Multiple Security Profiles**.

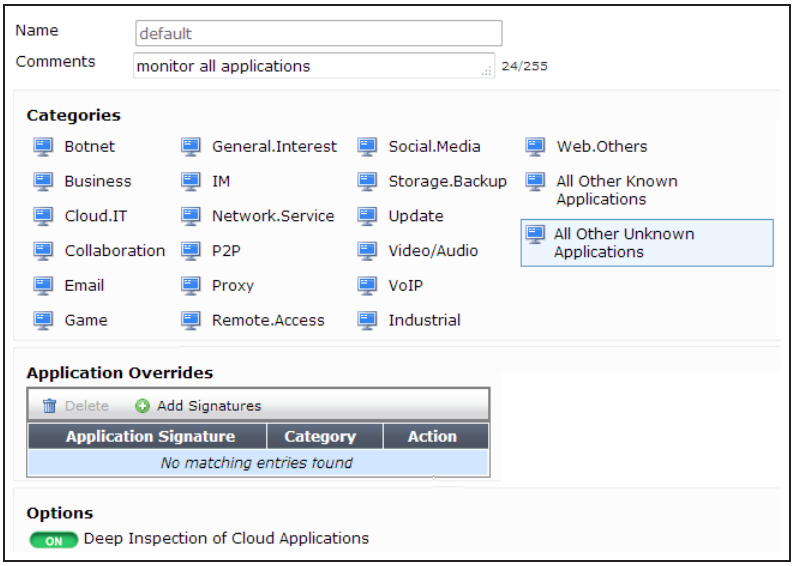
Apply the changes.

2. Using the default application profile to monitor network traffic

Go to **Security Profiles > Application Control** and view the **default** profile.

A list of application **Categories** is shown. By default, most categories are already set to **Monitor**. In order to monitor all applications, select **All Other Known Applications** and set it to **Monitor**. Do the same for **All Other Unknown Applications**.

The default profile also has Deep Inspection of Cloud Applications turned ON. This allows web-based applications, such as video streaming, to be monitored by your FortiGate.



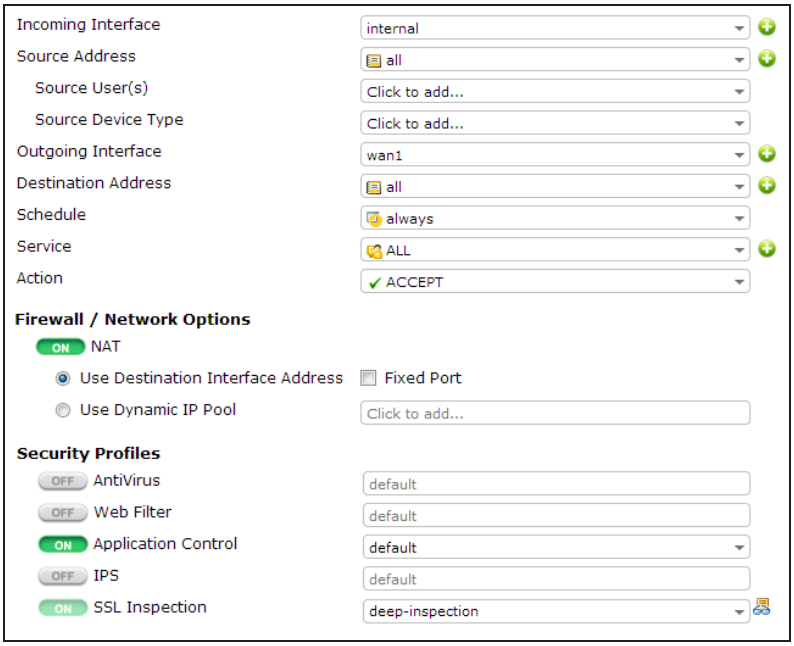
3. Adding the default profile to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Under **Security Profiles**, turn on **Application Control** and use the **default** profile.

Enabling Application Control will automatically enable **SSL Inspection**. In order to inspect traffic from Cloud Applications, the **deep-inspection** profile must be used.

*Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see Preventing certificate warnings.*



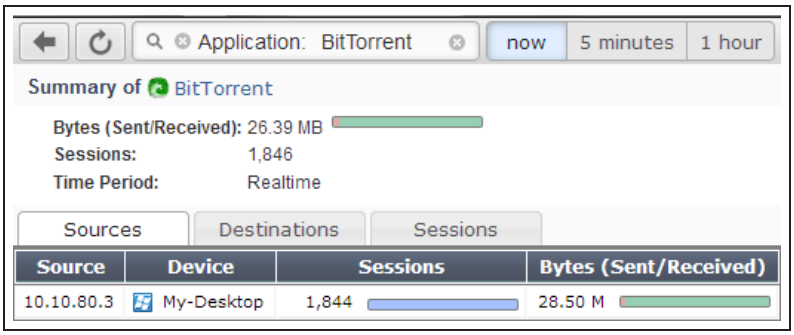
3. Reviewing the FortiView dashboards

Go to **System > FortiView > Applications** and select the **now** view.

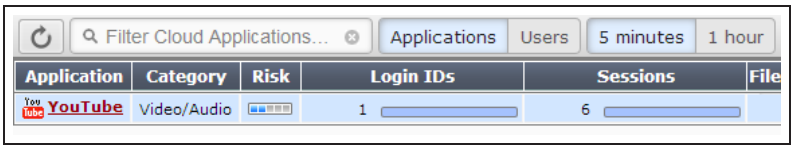
This dashboard shows the traffic that is currently flowing through your FortiGate, arranged by application (excluding Cloud Applications).

Application	Category	Risk	Sessions	Bytes (Sent/Received)
BitTorrent	P2P		78	410.37 K
DNS	Network.Service		66	16.94 K
SSL	Network.Service		21	16.04 M
Skype	P2P		13	273.90 K
Unknown			6	442
Twitter	Social.Media		3	29.61 K
LastPass	Storage.Backup		1	23.05 K
Google.Plus	Social.Media		1	17.78 K
Dropbox	Storage.Backup		1	340.18 K
Jabber	Collaboration		1	19.87 K
HTTP.Audio	General.Interest		1	33.38 M
Facebook	Social.Media		1	7.47 K

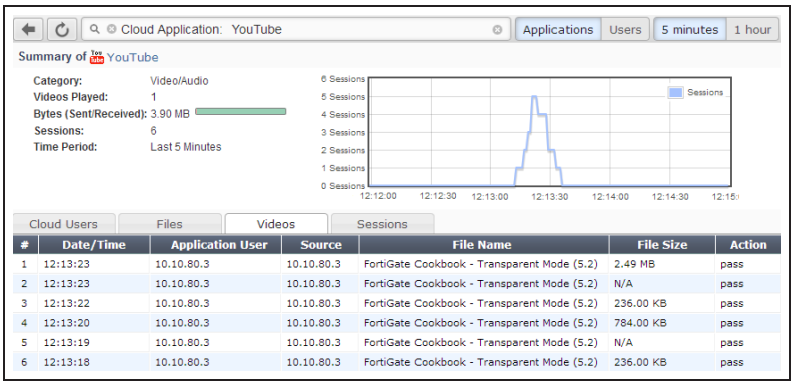
If you wish to know more about an application's traffic, double-click on its entry to view drilldown information, including traffic sources, traffic destinations, and information about individual sessions.



Similar information can be viewed for Cloud Applications by going to **System > FortiView > Cloud Applications** and selecting **Applications** that have been used in the last **5 Minutes**.



Cloud Applications also have drilldown options, including the ability to see which videos have been viewed if streaming video traffic was detected.



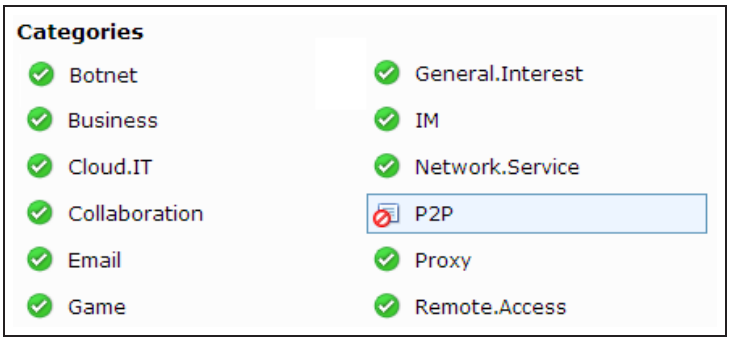
5. Creating an application profile to block applications

In the above example, traffic from BitTorrent, a Peer-to-Peer (P2P) downloading application, was detected. Now, you will create an application control profile that will block P2P traffic.

The new profile will also block all applications associated with YouTube, without blocking other applications in the **Video/Audio** category.

Go to **Security Profiles > Application Control** and create a new profile.

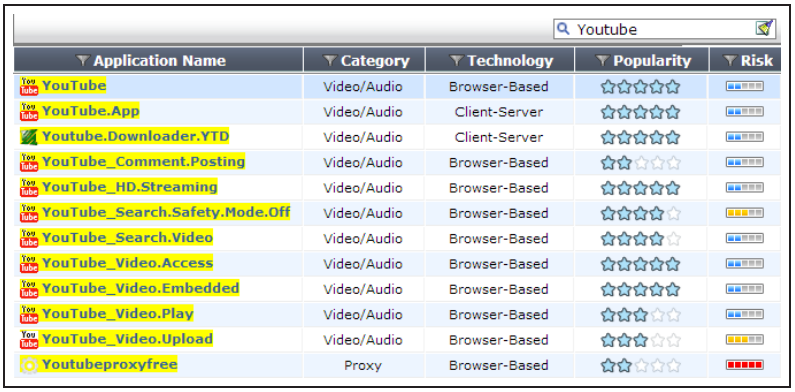
Select the **P2P** category and set it to **Block**.



Under **Application Overrides**, select **Add Signatures**.

Search for *Youtube* and select all the signatures that are shown.

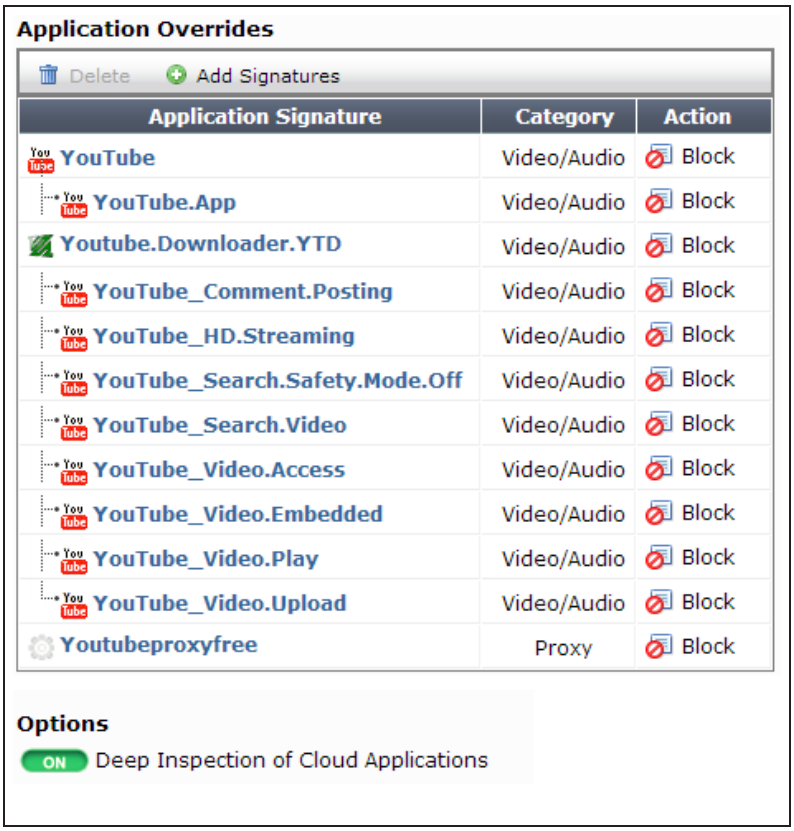
Select **Use Selected Signatures**.



Application Name	Category	Technology	Popularity	Risk
YouTube	Video/Audio	Browser-Based		
YouTube.App	Video/Audio	Client-Server		
Youtube.Downloader.YTD	Video/Audio	Client-Server		
YouTube_Comment.Posting	Video/Audio	Browser-Based		
YouTube_HD.Streaming	Video/Audio	Browser-Based		
YouTube_Search.Safety.Mode.Off	Video/Audio	Browser-Based		
YouTube_Search.Video	Video/Audio	Browser-Based		
YouTube_Video.Access	Video/Audio	Browser-Based		
YouTube_Video.Embedded	Video/Audio	Browser-Based		
YouTube_Video.Play	Video/Audio	Browser-Based		
YouTube_Video.Upload	Video/Audio	Browser-Based		
Youtubeproxyfree	Proxy	Browser-Based		

The signatures have been added to the Application Overrides list and have automatically been set to Block.

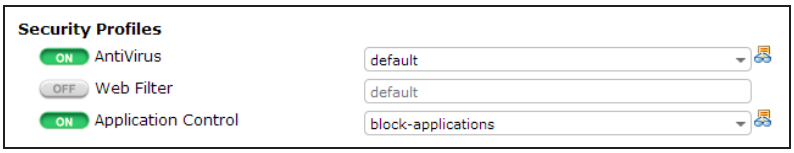
Enable **Deep Inspection of Cloud Applications**.



6. Adding the blocking profile to a security policy

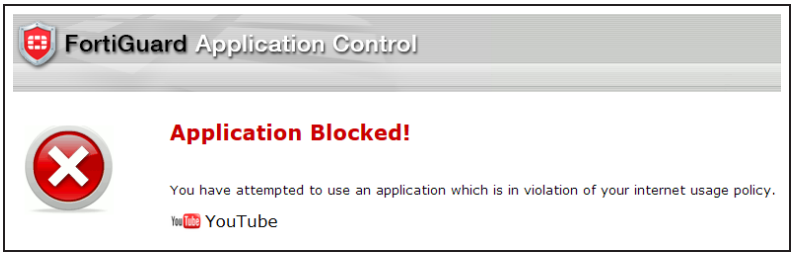
Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Set **Application Control** to use the new profile.



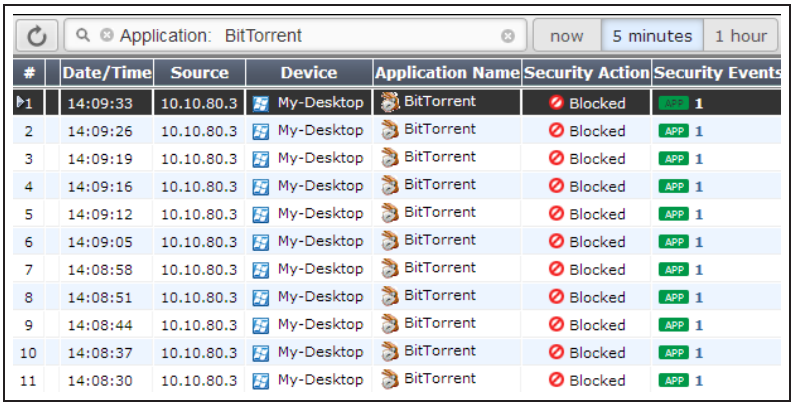
7. Results

Attempt to browse to YouTube. A warning message will appear, stating that the application was blocked.



Traffic from BitTorrent applications will also be blocked.

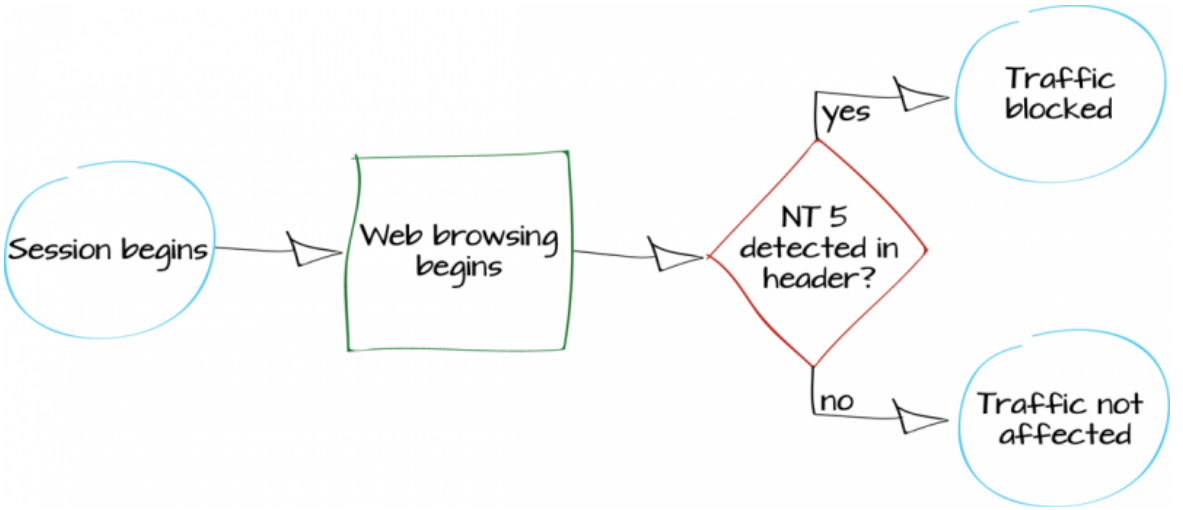
To see information about this blocked traffic, go to **System > FortiView > All Sessions**, select the **5 minutes** view, and filter the traffic by application.



#	Date/Time	Source	Device	Application Name	Security Action	Security Events
1	14:09:33	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
2	14:09:26	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
3	14:09:19	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
4	14:09:16	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
5	14:09:12	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
6	14:09:05	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
7	14:08:58	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
8	14:08:51	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
9	14:08:44	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
10	14:08:37	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1
11	14:08:30	10.10.80.3	My-Desktop	BitTorrent	Blocked	APP 1

For further reading, check out Application control in the FortiOS 5.2 Handbook.

Blocking Windows XP traffic



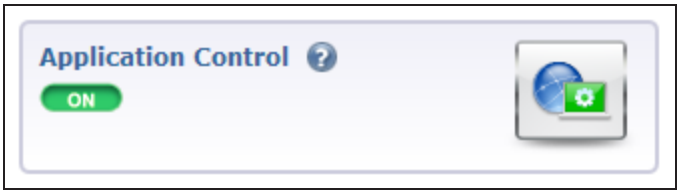
In this example, you will use application control to block web traffic from PCs running Windows operating systems that NT 5, including Windows XP and Windows Server 2003 (includes Windows virtual machines).

When a computer's operating system lacks vendor support, it becomes a threat to the network because newly discovered exploits will not be patched. Using the FortiGate application control feature, you can restrict these computers from accessing external resources.

This recipe will only block web traffic from computers running the affected operating systems. If you wish to block these computers from being on the network entirely, further action will be necessary. However, the logs generated by this recipe can be used to identify the computers you wish to block.

1. Enabling Application Control

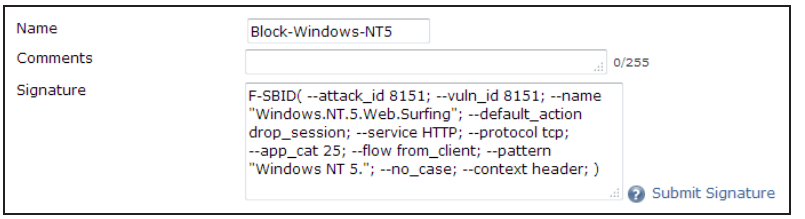
Go to **System > Config > Features**. Enable **Application Control** and **Apply** your changes.



2. Creating a custom application control signature

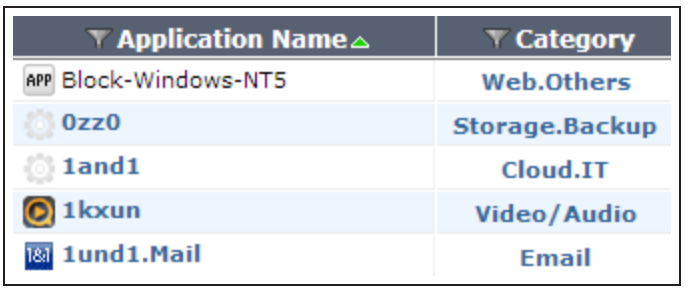
Go to **Security Profiles > Application Control** and select **View Application Signatures**.

Create a new signature with this syntax. (You can copy and paste this text into the **Signature** field.)




```
F-SBID( --attack_id 8151; --vuln_id 8151; --name
"Windows.NT.5.Web.Surfing"; --default_action drop_
[glossary_exclude]session[/glossary_exclude]; --
service [glossary_exclude]HTTP[/glossary_exclude]; --
protocol tcp; --app_cat 25; --flow from_client; --
pattern "Windows NT 5."; --no_case; --context header;
)
```

The signature will appear at the top of the application list and be listed in the **Web.Others** category.

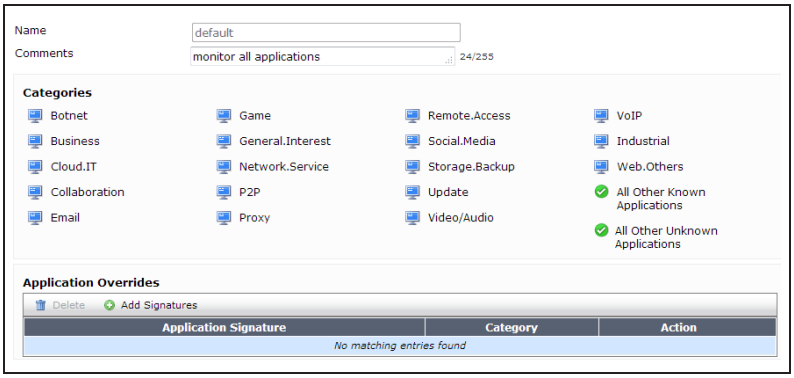


Application Name	Category
Block-Windows-NT5	Web.Others
0zz0	Storage.Backup
1and1	Cloud.IT
1kxun	Video/Audio
1und1.Mail	Email

3. Adding the signature to the default Application Control profile

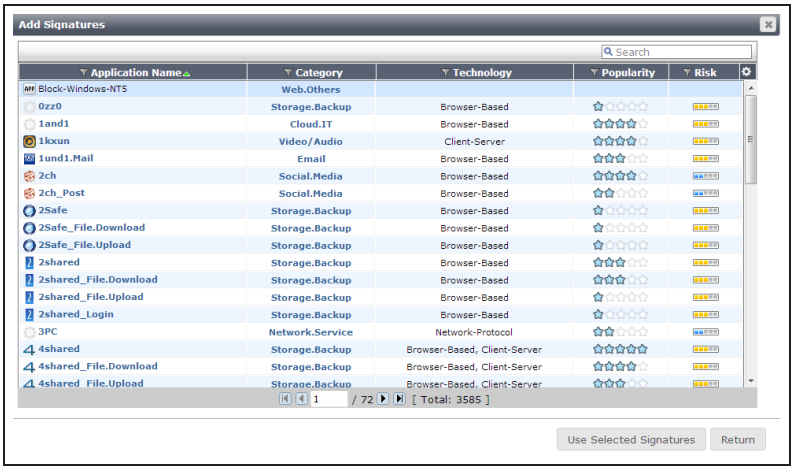
Go to **Security Profiles > Application Control** and edit the **default** policy.

Under **Application Overrides**, select **Add Signature**.



The new signature should appear at the top of the list. If it does not, search for the signature's name (in the example, *Block-Windows-NT5)*.

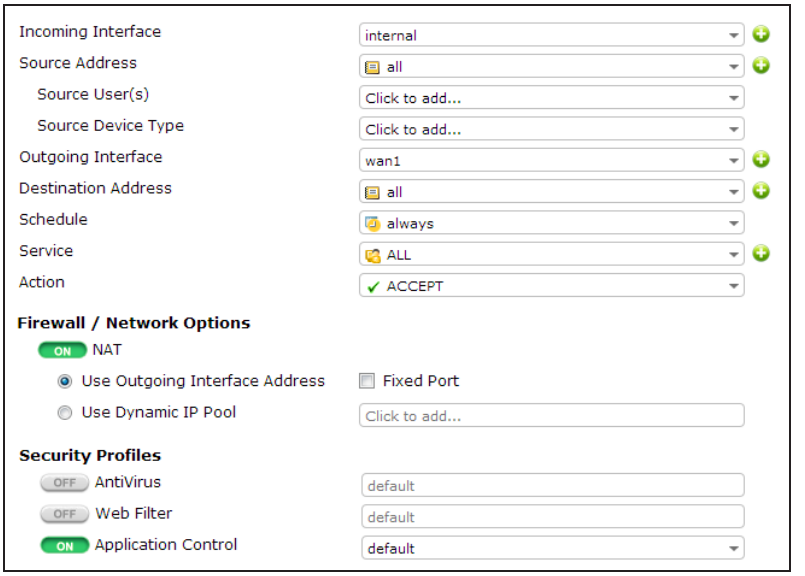
Select the signature, then select **Use Selected Signatures**.



4. Adding the default profile to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

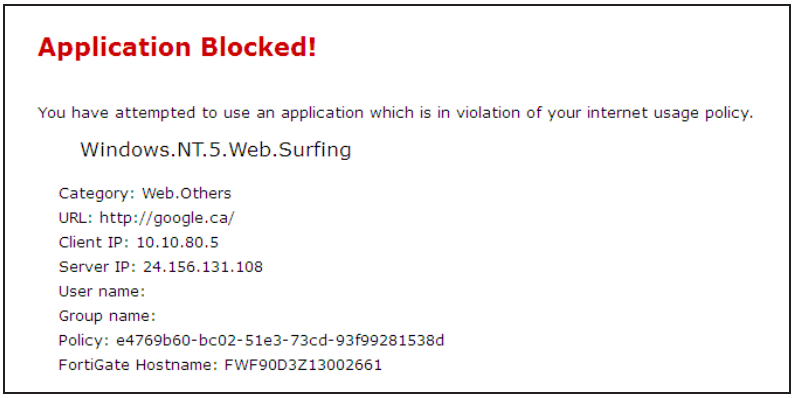
Under **Security Profiles**, turn on **Application Control** and use the **default** profile.



5. Results

When a PC running one of the affected operating systems attempts to connect to the Internet using a browser, a blocked message appears.

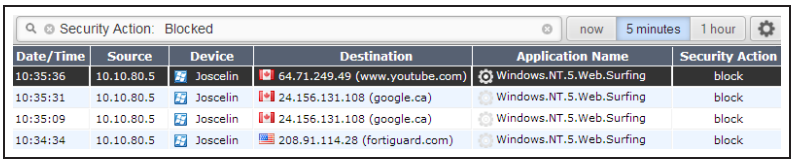
PCs running other operating systems, including later versions of Windows, are not affected.



Go to **System > FortiView > All Sessions** and select the **5 minutes** view.

Filter the results to show sessions that were blocked.

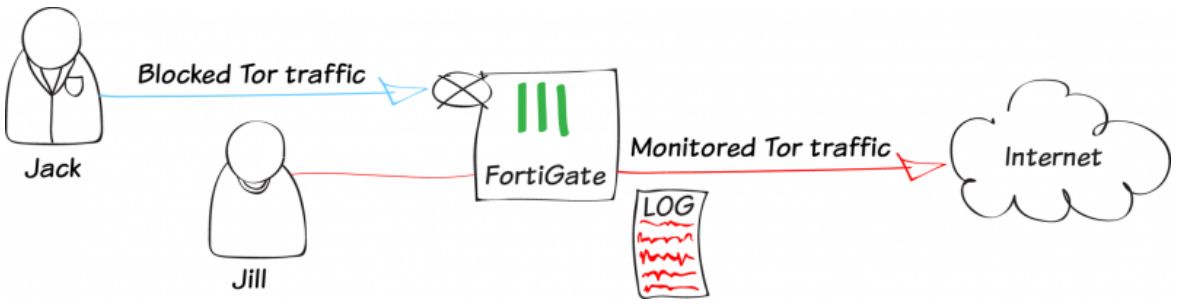
You will see that the Application Control signature, shown in the **Application Name** column, was used to block traffic from PCs running older Windows versions (in the example, the device **Joscelin**).



Date/Time	Source	Device	Destination	Application Name	Security Action
10:35:36	10.10.80.5	Joscelin	64.71.249.49 (www.youtube.com)	Windows.NT.5.Web.Surfing	block
10:35:31	10.10.80.5	Joscelin	24.156.131.108 (google.ca)	Windows.NT.5.Web.Surfing	block
10:35:09	10.10.80.5	Joscelin	24.156.131.108 (google.ca)	Windows.NT.5.Web.Surfing	block
10:34:34	10.10.80.5	Joscelin	208.91.114.28 (fortiguard.com)	Windows.NT.5.Web.Surfing	block

For further reading, check out Custom Application & IPS Signatures in the FortiOS 5.2 Handbook.

Blocking and monitoring Tor traffic



In this recipe, you will allow one user to use the Tor browser application for web traffic, while monitoring the user's activity. Use of the Tor browser will be blocked for all other users.

The Tor browser allows users to bounce communication traffic around a distributed network of relays located around the world. For more information about Tor, check out the Fortinet blog entry 5 ½ Things To Know About The Tor Browser And Your Network.

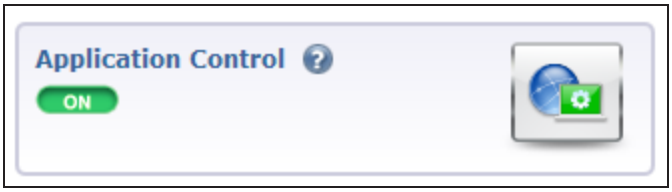
This recipe uses the default application control signatures for the Tor client and web-based Tor. These signatures will only match unmodified versions of the Tor application. Also, if a Tor session has already been established prior to connecting to the network, it may take up to 10 minutes before the FortiGate is able to monitor or block the traffic.

In this recipe, two user accounts, *jack* and *jill*, have already been configured. For more information about creating user accounts, see User and device authentication.

A video of this recipe is available here.

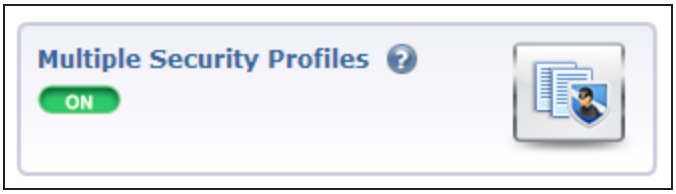
1. Enabling Application Control and multiple security profiles

Go to **System > Config > Features** and ensure that **Application Control** is turned **ON**.



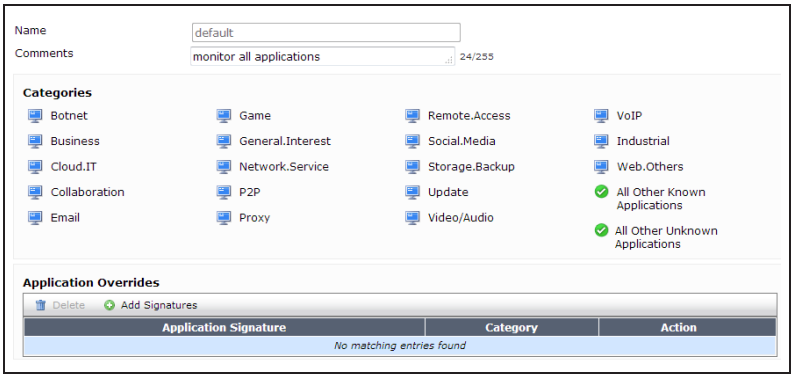
Select **Show More** and enable **Multiple Security Profiles**.

Apply the changes.



2. Blocking Tor traffic using the default profile

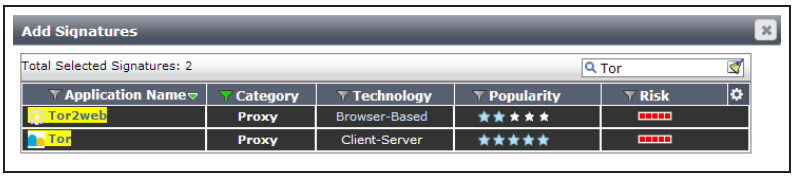
Go to **Security Profiles > Application Control** and edit the default profile.



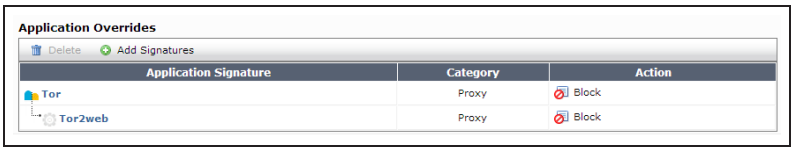
Under **Application Overrides**, select **Add Signatures**.

Search for *Tor*, then filter the results to show only the **Proxy** category. Two signatures will appear: one for the Tor client and one for web-based Tor use.

Highlight both signatures, and select **Use Selected Signatures**.

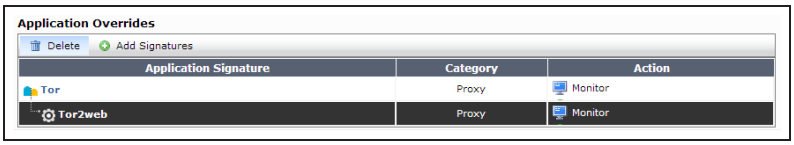


Both signatures now appear in the **Application Overrides** list, with the **Action** set to **Block**.



3. Creating a profile that monitors Tor traffic

Go to **Security Profiles > Application Control** and create a new profile. Under **Application Overrides**, select **Add Signatures**.



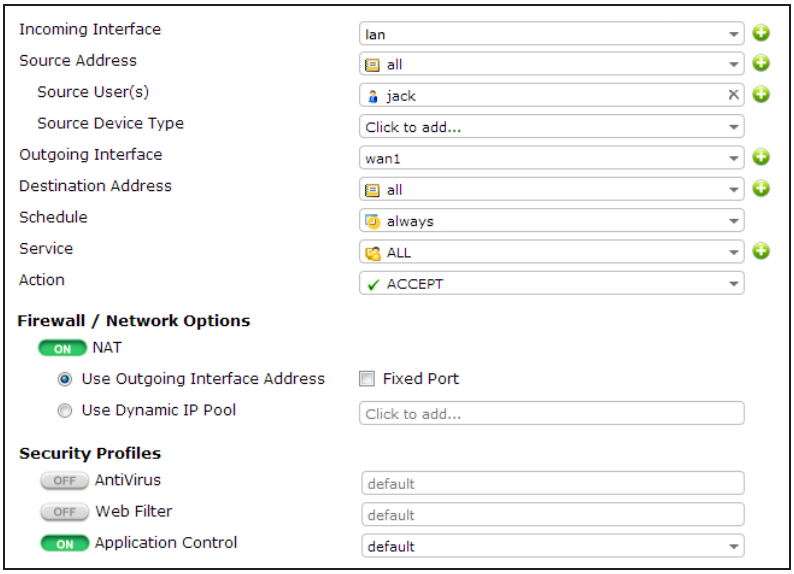
Search for and highlight both signatures, and select **Use Selected Signatures**.

In the **Application Overrides** list, double-click on the **Action** for each profile, and set it to **Monitor**.

4. Adding the application control profiles to your security policies

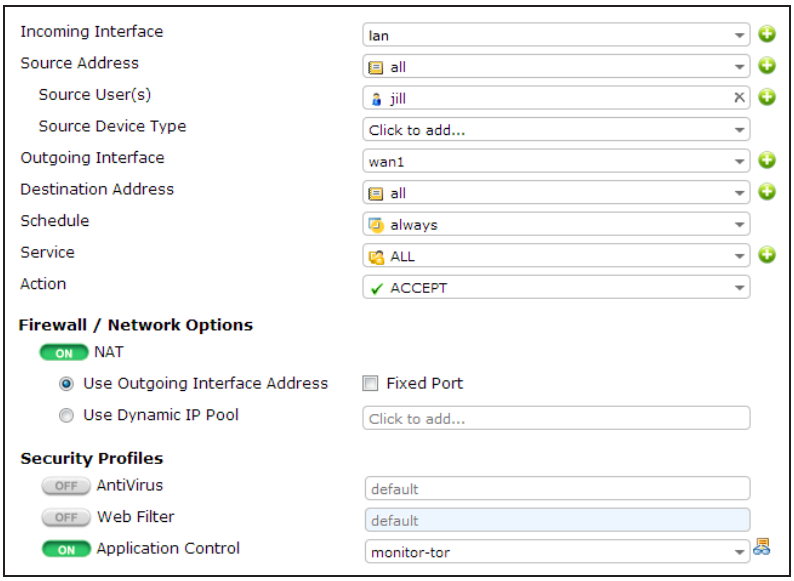
Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet. Make sure the user *jack* is included in the **Source User(s)**.

Under **Security Profiles**, turn on **Application Control** and use the **default** profile.

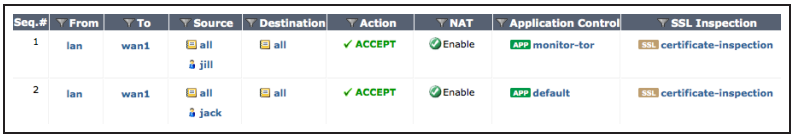


Create a second policy allowing connections from the internal network to the Internet. Set **Sourse User(s)** to *jill*.

Under **Security Profiles**, turn on **Application Control** and use the profile that will monitor Tor traffic.



Go to **Policy & Objects > Policy > IPv4** and view the policy list.



Seq.#	From	To	Source	Destination	Action	NAT	Application Control	SSL Inspection
1	lan	wan1	all jill	all	ACCEPT	Enable	monitor-tor	certificate-inspection
2	lan	wan1	all jack	all	ACCEPT	Enable	default	certificate-inspection

It is best to place more narrowly defined policies at the top of the list. In this case, the policy that monitors Tor is the most narrowly defined, because it is likely that less people will be using it than the policy that blocks Tor.

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

5. Results

The Tor browser cannot be used for user authentication, so use a different browser to authenticate using *jill*'s credentials.

Browse the Internet using the Tor browser. You will be able to connect to the Internet.

Go to **System > FortiView > Applications** and select the **now** view. You will see a listing for the **Tor** traffic.

Application	Category	Risk	Sessions	Bytes (Sent/Received)
Skype	Collaboration		38	38.74 KB
DNS	Network.Service		29	7.15 KB
UDP/40005	Unknown		7	2.62 KB
UDP/40021	Unknown		5	1.91 KB
UDP/40001	Unknown		5	1.18 KB
Tor	Proxy		4	1.82 MB

If you double-click on the listing, you can view more information about this traffic, including detailed information on the sessions.

Source	Device	Source Interface	Destination	Destination Interface	Application	Bytes (Sent/Received)
jill (10.10.80.3)	My-Desktop	lan	37.187.99.193	wan1	Tor	14.37 KB
jill (10.10.80.3)	My-Desktop	lan	37.252.190.133	wan1	Tor	1.96 MB
jill (10.10.80.3)	My-Desktop	lan	148.251.113.230	wan1	Tor	7.83 KB

Go to **User & Device > Monitor > Firewall**. Select the *jill* account and select **De-authenticate**.

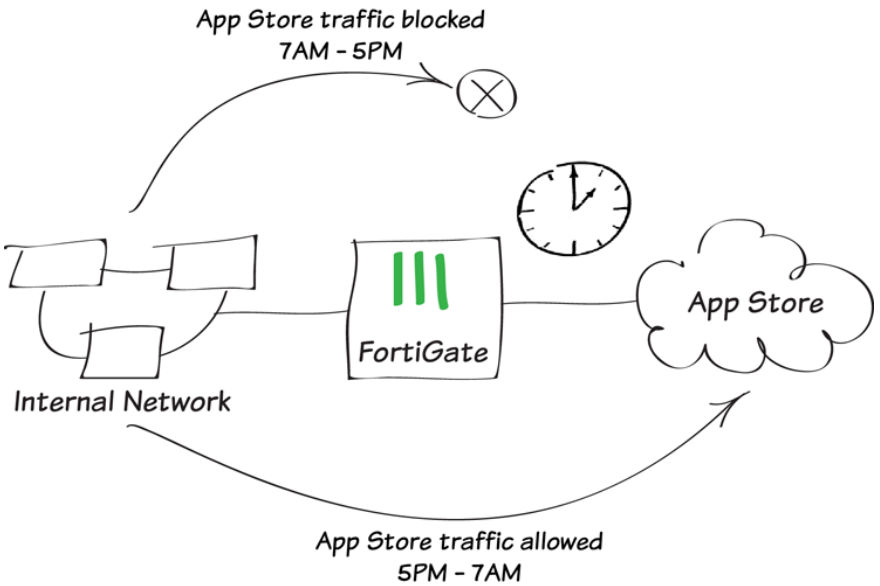
Authenticate using *jack*'s credentials. The Tor browser will be blocked.

Go to **System > FortiView > Applications** and select the **now** view. You will see that **Tor** traffic has been blocked.

Application	Category	Risk	Sessions (Blocked/Allowed)	Bytes (Sent/Received)
DNS	Network.Service		22	6.62 KB
Skype	Collaboration		9	13.71 KB
Tor	Proxy		1	476 B

For further reading, check out Application control in the FortiOS 5.2 Handbook.

Controlling access to Apple's App Store



In this recipe, access to Apple's App Store is blocked between 7AM and 5PM. During the rest of the day, access is allowed.

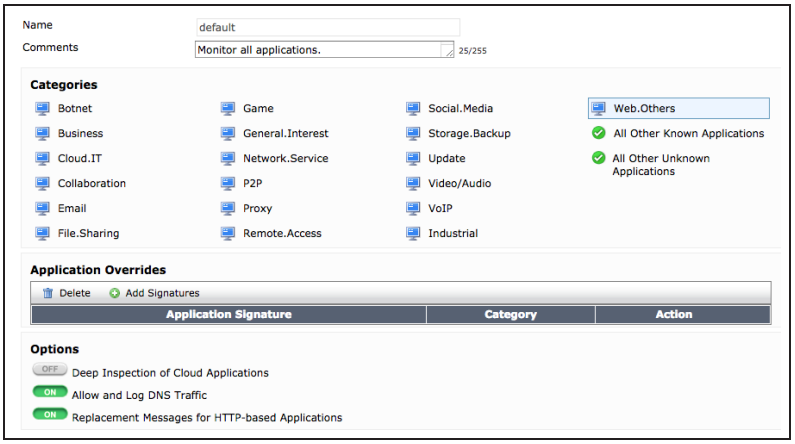
This recipe applies to devices running MacOS and iOS devices (iPhone, iPad, or iPod).

1. Enabling Application Control

Go to **System > Config > Features** and ensure that **Application Control** is turned **ON**.

2. Blocking the App Store

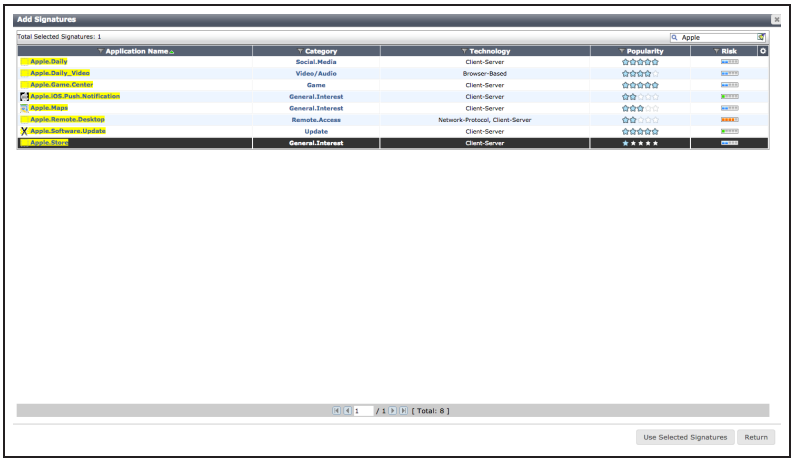
Go to **Security Profiles > Application Control** and edit the default profile.



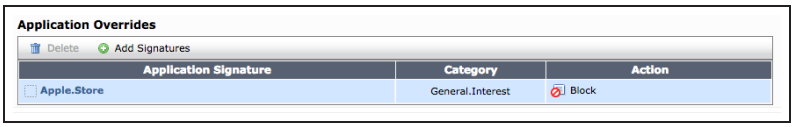
Under **Application Overrides**, select **Add Signatures**.

Search for *Apple*. Highlight the **Apple.Store** signature, then select **Use Selected Signatures**.

If you wish to restrict updates from the App Store, you should also select the **Apple.Software.Update** signature.



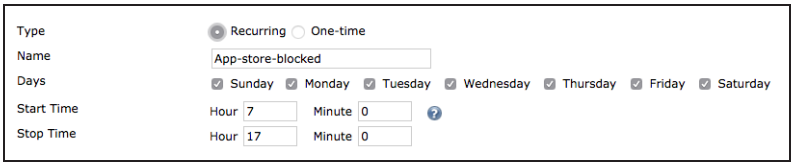
The signature now appear in the **Application Overrides** list, with the **Action** set to **Block**.



3. Creating a schedule

Go to **Policy & Objects > Objects > Schedules** and create a new schedule.

Set **Type** to **Recurring**, select the appropriate **Days**, and set **Start Time** to 7AM (Hour 7, Minute 0) and **Stop Time** to 5PM (Hour 17, Minute 0).



4. Creating a security policy to block the App Store

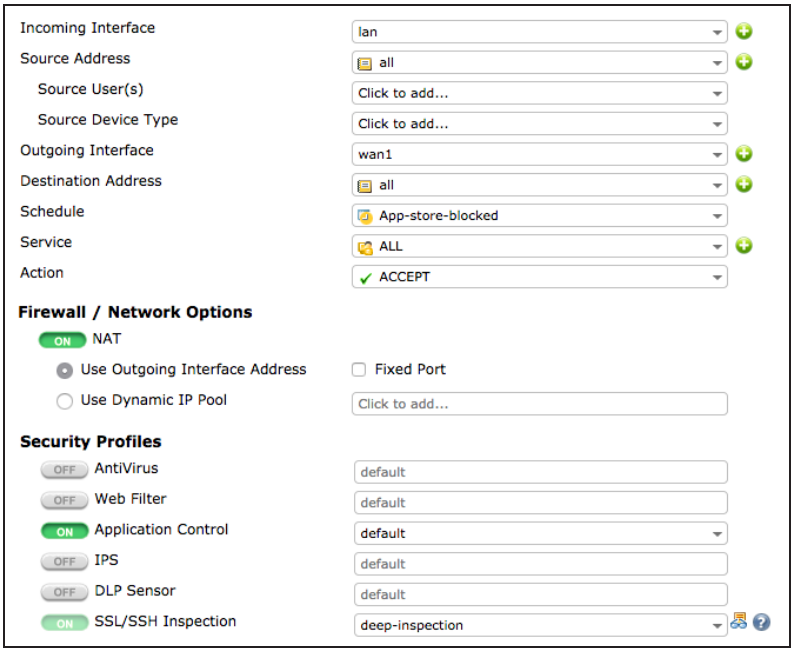
Go to **Policy & Objects > Policy > IPv4** and create a new policy that allows connections from the internal network to the Internet.

Set **Schedule** to the new schedule.

Enable **Application Control** and set it to use the new profile.

Enabling Application Control will automatically enable **SSL Inspection**. In order to inspect traffic from Cloud Applications, the **deep-inspection** profile must be used.

Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see Preventing certificate warnings.



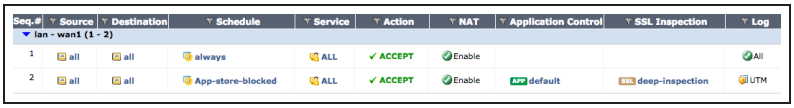
.

5. Ordering the security policies

If you do not have a general policy that allows connections from the internal network to the Internet without blocking the App Store, you will need to create one before you can continue with this step.

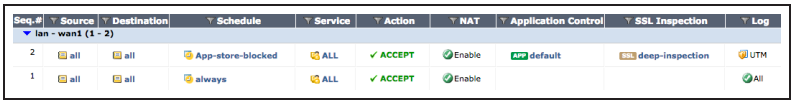
Go to **Policy & Objects > Policy > IPv4** and view your **lan - wan1** policies.

In the example, the general policy allowing Internet access appears first in the list, followed by the new policy that blocks the App Store. To make sure the App Store is blocked, you must re-order the policies so that the new policy is higher on the list.



Seq.#	Source	Destination	Schedule	Service	Action	NAT	Application Control	SSL Inspection	Log
lan - wan1 (1 - 2)									
1	all	all	always	ALL	✓ ACCEPT	Enable			All
2	all	all	App-store-blocked	ALL	✓ ACCEPT	Enable	APP default	SSL deep-inspection	UTM

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



Seq.#	Source	Destination	Schedule	Service	Action	NAT	Application Control	SSL Inspection	Log
lan - wan1 (1 - 2)									
2	all	all	App-store-blocked	ALL	✓ ACCEPT	Enable	APP default	SSL deep-inspection	UTM
1	all	all	always	ALL	✓ ACCEPT	Enable			All

6. Enforcing the schedule

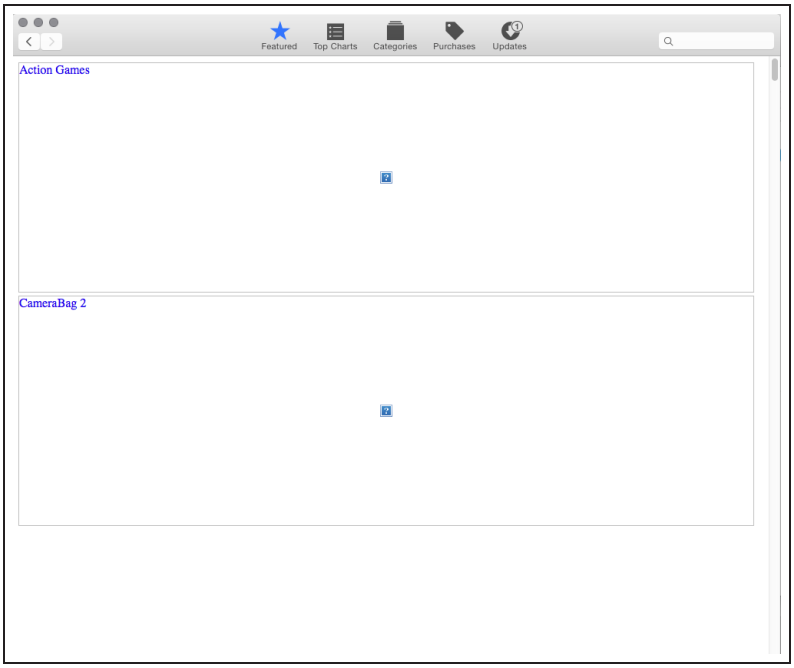
Go to **System > Dashboard > Status** and enter the following into the **CLI Console**, substituting the correct Policy ID for the new policy.

```
config firewall policy
   edit <policy-id>
     set schedule-timeout enable
   end
 end
```

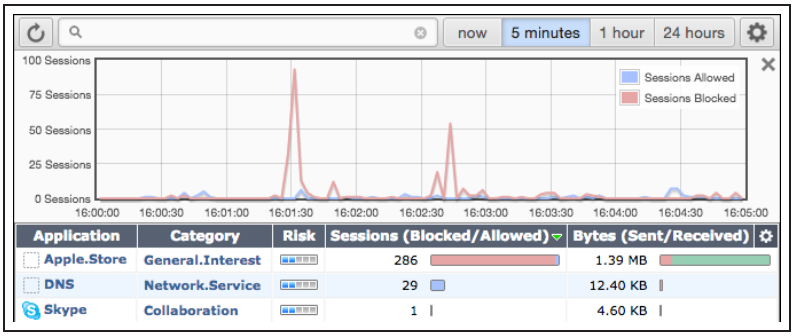
This ensures that the App Store is consistently blocked between 7AM and 5PM, even for sessions that start before 7AM.

7. Results

On a Mac or iOS device, attempt to run the App Store application between 7AM and 5PM. The application will not be able to fully load and no new apps can be downloaded.



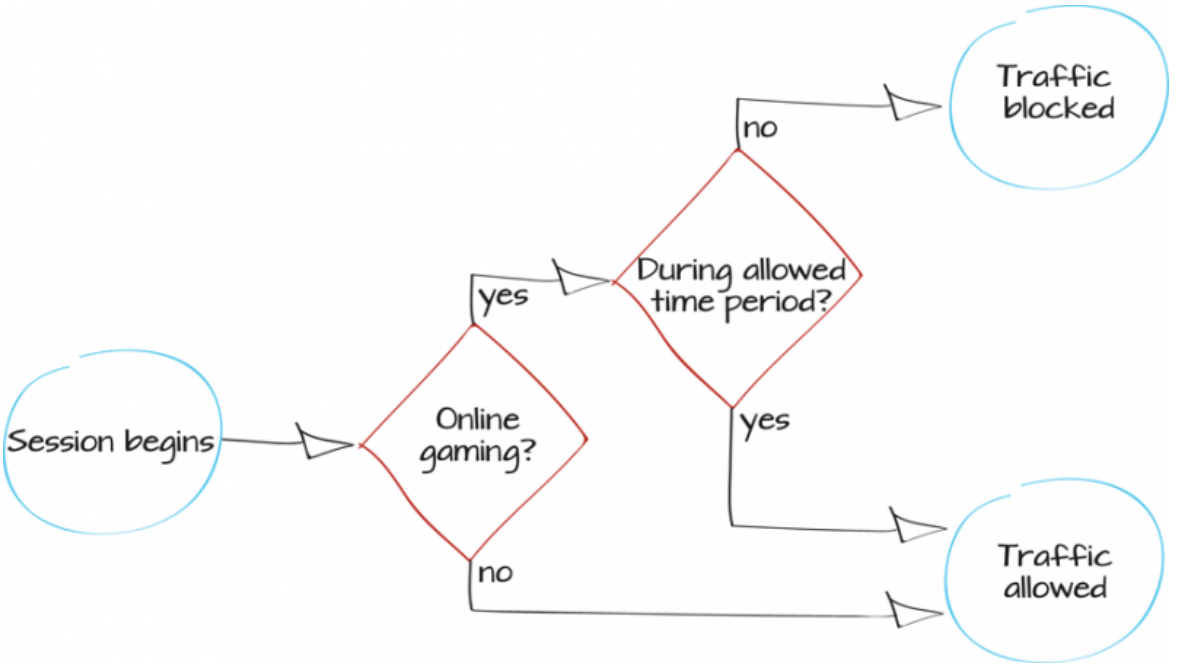
You can find information about the blocked traffic by going to **System > FortiView > Applications** and selecting the **5 minutes** view.



After 5PM, you will be able to connect to the App Store.

For further reading, check out Application control in the FortiOS 5.2 Handbook.

Restricting online gaming to evenings



In this example, online gaming will only be allowed from 7-11PM. This includes gaming websites, applications, and consoles.

This example assumes that a general policy allowing connections from the internal network to the Internet has already been configured.

1. Enabling application control, web filtering, and device identification

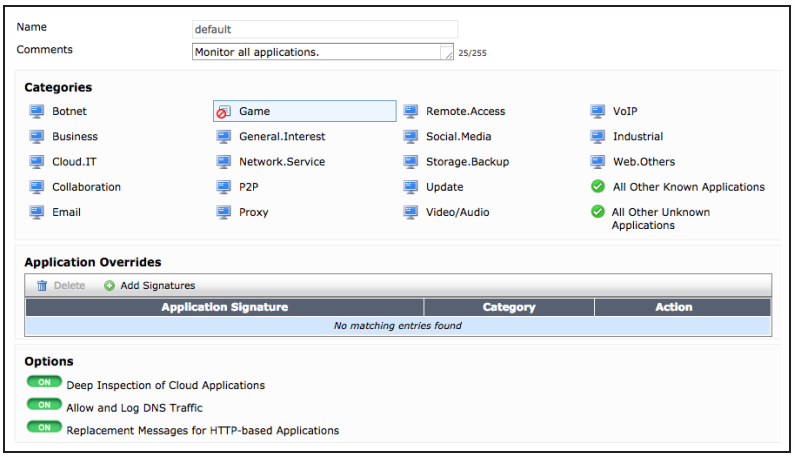
Go to **System > Config > Features** and enable both **Application Control** and **Web Filter**. Apply your changes.

Go to **System > Network > Interfaces** and edit your **lan** interface.
Enable **Detect and Identify Devices**.

2. Configuring application control and web filtering

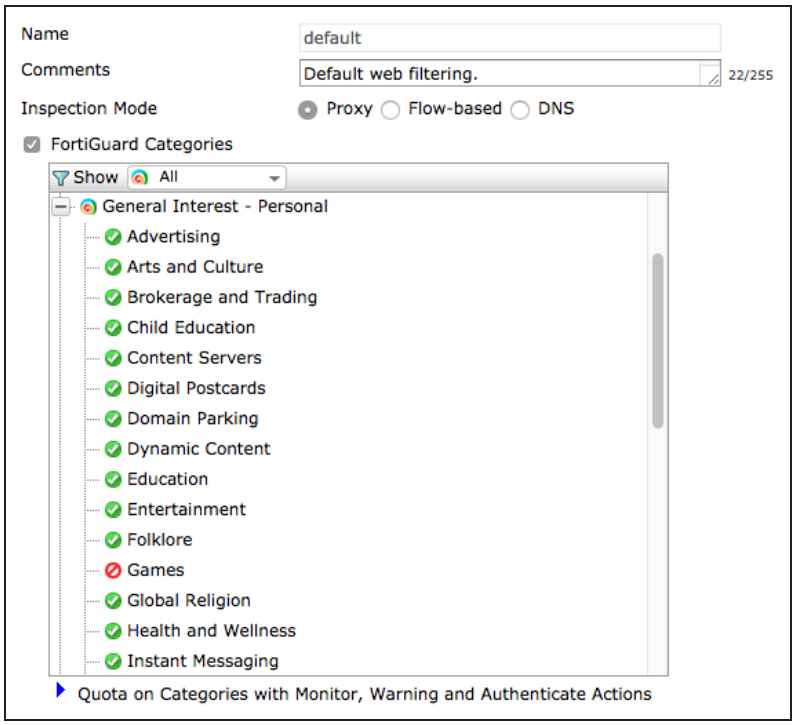
Go to **Security Profiles > Application Control** and edit the **default** policy.

Under **Categories**, select **Game**, and set the category to **Block**.
Under **Options**, enable **Deep Inspection of Cloud Applications**.



Go to **Security Profiles > Web Filter** and edit the **default** profile.

Enable **FortiGuard Categories**. Expand the **General Interest - Personal** category and select the sub-category **Games**. Set this sub-category to **Block**.



3. Editing your general policy to block gaming

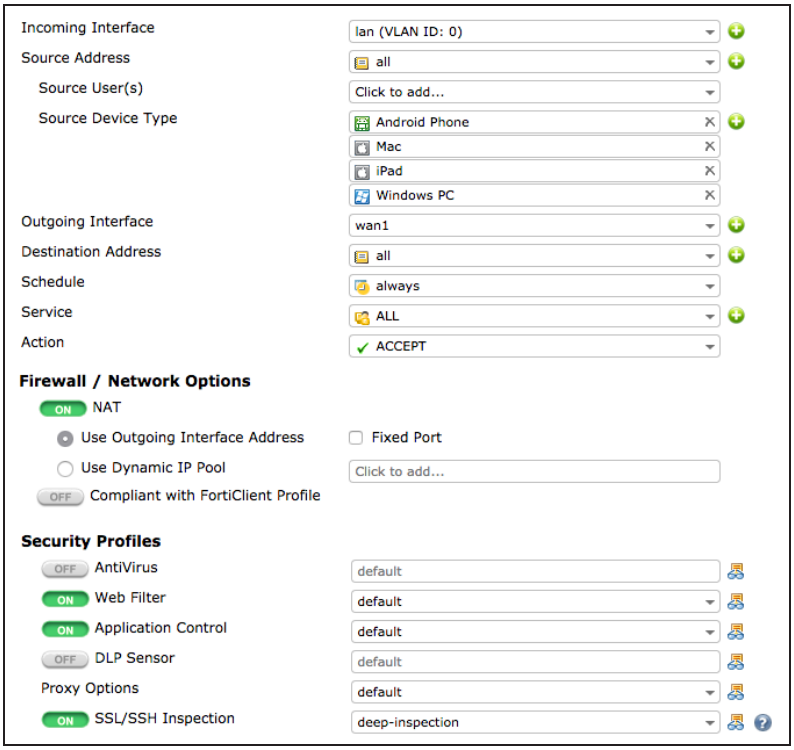
Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Set **Source Device Type** to all devices types that will be allowed on your network.

If you need to check the types of devices that are connecting to your network, go to **User & Device > Device > Device Definitions.** Do not include **Gaming Consoles**.

Under **Security Profiles**, enable both **Application Control** and **Web Filter** and set both to use to **default** profiles. Set **SSL/SSH Inspection** to **deep-inspection**.

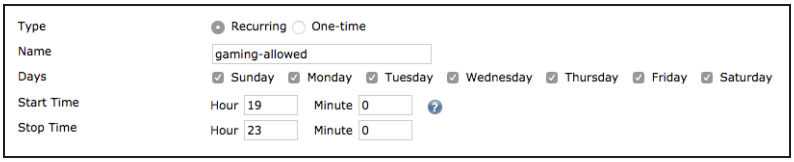
*Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see Preventing certificate warnings.*



3. Creating a schedule for when gaming is allowed

Go to **Policy & Objects > Objects > Schedules** and create a new recurring schedule.

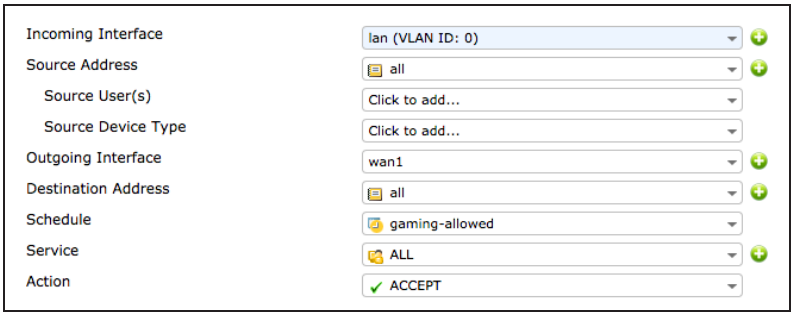
Select all **Days** and set **Start Time** to *Hour 19* (7PM) and **Stop Time** to *Hour 23* (11PM).



4. Creating a policy that allows gaming between 7-11PM

Go to **Policy & Objects > Policy > IPv4** and create a new policy that will allow devices on the LAN to have Internet access.

Set **Schedule** to use the new schedule.



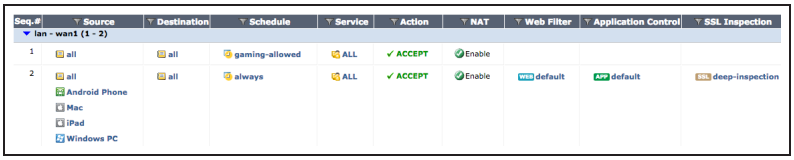
Go to **System > Dashboard > Status** and enter the following in the CLI console, substituting the ID for the new policy.

```
config firewall policy
  edit <policy_id>
    set schedule-timeout enable
  end
end
```

This will make sure that if someone is gaming during the allowed time, their session will be blocked after 11PM.

6. Ordering the policies

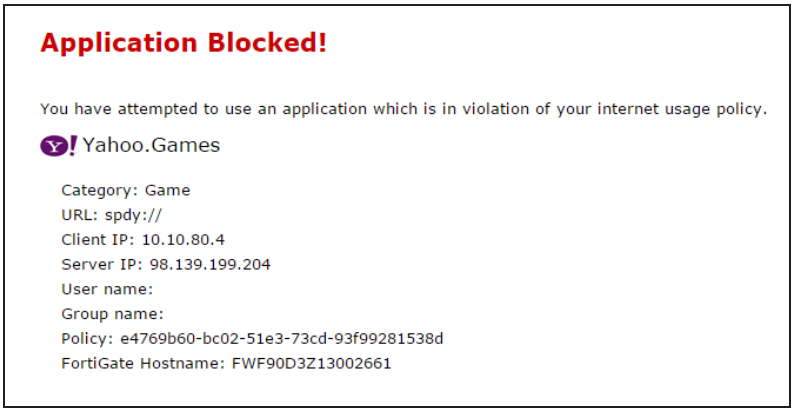
Go to **Policy & Objects > Policy > IPv4** and order the policies so that the general policy is located below the policy that allows gaming between 7-11PM.



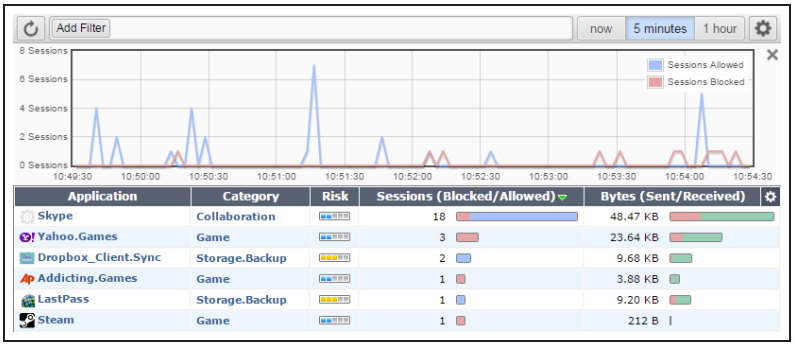
7. Results

During the time that gaming is blocked, attempt to browse to a gaming website, such as Yahoo Games. The site is blocked.

Attempt to run an online gaming application, such Steam. The application will be unable to connect to the Internet.



To view information about this blocked traffic, go to **System > FortiView > Applications**.

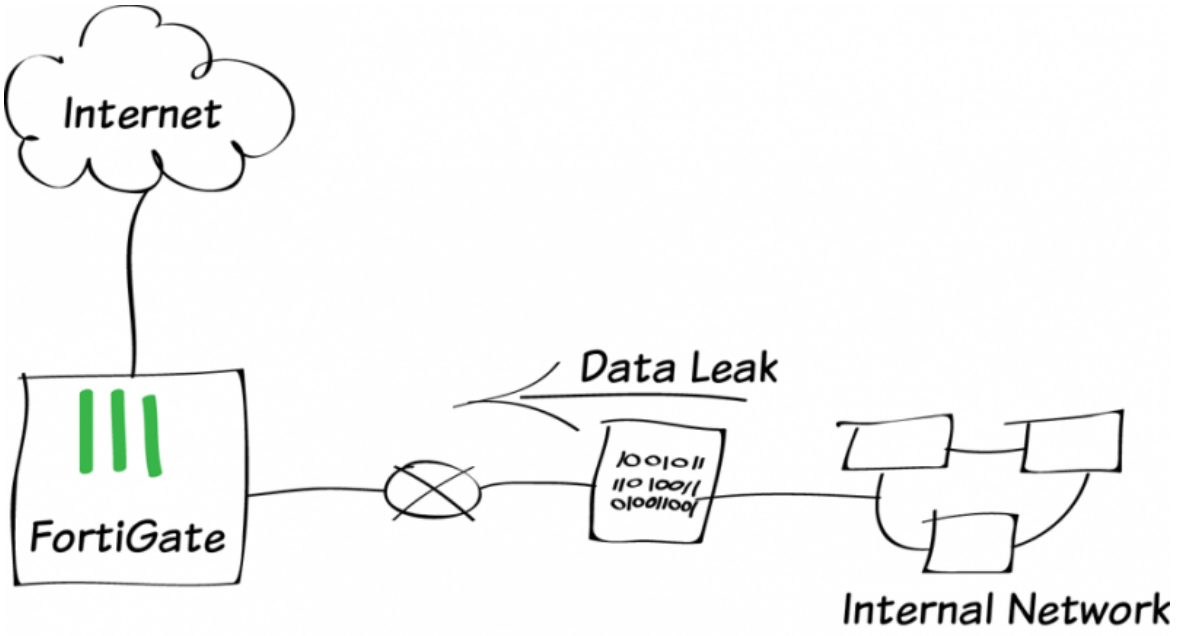


Attempt to connect to the Internet using a gaming console. The console will be unable to connect to the Internet.

Between 7-11PM, you are able to access the website, and all gaming applications and consoles can connect to the Internet.

For further reading, check out the Security Profiles in the FortiOS 5.2 Handbook.

Preventing data leaks



In this example, you will block files that contain sensitive information from leaving your network. To do this, a Data Leak Prevention (DLP) profile will be used that blocks files that have a DLP watermark applied to them, as well as any .exe files.

1. Enabling DLP and multiple security profiles

Go to **System > Config > Features** and ensure that **DLP** is turned **ON**.

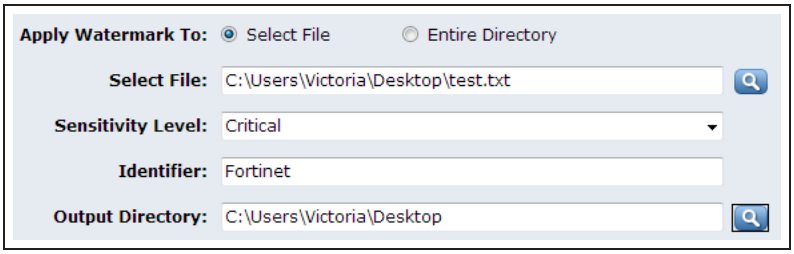
Select **Show More** and ensure that **Multiple Security Profiles** is also turned **ON**. If necessary, **Apply** your changes.

2. Applying a DLP watermark to a file

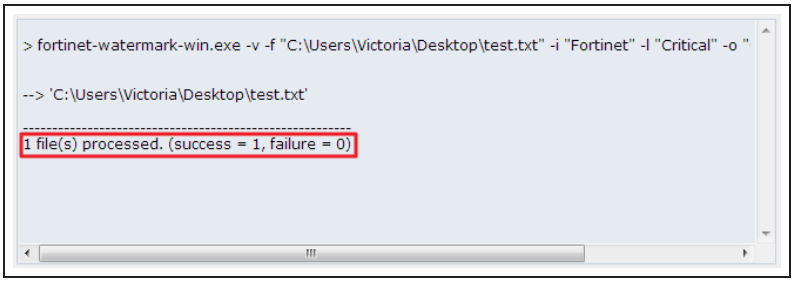
The DLP watermarking client is available as part of FortiExplorer. This feature is currently only available using FortiExplorer for Microsoft Windows.

If you do not already have FortiExplorer on your computer, click here to download it.

Open FortiExplorer. Under **Tools**, select **DLP Watermark**.Select **Apply Watermark to Select File**. Select the file and set the **Sensitivity Level**, **Identifier**, and **Output Directory**. Select **Apply Watermark**.

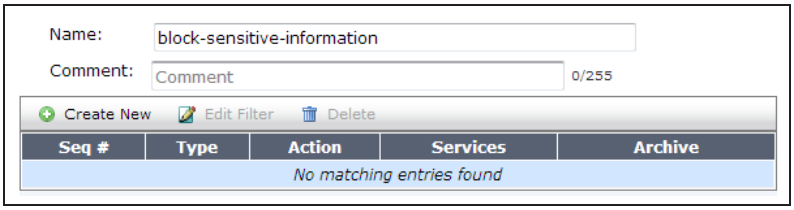


The dialogue box will show the file being processed. Ensure that the process was successful.



3. Creating a DLP profile

Go to **Security Profiles > Data Leak Prevention** and create a new profile.

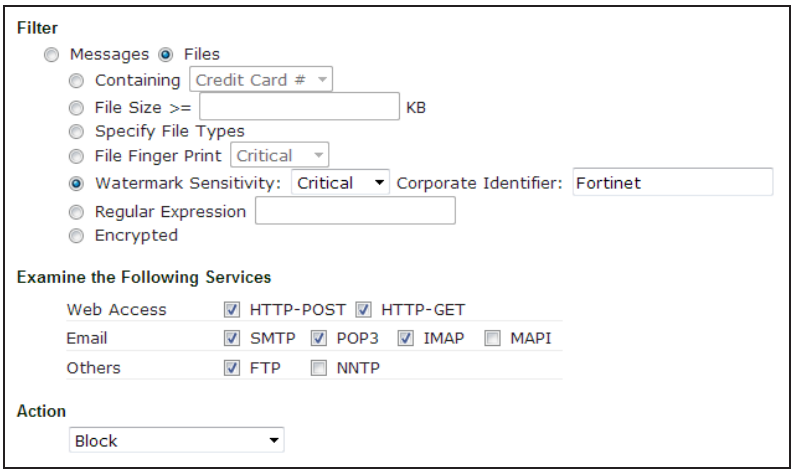


In the Filter list, select **Create New**.

Set the filter to look for **Files**. Select **Watermark Sensitivity** and set it to match the watermark applied to the file. Do the same for **Corporate Identifier**.

Set **Examine the Following Services** to all the services required by your network.

Set **Action** to **Block**.

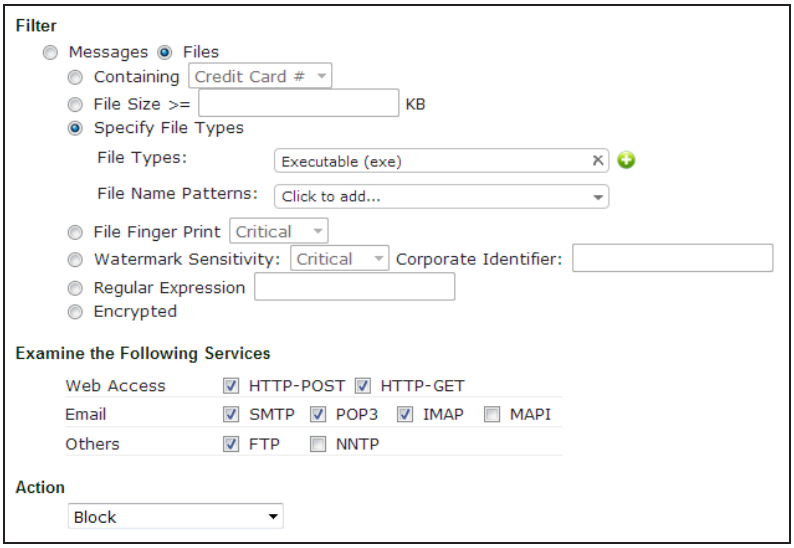


Create a second filter.

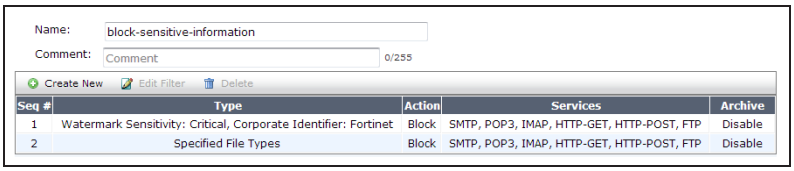
Set the filter to look for **Files**. Select **Specify File Types** and set **File Types** to **Executable (exe)**.

Set **Examine the Following Services** to all the services required by your network.

Set **Action** to **Block**.



Both filters now appear in the Filters list.



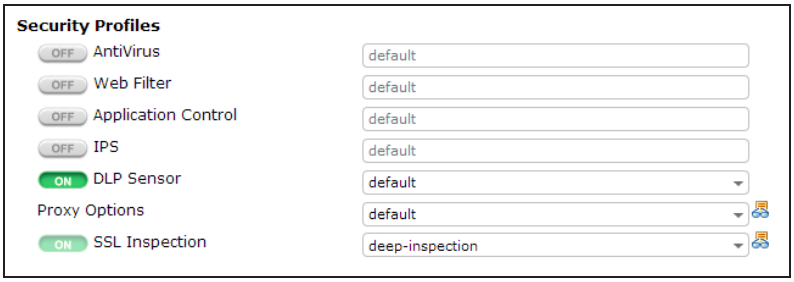
4. Adding the profile to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit your Internet-access policy.

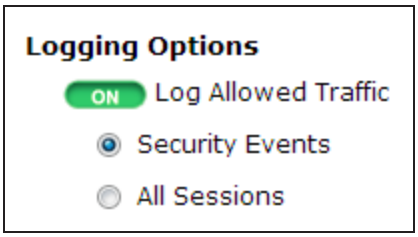
Under **Security Profiles**, enable **DLP Sensor** and set it to use the new profile.

SSL Inspection is automatically enabled. Set it to use the **deep-inspection** profile to ensure that DLP is applied to encrypted traffic.

*Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see Preventing certificate warnings.*



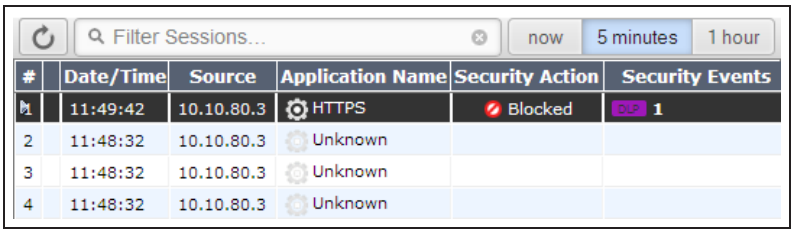
Under **Logging Options**, enable **Log Allowed Traffic** and select **Security Events**.



5. Results

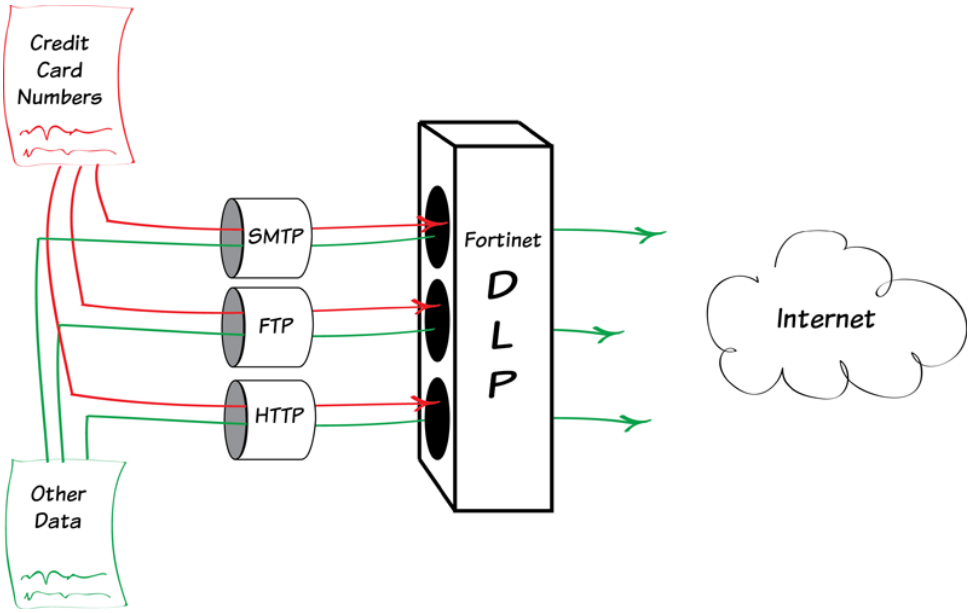
Attempt to send either the watermarked file or an .exe file using a protocol that the DLP filer is examining.Depending on which protocol is used, the attempt will either be blocked by the FortiGate or it will timeout.

Go to **System > FortiView > All Sessions** and select the **5 minutes** view for information about the blocked session.



For further reading, check out Data leak prevention in the FortiOS 5.2 Handbook.

Prevent credit card numbers from being leaked



In this example, you will use DLP to prevent credit card numbers from being sent out of your network using HTTP, FTP, or SMTP.

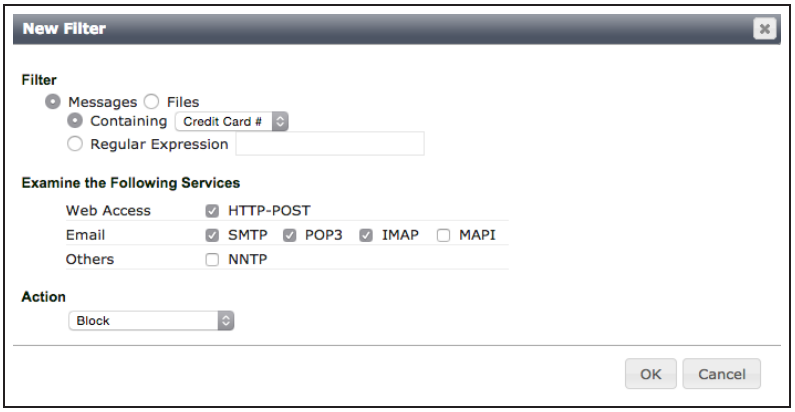
1. Enabling DLP

Go to **System > Config > Features** and make sure that **DLP** is turned **ON**.

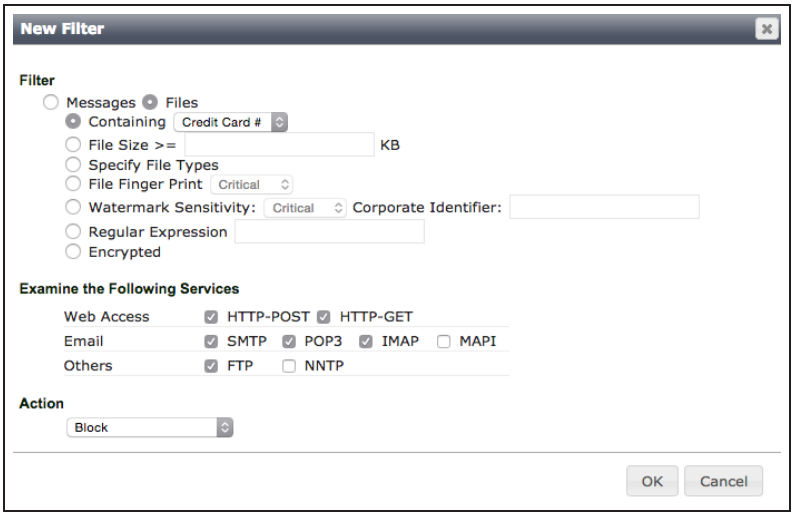
2. Adding two filters to the default DLP sensor

Go to **Security Profiles > Data Leak Prevention** and edit the default sensor. Select **Create New** to add a new filter.

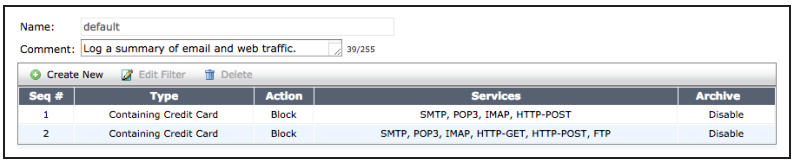
The first filter blocks web pages and email **Messages** containing credit card numbers.



The second filter blocks **Files** containing credit card numbers. This includes email attachments and files uploaded with a web browser or using FTP.



Both filters appear in the default sensor.

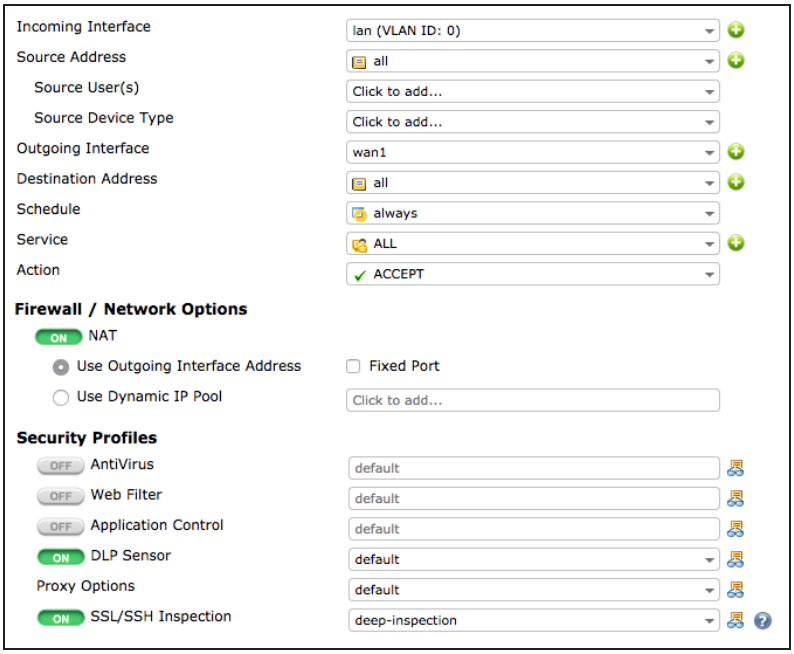


3. Adding the new DLP sensor to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network (in this case connected to the **lan** interface) to the Internet.

Under **Security Profiles**, turn on **DLP Sensor** and use the **default** sensor. Set **SSL/SSH Inspection** to **deep-inspection**.

*Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see Preventing certificate warnings.*



4. Results

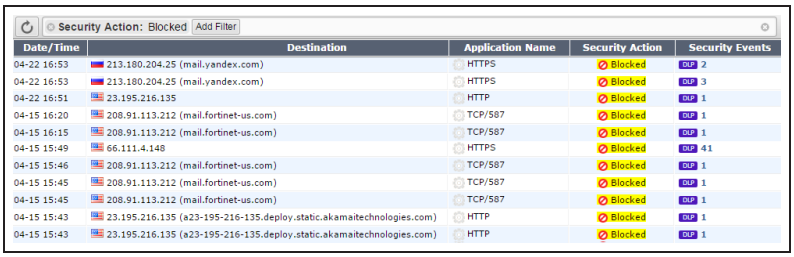
Locate some example credit card numbers to use for testing purposes. These can be found from a variety of locations, including PayPal.

Testing HTTP: Go to a website with a comment section and attempt to post an example credit card number. The comment is blocked.

Testing FTP: Transfer a file containing an example credit card number using FTP. This transfer is blocked.

Testing SNMP: Send an email containing an example credit card number using a SNMP email client. This email is blocked.

To view more information about the blocked traffic, go to **Log & Report > Traffic Log > Forward Traffic** and filter for **Security Actions: Blocked**.

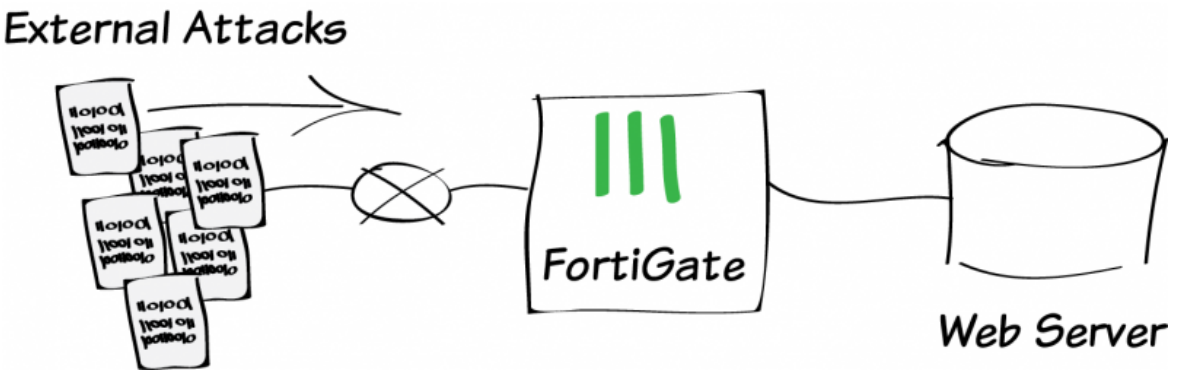


Security Action: Blocked Add Filter

Date/Time	Destination	Application Name	Security Action	Security Events
04-22 16:53	213.180.204.25 (mail.yandex.com)	HTTPS	Blocked	DLP 2
04-22 16:53	213.180.204.25 (mail.yandex.com)	HTTPS	Blocked	DLP 3
04-22 16:51	23.195.216.135	HTTP	Blocked	DLP 1
04-15 16:20	208.91.113.212 (mail.fortinet-us.com)	TCP/587	Blocked	DLP 1
04-15 16:15	208.91.113.212 (mail.fortinet-us.com)	TCP/587	Blocked	DLP 1
04-15 15:49	66.111.4.148	HTTPS	Blocked	DLP 41
04-15 15:46	208.91.113.212 (mail.fortinet-us.com)	TCP/587	Blocked	DLP 1
04-15 15:45	208.91.113.212 (mail.fortinet-us.com)	TCP/587	Blocked	DLP 1
04-15 15:45	208.91.113.212 (mail.fortinet-us.com)	TCP/587	Blocked	DLP 1
04-15 15:43	23.195.216.135 (a23-195-216-135.deploy.static.akamaitechnologies.com)	HTTP	Blocked	DLP 1
04-15 15:43	23.195.216.135 (a23-195-216-135.deploy.static.akamaitechnologies.com)	HTTP	Blocked	DLP 1

For further reading, check out Data leak prevention in the FortiOS 5.2 Handbook.

Protecting a web server



In this example, you will protect a web server using an Intrusion Prevention System (IPS) profile and a Denial of Service (DoS) policy. This will prevent a variety of different attacks from reaching the server.

A video of this recipe is available here.

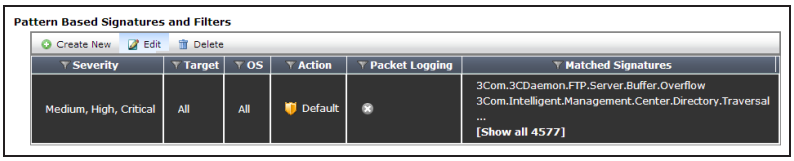
1. Enabling Intrusion Protection

Go to **System > Config > Features** and ensure that **Intrusion Protection** is turned **ON**. Apply your changes if necessary.

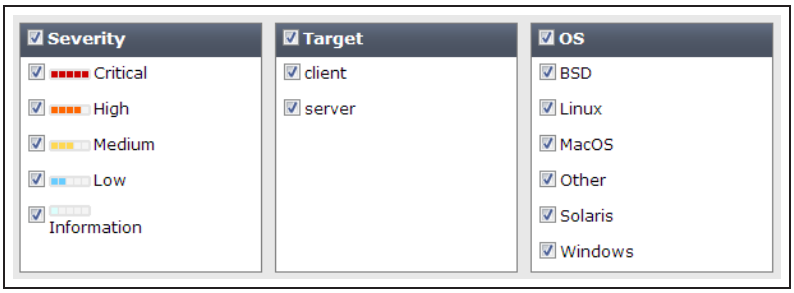
2. Configuring the default IPS profile to block common attacks

Go to **Security Profiles > Intrusion Protection** and edit the **default** profile.

In the **Pattern Based Signatures and Filters** list, highlight the default entry and select **Edit**.



Select **Severity** to view all signatures in the database.



Scroll down and set the **Action** to **Block All**.

Enable all the listed **Rate Based Signatures**.

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (minutes)
ON	Apache.HTTP.Server.Range.DoS	30	1	Any	Block	0
ON	Digium.Asterisk.File.Descriptor.DoS	20	1	Any	Block	0
ON	Digium.Asterisk.IAX2.Call.Number.DoS	275	1	Any	Block	0
ON	DotNetNuke.Padding.Oracle.Attack	1000	5	Any	Block	0
ON	FTP.Login.Brute.Force	200	10	Any	Block	0
ON	FreeBSD.TCP.Reassembly.DoS	10	2	Any	Block	0
ON	IMAP.Login.Brute.Force	60	10	Any	Block	0
ON	Lotus.Domino.Login.Brute.Force	300	10	Any	Block	0
ON	MS.Active.Directory.LDAP.Packet.Handling.DoS	100	1	Any	Block	0
ON	MS.RDP.Connection.Brute.Force	200	10	Any	Block	0
ON	MS.Windows.SMB.NTLM.Authentication.Lack.Of.Entropy	35	1	Any	Block	0
ON	MS.Windows.SMB.Server.NTLM.Authentication.Bypass	1000	1	Any	Block	0
ON	MS.XML.Core.Services.Memory.Corruption	5	10	Any	Block	0
ON	MySQL.Login.Brute.Force	60	60	Any	Block	0
ON	Novell.Open.Enterprise.Server.HTTPSTK.DoS	19	1	Any	Block	0
ON	POP3.Login.Brute.Force	200	10	Any	Block	0
ON	SMB.Login.Brute.Force	500	60	Any	Block	0
ON	SSH.Connection.Brute.Force	200	10	Any	Block	0
ON	Telnet.Login.Brute.Force	60	60	Any	Block	0
ON	Wordpress.Login.Brute.Force	1000	10	Any	Block	0

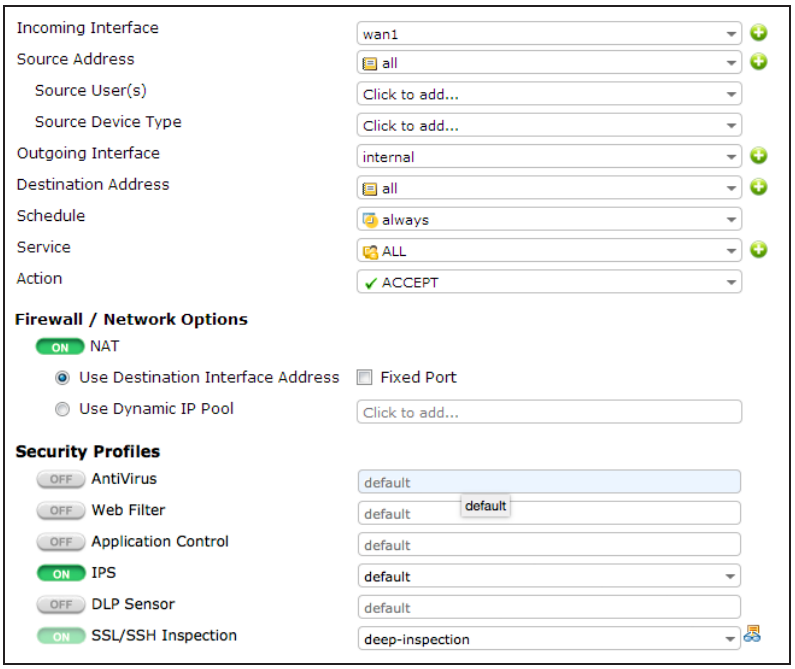
3. Adding the IPS sensor to the server access security policy

Go to **Policy & Objects > Policy > IPv4** and edit the security policy allowing traffic to the web server from the Internet.

Enable **IPS** under **Security Profiles** and set it to use the **default** profile.

Enabling IPS will automatically enable **SSL Inspection**. In order to inspect encrypted traffic, the **deep-inspection** profile must be used.

Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see Preventing certificate warnings.

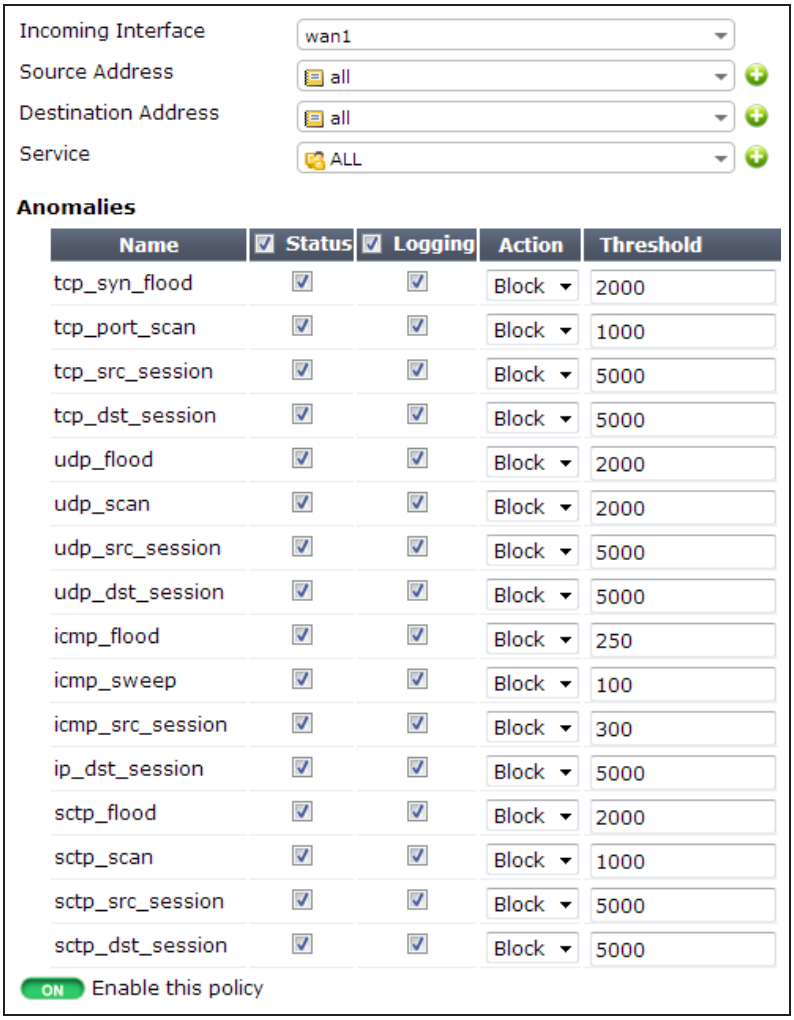


4. Creating a DoS policy

Go to **Policy & Objects > Policy > DoS** and create a new policy.

Set **Incoming Interface** to your Internet-facing interface.

In the **Anomalies** list, enable **Status** and **Logging** and set the **Action** to **Block** for all types.



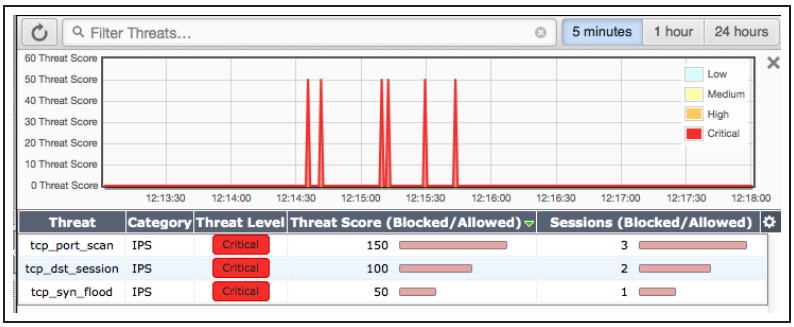
5. Results

Warning: DoS attacks are illegal, unless you own the server under attack. Before performing an attack, ensure that you have the correct server IP.

Launch a DoS attack on your web server's IP address.

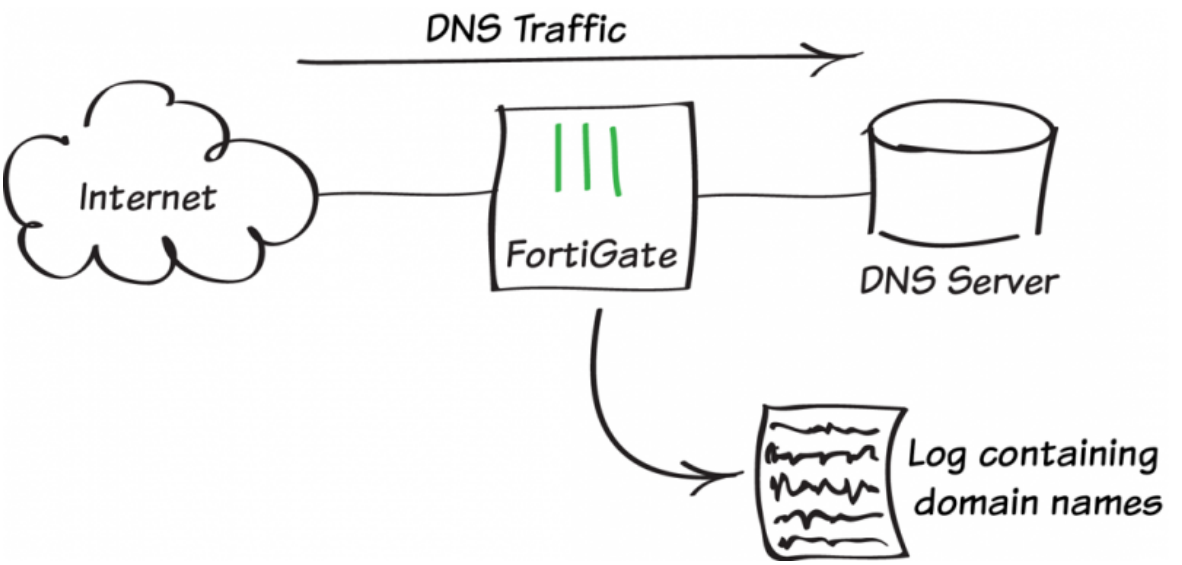
Go to **System > FortiView > Threats** and select the **5 Minutes** view.

You will see that a DoS attack has been detected and blocked.



For further reading, check out Intrustion Protection in the FortiOS 5.2 Handbook.

Logging DNS domain lookups



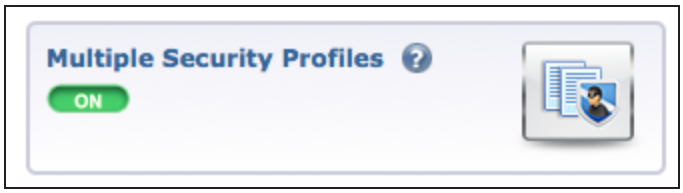
In this recipe, you will add a custom Intrusion Protection (IPS) signature to a security policy to record all domain lookups accepted by the policy. The signature records an IPS log message containing the domain name every time a DNS lookup occurs.

1. Enabling Intrusion Protection and multiple security profiles

Go to **System > Config > Features** and enable **Intrusion Protection**.

Select **Show More** and enable **Multiple security profiles.**

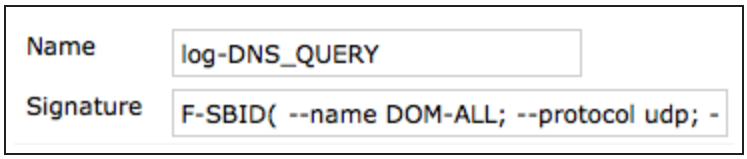
Apply the changes.



2. Creating a custom IPS signature

Go to **Security Profiles > Intrustion Protection** and select **View IPS Signatures**.

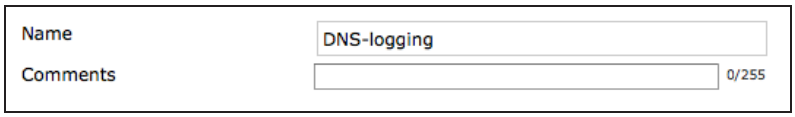
Create a new signature with this syntax. (You can copy and paste this text into the **Signature** field.)




```
F-SBID( --name DOM-ALL; --protocol udp; --service
dns; --log DNS_QUERY;)
```

3. Adding the signature to an IPS profile

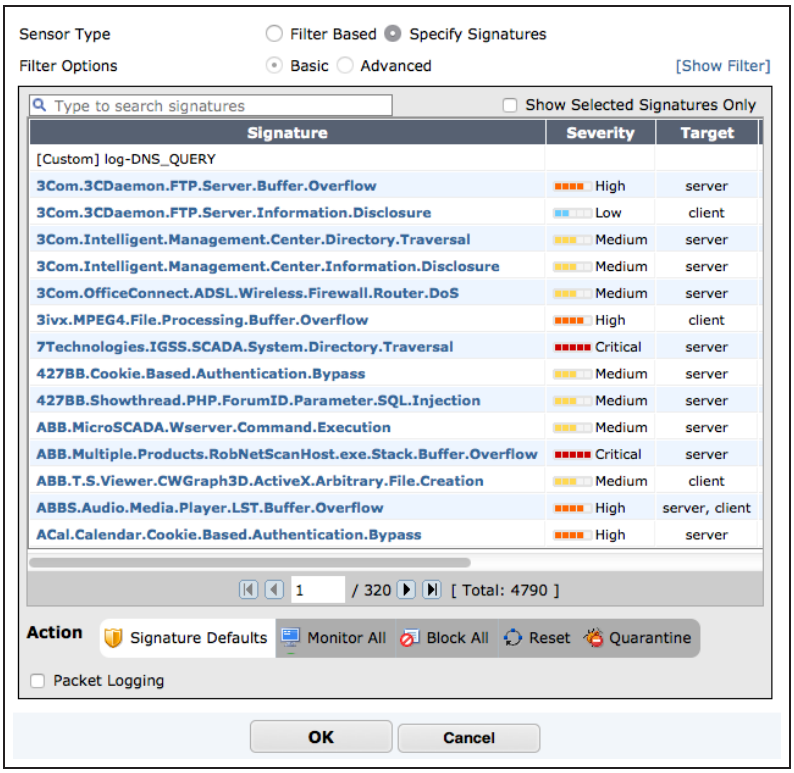
Go to **Security Profiles > Intrusion Protection** and create a new profile.



Under **Pattern Based Signatures and Filters**, select **Create New**.

Set **Sensor Type** to Specify Signatures. The new signature should appear at the top of the list. If it does not, search for the signature's name (in the example, *log-DNS_QUERY)*.

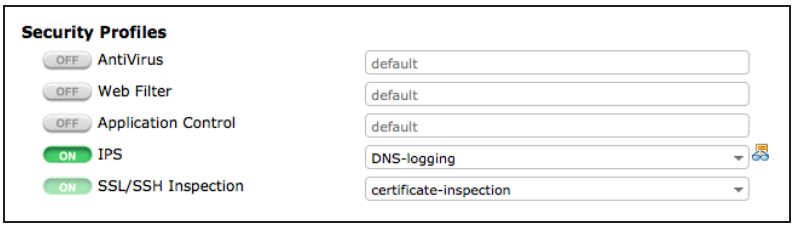
Select the signature, then select **OK**.



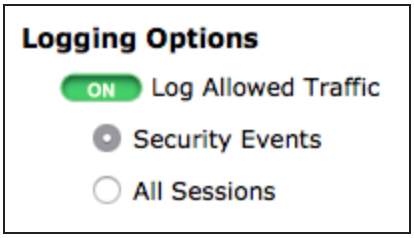
4. Adding the profile to the DNS server's security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy allowing traffic to reach the DNS server.

Under **Security Profiles**, enable **IPS** and select the new profile.



Under **Logging Options**, enable **Log Allowed Traffic** and select **Security Events**.



5. Results

Go to **Log & Report > Security Log > Intrustion Protection**.

This log only appears when an IPS event has occurred.

You will see that the IPS profile has detected matching traffic.

#	Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
1	07:51:31		192.168.200.110	udp		detected		DOM-ALL
2	07:51:32		192.168.200.110	udp		detected		DOM-ALL
3	07:51:32		192.168.200.110	udp		detected		DOM-ALL
4	07:51:31		192.168.200.110	udp		detected		DOM-ALL
5	07:51:32		192.168.200.110	udp		detected		DOM-ALL
6	07:51:31		192.168.200.110	udp		detected		DOM-ALL
7	07:51:31		192.168.200.110	udp		detected		DOM-ALL
8	07:51:32		192.168.200.110	udp		detected		DOM-ALL
9	07:51:32		192.168.200.110	udp		detected		DOM-ALL
10	07:51:31		192.168.200.110	udp		detected		DOM-ALL

If you select an entry, you can view more information.

The domain name is shown in the **Message** field.

#	38	**Action**	detected
Attack ID	4153	**Attack Name**	DOM-ALL
Date/Time	07:51:29	**Destination**	192.168.110.9
Direction	0	**Dst Port**	53
Event Type	signature	**Incident Serial No.**	216891970
Level		**Log ID**	16384
Message	custom: DOM-ALL, dns_query=trello.com;	**Profile Name**	DNS-logging
Protocol	udp	**Protocol Number**	17

If you have a FortiAnalyzer, you can create a custom dataset for the DNS query by going to **Reports > Advanced > Dataset**.

Name: DNS-Query

Log Type: Attack

Query:

```
select msg, sum(totalnum) as totalnum from
###(select srcip, msg, count(*) as totalnum from
$log where $filter-exclude-var group by srcip,
msg order by totalnum desc)### t where $filter-
var-only and msg is not null group by msg order
by totalnum desc
```

This dataset can then be used in a custom report.

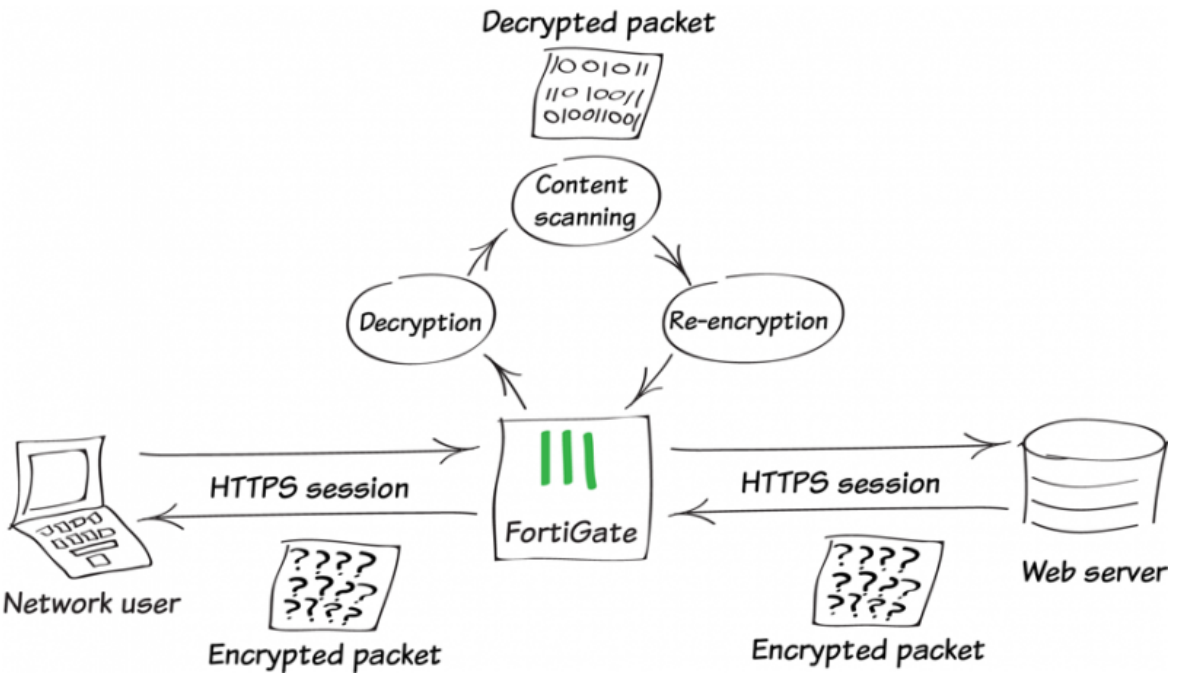
FORTINET

TOP 10 requested DNS Domains

#	Message	totalnum	% of Total
1	custom: DNS-A-Request, dns_query=init-p01st.push.apple.com;	57	3.68
2	custom: DNS-A-Request, dns_query=init-s01st.push.apple.com;	49	3.17
3	custom: DNS-A-Request, dns_query=www.google.com;	49	3.17
4	custom: DNS-A-Request, dns_query=www.apple.com;	44	2.84
5	custom: DNS-A-Request, dns_query=local;	40	2.58
6	custom: DNS-A-Request, dns_query=apple.com;	38	2.45
7	custom: DNS-A-Request, dns_query=p07-btmmdns.icloud.com;	34	2.20
8	custom: DNS-A-Request, dns_query=apple-mobile.query.yahooapis.com;	31	2.00
9	custom: DNS-A-Request, dns_query=dell.com;	30	1.94
10	custom: DNS-A-Request, dns_query=api.bing.com;	26	1.68
11	**Others**	**1150**	**74.29**
12	**Total**	**1548**	**100.00**

For further reading, check out DNS Service in the FortiOS 5.2 Handbook.

Why you should use SSL inspection



Most of us are familiar with the benefits of Hypertext Transfer Protocol Secure (HTTPS) and how it protects most commerce activities on the Internet. HTTPS applies Secure Sockets Layer (SSL) encryption to secure web traffic from prying eyes. The benefits are obvious; the risks, however are not as obvious, though they do exist.

One major risk is that encrypted traffic could be used in attacks that get around your normal defences. For example, you could download a file containing a virus during an e-commerce session. Because the session is encrypted your normal defences would miss it.

In another example, you could receive a phishing email that contains a seemingly harmless downloader file. When launched, the downloader could create an encrypted HTTPS session to a command and control (C&C) server that downloads malware onto your computer. Because the session containing the malware is encrypted, your antivirus protection can't see and block the threat.

To protect your network from these threats, SSL inspection is the key that your FortiGate can use to unlock encrypted sessions, see into encrypted packets, find threats, and block them. SSL inspection not only protects you from attacks that use HTTPS, but also from other commonly used SSL-encrypted protocols, such as SMTPS, POP3S, IMAPS, and FTPS.

Full SSL inspection

To make sure that all SSL encrypted content is inspected, you must use full SSL inspection, which is also known as deep inspection. When full SSL inspection is used, the FortiGate impersonates the recipient of the originating SSL session, decrypts and inspects the content. The FortiGate then re-encrypts the content, creates a new SSL session between the FortiGate and the recipient by impersonating the sender and sends the content to the sender.

When the FortiGate re-encrypts the content it uses a certificate stored on the FortiGate. The client must trust this certificate to avoid certificate errors. Whether or not this trust exists depends on the client, which can be the computer's OS, a browser or some other application, which will likely maintain it's own certificate repository. For more information about this, see the recipe Preventing certificate warnings.

There are two deployment methods for full SSL inspection:

Multiple Clients Connecting to Multiple Servers:

- Uses a CA certificate (which can be upload by going to **System > Certificates > CA Certificates**).
- Typically applied to outbound policies where destination are unknown (i.e. normal web traffic).
- Address and web category whitelists can be configured to bypass SSL inspection.

Protecting SSL Server

- Uses a server certificate (which can be upload by going to **System > Certificates > CA Certificates**) to protect a single server.
- Typically used on inbound policies to protect servers available externally through Virtual IPs
- Since this is typically deployed "outside-in" (clients on the Internet accessing server(s) on the internal side of the FortiGate), server certificates using the public FQDN of the server are often purchased from a commercial Certificate Authority and uploaded to the FortiGate. This avoids client applications generating SSL certificate errors due to certificate mismatch.

More detail is available in the FortiOS 5.2 Handbook. Also, check the Fortinet Knowledge Base for these technical notes:

- How to Enable SSL inspection from the CLI and Apply it to a Policy
- How to block web-based chat on Gmail webmail using App Sensor + SSL inspection

SSL certificate inspection

FortiGates also support a second type of SSL inspection, called SSL certificate inspection. When certificate inspection is used, the FortiGate only inspects the header information of the packets.

Certificate inspection is used to verify the identity of web servers and can be used to make sure that HTTPS protocol isn't used as a workaround to access sites you have blocked using web filtering.

The only security feature that can be applied using SSL certificate inspection mode is web filtering. However, since only the packet is inspected, this method does not introduce certificate errors and can be a useful alternative to full SSL inspection when web filtering is used.

Troubleshooting

The most common problem with SSL inspection is users receiving SSL errors when the CA certificate is not trusted. This is because by default the FortiGate uses a certificate that is not trusted by the client. There are two ways to fix this:

- All users must import the FortiGate's default certificate into their client applications as a trusted certificate.
- Configure the FortiGate to use a certificate that is already trusted by your clients. For example, a certification signed by a CA that your clients already trust.

The first method can be more labor intensive because you have to distribute a certification to all clients. This can also be an ongoing problem as new clients are added to your network. The second method is usually less work but may require paying for a CA. Both of these methods are covered in the recipe Preventing Certificate Warnings.

If you choose to install the cert on clients, this can be easier in a Microsoft Active Directory domain by using Group Policy Objects to install the certificate on domain members. Check that the Group Policy has propagated to all computers by opening Internet Explorer on a workstation PC, opening **Tools > Internet Options > Content > Certificates >Trusted Root Certification Authorities**, and ensuring that the FortiGate's certificate is present.

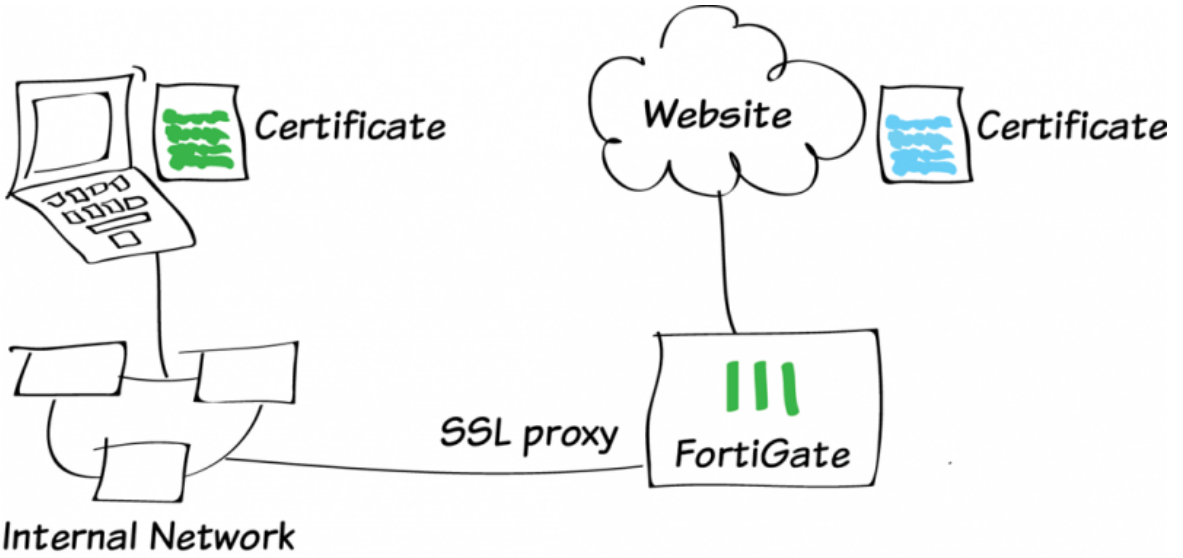
For corporate-owned mobile devices, MDM solutions like AirWatch, MobileIron, or Fiberlink, use Simple Certificate Enrollment Protocol (SCEP) to ease certificate enrollment.

Best practices

Because all traffic needs to be decrypted, inspected, and re-encrypted, using SSL inspection can reduce overall performance of your FortiGate. To make sure you aren't using too many resources for SSL inspection, do the following:

- **Know your traffic** – Know how much traffic is expected and what percent of the traffic is encrypted. You can also limit the number of policies that allow encrypted traffic.
- **Be selective** – Use white lists or trim your policy to apply SSL inspection only where it is needed.
- **Use hardware acceleration** - FortiGate models with either the CP6 or CPU processor have an SSL/TLS protocol processor for SSL content scanning and SSL acceleration. For more information about this, see the Hardware Acceleration handbook.
- **Test real-world SSL inspection performance yourself** - Use the flexibility of FortiGate's security policy to gradually deploy SSL inspection, rather than enabling it all at once.

Preventing certificate warnings



This example illustrates how to prevent your users from getting a security certificate warning when you have enabled full SSL inspection (also called deep inspection).

Instead of having users select **Continue** when they receive a warning, a bad habit to encourage, you can use the examples below to prevent certificate warnings from appearing: Using the default FortiGate certificate or Using a custom certificate .

For more information about SSL inspection, seeWhy you should use SSL inspection.

Using the default FortiGate certificate

All FortiGates have a default certificate that is used for SSL deep inspection. This certificate is also used in the default **deep-inspection** profile.

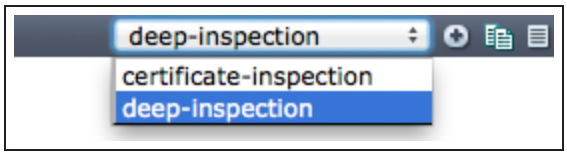
To prevent your users from seeing certificate warnings you can distribute this certificate to your user's devices.

A video of this example can be found here.

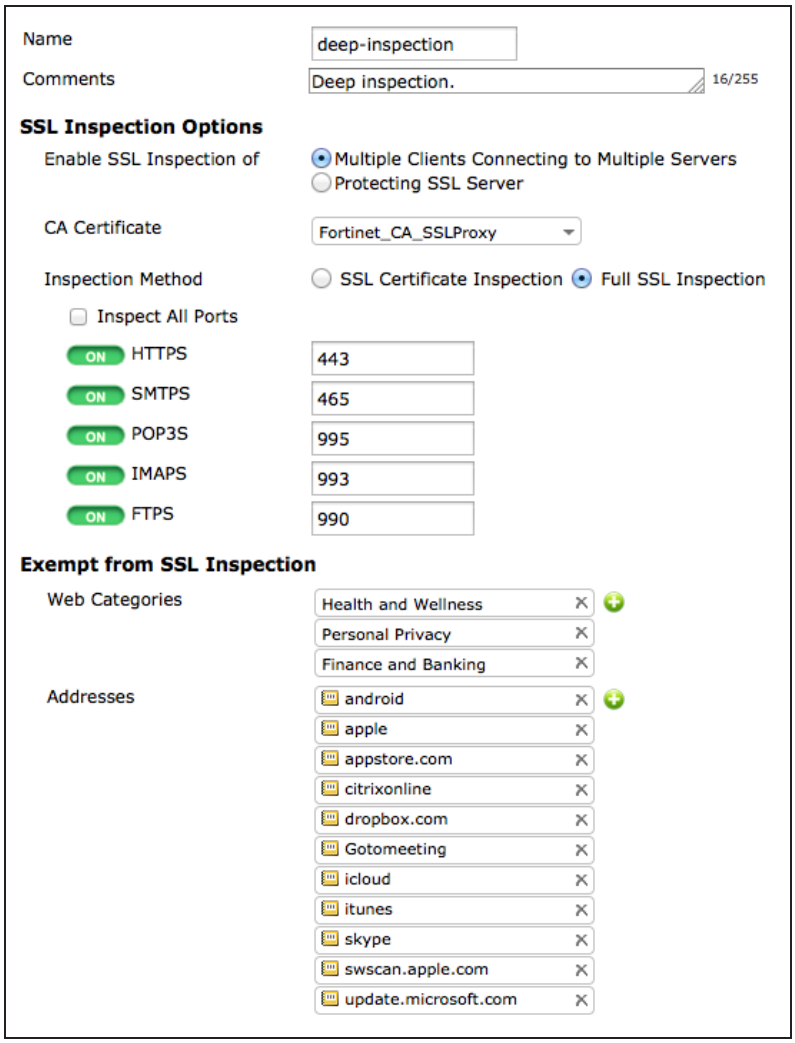
1. Viewing the deep-inspection SSL profile

Go to **Policy & Objects > SSL/SSH Inspection**. In the upper-right hand drop down menu, select **deep-inspection**.

The deep-inspection profile will apply SSL inspection to the content of all encrypted traffic.

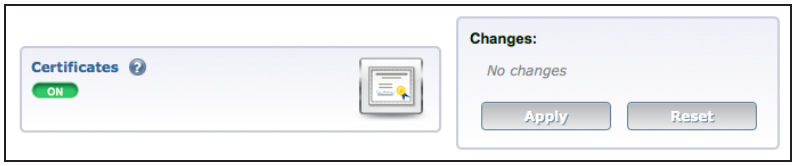


In this policy, the web categories **Health and Wellness**, **Personal Privacy**, and **Finance and Banking** are excluded from SSL inspection by default. Applications that require unique certificates, such as iTunes and Dropbox, have also been excluded.



2. Enabling certificate configuration in the web-based manager

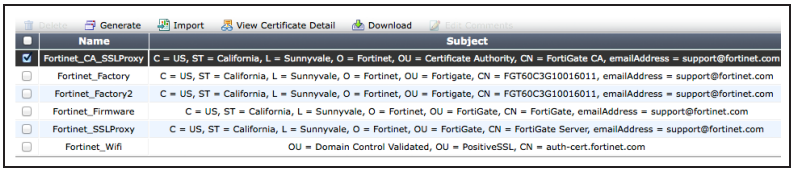
Go to **System > Config > Features**. Click **Show More**, enable **Certificates**, and **Apply** the changes.



3. Downloading the Fortinet_CA_SSLProxy certificate

Go to **System > Certificates > Local Certificates** to download the **Fortinet_CA_SSLProxy** certificate.

Make the CA certificate file available to your users by checkmarking the box next to the certificate name.



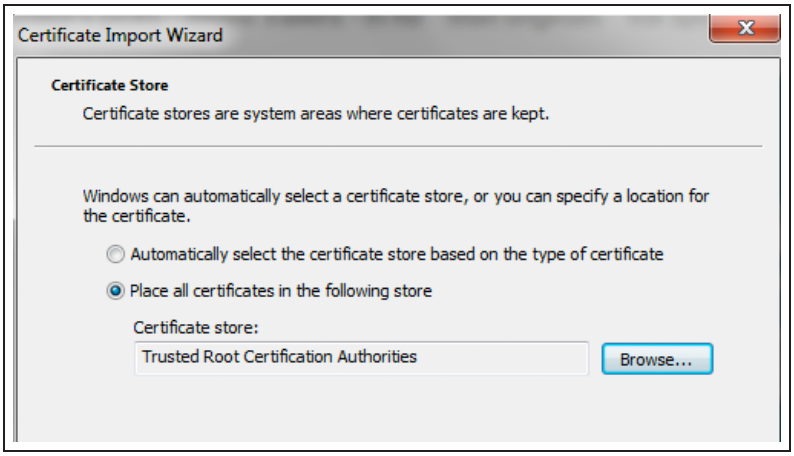
4. Importing the CA certificate into the web browser

For Internet Explorer:

Go to **Tools > Internet Options**. On the **Content** tab, select **Certificates** and find the **Trusted Root Certification Authorities**.

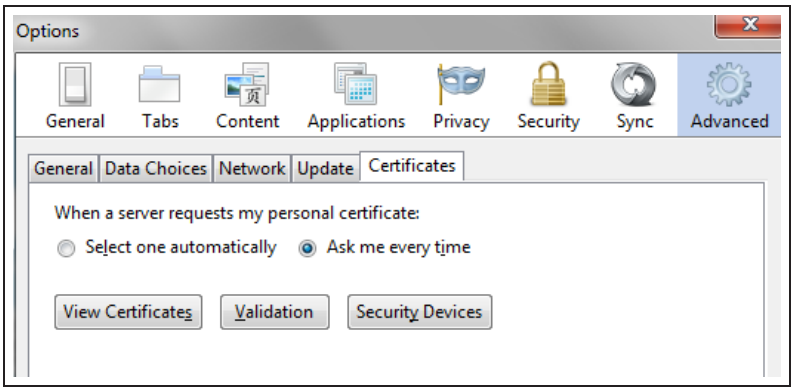
Import the certificate using the Import Wizard. Make sure that the certificate is imported into **Trusted Root Certification Authorities**.

You will see a warning because the FortiGate unit's certificate is self-signed. It is safe to select **Yes** to install the certificate.

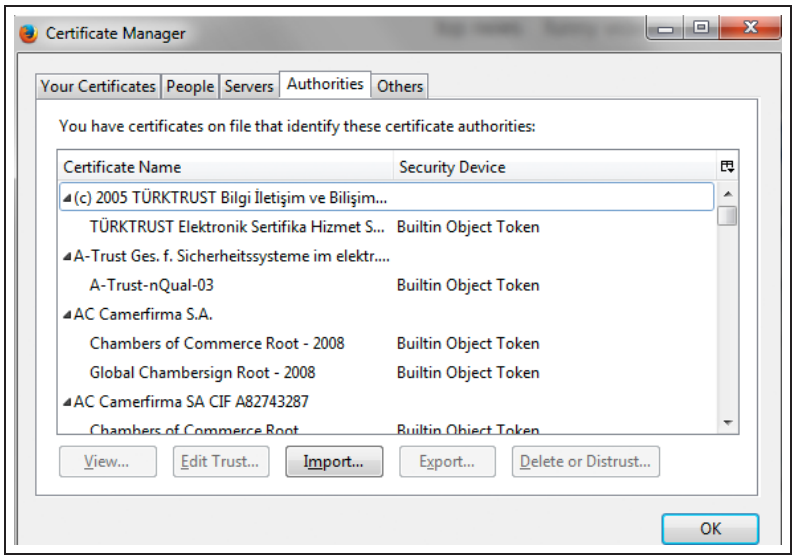


For Firefox:

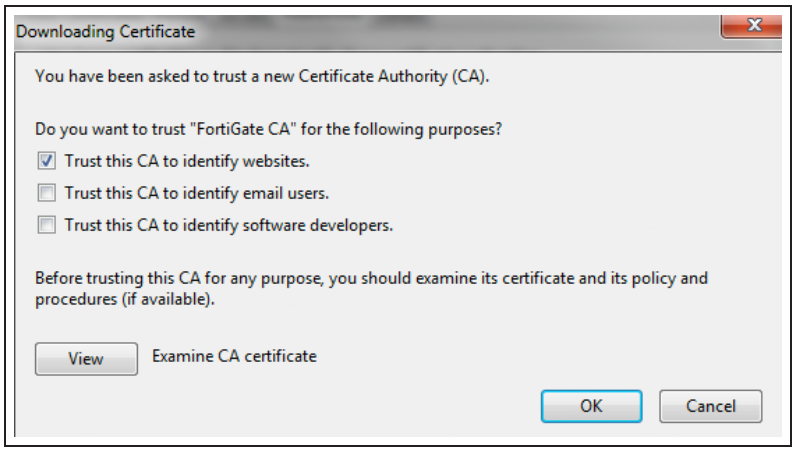
Depending on the platform, go to **Menu > Options** or **Preferences > Advanced** and find the **Certificates** tab.



Click **View Certificates**, specifically the **Authorities** certificate list.

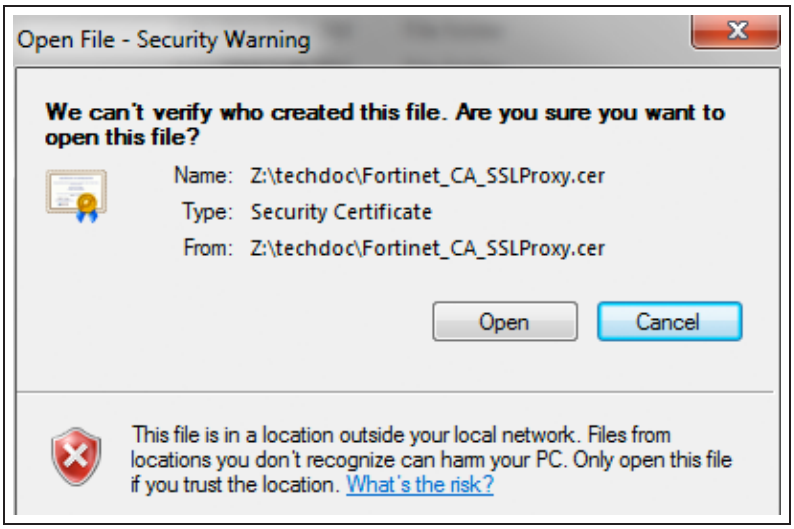


Click **Import** and select the **Fortinet_CA_SSLProxy** certificate file.



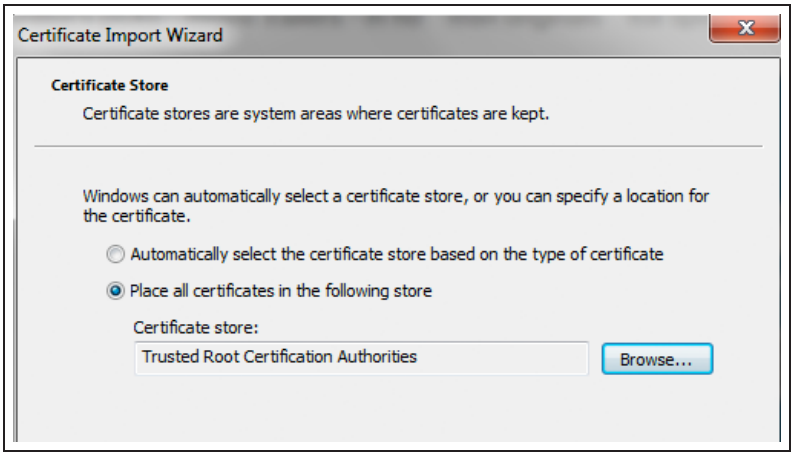
For Google Chrome and Safari:

Locate and open the downloaded **Fortinet_CA_SSLProxy** certificate file. Choose **Open** and click **Install Certificate**. The Import Wizard appears.



Import the certificate using the Import Wizard. Make sure that the certificate is imported into **Trusted Root Certification Authorities**.

You will see a warning because the FortiGate unit's certificate is self-signed. It is safe to select **Yes** to install the certificate.



5. Results

Before installing the FortiGate SSL CA certificate, even if you bypass the error message by selecting **Continue to this website**, the browser may still show an error in the toolbar.

After you install the FortiGate SSL CA certificate, you should not experience a certificate security issue when you browse to sites on which the FortiGate

unit performs SSL content inspection.

iTunes will now be able to run without a certificate error.

For further reading, check out SSL/SSH Inspection in the FortiOS 5.2 Handbook.

Using a custom certificate

In this method, a custom certificate is first signed by a recognized third-party CA and then installed on the FortiGate. This results in a chain of trust that does not exist when the FortiGate's default certificate is used. This example allows network users to trust the FortiGate as a CA in its own right. Once the FortiGate is trusted you users should no longer see certificate warnings without having to distribute certificates to your users.

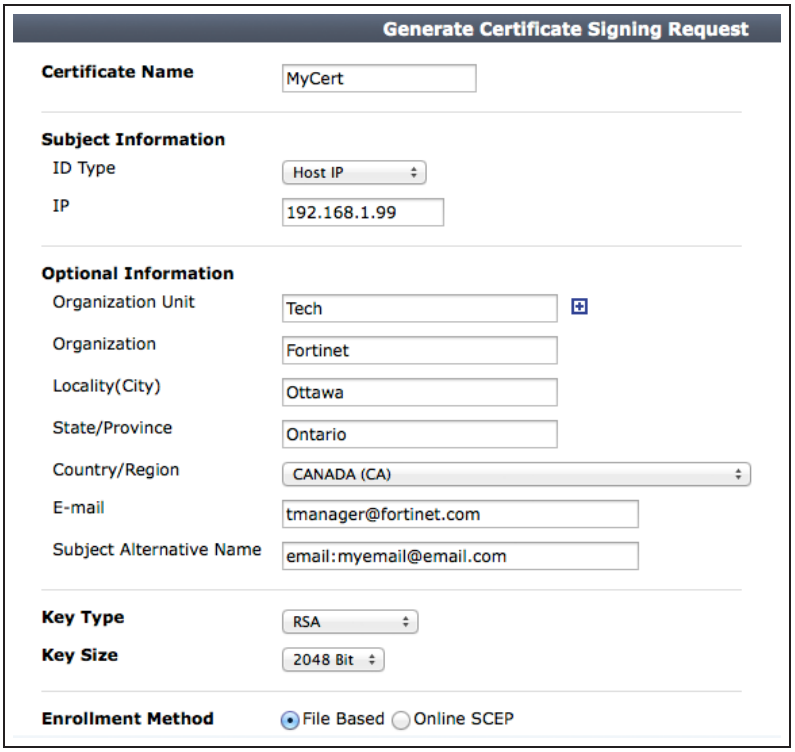
1. Generating a certificate signing request (CSR)

Go to **System > Certificates > Local Certificates** and select **Generate**.

In the **Generate Certificate Signing Request** page, fill out the required fields. You can enter a maximum of five **Organizational Units**.

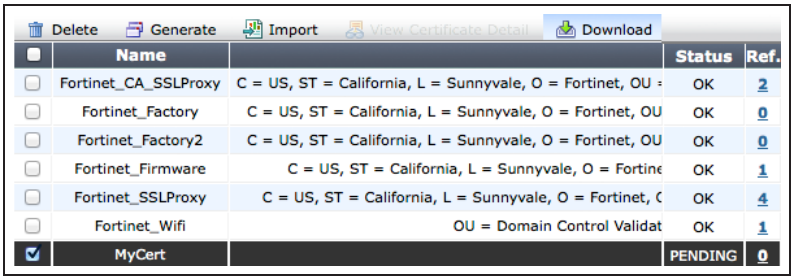
You may enter **Subject Alternative Names** for which the certificate is valid. Separate the names using commas.

To ensure PKCS12 compatibility, do not include spaces in the certificate name.



Go to **System > Certificates > Local Certificates** to view the certificate list. The status of the CSR created will be listed as **Pending**. Select the certificate and click **Download**.

This CSR will need to be submitted and signed by an enterprise root CA before it can be used. When submitting the file, ensure that the template for a



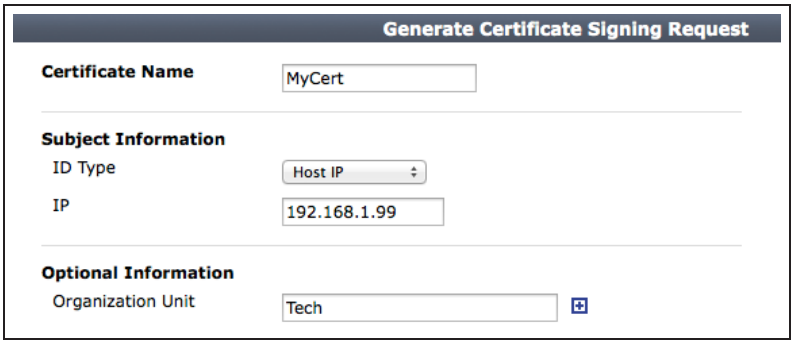
Subordinate Certificate Authority is used.

2. Importing a signed server certificate from an enterprise root CA

Once the CSR is signed by an enterprise root CA, you can import it into the FortiGate Unit.

Go to **System > Certificates > Local Certificates** and click **Import**.

From the **Type** drop down menu select **Local Certificate** and click **Choose File**.



Locate the certificate you wish to import, select it, and click **Open**.The CA signed certificate will now appear on the **Local Certificates** list.

3. Creating an SSL inspection profile

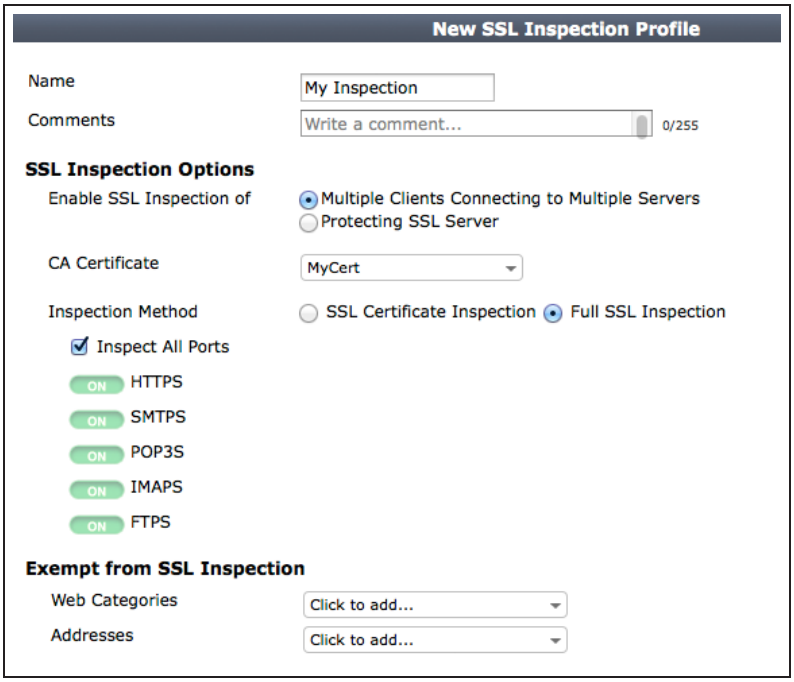
To use your certificate in an SSL inspection profile go to **Policy & Objects > Policy > SSL/SSH Inspection**.Create a new **SSL Inspection Profile**.

In the **CA Certificate** drop down menu, select the certificate you imported.

If the certificate does not appear in the list, verify that the template used to sign the certificate was for a CA and not simply for user or server identification.

Set the **Inspection Method** to **Full SSL Inspection** and **Inspect All Ports**.

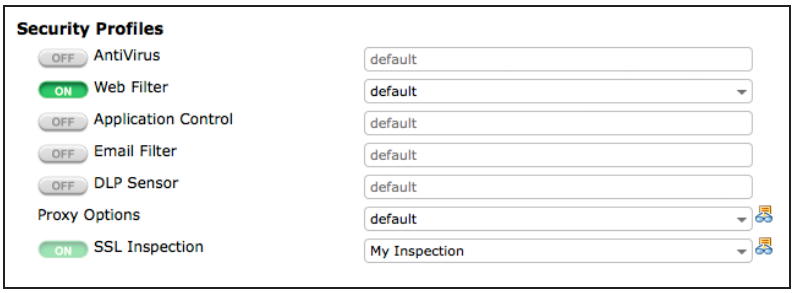
You may also need to select web categories and addresses to be exempt from SSL inspection. For more information on exemptions, seeUsing the default FortiGate certificate .



4. Editing your Internet policy to use the new SSL inspection profile

Go to **Policy & Objects > Policy > IPv4** and edit the policy controlling Internet traffic. Under **Security Profiles**, ensure that **SSL Inspection** dropdown menu, select your new profile.

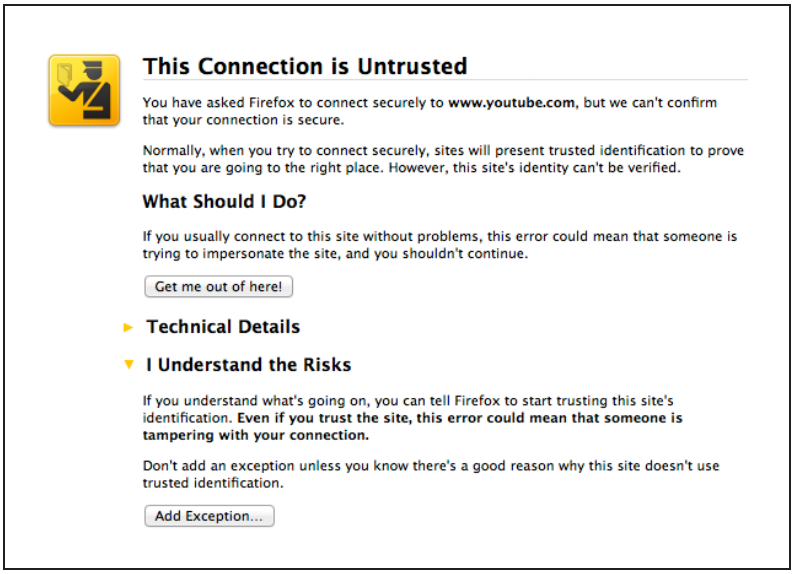
The **Web Filter** can remain as **default**.



5. Results

When visiting an HTTPS website such as https://www.youtube.com/ a warning would normally appear if you are using a self-signed certificate.

If you have the correct type of certificate, signed by a recognized CA, warnings should no longer appear.



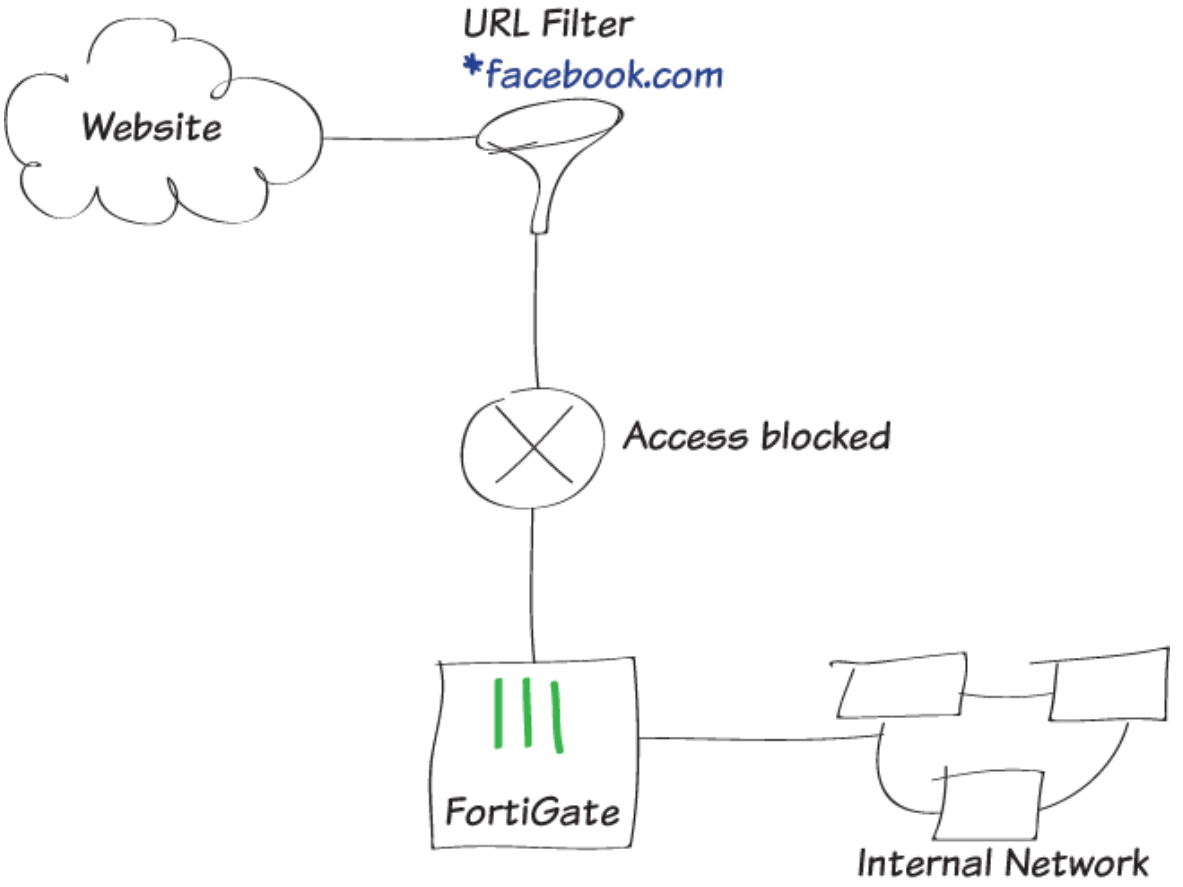
If you view the website's certificate information the **Issued By** section should contain the information of your custom certificate, indicating that the traffic is subject to deep inspection.

Network users can now manually import the certificate into their trusted root CA certificate into their trusted root CA certificate store (IE and Chrome) and/or into their browsers (Firefox).

Alternately, if the users are members of a Windows domain, the domain administrator can use a group policy to force them to trust the self-signed certificate the FortiGate is presenting.

For further reading, check out SSL/SSH Inspection in the FortiOS 5.2 Handbook.

Blocking Facebook



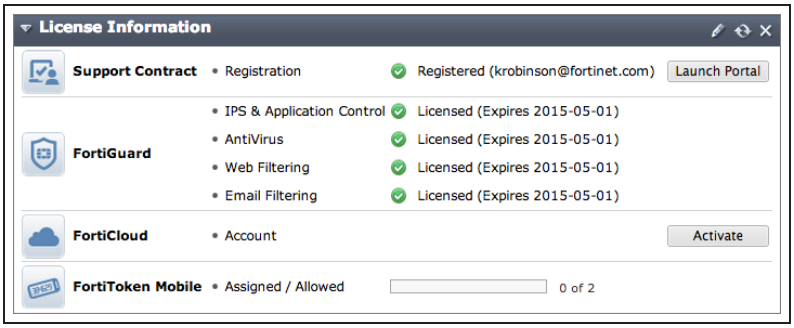
In this example, you will learn how to configure a FortiGate to prevent access to a specific social networking website, including its subdomains, by means of a static URL filter.

When you allow access to a particular type of content, such as the FortiGuard Social Networking category, there may still be certain websites in that category that you wish to prohibit. And by using SSL inspection, you ensure that this website is also blocked when accessed through HTTPS protocol.

A video of this recipe is available here.

1. Verifying FortiGuard Services subscription

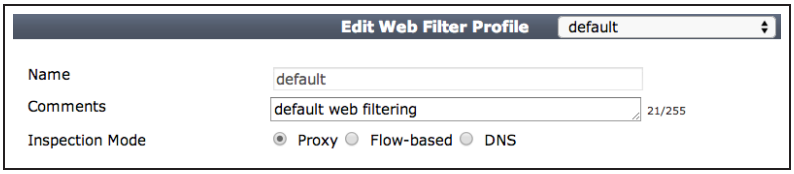
Go to **System > Dashboard > Status**. In the **License Information** widget, verify that you have an active subscription to FortiGuard Web Filtering. If you have a subscription, the service will have a green checkmark beside it.



2. Editing the Web Filter profile

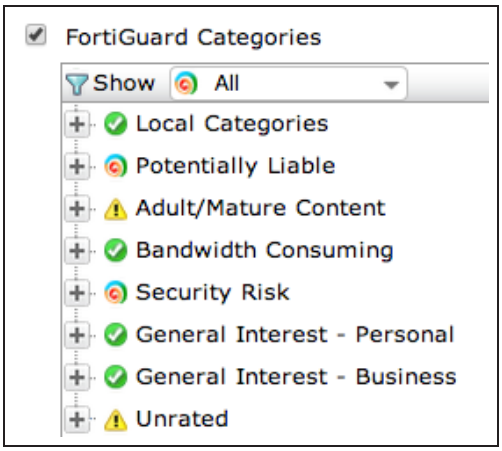
Go to **Security Profiles > Web Filter** and edit the default Web Filter profile.

Set **Inspection Mode** to **Proxy.**

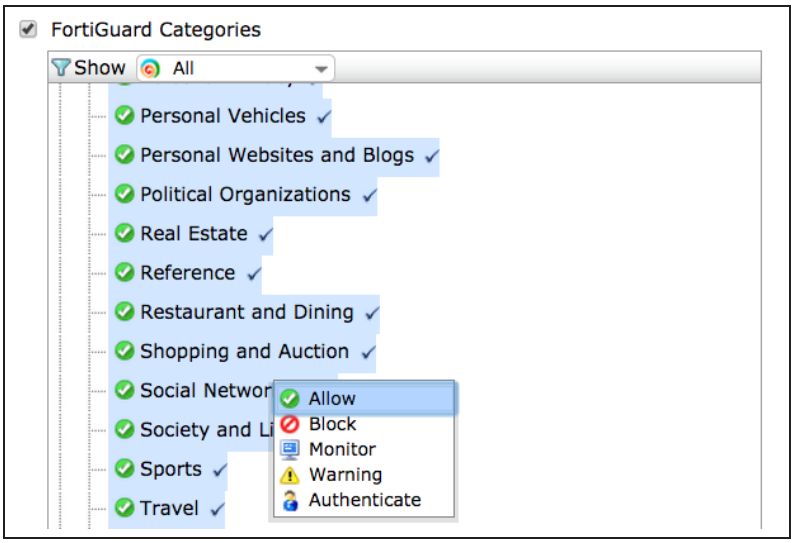


Enable the FortiGuard Categories that allow, block, monitor, warn or authenticate depending on the type of content.

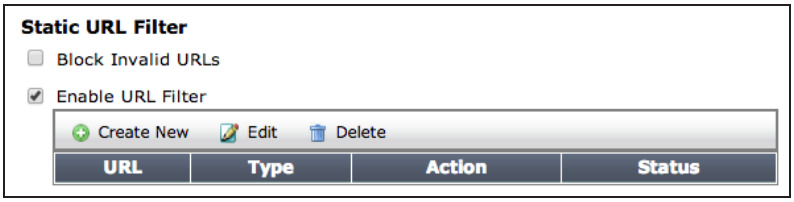
Learn more about FortiGuard Categories at the FortiGuard Center web filtering rating page:
www.fortiguard.com/static/webfiltering.html



Under FortiGuard Categories, go to **General Interest - Personal**. Right-click on the **Social Networking** subcategory and ensure it is set to **Allow**.

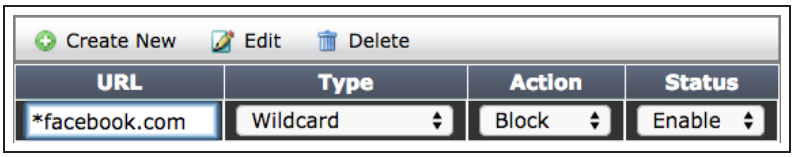


To prohibit visiting one particular social networking site in that category, go to **Static URL filter**, select **Enable URL Filter**, and then click **Create New.**



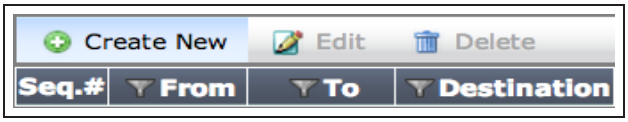
For your new web filter, enter the URL of the website you are attempting to block. If you want to block all of the subdomains for that website, omit the protocol in the URL and enter an asterisk (*). For this example, enter: **facebook.com*

Set **Type** to **Wildcard**, set **Action** to **block**, and set **Status** to **Enable**.



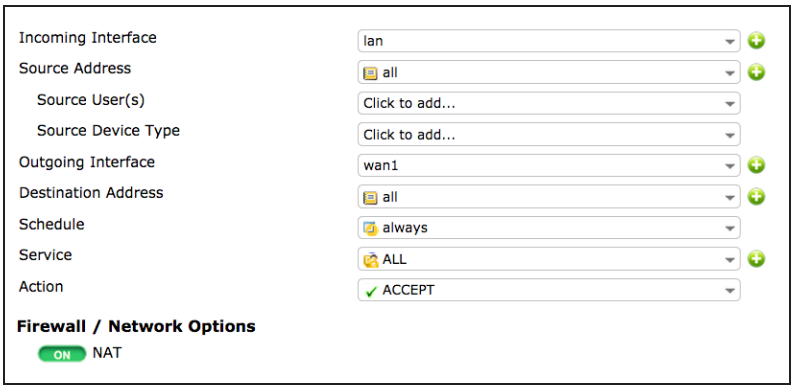
3. Creating a security policy

Go to **Policy & Objects > Policy > IPv4**, and click **Create New**.

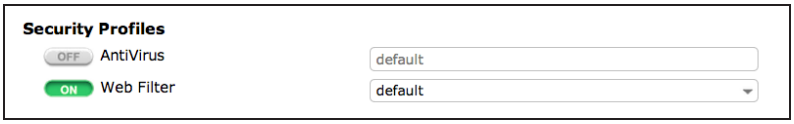


Set the **Incoming Interface** to allow packets from your internal network and set the **Outgoing Interface** to proceed to the Internet-facing interface (typically **wan1**).

Enable **NAT**.

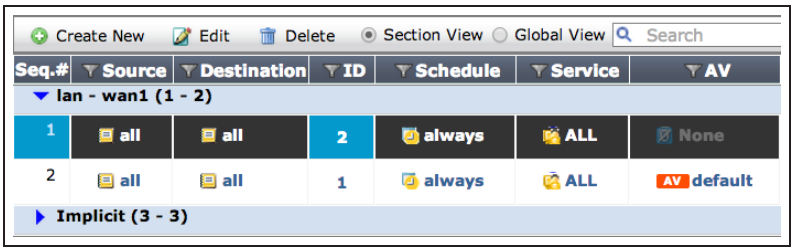


Under **Security Profiles**, enable **Web Filter** and select the **default** web filter.



This automatically enables **SSL/SSH Inspection**. Select **certificate-inspection** from the dropdown menu. This profile allows the FortiGate to inspect and apply web filtering to HTTPS traffic.

After you have created your new policy, ensure that it is at the top of the policy list. To move your policy up or down, click and drag the far left column of the policy.



4. Results

Visit the following sites to verify that your web filter is blocking websites ending in facebook.com:

- facebook.com
- attachments.facebook.com
- camdencc.facebook.com
- mariancollege.facebook.com

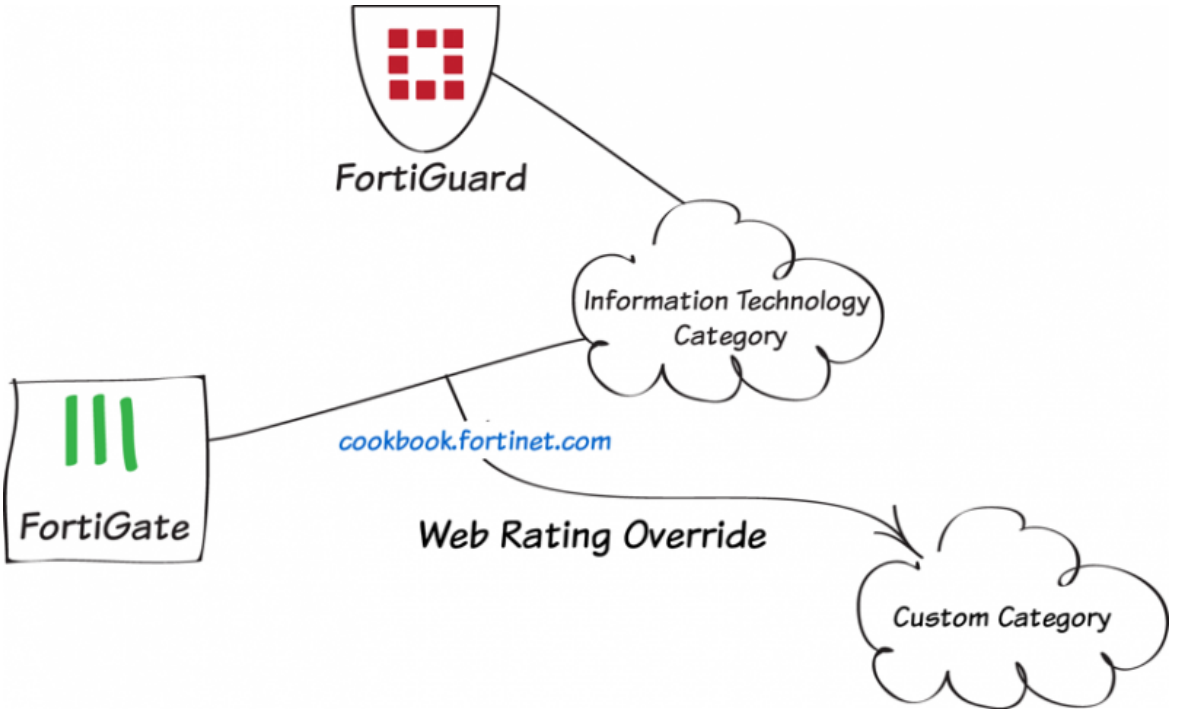
A FortiGuard **Web Page Blocked!** page should appear.

Visit https://www.facebook.com to verify that HTTPS protocol is blocked.

A **Web Page Blocked!** page should appear.

For further reading, check out Static URL Filter in the FortiOS 5.2 Handbook.

Web rating overrides



In this recipe, you will change a website's FortiGuard web rating

An active license for FortiGuard Web Filtering Services is required to use web ratings.

For testing purposes, the Cookbook website (cookbook.fortinet.com) will be changed from the category **Information Technology** to a custom category named **Allowed Sites**.

By changing the web rating for a website, you can control access to the site without affecting the rest of the sites in its original category.

This recipe only changes the website's rating on your FortiGate. To request that the rating is changed for all of FortiGuard, go here.

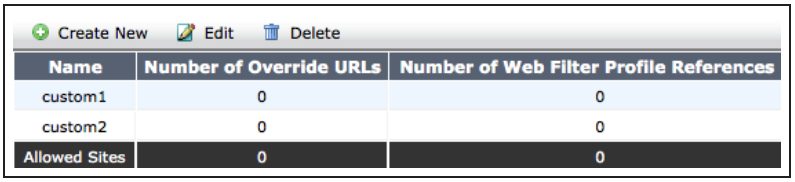
1. Enabling web filtering

Go to **System > Config > Features** and make sure that **Web Filter** is **ON.** If necessary, **Apply** your changes.

2. Creating a custom category and web rating override

Go to **Security Profiles > Advanced > Web Rating Overrides** and select **Custom Categories**.

Create a new category named *Allowed Sites.*



Name	Number of Override URLs	Number of Web Filter Profile References
custom1	0	0
custom2	0	0
Allowed Sites	0	0

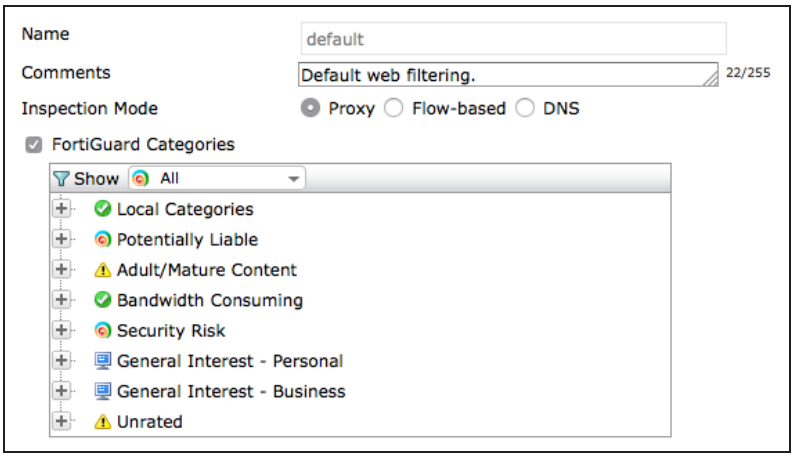
Go to **Security Profiles > Advanced > Web Rating Overrides** and create a new override.

Enter the website's **URL** and select **Lookup Rating** to see the current rating.

In the **Override to** section, set **Category** to **Custom Categories** and **Sub-category** to **Allowed Sites**.

3. Adding FortiGuard blocking to the default web filter profile

Go to **Security Profiles > Web Filter** and edit the default profile. Enable **FortiGuard Categories**.



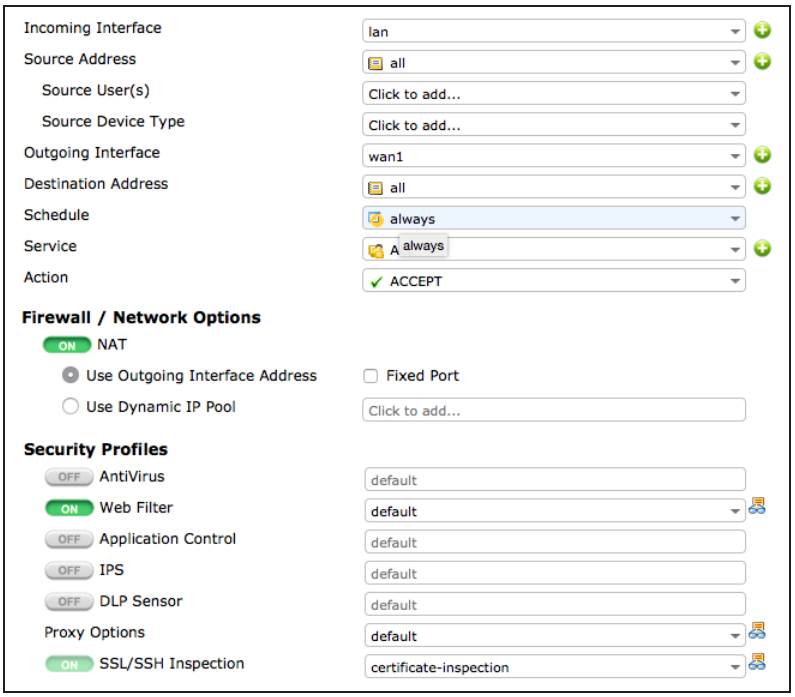
Expand **Local Categories** to make sure that the **Allowed Sites** category is set to **Allow**.

Expand **General Interest - Business.** Right-click on **Information Technology** to set it to **Block**.

4. Adding the default web filter profile to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Under **Security Profiles**, turn on **Web Filter** and use the **default** profile.



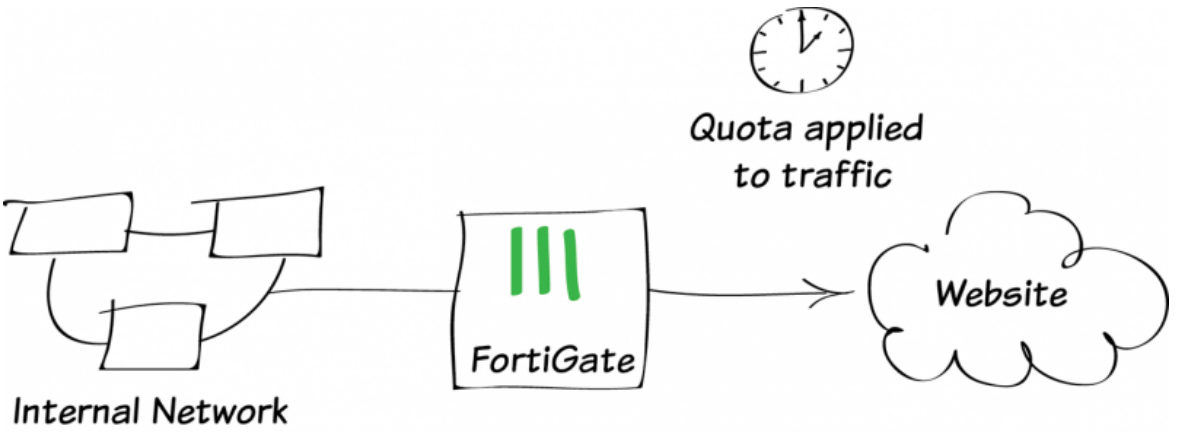
5. Results

Browse to www.fortinet.com, which is part of the **Information Technology** category. A message will appear from FortiGuard, stating that access to this website is blocked.

If you browse to cookbook.fortinet.com, you will still be able to access the site.

For further reading, check out FortiGuard Web Filtering Service in the FortiOS 5.2 Handbook.

Web filtering using quotas



In this example, you will create a web filter profile that allows access to websites that are categorized as "Personal Interest" at any point during the day, but limits access for a total of 5 minutes for each user.

An active license for FortiGuard Web Filtering Services is required to use web filtering with quotas.

Quotas are the most efficient way of allowing limited access to websites, as they do not require set schedules. To apply web filtering using quotas, you must use a security policy with either user or device authentication. In this recipe, a user account, *alistair*, has already been configured. For more information about creating user accounts, see User and device authentication.

1. Enabling web filtering

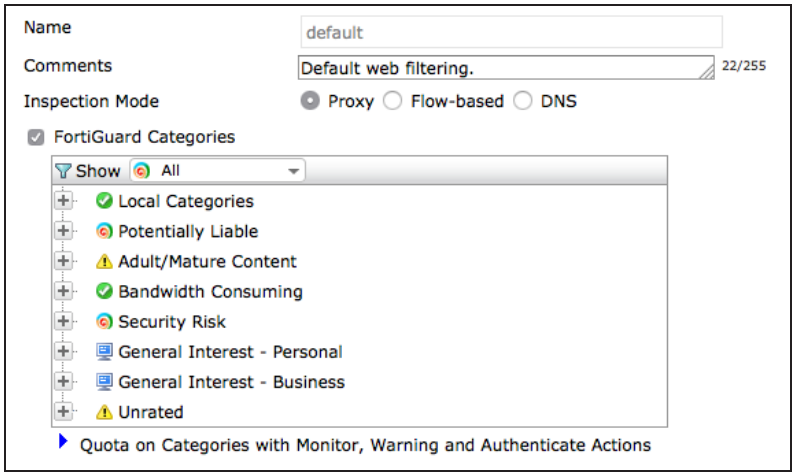
Go to **System > Config > Features** and make sure that **Web Filter** is **ON**. If necessary, **Apply** your changes.

2. Creating a web filter profile that uses quotas

Go to **Security Profiles > Web Filter > Profiles**. Edit the **default** profile and enable **FortiGuard Categories**.

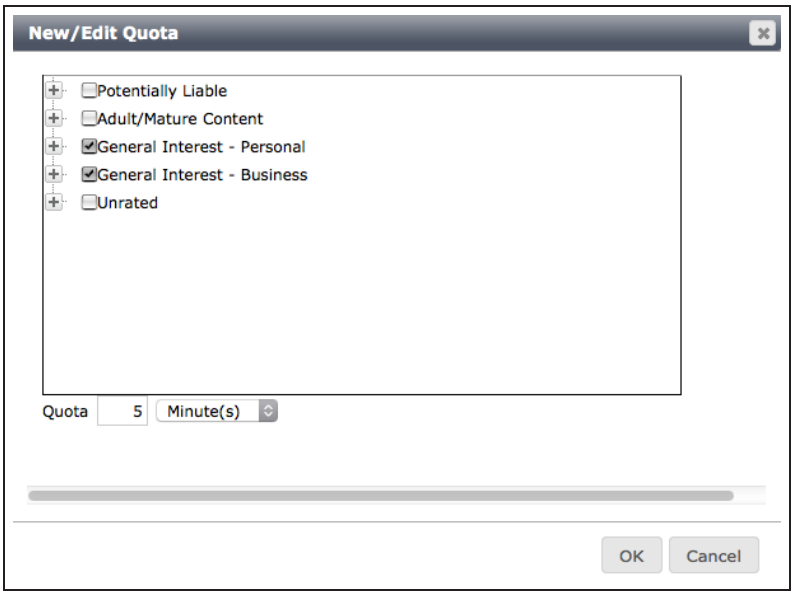
Right-click on the category **General Interest - Personal** and select **Monitor**. Do the same for the category **General Interest - Business**.

These categories include a variety of sites that are commonly blocked in the workplace, such as games, instant messaging, and social media.



Expand **Quota on Categories with Monitor, Warning and Authenticate Actions** and select **Create New**.

Select both **General Interest - Personal** and **General Interest - Business**. For testing purposes, set the **Quota** amount to **5 Minutes**.

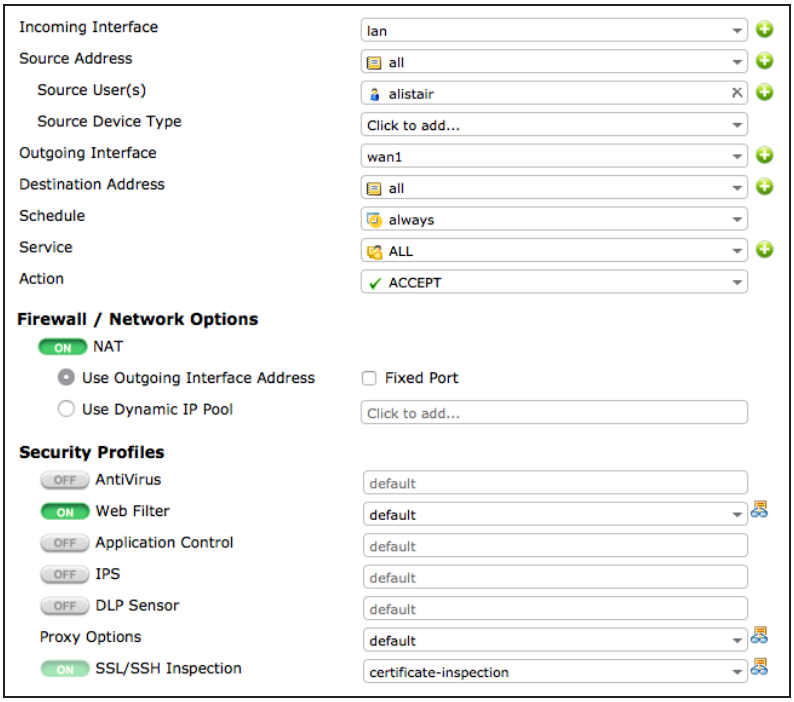


The web filter will now list all the sub-categories listed in the two categories and the applied quota.

3. Adding web filtering to a security policy with user authentication

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Under **Security Profiles**, turn on **Web Filter** and use the **default** profile.

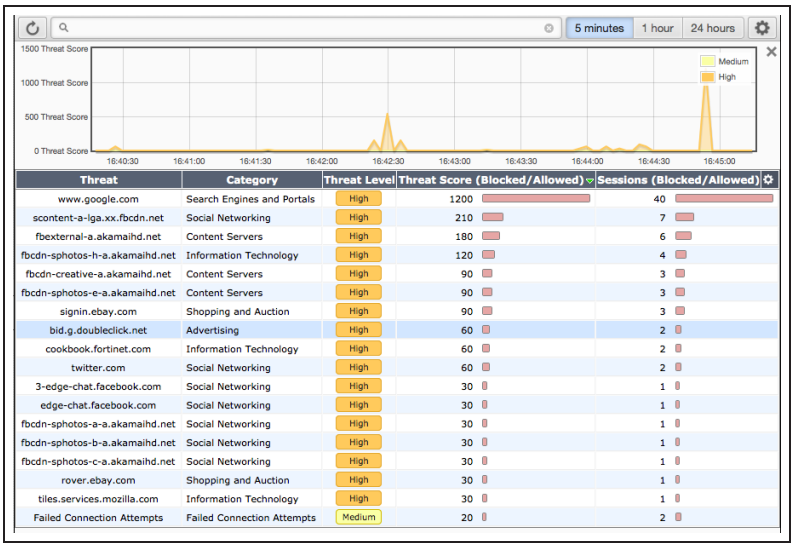


4. Results

Browse to www.ebay.com, a website that is found within the General Interest - Personal category.

Access to the website is allowed for 5 minutes, after which a block message appears. The message will persist for all General Interest - Personal sites until the quota is reset, which occurs every 24 hours at midnight.

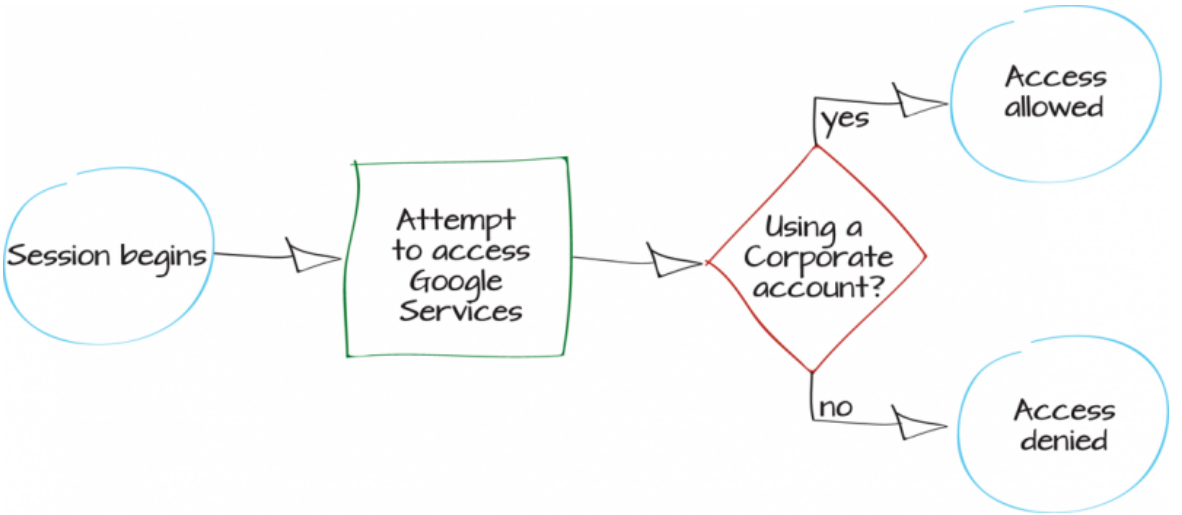
Go to **System > FortiView > Threats** and select the **5 minutes** view. You will be able to see the blocked traffic.



Threat	Category	Threat Level	Threat Score (Blocked/Allowed)	Sessions (Blocked/Allowed)
www.google.com	Search Engines and Portals	High	1200	40
scontent-a-lga.xx.fbcdn.net	Social Networking	High	210	7
fbexternal-a.akamaihd.net	Content Servers	High	180	6
fbcdn-sphotos-h-a.akamaihd.net	Information Technology	High	120	4
fbcdn-creative-a.akamaihd.net	Content Servers	High	90	3
fbcdn-sphotos-e-a.akamaihd.net	Content Servers	High	90	3
signin.ebay.com	Shopping and Auction	High	90	3
bid.g.doubleclick.net	Advertising	High	60	2
cookbook.fortinet.com	Information Technology	High	60	2
twitter.com	Social Networking	High	60	2
3-edge-chat.facebook.com	Social Networking	High	30	1
edge-chat.facebook.com	Social Networking	High	30	1
fbcdn-sphotos-a-a.akamaihd.net	Social Networking	High	30	1
fbcdn-sphotos-b-a.akamaihd.net	Social Networking	High	30	1
fbcdn-sphotos-c-a.akamaihd.net	Social Networking	High	30	1
rover.ebay.com	Shopping and Auction	High	30	1
tiles.services.mozilla.com	Information Technology	High	30	1
Failed Connection Attempts	Failed Connection Attempts	Medium	20	2

For further reading, check out FortiGuard Web Filtering Service in the FortiOS 5.2 Handbook.

Blocking Google access for consumer accounts



In this recipe, you will block access to Google services for consumer accounts, while allowing access for corporate accounts.

If your organization has set up a Google corporate account to be able to use Google services, such as Gmail and Google Docs, this recipe can be used to block users from accessing those services with their own personal accounts. In this example, a corporate account has been created that uses the domain *fortidocs.com*.

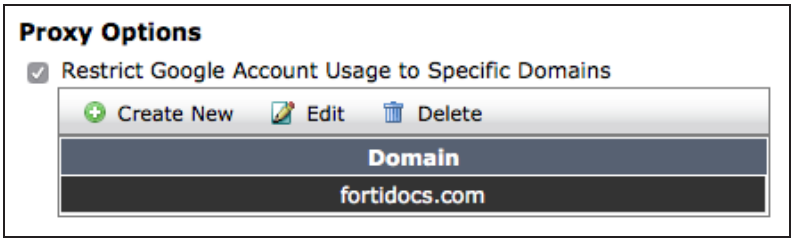
A video of this recipe is available here.

1. Editing the default web filter profile to restrict Google access

Go to **Security Profiles > Web Filter** and edit the default profile.

Make sure that **Inspection Mode** is set to **Proxy**. Under **Proxy Options**, select **Restrict Google Account Usage to Specific Domains**.

Select **Create New** in the list that appears and add an entry for the domains for your Corporate Google accounts (in the example, *fortidocs.com*).

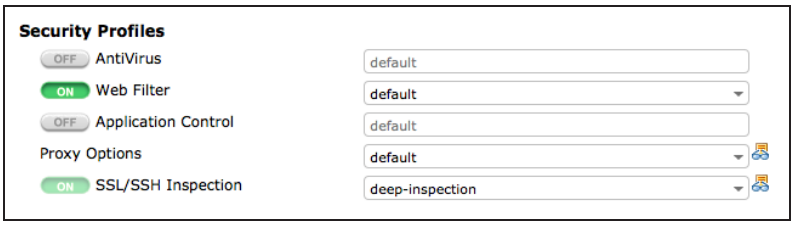


2. Adding the profile to your Internet-access policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Enable **Web Filter** and set it to use the **default** profile. Doing this will automatically enable **SSL/SSH Inspection**. Set this to use the **deep-inspection** profile.

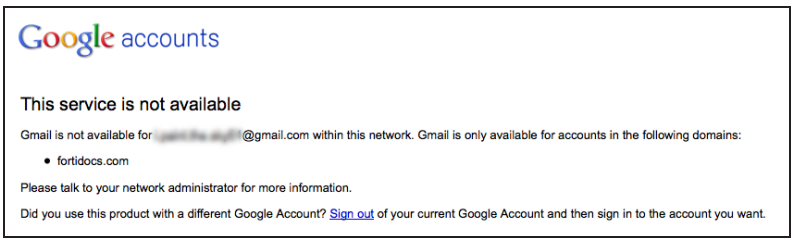
Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see Preventing certificate warnings.



3. Results

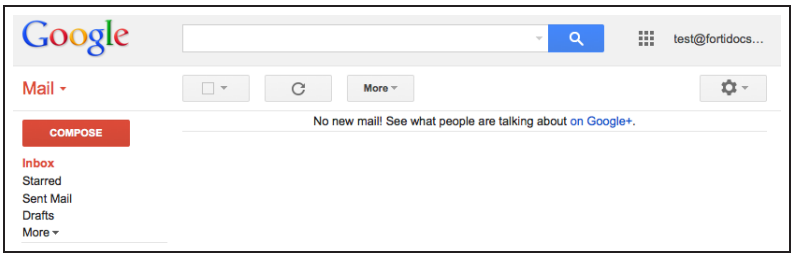
Log in to Google using a personal account. After you are authenticated, attempt to access a Google service, such as Gmail or Google Drive.

A message appears from Google stating that the service is not available.



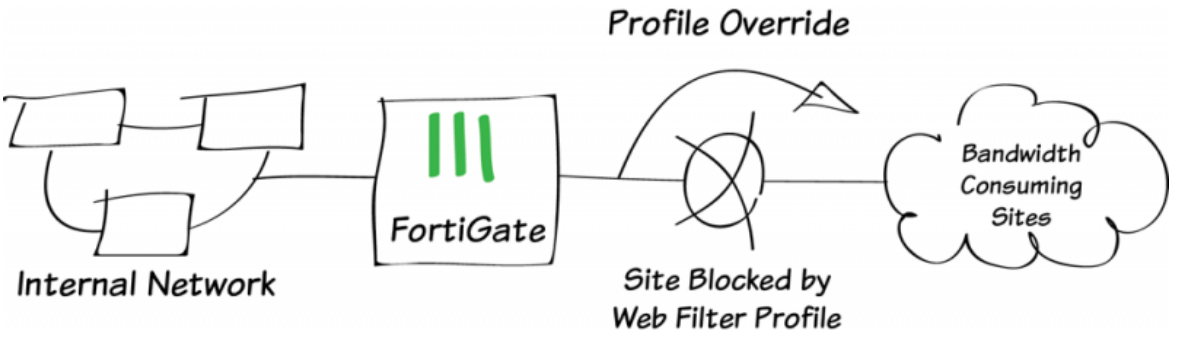
Sign out of the personal account and instead use your corporate account (in the example, *test@fortidocs.com*).

You can now access the Google service.



For further reading, check out Web filter in the FortiOS 5.2 Handbook.

Overriding a web filter profile



In this example, one user is temporarily allowed to override a web filter profile to be able to access sites that would otherwise be blocked.

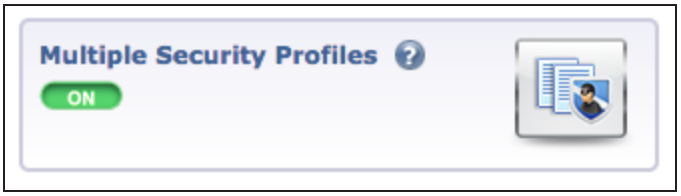
In this example, web filtering blocks the **Bandwidth Consuming** category for all users, except those who can override the filter.

1. Enabling web filtering and multiple profiles

Go to **System > Config > Features** and make sure that **Web Filter** is turned **ON**.

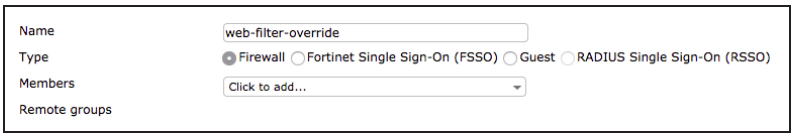
Select **Show More** and enable **Multiple Security Profiles**.

Apply the changes.

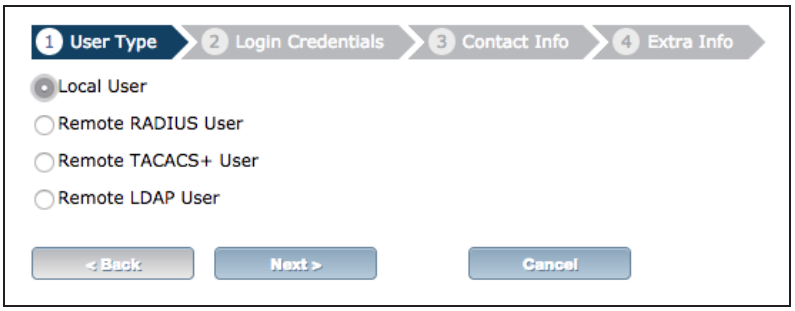


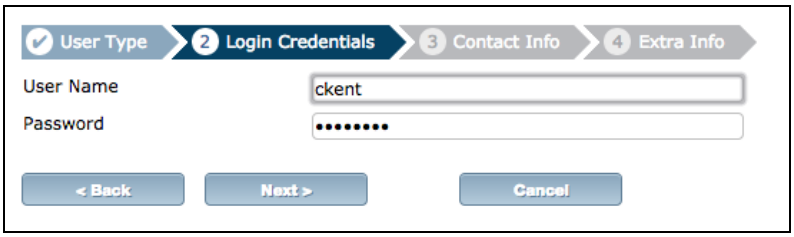
2. Creating a user group and two users

Go to **User & Device > User > User Groups**. Create a new group for users who can override web filtering (in the example, *web-filter-override)*.

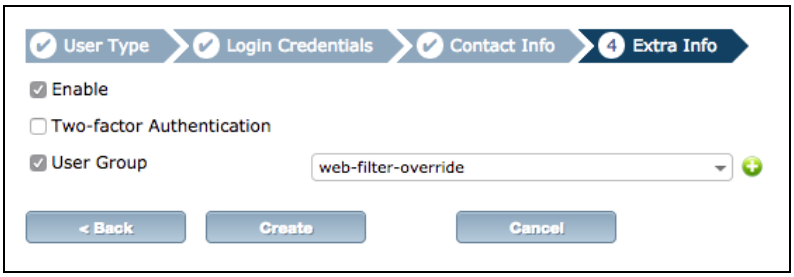


Go to **User & Device > User > User Definition** and create two users (in the example, *ckent* and *bwayne*).





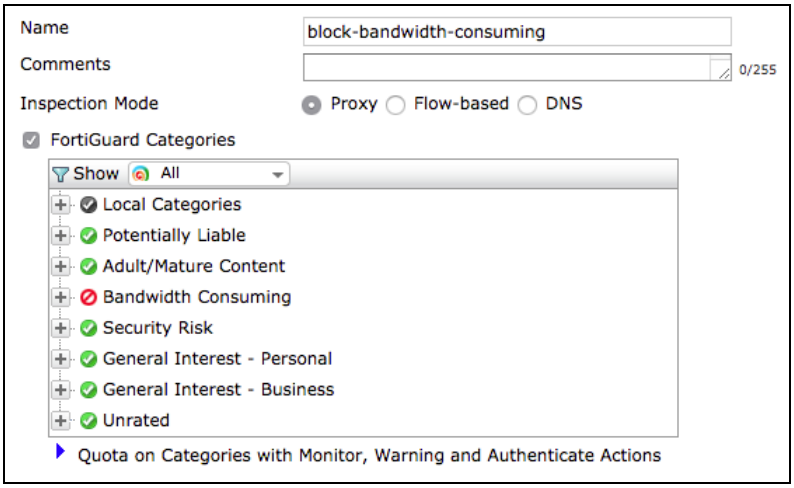
Assign *ckent* to the *web-filter-override* group, but not *bwayne*.



3. Creating a web filter profile and override

Go to **Security Profiles > Web Filter** and create a new profile (in the example, *block-bandwidth-consuming*).

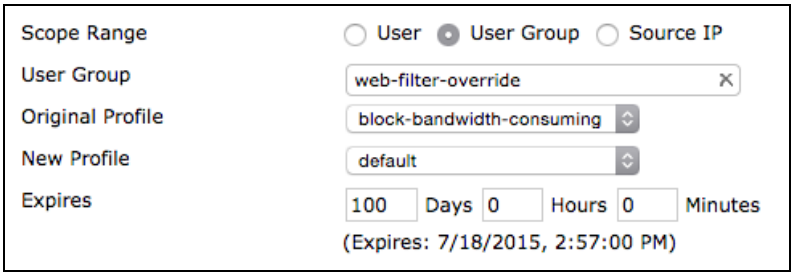
Enable FortiGuard Categories, then right-click **Bandwidth Consuming** and select **Block**.



Go to **Security Profiles > Advanced > Web Profile Overrides** and create a new override.

Set **Scope Range** to **User Group**, **User Group** to the *web-filter-override* group, **Original Profile** to the *block-bandwidth-consuming* profile, and **New Profile** to the **default** profile.

Set an appropriate **Expires** time to control how long the override can be used (in the example, *100 hours* after the override is created).

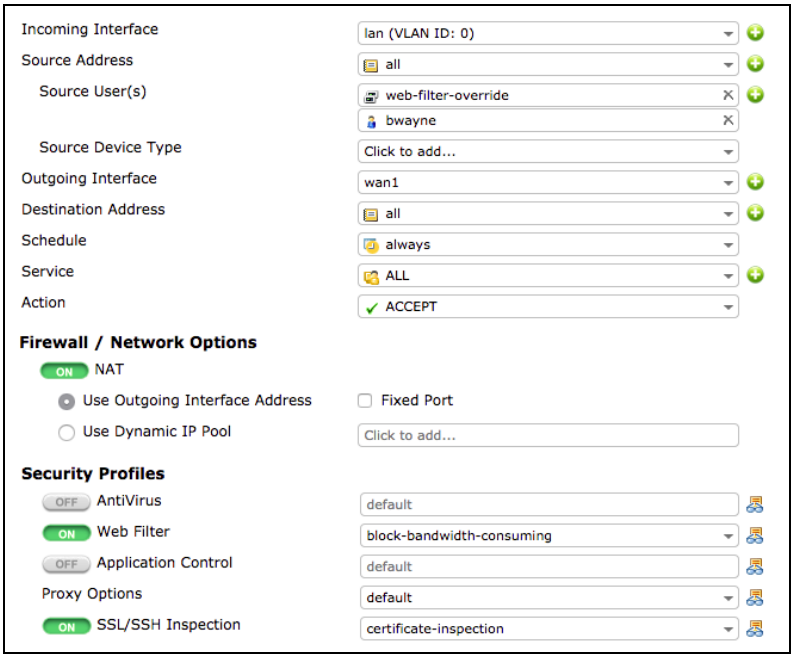


4. Adding the new web filter profile to a security policy

Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

Set **Source User(s)** to allow both the *web-filter-override* group and user *bwayne.*

Under **Security Profiles**, turn on **Web Filter** and use the new profile.



5. Results

Browse to blip.tv, a website that is part of the **Bandwidth Consuming** category.

Authenticate using the *bwayne* account. The website is blocked.

Go to **User & Device > Monitor > Firewall** and **De-authenticate** *bwayne*.

Browse to blip.tv again, this time authenticating using the *ckent* account. You can access the website until the override expires.

For further reading, check out Web Filter in the FortiOS 5.2 Handbook.

Troubleshooting web filtering

This section contains tips to help you with some common challenges of FortiGate web filtering.

The Web Filter option does not appear in the GUI.

Go to **Config > System > Features** and enable **Web Filter**.

New Web Filter profiles cannot be created.

Go to **Config > System > Features** and select **Show More**. Enable **Multiple Security Profiles**.

Web Filtering has been configured but is not working.

Make sure that web filtering is enabled in a policy. If it is enabled, check that the policy is the policy being used for the correct traffic. Also check that the policy is getting traffic by going to the policy list and adding the Sessions column to the list.

An active FortiGuard Web Filtering license displays as expired/unreachable.

First, ensure that web filtering is enabled in one of your security policies. The FortiGuard service will sometimes show as expired when it is not being used, to save CPU cycles.

If web filtering is enabled in a policy, go to **System > Config > FortiGuard** and expand **Web Filtering**. Under **Port Selection**, select **Use Alternate Port (8888)**. Select **Apply** to save the changes. Check whether the license is shown as active. If it is still inactive/expired, switch back to the default port and check again.

WiFi

These recipes describe how to use FortiAPs to add WiFi (or Wi-Fi) services to your network.

FortiAPs, managed by FortiGates, provide a full suite of WiFi features. Small offices can use FortiAPs to quickly add WiFi. Enterprises and educational institutions can take advantage of FortiAP access control features. Each WiFi network, or SSID, is represented by a WiFi network interface to which you can apply firewall policies, security profiles, and other features in the same way you would for wired networks.

Getting started with WiFi

- Setting up WiFi with FortiAP
- Setting up a WiFi bridge with a FortiAP
- Combining WiFi and wired networks with a software switch
- WiFi network with external DHCP service
- Providing remote access to the office and Internet
- Extending WiFi range with mesh topology

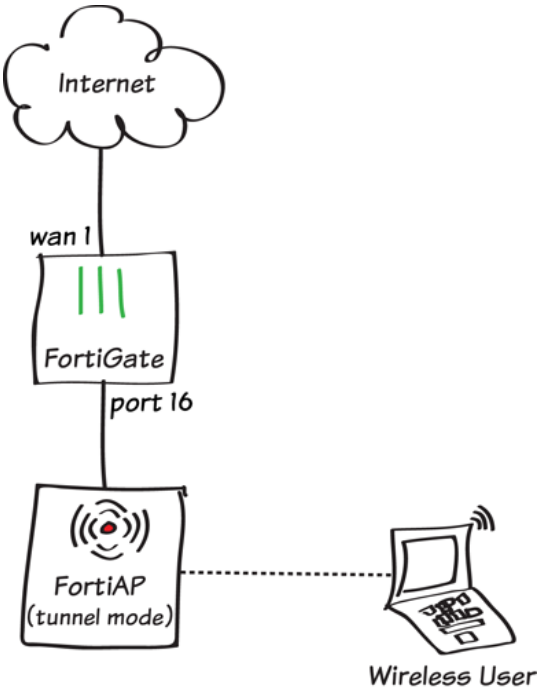
WiFi access control

- Guest WiFi accounts
- Captive portal WiFi access control
- WP2A WiFi access control
- WiFi with external RADIUS authentication
- MAC access control
- BYOD scheduling
- BYOD for a user with multiple wireless devices

WiFi with other technologies

- Explicit proxy with web caching
- AirPlay for Apple TV

Setting up WiFi with FortiAP



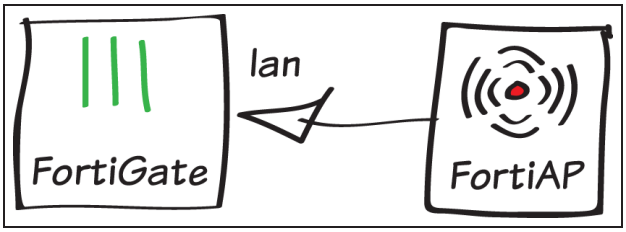
In this example, a FortiAP unit is connected to and managed by a FortiGate unit in Tunnel mode, allowing wireless access to the network.

You can configure a FortiAP unit in either Tunnel mode or Bridge mode. When a FortiAP is in Tunnel mode, a wireless-only subnet is used for wireless traffic. When a FortiAP is in Bridge mode, the Ethernet and WiFi interfaces are connected (or bridged), allowing wired and wireless networks to be on the same subnet. Tunnel mode is the default mode for a FortiAP.

For information about using a FortiAP in Bridge mode, seeSetting up a WiFi bridge with a FortiAP.

1. Connecting and authorizing the FortiAP unit

Connect the FortiAP unit to the the **lan** interface.



Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. The FortiAP is listed, with a yellow question mark beside it because the device is not authorized.

The FortiAP may not appear until a few minutes have passed.

Highlight the FortiAP unit on the list and select **Authorize**. A grey checkmark is now shown beside the FortiAP, showing that it is authorized but not yet online.

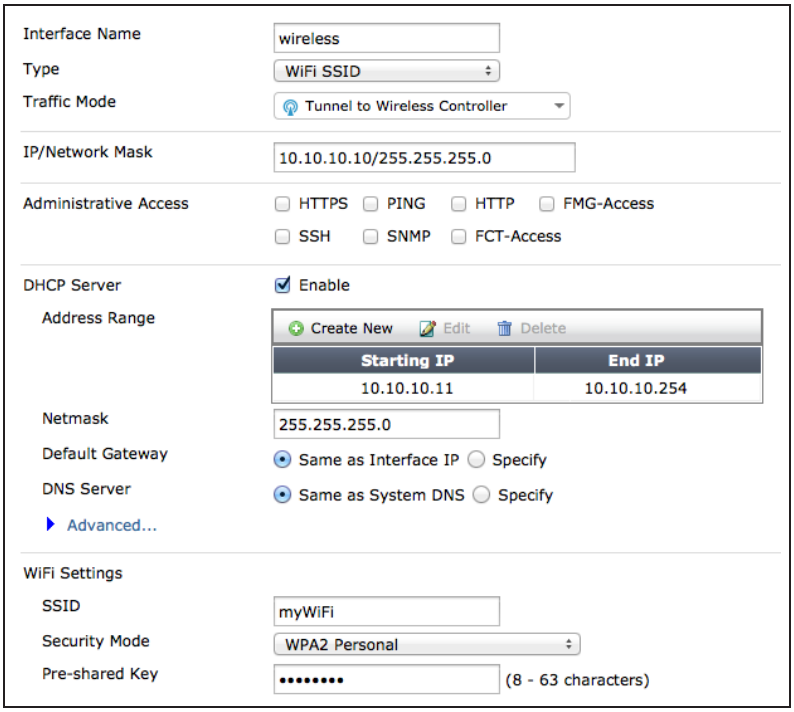
2. Creating an SSID

Go to **WiFi Controller > WiFi Network > SSID** and create a new SSID.

Set **Traffic Mode** to **Tunnel to Wireless Controller**.

Select an **IP/Network Mask** for the wireless interface and enable **DHCP Server**.

Set the **WiFi Settings** as required, including a secure **Pre-shared Key**.

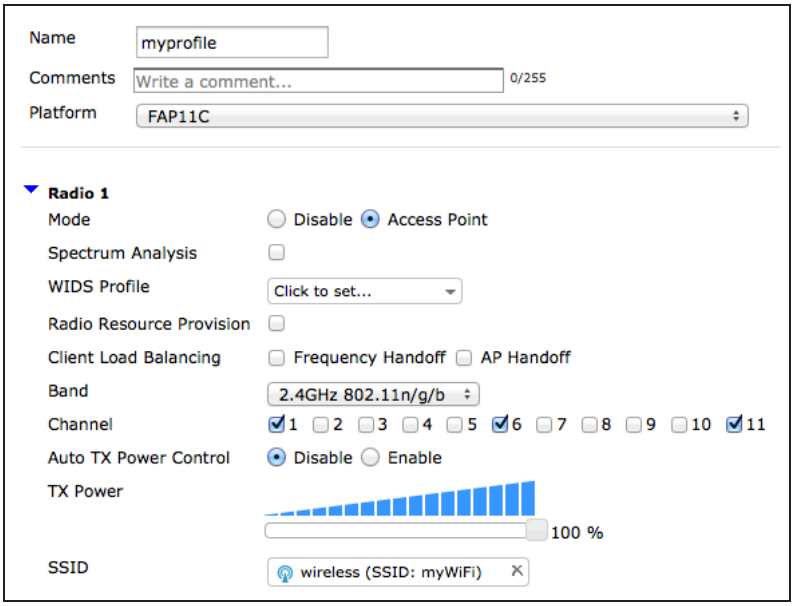


3. Creating a custom FortiAP profile

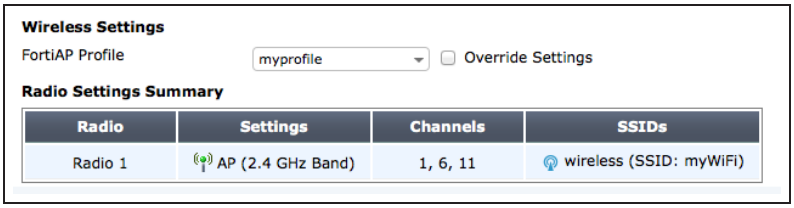
Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and create a new profile.

Set **Platform** to the correct FortiAP model you are using (FAP11C in the example).

Set **SSID** to use the new SSID.



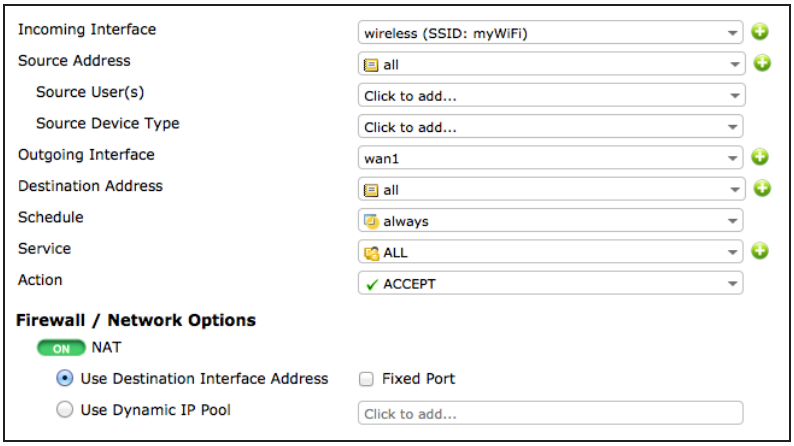
Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and edit the FortiAP. Set **FortiAP Profile** to use the new profile.



4. Allowing wireless access to the Internet

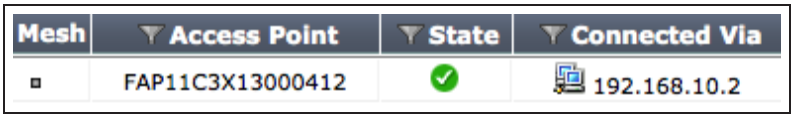
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the SSID and **Outgoing Interface** to your Internet-facing interface. Ensure that **NAT** is turned **ON**.



5. Results

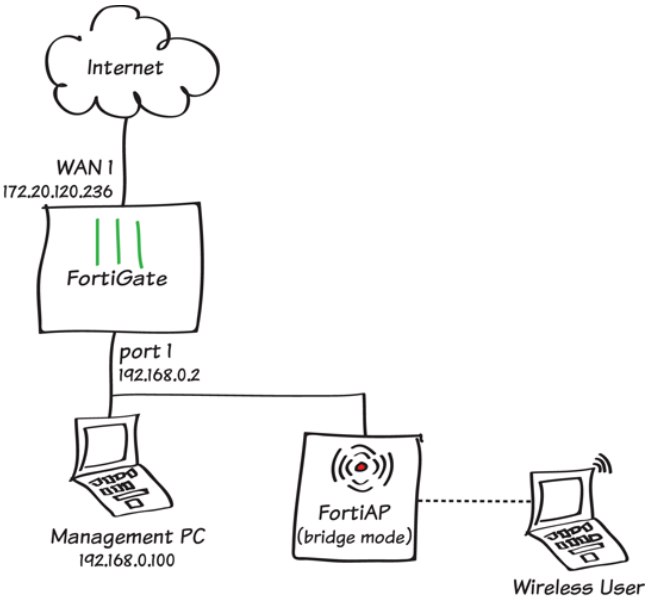
Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. A green checkmark now appears beside the FortiAP, showing that the unit is authorized and online.



Connect to the SSID with a wireless device. After a connection is established, you are able to browse the Internet.

For further reading, check out Configuring a WiFi LAN in the FortiOS 5.2 Handbook.

Setting up a WiFi bridge with a FortiAP



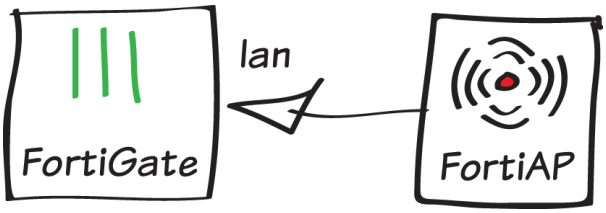
In this example, a FortiAP unit is connected to and managed by a FortiGate unit in Bridge mode.

You can configure a FortiAP unit in either Tunnel mode or Bridge mode. When a FortiAP is in Tunnel mode, a wireless-only subnet is used for wireless traffic. When a FortiAP is in Bridge mode, the Ethernet and WiFi interfaces are connected (or bridged), allowing wired and wireless networks to be on the same subnet. Tunnel mode is the default mode for a FortiAP.

For information about using a FortiAP in Tunnel mode, see Setting up WiFi with FortiAP.

1. Connecting and authorizing the FortiAP unit

Connect the FortiAP unit to the the **lan** interface.



Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. The FortiAP is listed, with a yellow question mark beside it because the device is not authorized.

The FortiAP may not appear until a few minutes have passed.

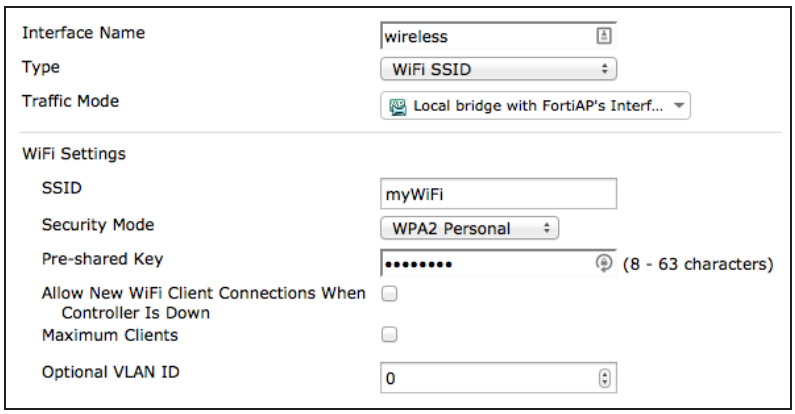
Highlight the FortiAP unit on the list and select **Authorize**. A grey checkmark is now shown beside the FortiAP, showing that it is authorized but not yet online.

2. Creating an SSID

Go to **WiFi Controller > WiFi Network > SSID** and create a new SSID.

Set **Traffic Mode** to **Local bridge with FortiAP's Interface**.

Set the **WiFi Settings** as required, including a secure **Pre-shared Key**.

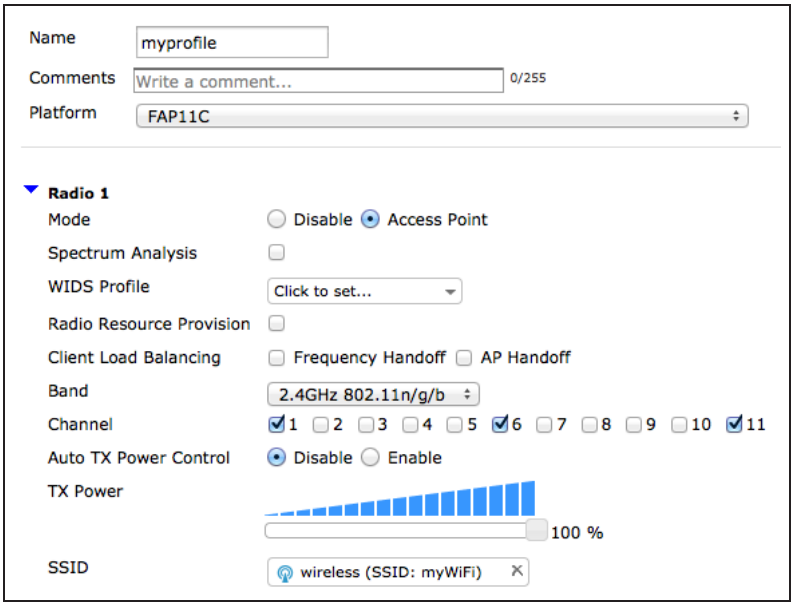


3. Creating a custom FortiAP profile

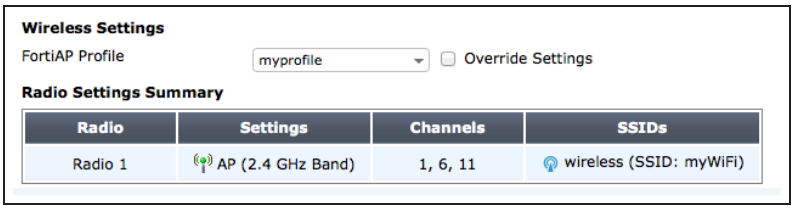
Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and create a new profile.

Set **Platform** to the correct FortiAP model you are using (FAP11C in the example).

Set **SSID** to use the new SSID.

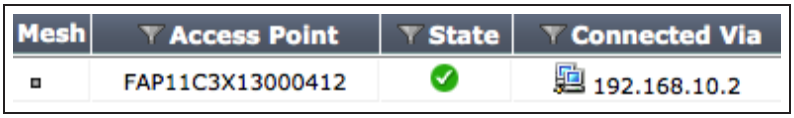


Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and edit the FortiAP. Set **FortiAP Profile** to use the new profile.



4. Results

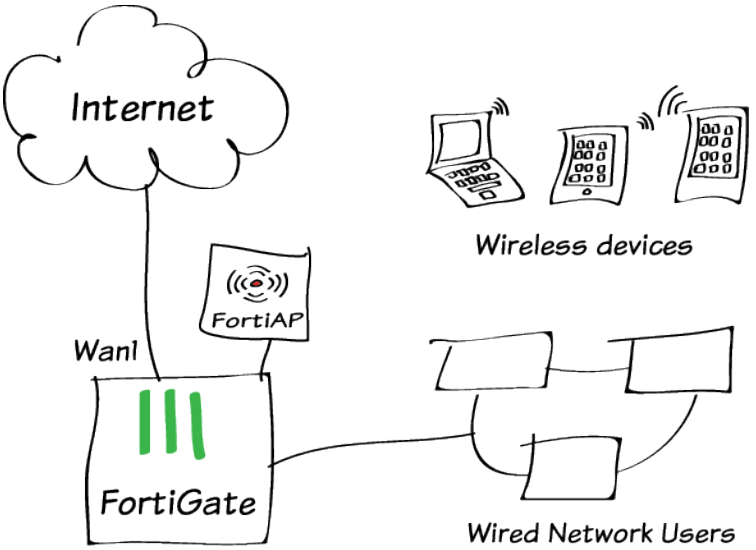
Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. A green checkmark now appears beside the FortiAP, showing that the unit is authorized and online.



Connect to the SSID with a wireless device. After a connection is established, you are able to browse the Internet.

For further reading, check out Bridge SSID to FortiGate wired network in the FortiOS 5.2 Handbook.

Combining WiFi and wired networks with a software switch



Including mobile (WiFi) users on your office LAN can be more convenient than putting them on a separate wireless network. The Software Switch feature of your FortiGate is a simple way to do this.

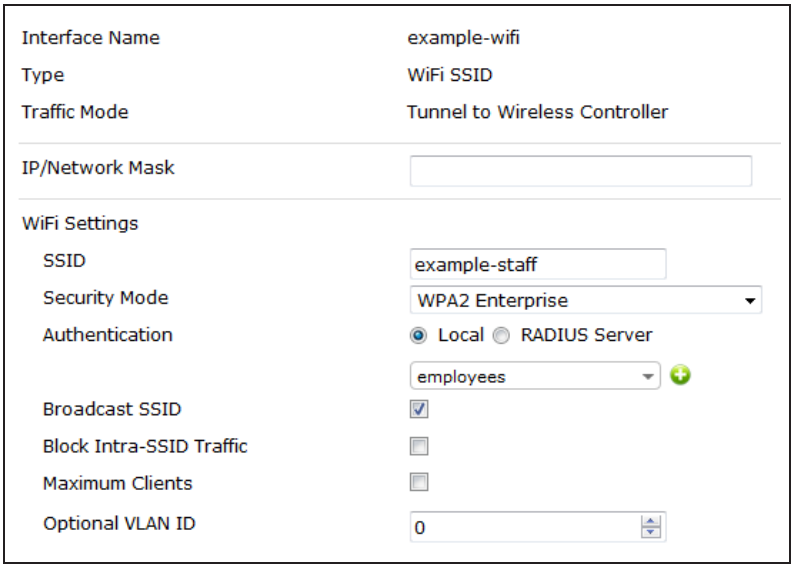
Software Switches are only available if your FortiGate is in Interface mode. For more information, see Choosing your FortiGate's switch mode.

1. Create the SSID

Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network.

Leave the IP address empty. This is allowed.

You can use any type of security/authentication. In this example, your users must be members of the *employees* group to access the network.

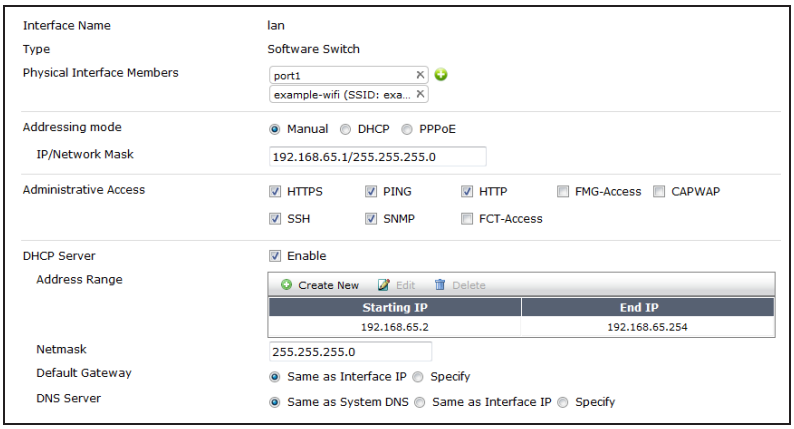


2. Combine the WiFi and wired interfaces

Go to **System > Network > Interface**. Edit the existing **lan** software switch interface or create a new one.

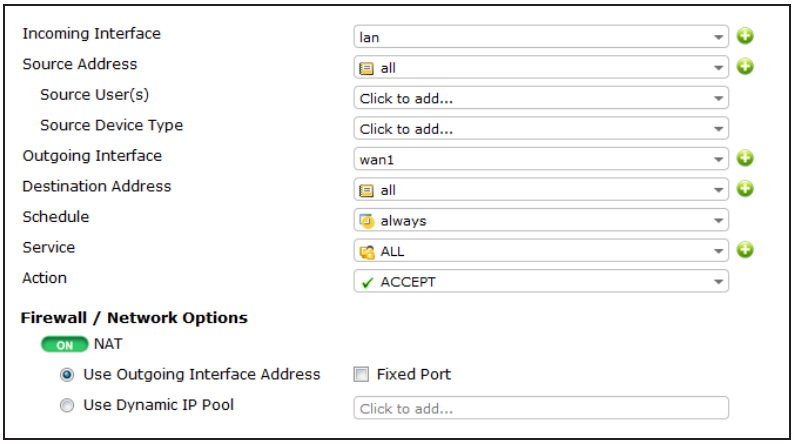
Make sure your wired and WiFi interfaces are both included.

Make sure there is a **DHCP Server** configured. It will provide IP addresses to both WiFi and wired users.



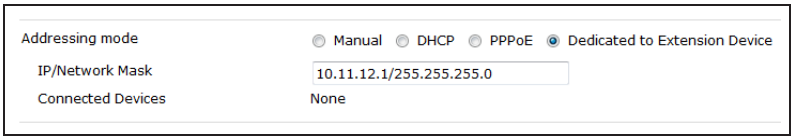
3. Create the security policy

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing all users on the software switch interface to connect to the Internet.



4. Connect and authorize the FortiAP unit

Go to **System > Network > Interface**. Configure a network interface that is dedicated to extension devices.



Connect the FortiAP unit and wait for it to be listed in **WiFi Controller > Managed Access Points > Managed FortiAPs**.

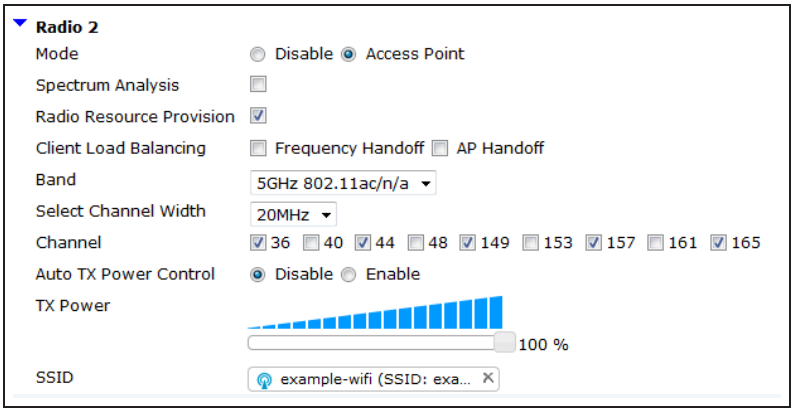
Highlight the FortiAP unit on the list and select **Authorize**.

5. Add the SSID to the FortiAP profile

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the profile for your FortiAP model.

For each radio:

- Enable **Radio Resource Provision**.
- Select your SSID.



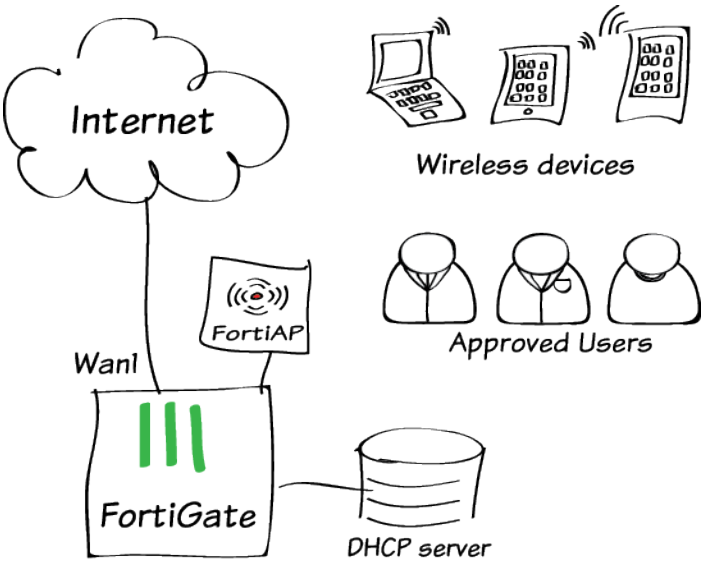
Results

Go to **WiFi Controller > Monitor > Client Monitor** to see connected users.

SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength
example-staff	FP221C3X14019926 (1)	rgreen	192.168.65.2	08:fd:0e:ff:0c:56	1	906 bps	30 dB

For further reading, check out Software switch in the FortiOS 5.2 Handbook.

WiFi network with external DHCP service



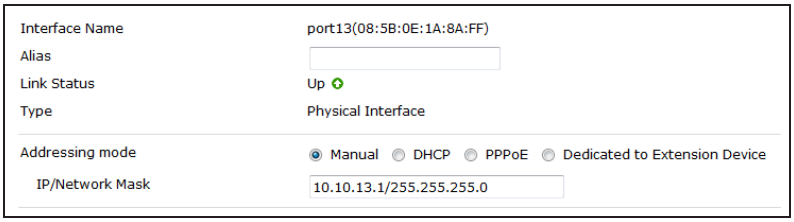
In this example, you use an external DHCP server to assign IP addresses to your WiFi clients.

The DHCP server assigns IP addresses in the range of 10.10.12.100 to 10.10.12.200. The server is attached to Port 13 of the FortiGate and has an IP address of 10.10.13.254.

1. Configure the FortiGate network interface for the DHCP server

Go to **System > Network > Interfaces** and edit Port13.

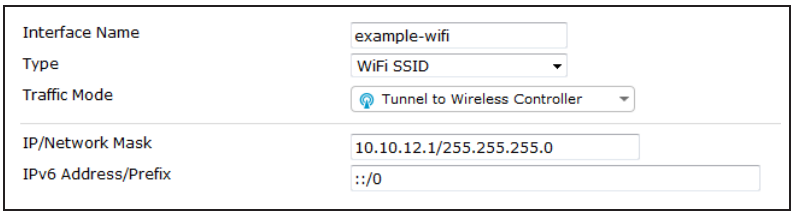
The external DHCP server is on the 10.10.13.0 network, so put the interface on that network.



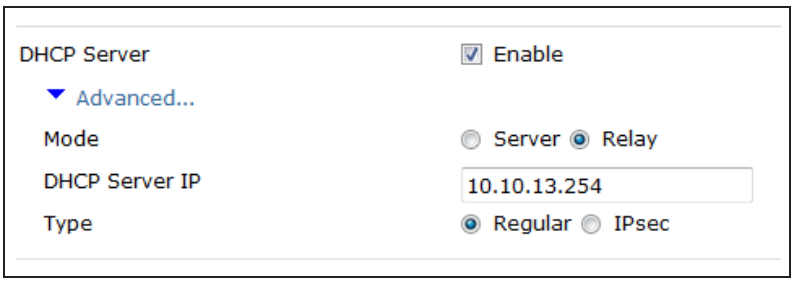
2. Create the SSID

Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network.

The DHCP server assigns IP addresses on the 10.10.12.0 network, so configure the SSID address on this network.

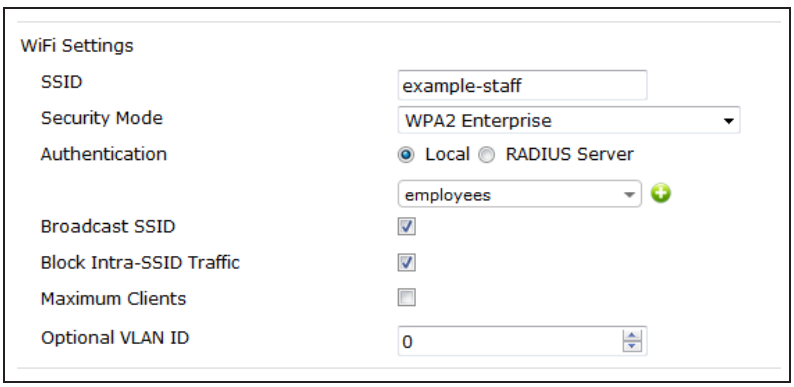


Enable **DHCP Server**, then expand **Advanced** and change the mode to **Relay**. Enter the external **DHCP server IP** address.



Set up security and authentication for your SSID.

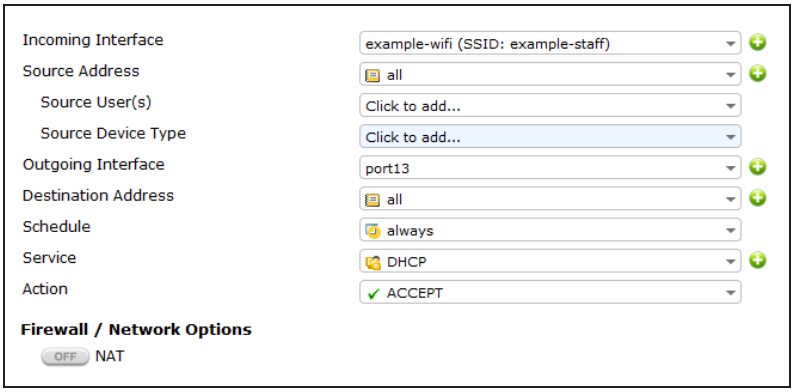
In this case, WPA2 Enterprise authentication allows access only to members of the *employees* user group.



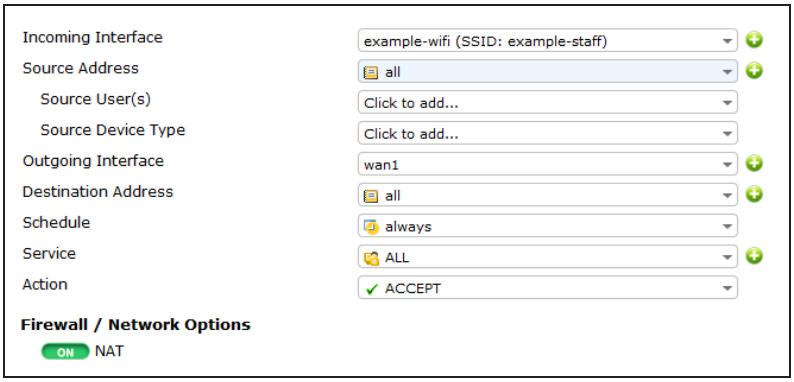
3. Create the security policies

Create a policy to allow the WiFi network to communicate with the DHCP Server on Port 13.

The source and destination networks are directly visible to each other, so NAT is not required.

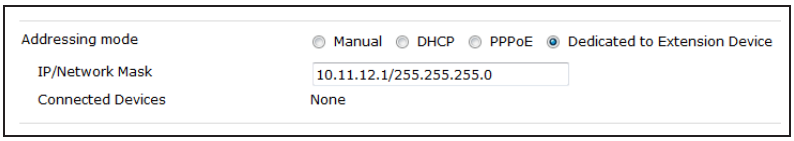


Create a policy to allow WiFi clients to connect to the Internet on wan1.



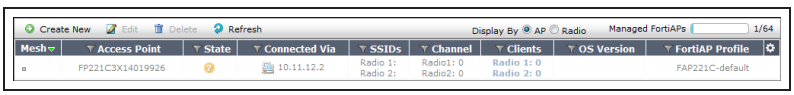
4. Connect and authorize the FortiAP unit

Configure the network interface where the FortiAP will be connected.



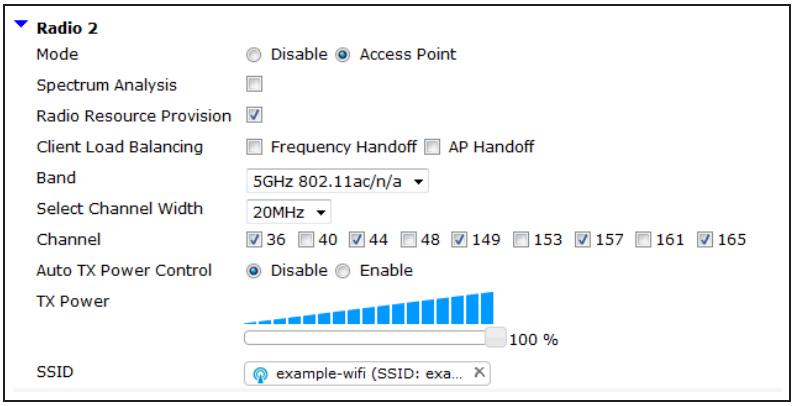
Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. The FortiAP is listed, with a yellow question mark beside it because the device is not authorized.

The FortiAP may not appear until a few minutes have passed.



Highlight the FortiAP unit on the list and select **Authorize**. A grey checkmark is now shown beside the FortiAP, showing that it is authorized but not yet online.

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the profile, adding your SSID to each radio.

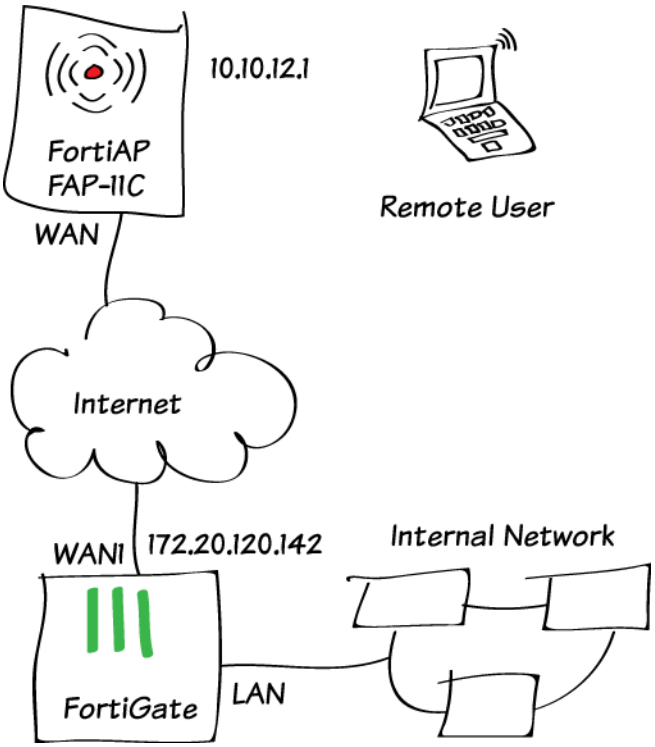


Results

WiFi devices can connect to the Internet. You can see them in the client monitor (**WiFi Controller > Monitor > Client Monitor**). Note the IP addresses assigned by the external DHCP server.

For further reading, check out the Deploying Wireless Networks in the FortiOS 5.2 Handbook.

Providing remote access to the office and Internet



In this example, you pre-configure a FortiAP to provide access to the office network from any remote location simply by connecting the FortiAP to the Internet. This FortiAP could be given to an employee to use at home or when traveling.

The FortiAP's configuration also supports Internet browsing from behind the corporate firewall. The remote user's local network remains accessible by defining it as a split tunnel destination that is not routed through the FortiGate unit.

1. Enable the split tunneling feature

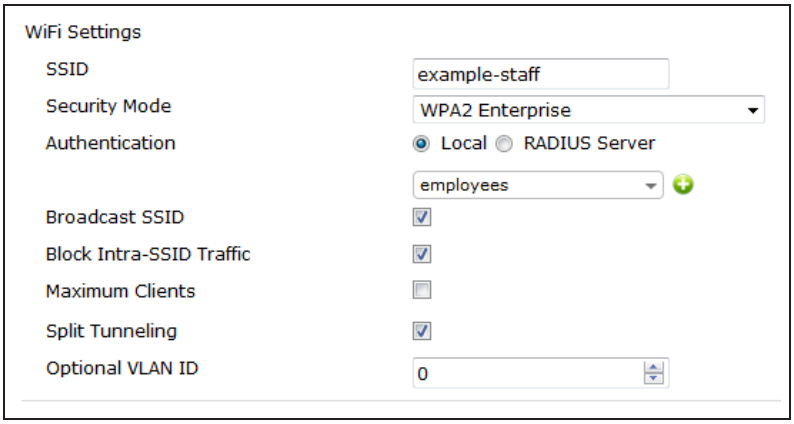
By default, split tunneling options are not visible in the FortiGate GUI. You can make these options visible using the CLI.

Go to **System > Dashboard > Status** and use the CLI Console.

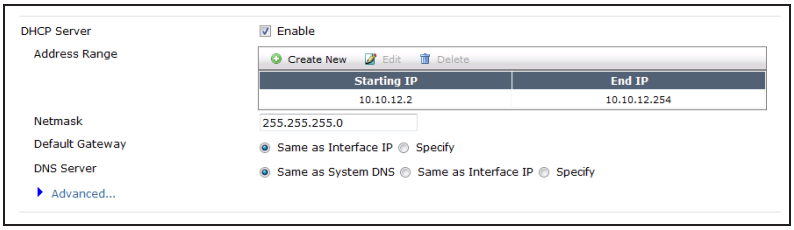
```
config system global
  set gui-fortiap-split-tunneling enable
end
```

2. Create the WiFi network

Go to **WiFi Controller > WiFi Network > SSID** and create a new SSID. The SSID will accept logons from the *employees* user group.

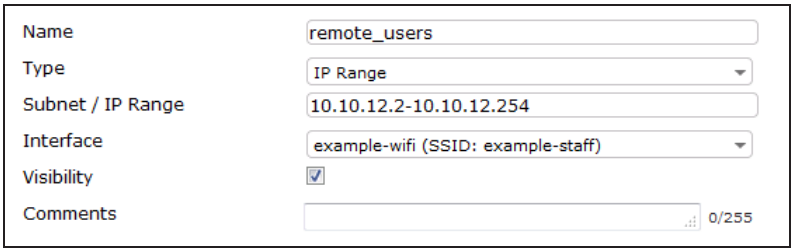


Enable the DHCP Server and make note of the IP range.

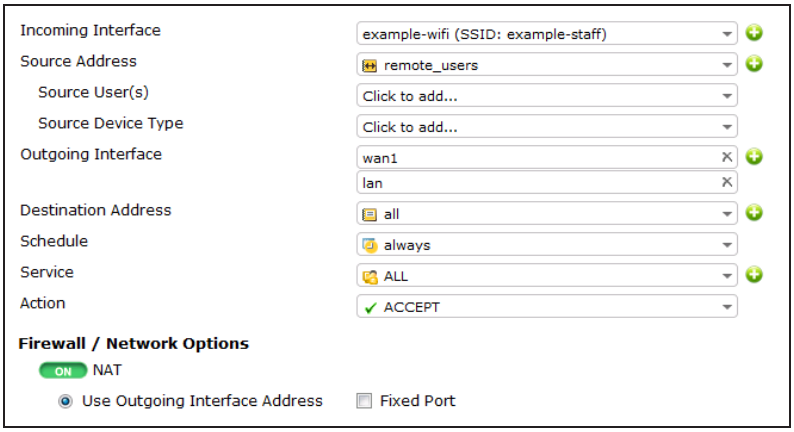


3. Create the security policy

Go to **Policy & Objects > Objects > Addresses** and create an address representing the range of remote user addresses that the DHCP server can assign.



Go to **Policy & Objects > Policy > IPv4** and create a policy that allows remote wireless users to access the Internet and the corporate network.

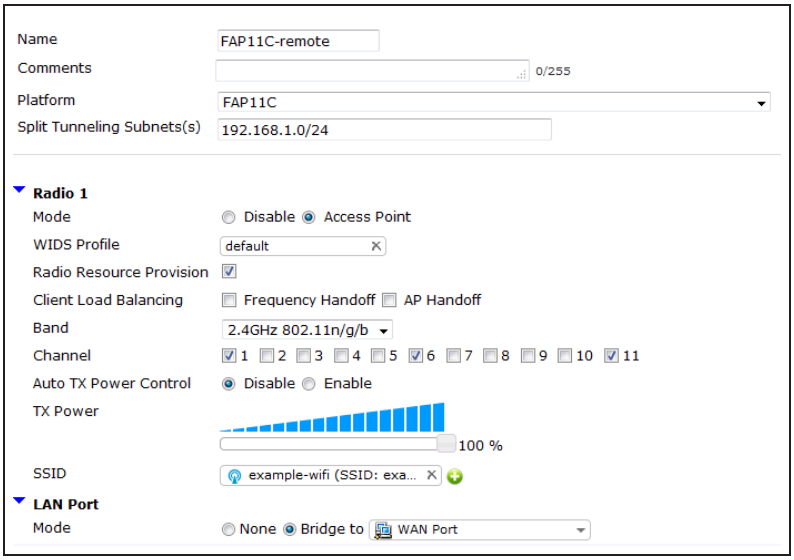


4. Create the FortiAP Profile

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and create a new profile for the FortiAP model you are using.

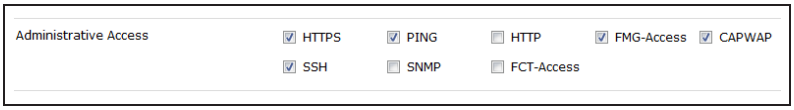
The **Split Tunneling Subnet(s)** entry exempts a typical home network subnet from being routed through the FortiGate.

Select the **SSID** that the remote FortiAP will broadcast.



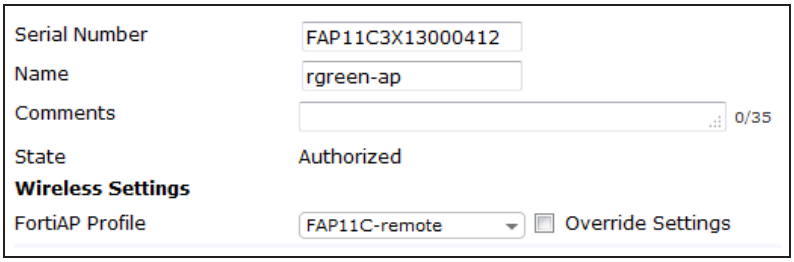
5. Enable CAPWAP on the Internet interface

Go to **System > Network > Interfaces** and edit the Internet-facing interface. In **Administrative Access**, enable CAPWAP.



6. Pre-authorize the FortiAP unit

Go to **WiFi Controller > Managed Devices > Managed FortiAPs** and create a new entry.
Enter your FortiAP's **Serial Number** and a **Name** to identify whose device it is.
Choose the **FortiAP Profile** that you created.



7. Configure the FortiAP unit

Use FortiExplorer to access the FortiAP CLI through the USB MGMT port.

Enter these commands to specify the IP address of the FortiGate WiFi controller, which will be the Internet-facing interface IP address. Enter *exit* to end.

```
FAP11C3X13000412 # login: admin
FAP11C3X13000412 # cfg -a AC_IPADDR_1=172.20.120.142
FAP11C3X13000412 # cfg -c
FAP11C3X13000412 # exit
```

The remote user can now take this device to a remote location to connect securely to the corporate FortiGate unit.

Results

At the remote location, connect the FortiAP to the Internet using an Ethernet cable. Next, connect the FortiAP to power. The network must provide DHCP service and allow the FortiAP to access the internet.

Once connected, the FortiAP requests an IP address and locates the FortiGate wireless controller.
The remote WiFi user can now access the corporate network and browse the Internet securely from behind the corporate firewall.

Connections to destinations on the "split tunneling" network are possible, but will not be visible in the FortiGate logs as the traffic remains local to the FortiAP.

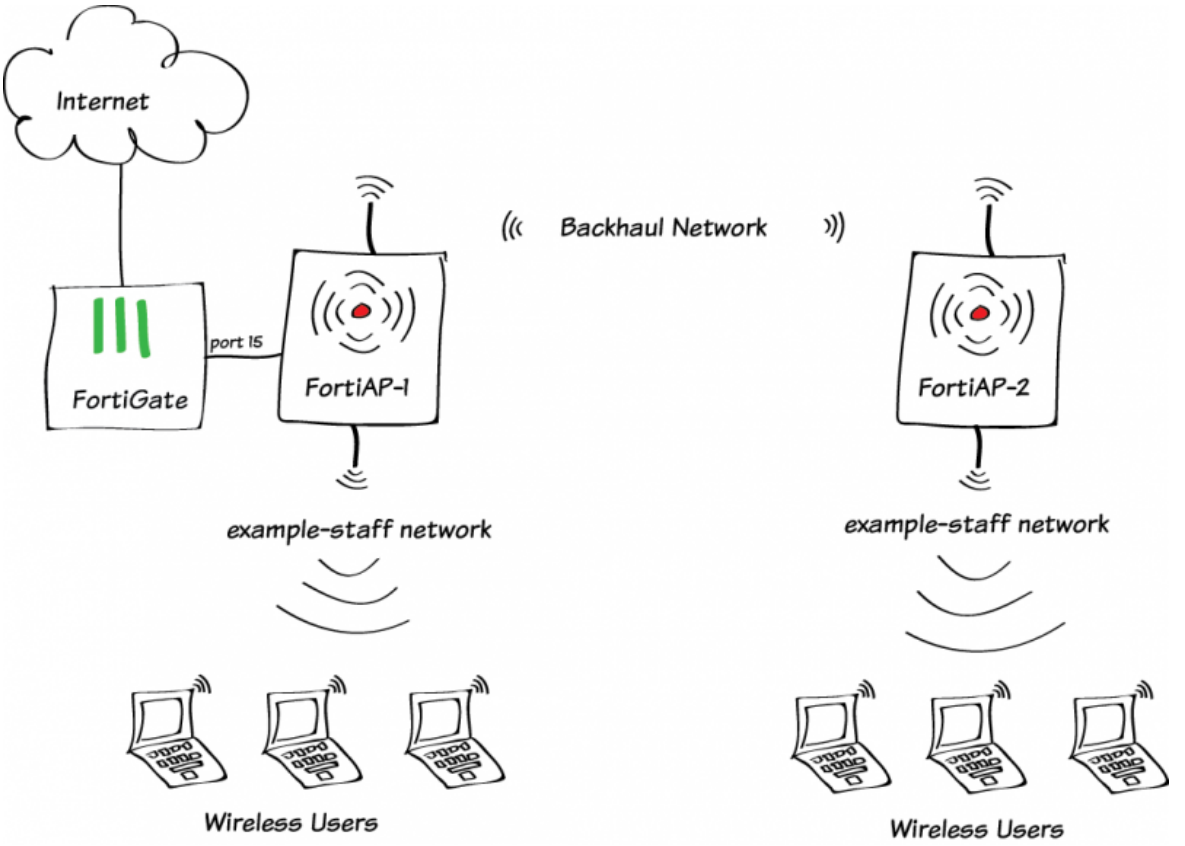
Go to **WiFi Controller > Monitor > Client Monitor** to see remote wireless users connected to the FortiAP unit.

Go to **Log & Report > Traffic Log > Forward Traffic** to see remote wireless users appear in the logs. Select an entry to view more information about remote traffic to the corporate network and to the Internet.

#	1	**Action**	ip-conn
Date/Time	11:46:46	**Destination**	208.91.112.52
Dst Interface	wan1	**Dst Port**	53
Group	employees	**Level**	
Log ID	11	**Policy ID**	8
Policy UUID	450ac232-ce5c-51e4-c482-a35b6764918e	**Sequence Number**	4011
Source	rgreen (10.10.12.4)	**Source SSID**	example-staff
Src Interface	example-wifi	**Src Name**	android-1b1c4f3382fbb4b0
Src Port	35023	**Sub Type**	forward
Threat	262144	**Threat Level**	medium
Threat Score	10	**Timestamp**	4/30/2015, 11:46:46 AM
User	rgreen	**Virtual Domain**	root

For further reading, check out Deploying Wireless Networks in the FortiOS 5.2 Handbook.

Extending WiFi range with mesh topology



In this example, two FortiAPs are used to extend the range of a single WiFi network. The second FortiAP is connected to the FortiGate WiFi controller through a dedicated WiFi backhaul network.

In this example, both FortiAPs provide the example-staff network to clients that are in range.

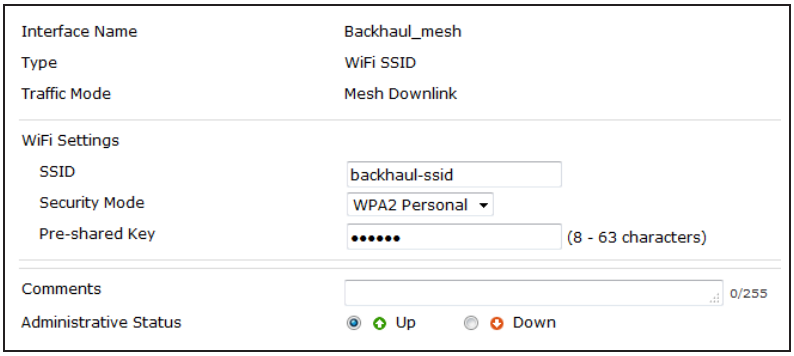
More mesh-connected FortiAPs could be added to further expand the coverage range of the network. Each AP must be within range of at least one other FortiAP. Mesh operation requires FortiAP models with two radios, such as the FortiAP-221C units used here.

1. Create the backhaul SSID

Go to **WiFi Controller > WiFi Network > SSID**.

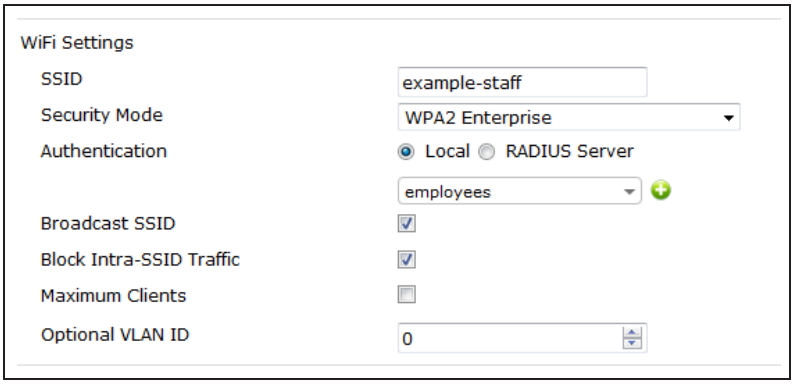
Create a new SSID. Set **Traffic Mode** to **Mesh Downlink**.

You will need the pre-shared key when configuring the mesh-connected FortiAP.

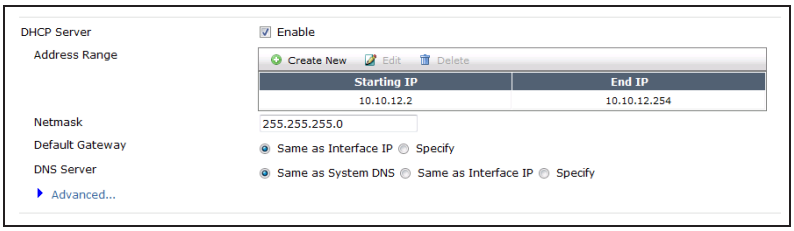


2. Create the client SSID

Go to **WiFi Controller > WiFi Network > SSID**. Create the WiFi network (SSID) that clients will use.



Configure DHCP for your clients.

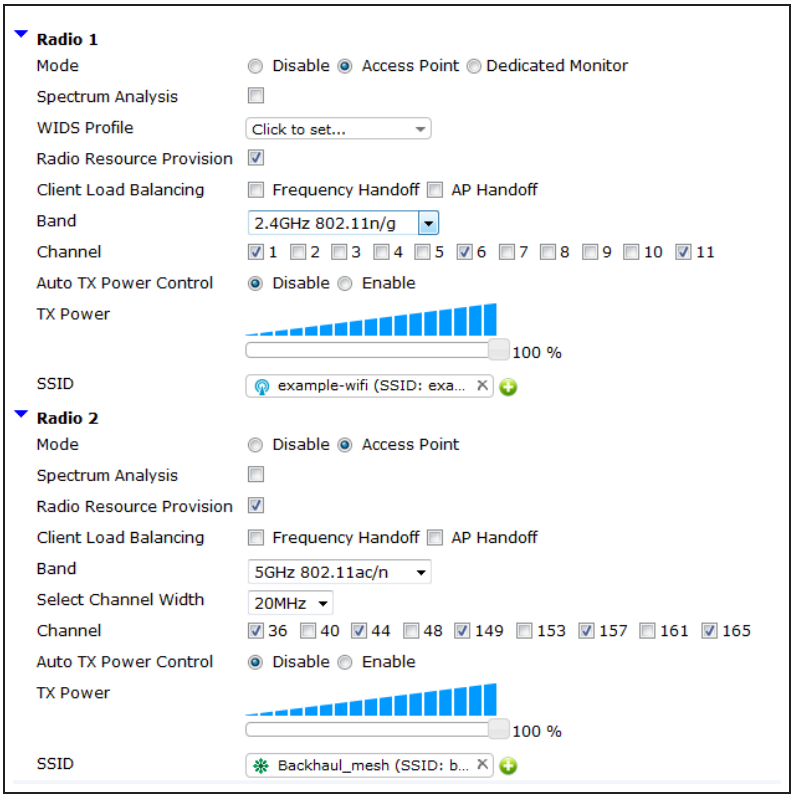


3. Create the FortiAP Profile

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and create a profile for the Platform (FortiAP model) that you are using.

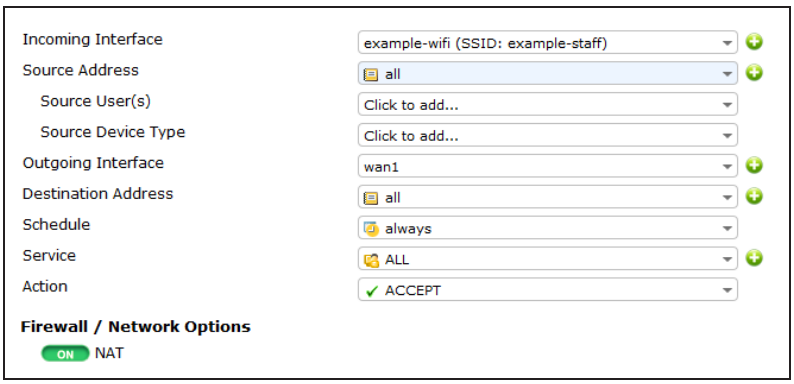
Configure Radio 1 for the client channel on the 2.4GHz 802.11n/g Band.

Configure Radio 2 for the backhaul channel on the 5GHz 802.11ac/n Band.



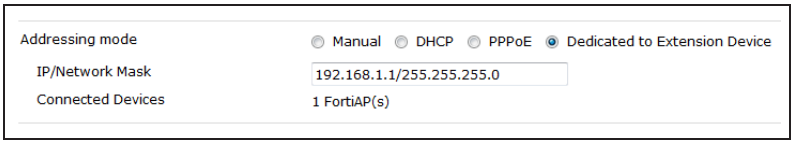
4. Configure the security policy

Go to **Policy & Objects > Policy > IPv4** and create a new policy.



5. Configure an interface dedicated to FortiAP

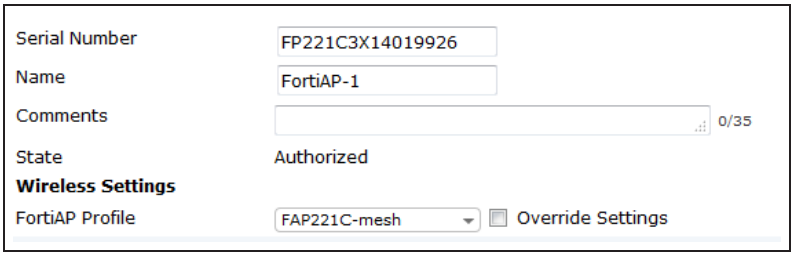
Go to **System > Network > Interfaces** and edit an available interface (in this example, port 15). Set **Addressing mode** to **Dedicate to Extension Device**.



6. Preauthorize FortiAP-1

Go to **WiFi Controller > Managed Devices > Managed FortiAPs** and create a new entry.

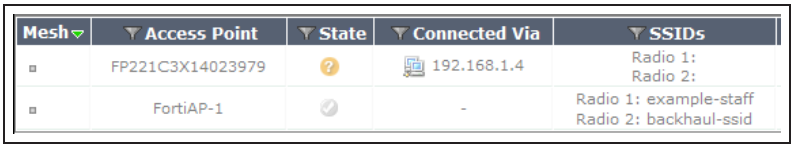
Enter the serial number of the FortiAP unit and give it a name. Select the FortiAP profile that you created earlier.



7. Configure FortiAP-2 for mesh operation

Connect FortiAP-2 to Port 15.

Go to **WiFi Controller > Managed Devices > Managed FortiAPs**. FortiAP-2, identified by serial number, will be listed within two minutes. Note the **Connected Via** IP address.



Go to **System > Dashboard > Status**.

In the CLI Console, enter *exec telnet 192.168.1.4* (your address might be different) to log in to the FortiAP as *admin*. Enter the commands to change the AP to mesh uplink on the *backhaul-ssid* network. Enter *exit* to end.

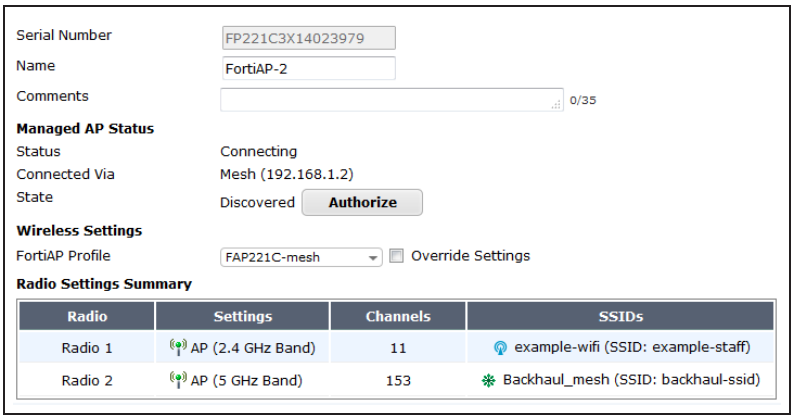
```
FP221C3X14019926 login: admin

FP221C3X14019926 # cfg -a MESH_AP_TYPE=1
 FP221C3X14019926 # cfg -a MESH_AP_SSID=backhaul-
ssid
 FP221C3X14019926 # cfg -a MESH_AP_
PASSWD=backhaul-ssid-passwd
 FP221C3X14019926 # cfg -c
 FP221C3X14019926 # exit
```

Disconnect FortiAP-2 from the FortiGate. Install it in its planned location and apply power.

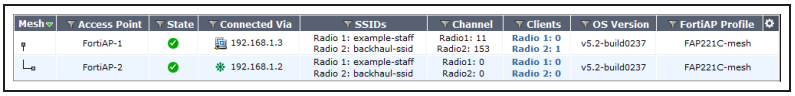
Connect FortiAP-1 to Port 15 and apply power.

Go to **WiFi Controller > Managed Devices > Managed FortiAPs**. Select the FortiAP-2 entry (identified by serial number) and edit the new entry. Enter the **Name**, FortiAP-2. Select the **FortiAP Profile** that you created earlier. Click **Authorize**. Click **OK**.



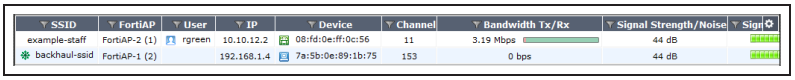
8. Connect and authorize the FortiAPs

Go to **WiFi Controller > Managed Devices > Managed FortiAPs**. The FortiAPs will be listed as online within about two minutes. (Click **Refresh** to update the display.)



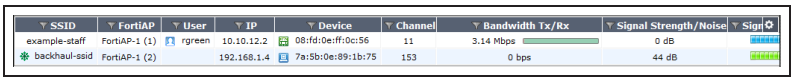
9. Results

Go to **WiFi Controller > Monitor > Client Monitor**. Click **Refresh** to see updated information.



Use a mobile device near FortiAP-2 to connect to the *example-staff* network. The monitor shows the mobile user *rgreen* as a client of FortiAP-2.

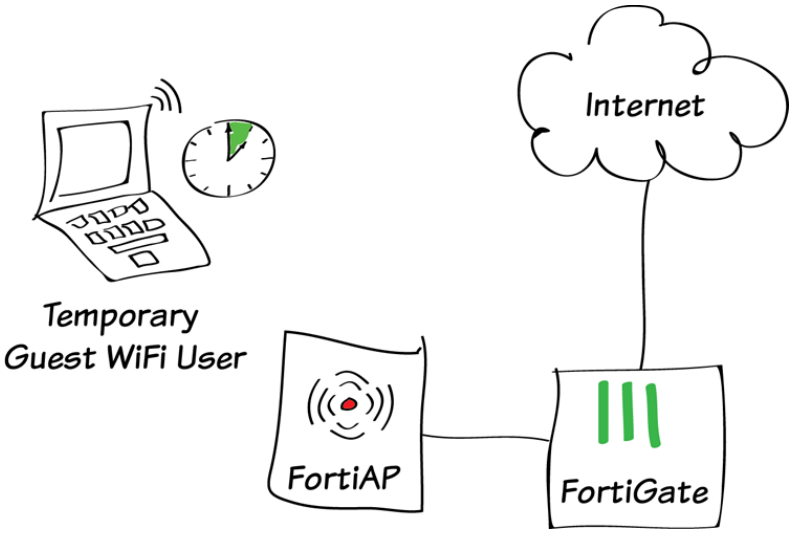
Disconnect from the *example-staff* network and then reconnect near FortiAP-1. The monitor shows the mobile user *rgreen* as a client of FortiAP-1.



Notice that in both cases FortiAP-2 is listed on *backhaul-ssid* as a client of FortiAP-1.

For further reading, check out Wireless Mesh in the FortiOS 5.2 Handbook.

Guest WiFi accounts



In this example, a guest user account will be created to allow temporary wireless access to the Internet. Access will only be allowed using HTTP, HTTPS, and DNS protocols.

In this example, a FortiAP in Tunnel mode is used to provide wireless access to guests.

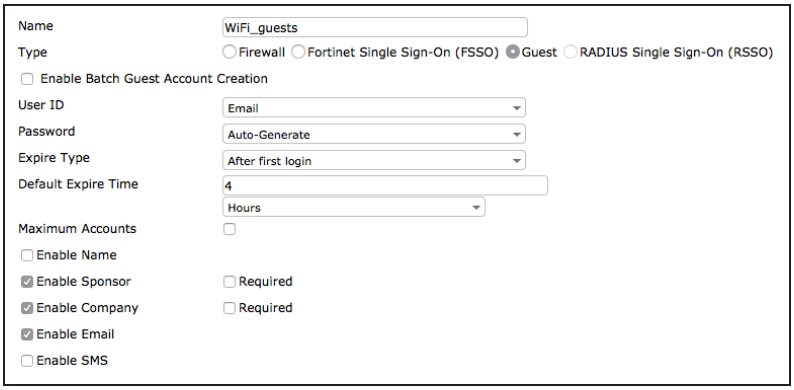
If you have not already set up a wireless network, see Setting up WiFi with FortiAP.

A video of this recipe is available here.

1. Creating a WiFi guest user group

Go to **User & Device > User > User Groups** and create a new group.

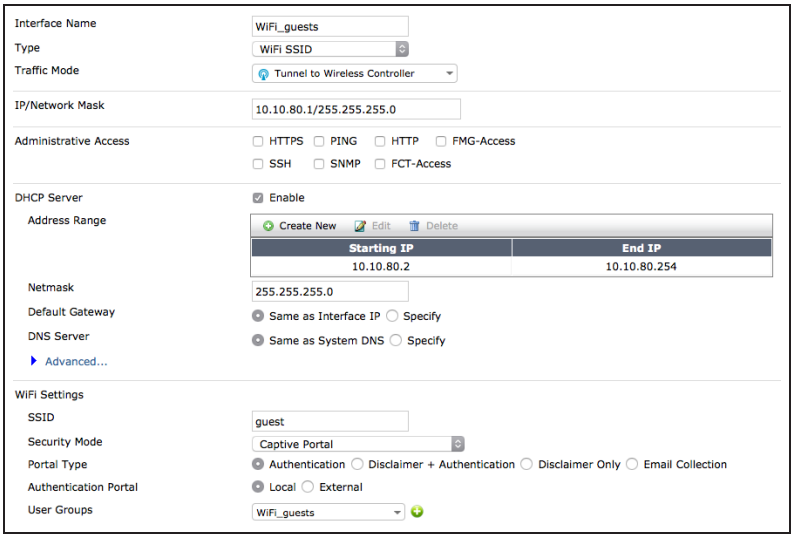
Set **Type** to **Guest**. Set **User ID** to **Email**, ensure that **Password** is set to **Auto-Generate**, and set **Expiry Type** to **After first login**. Leave **Default Expiry Time** set to **4 Hours**.



2. Creating a guest SSID that uses Captive Portal

Go to **Wireless Controller > WiFi Network > SSID** and create a new SSID.

Set **Traffic Mode** to **Tunnel to Wireless Controller**. Assign an **IP/Network Mask** to the interface and enable **DHCP server**. Under **WiFi Settings**, set **Security Mode** to **Captive Portal** and **User Group(s)** to the WiFi guest user group.



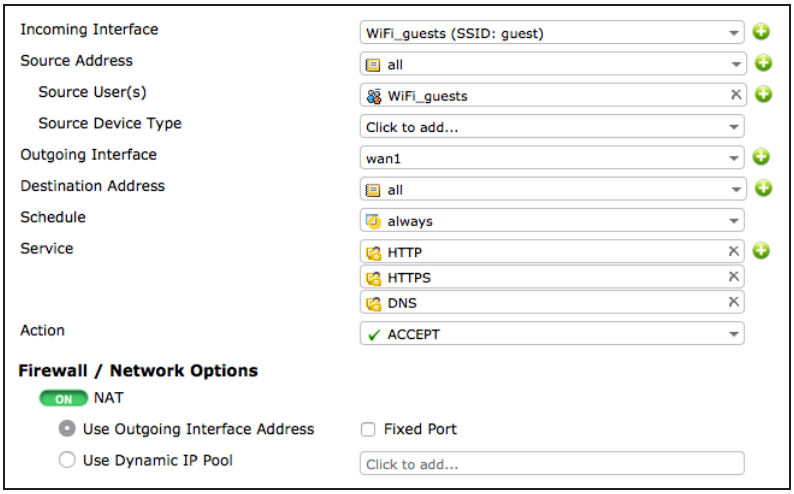
Go to **Wireless Controller > WiFi Network > FortiAP Profiles** and edit the profile for your FortiAP model (in the example, FortiAP-11C).

Set the FortiAP to broadcast the new **SSID**.

3. Creating a security policy for WiFi guests

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

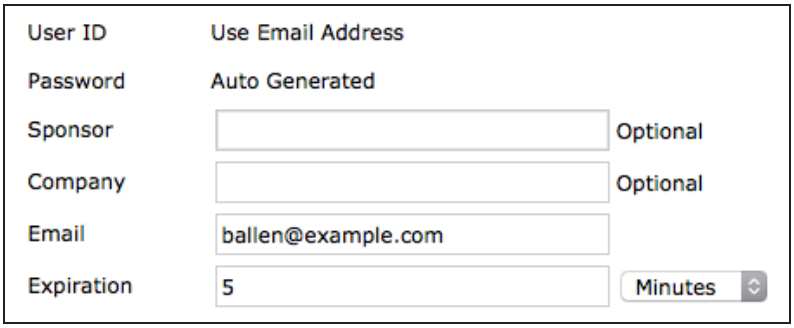
Set **Incoming Interface** to the guest SSID, **Source User(s)** to the WiFi guest user group, the **Outgoing Interface** to your Internet-facing interface, and **Service** to **HTTP**, **HTTPS**, and **DNS**.



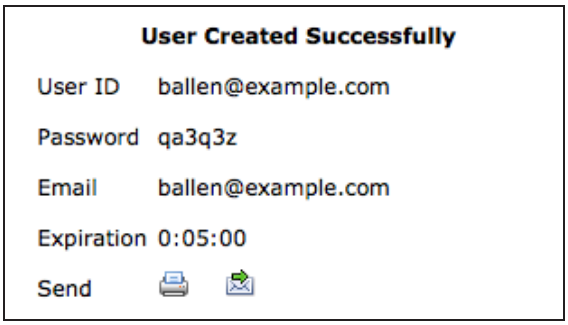
4. Creating a guest user account

Go to **User & Device > User > Guest Management** and create a new account.

Set **Email** to the user's email address (in the example, *ballen@example.com*). To test the account, set **Expiration** to **5 Minutes**.



After you select **OK**, a **User Created Successfully** notice will appear, listing the generated Password. This password can then be printed or emailed to the guest user.

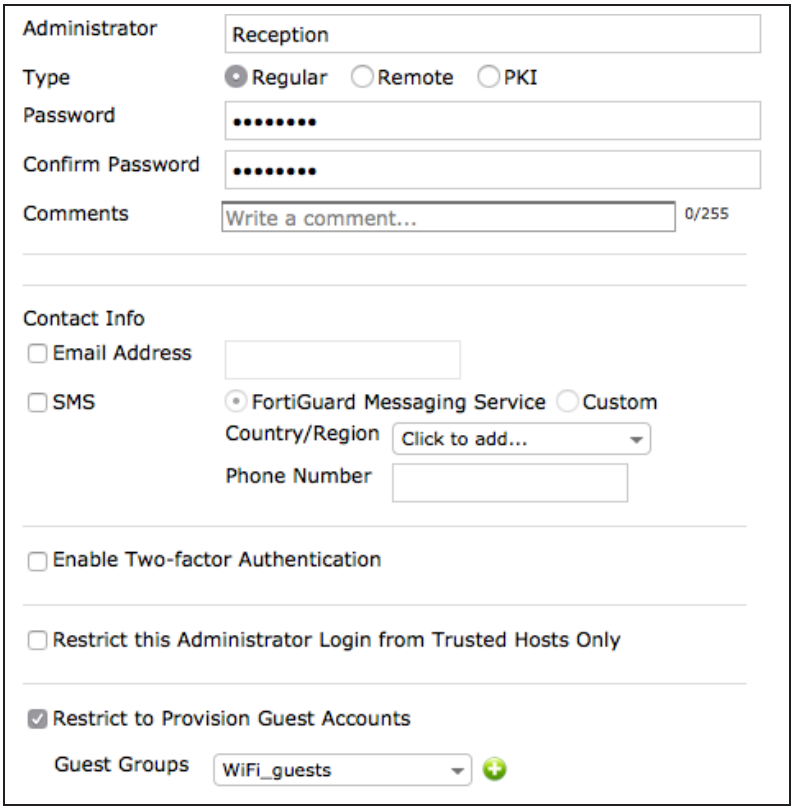


(Optional) 5. Creating a restricted admin account for guest user management

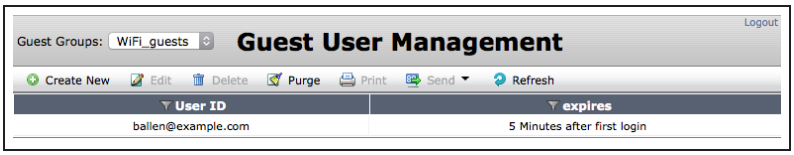
To make it easier for guest accounts to be created, an admin account can be made that is only used for guest user management. In this example, the account is made for use by the receptionist.

Go to **System > Admin > Administrators** and create a new account.

Set **Type** to **Regular** and set a **Password**. Select **Restrict to Provision Guest Accounts** and set **Guest Groups** to the WiFi guest user group.

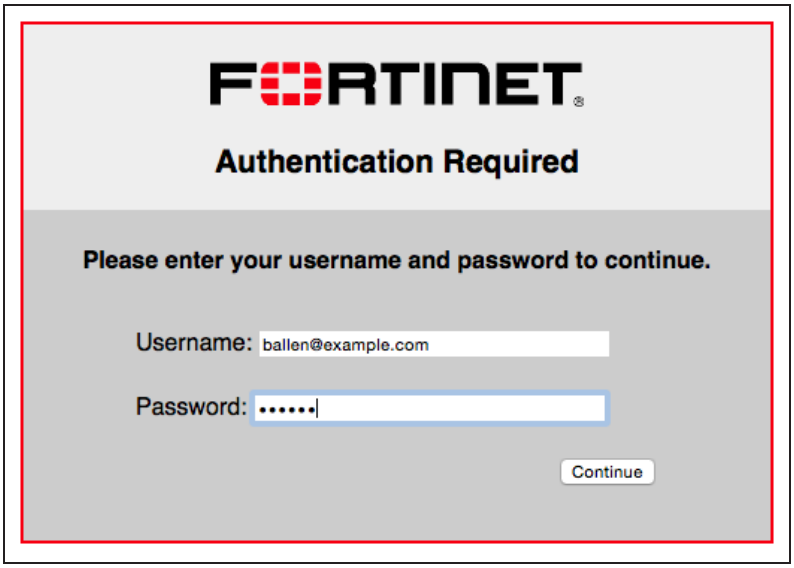


Sign in to the FortiGate using this account. You will only be able to see the menu for **Guest User Management.**



6. Results

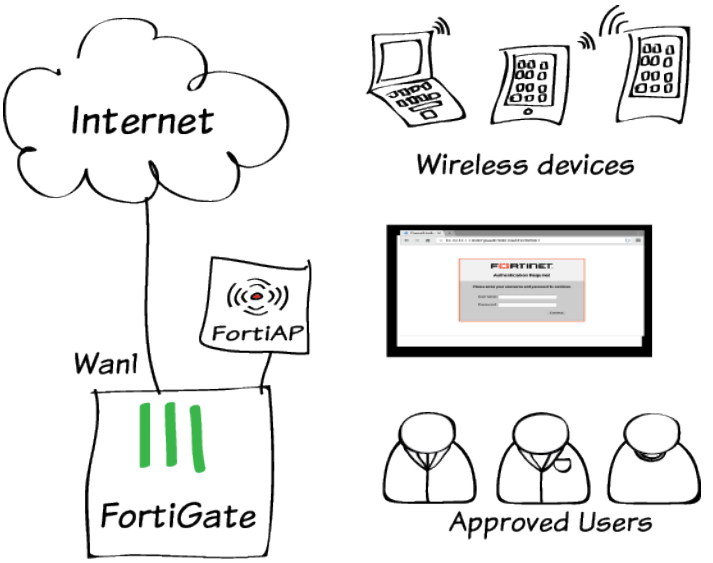
On a PC, connect to the guest SSID. When the authentication screen appears, log in using the guest user's credentials. You will be able to connect to the Internet.



Five minutes after the initial login, the user account will expire and you will no longer be able to log in using those credentials.

For further reading, check out Managing Guest Access in the FortiOS 5.2 Handbook.

Captive portal WiFi access control



In this example, your employees can log on to your Wi-Fi network through a captive portal.

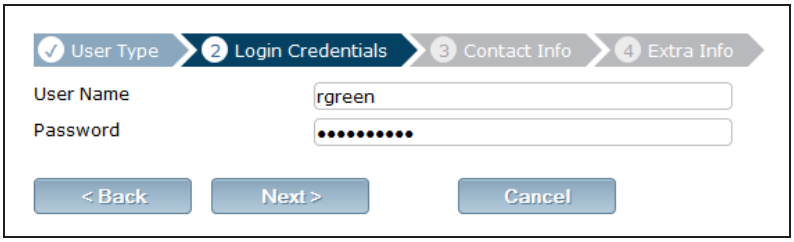
Captive portals are often used for public Wi-Fi networks where you want Wi-Fi users to respond to a disclaimer. Captive portals can also be used to provide unlimited access to open Wi-Fi networks.

As shown in this example, captive portals can also be used as the authentication method for restricting access to a wireless network. Some users may find it more intuitive to add their account information to a captive portal web page instead of a entering their user name and password into a wireless network configuration.

1. Create user accounts

Go to **User & Device > User > User Definition** and create a Local user.

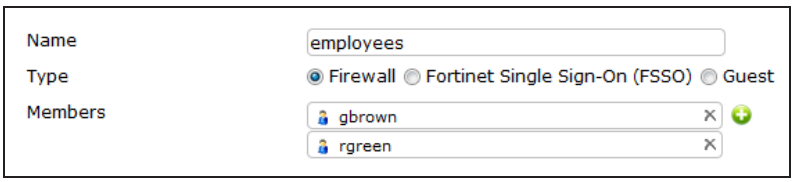
Create additional users as needed. You can use any authentication method.



2. Create a user group

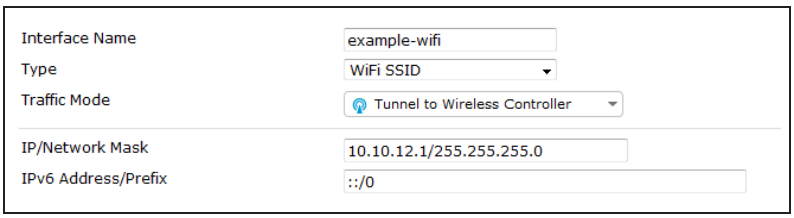
Go to **User & Device > User > User Groups**.

Create a user group for employees and add the new user(s) to the group.

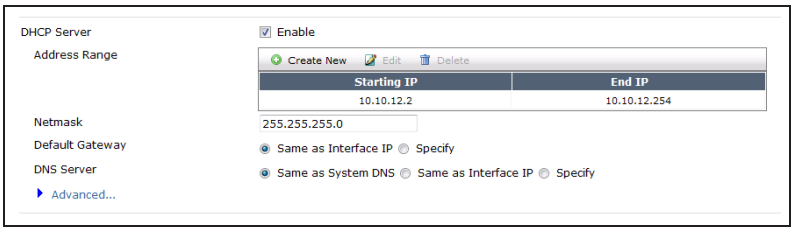


3. Create the SSID

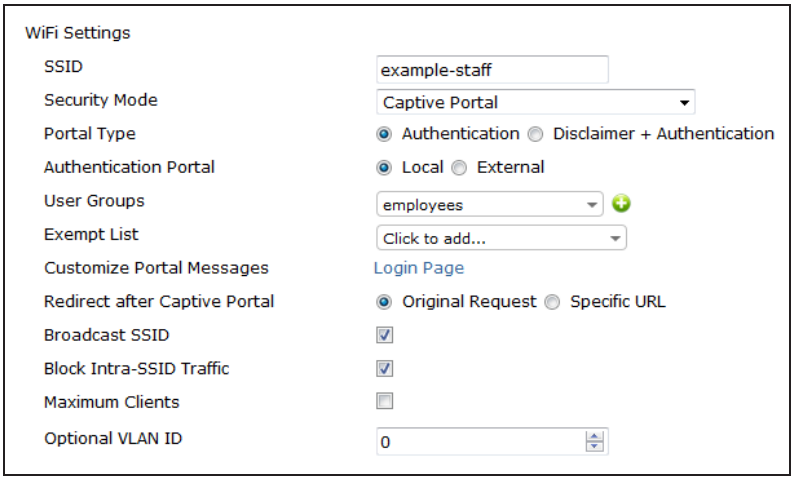
Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network.



Configure DHCP addressing for clients.

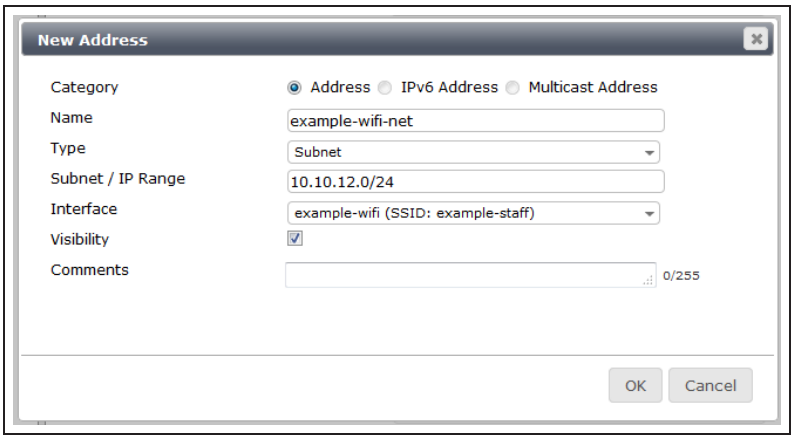


Configure Captive Portal authentication using the *employees* user group.

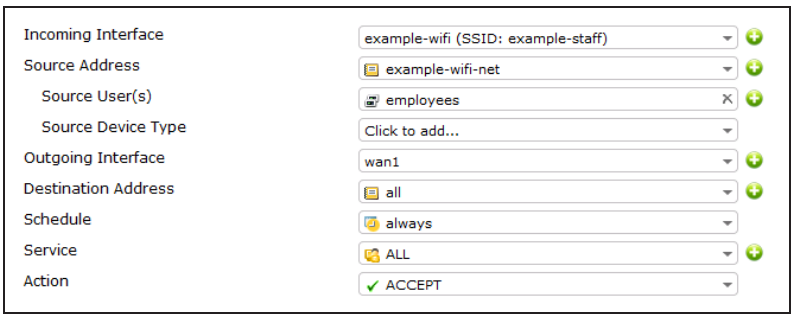


4. Create the security policy

Create an address for your SSID, using the same IP range that was set on the DHCP server.

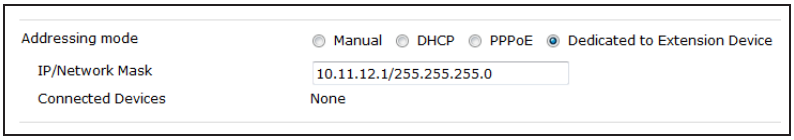


Go to **Policy & Objects > Policy > IPv4** and create a policy allowing WiFi users to connect to the Internet. Select the *employees* user group as permitted **Source Users**.



5. Connect and authorize the FortiAP unit

Go to **System > Network > Interface**. Configure an interface dedicated to extension devices and assign it an IP address.

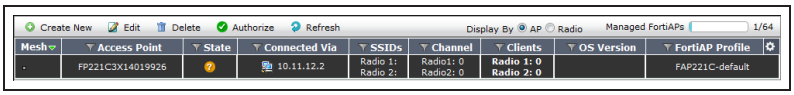


Connect the FortiAP unit to the interface and go to **WiFi Controller > Managed Access Points > Managed FortiAPs**.

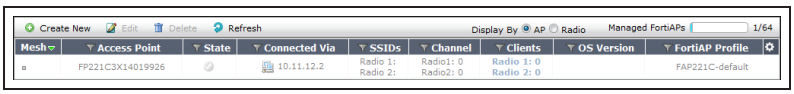
The FortiAP is listed, with a yellow question mark beside it because the device is not authorized.

The FortiAP may not appear for a minute or two.

Highlight the FortiAP unit on the list and select **Authorize**.



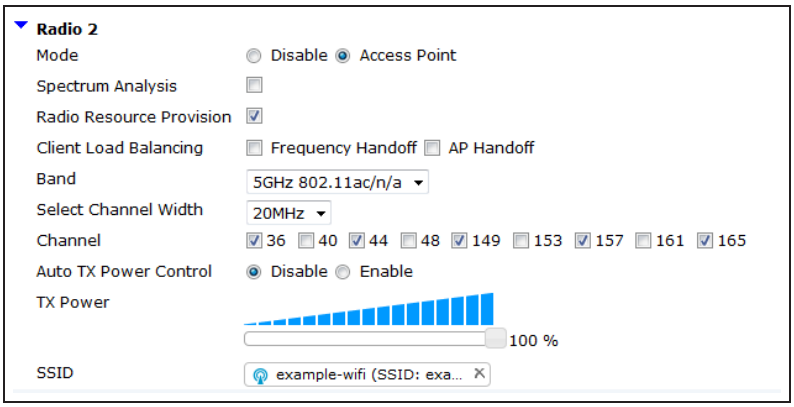
A grey check mark is now shown beside the FortiAP, showing that it is authorized but not yet online.



Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the profile. For each radio:

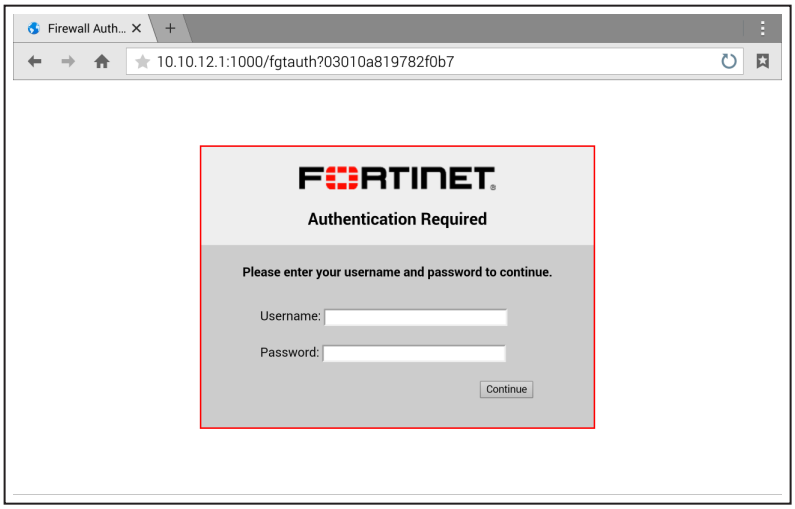
Enable **Radio Resource Provision**.

Select your SSID.

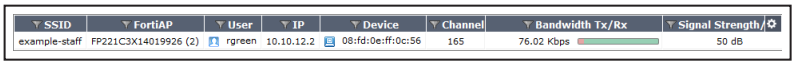


6. Results

The user's device shows the WiFi network as "open" and associates with it without requesting credentials. The first time that a wireless user attempts to use a web browser, the captive portal login screen is displayed. Users who are members of the *employees* group can log on using their username and password and proceed to access the wireless network.



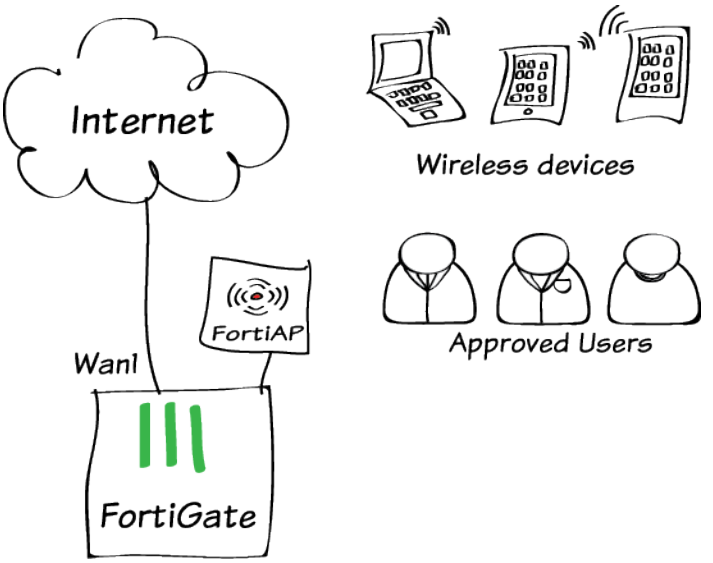
Go to **WiFi Controller > Monitor > Client Monitor** to see connected users.



SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength/
example-staff	FP221C3X14019926 (2)	rgreen	10.10.12.2	08:fd:0e:ff:0c:56	165	76.02 Kbps	50 dB

For further reading, check out Captive portals in the FortiOS 5.2 Handbook.

WP2A WiFi access control



In this example, you will improve your WiFi security with WPA2 enterprise authentication.

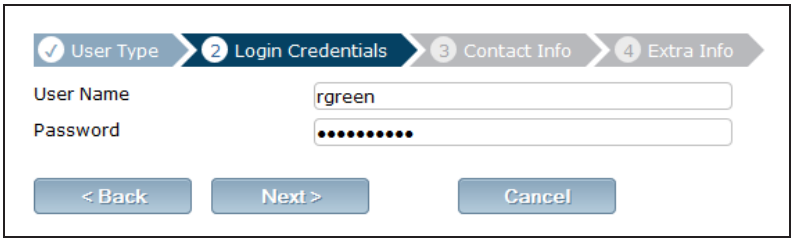
In the Setting up WiFi with FortiAP recipe, you set up a WiFi network with a single pre-shared key. In this example, there is no longer a pre-shared key that could fall into the wrong hands, or that needs to be changed if someone leaves the company. Each user has an individual user account and password, and accounts can be added or removed later as needed.

This example shows how to authenticate local FortiGate users. You can also integrate WPA2 security with most 3rd party authentication solutions including RADIUS.

1. Create user accounts

Go to **User & Device > User > User Definition** and create a Local user.

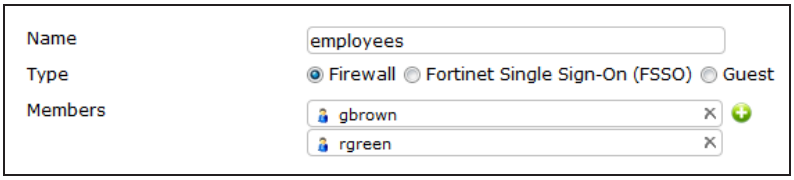
Create additional users as needed. You can use any authentication method.



2. Create a user group

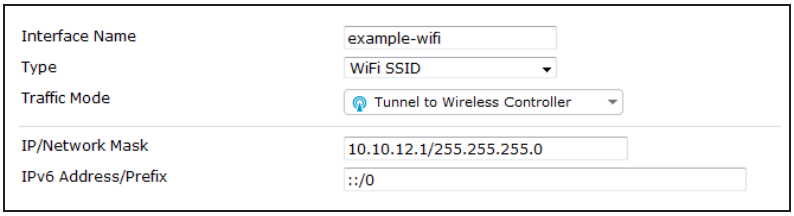
Go to **User & Device > User > User Groups**.

Create a user group for employees and add the new user(s) to the group.

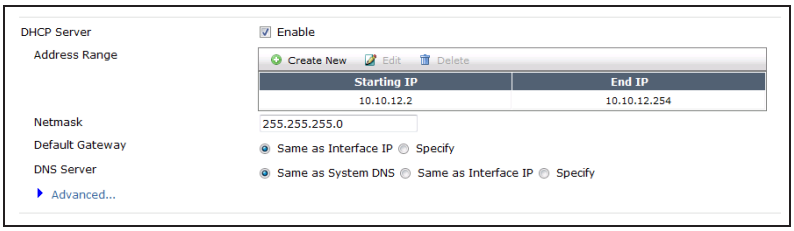


3. Create the SSID and enable the WiFi radio

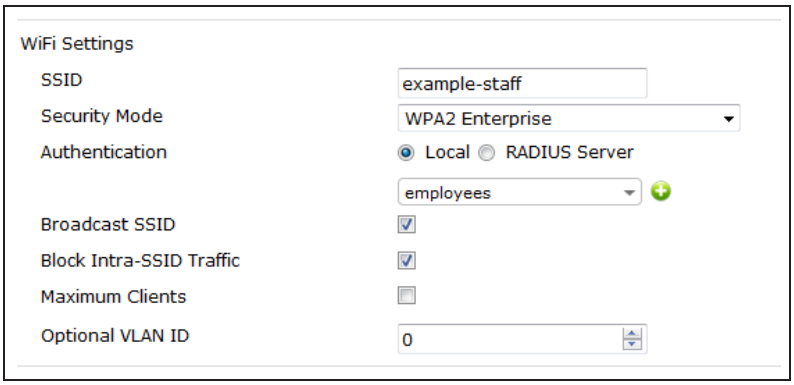
Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network.



Configure DHCP addressing for clients.

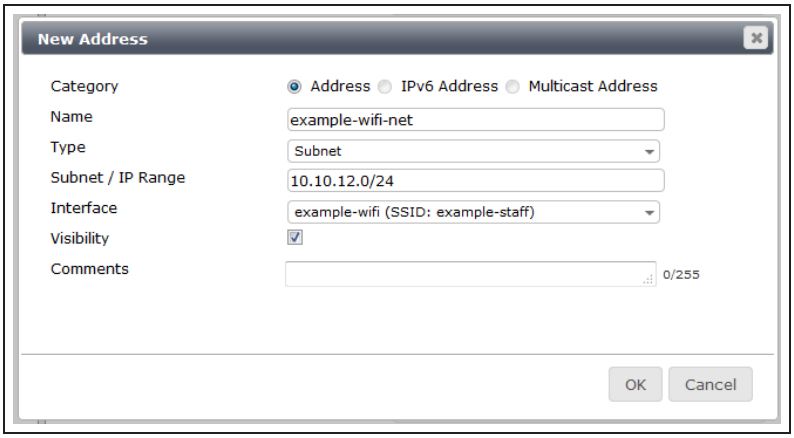


Configure WPA2-Enterprise authentication using the *employees* user group.

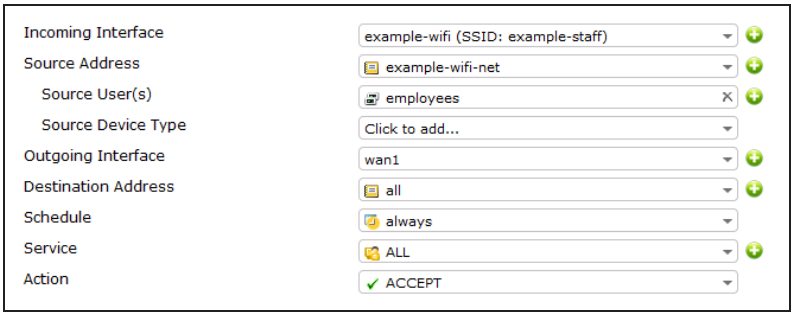


4. Create the security policy

Create an address for your SSID, using the same IP range that was set on the DHCP server.



Go to **Policy & Objects > Policy > IPv4** and create a policy allowing WiFi users to connect to the Internet.



Results

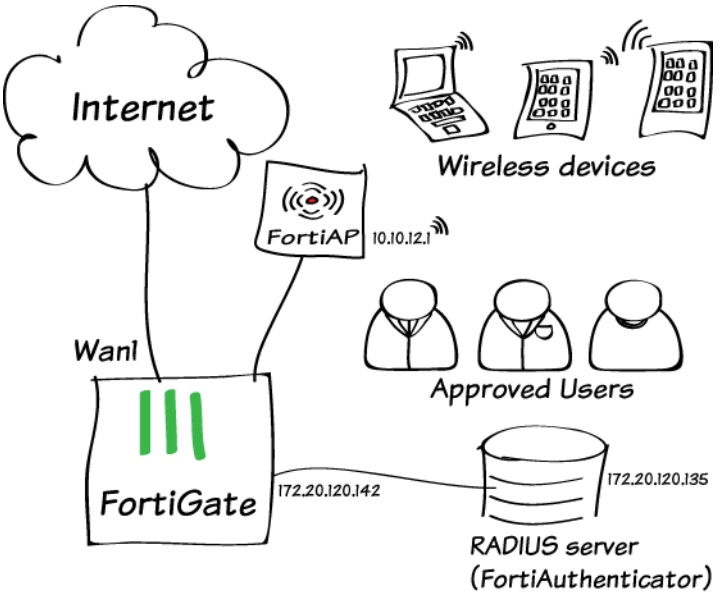
Users who are members of the *employees* group can log on to the WiFi network using their username and password.

Go to **WiFi Controller > Monitor > Client Monitor** to see connected users.

SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength/
example-staff	FP221C3X14019926 (2)	rgreen	10.10.12.2	08:fd:0e:ff:0c:56	165	76.02 Kbps	50 dB

For further reading, check out Deploying Wireless Networks in the FortiOS 5.2 Handbook.

WiFi with external RADIUS authentication



In this example, you use an external RADIUS server to authenticate your WiFi clients.

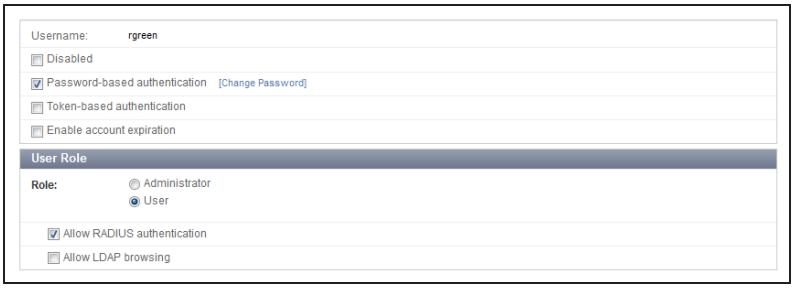
In the example, a FortiAuthenticator (v3.00-build0176) is used as a RADIUS server to authenticate users who belong to the employees user group.

1. Create the user accounts and user group on the FortiAuthenticator

Go to **Authentication > User Management > Local Users** and create a user account.

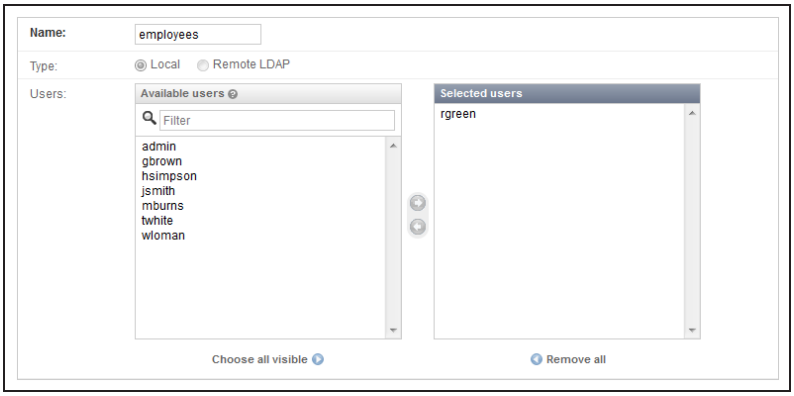
User Role settings are available after you click **OK**.

Create additional user accounts as needed, one for each employee.



Go to **Authentication > User Management > User Groups** and create the local user group "employees" on the FortiAuthenticator.

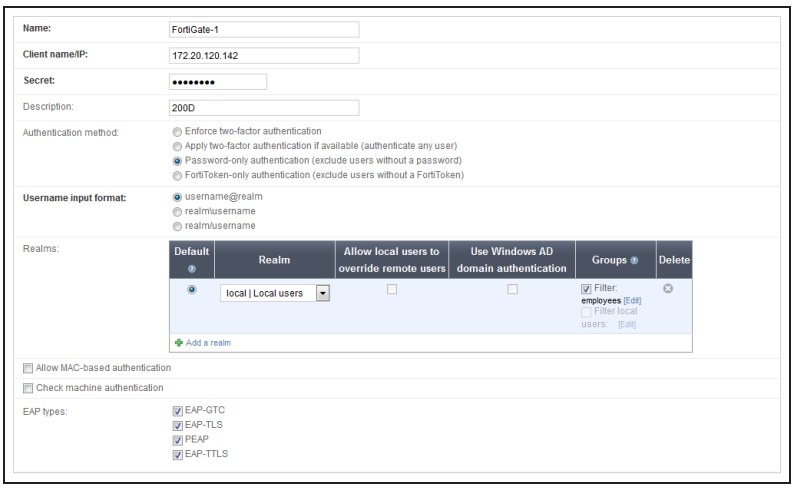
Add users who are allowed to use the WiFi network.



2. Register the FortiGate as a RADIUS client on the FortiAuthenticator

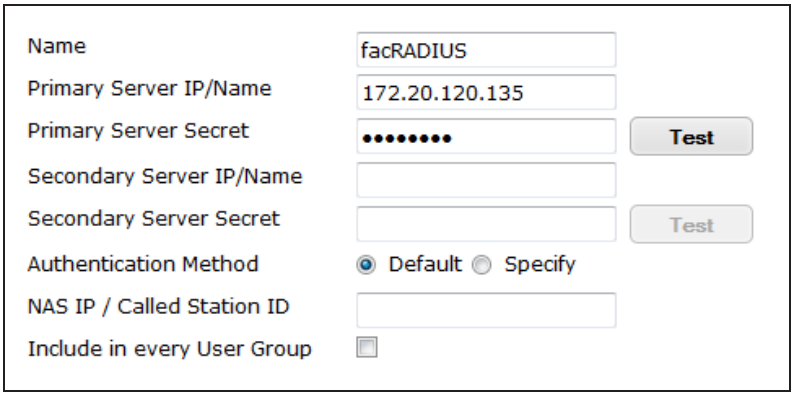
Go to **Authentication > RADIUS Service > Clients** and create a user account.

Enable all of the **EAP types**.



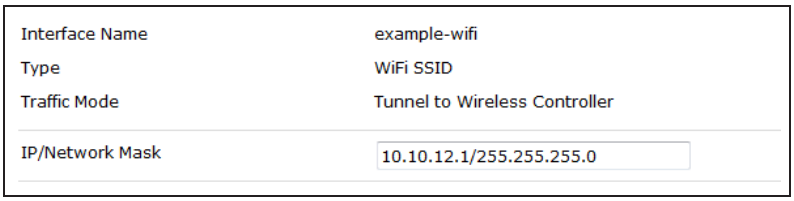
3. Configure FortiGate to use the RADIUS server

Go to **User & Device > Authentication > RADIUS Servers** and add the FortiAuthenticator unit as a RADIUS server.

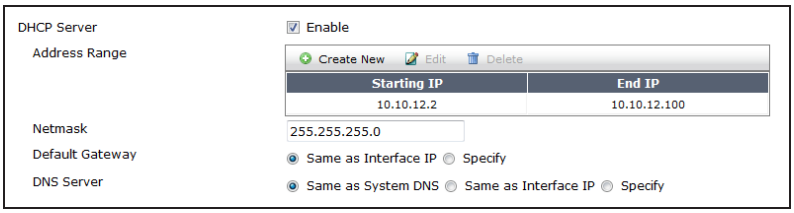


4. Create the SSID and set up authentication

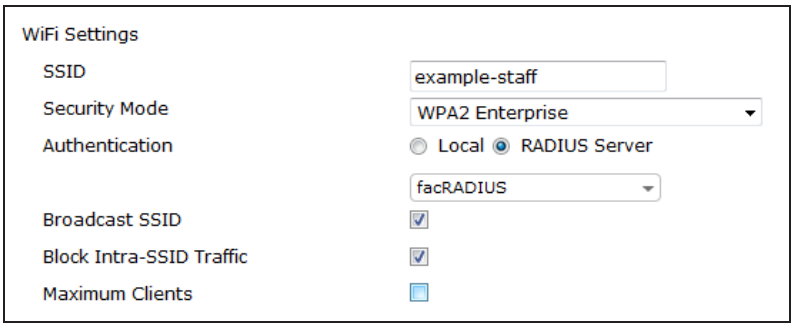
Go to **WiFi Controller > WiFi Network > SSID** and define your wireless network.



Set up DHCP for your clients.

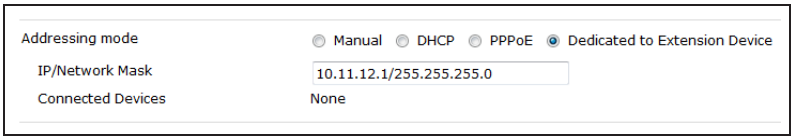


Configure WPA2 Enterprise security that uses the external RADIUS server.



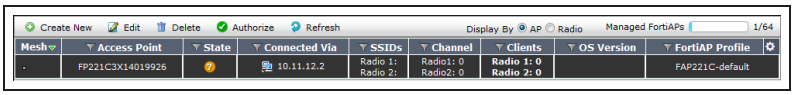
5. Connect and authorize the FortiAP

Go to **System > Network > Interfaces** and configure a dedicated interface for the FortiAP.



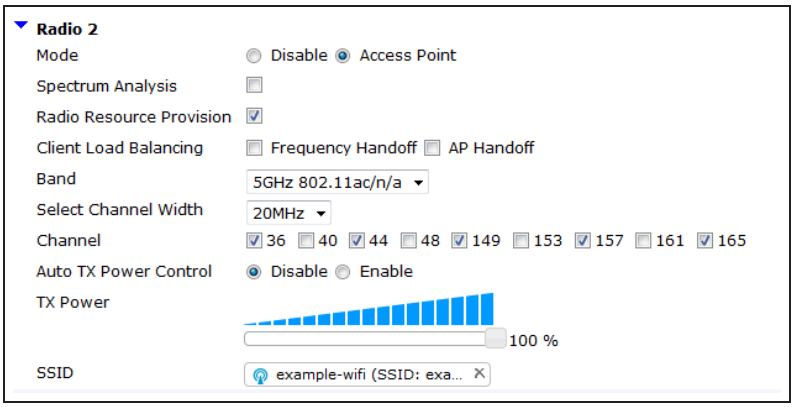
Connect the FortiAP unit. Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**.

When the FortiAP is listed, select and authorize it.



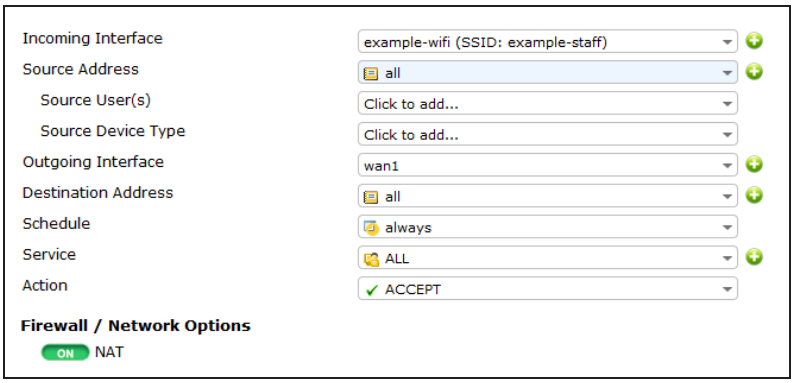
Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the profile. For each radio:

- Enable **Radio Resource Provision**.
- Select your SSID.



5. Create the security policy

Go to **Policy & Objects > Policy > IPv4** and add a policy that allows WiFi users to access the Internet.



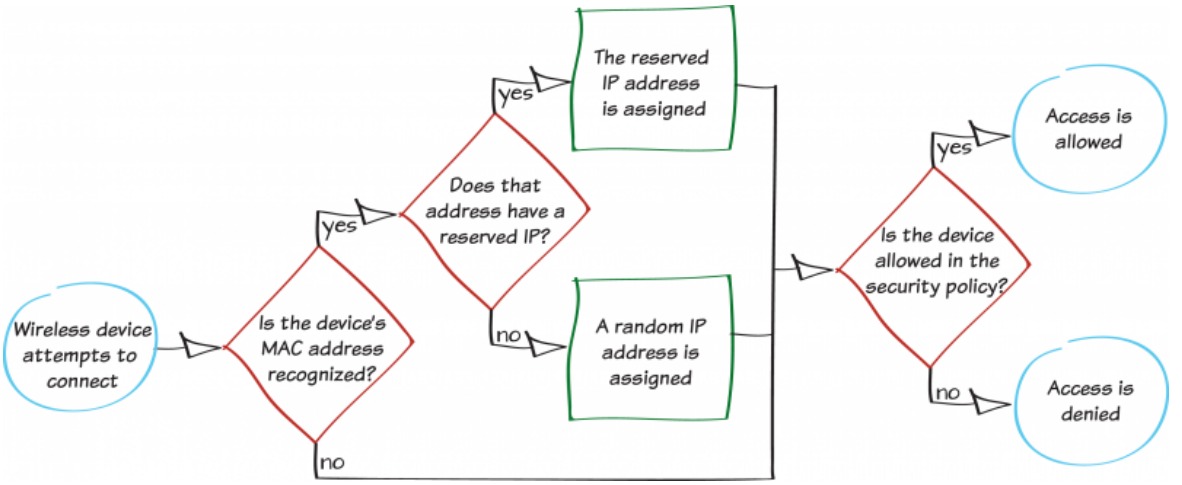
Results

Go to **WiFi Controller > Monitor > Client Monitor** to see that clients connect and authenticate.

SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx
example-staff	FP221C3X14019926 (2)	rgreen	10.10.12.2	08:fd:0e:ff:0c:56	165	10.18 Kbps

For further reading, check out the Deploying Wireless Networks in the FortiOS 5.2 Handbook.

MAC access control



In this example, you will add device definitions to your FortiGate using Media Access Control (MAC) addresses. These definitions are then used to determine which devices can access the wireless network.

By using a MAC address for identification, you will also be able to assign a reserved IP for exclusive use by the device when it connects to the wireless network.

Warning: Since MAC addresses can be easily spoofed, using MAC access control should not be considered a security measure.

1. Finding the MAC address of a device

The instructions below were written for the most recent OS versions. Older versions may use different methods.

For Windows devices:

Open the command prompt and type `ipconfig /all`

This output displays configuration information for all of your network connections. Look for the information about the wireless adapter and take note of the **Physical Address**.

```
Wireless LAN adapter Wireless Network Connection 3:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : 802.11n USB Wireless LAN Card
   Physical Address. . . . . . . . . : C8-3A-35-C4-2F-B7
   DHCP Enabled. . . . . . . . . . . : Yes
```

For Mac OS X devices:

Open **Terminal** and type `ifconfig en1 | grep ether`.

Take note of the displayed MAC address.

```
drs:~ [illegible] ifconfig en1 | grep ether
        ether c8:bc:c8:de:26:3c
```

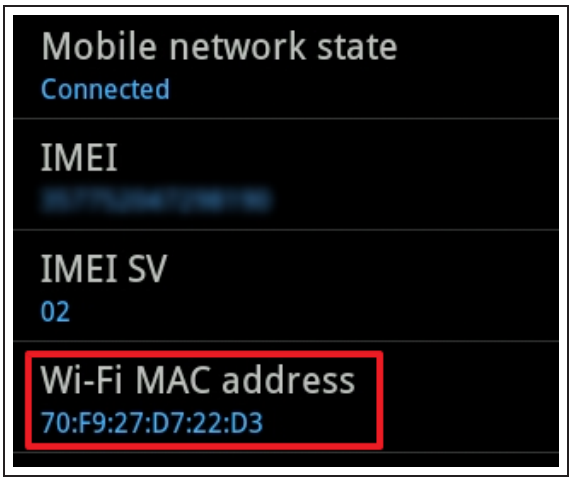
For iOS devices:

Open **Settings > General** and take note of the **Wi-Fi Address**.

Version	[illegible]
Model	[illegible]
Serial Number	[illegible]
Wi-Fi Address	B0:34:95:C2:EF:D8

For Android devices:

Open **Settings > More > About Device > Status** and take note of the **Wi-Fi MAC address**.



2. Defining a device using its MAC address

Go to **User & Device > Device > Device Definitions** and create a new device definition.

Set MAC Address to the address of the device and set the other fields as required. In the example, a device definition is created for an iPhone with the MAC Address B0:34:95:C2:EF:D8.

The new definition will now appear in your device list.

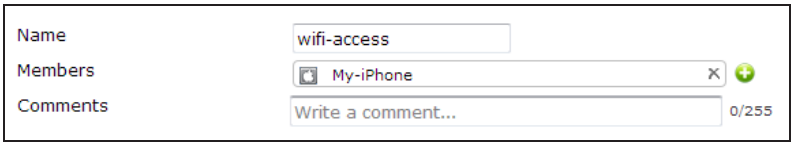
If you have enabled device identification on the wireless interface, device definitions will be created automatically. You can then use MAC addresses to identify which device a definition refers to.

Status	Device	OS	IP Address
Online	My-Desktop	Windows	10.10.80.3
Offline	My-Android	Android / 2.2.2	10.10.80.4
Offline	My-iPhone	iPod / iOS	10.10.80.7
Offline	My-Netbook	Windows	10.10.80.5
Offline	My-Printer	Linux	10.10.80.6

3. Creating a device group

Go to **User & Device > Device > Device Groups** and create a new group.

Add the new device to the **Members** list.

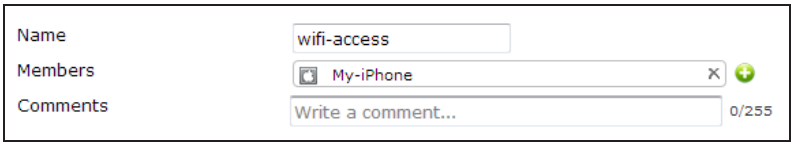


4. Reserving an IP address for the device

Go to **System > Network > Interfaces** and edit the wireless interface.

If the FortiAP is in bridge mode, you will need to edit the internal interface.

Under **DHCP Server**, expand **Advanced**. Create a new entry in the **MAC Reservation + Access Control** list that reserves an IP address within the DHCP range for the device's MAC address.

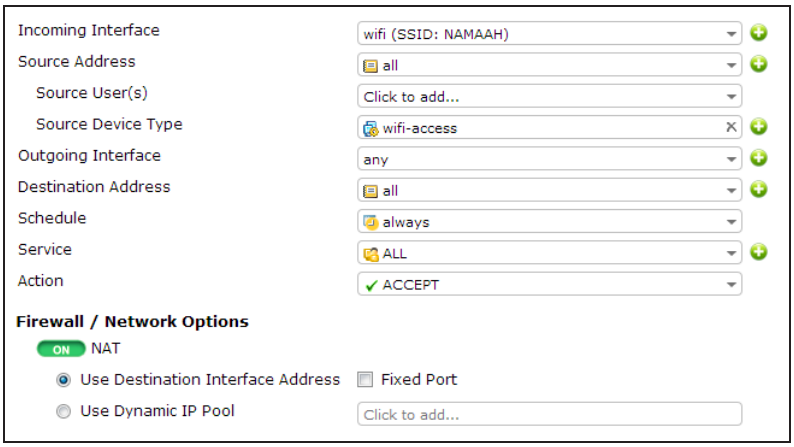


5. Creating a security policy for wireless traffic

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to your wireless interface, **Source Device Type** to the device group, and **Outgoing Interface** to the Internet-facing interface.

Ensure that **NAT** is turned on.

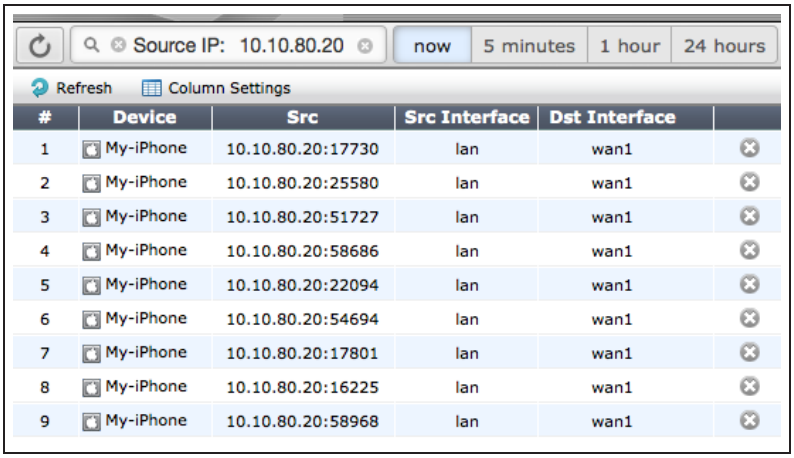


6. Results

Connect to the wireless network with a device that is a member of the device group. The device should be able to connect and allow Internet access.

Connection attempts from a device that is not a group member will fail.

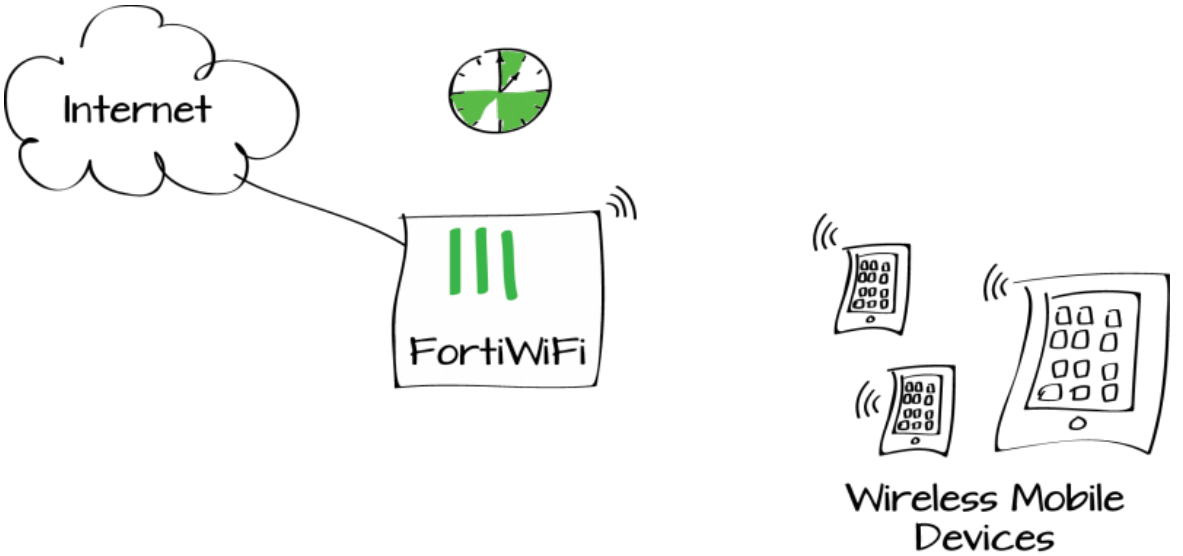
Go to **System > FortiView > All Sessions** and view the results for now. Filter the results using the reserved **Source IP** (in the example, 10.10.80.20), to see that it is being used exclusively by the wireless device.



#	Device	Src	Src Interface	Dst Interface
1	My-iPhone	10.10.80.20:17730	lan	wan1
2	My-iPhone	10.10.80.20:25580	lan	wan1
3	My-iPhone	10.10.80.20:51727	lan	wan1
4	My-iPhone	10.10.80.20:58686	lan	wan1
5	My-iPhone	10.10.80.20:22094	lan	wan1
6	My-iPhone	10.10.80.20:54694	lan	wan1
7	My-iPhone	10.10.80.20:17801	lan	wan1
8	My-iPhone	10.10.80.20:16225	lan	wan1
9	My-iPhone	10.10.80.20:58968	lan	wan1

For further reading, check out Managing "bring your own device" in the FortiOS 5.2 Handbook.

BYOD scheduling



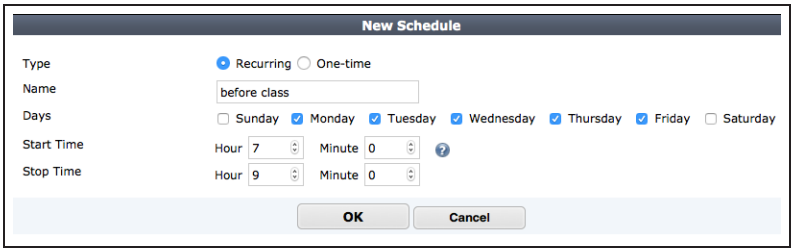
In this example, a school blocks Internet access to mobile devices during class time (9am - 12pm and 1pm - 3pm).

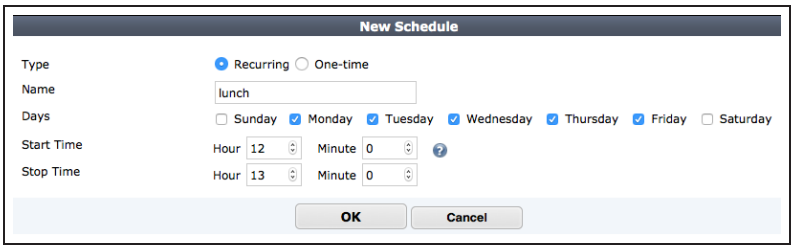
This recipe shows how to use a schedule group and a BYOD device policy to permit mobile device Internet access before and after class time and during lunch. The school is open from 7am to 6pm.

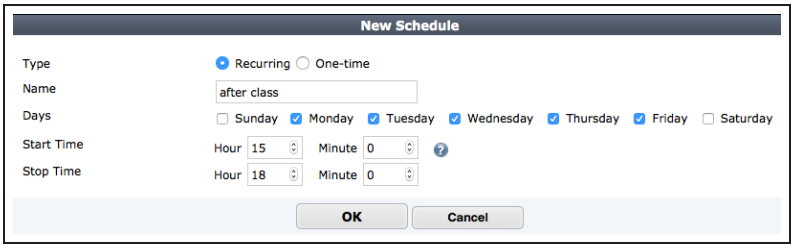
]In this example a FortiWiFi unit provides the wireless network. The steps are the same if the wireless network is provided by FortiAP with a FortiGate as a wireless controller.

1. Creating schedules and a schedule group

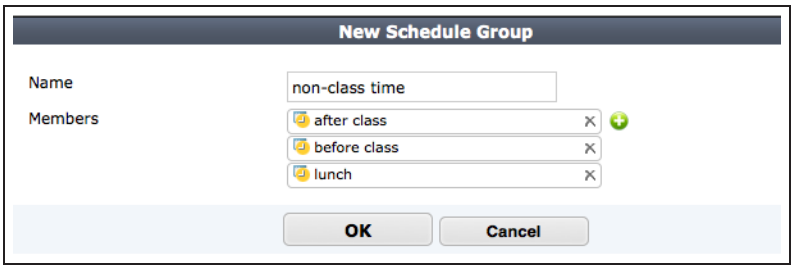
Go to **Policy & Objects > Objects > Schedules**. Create recurring schedules for
the before class (7-9 am), lunch (12-1 pm), and
after class (3-6 pm) periods.







Select **Create New > Schedule Group** and add create the schedule group by adding the outside of class time schedules to a schedule group.

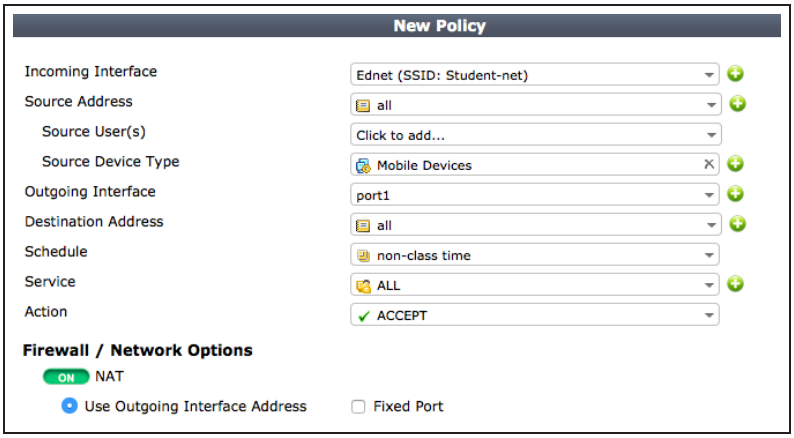


2. Creating a policy to block mobile devices outside of class time

Go to **Policy & Objects > Policy > IPv4** and create a policy that allows Internet access for mobile devices on the Student-net wireless network according to the schedule.

Set **Incoming Interface** to the wireless interface, **Source Device Type** to **Mobile Devices** (a default device group that includes tablets and mobile phones), **Outgoing Interface** to the Internet-facing interface, and set **Schedule** to the new schedule group.

Using a device group will automatically enable device identification on the wireless interface.



3. Results

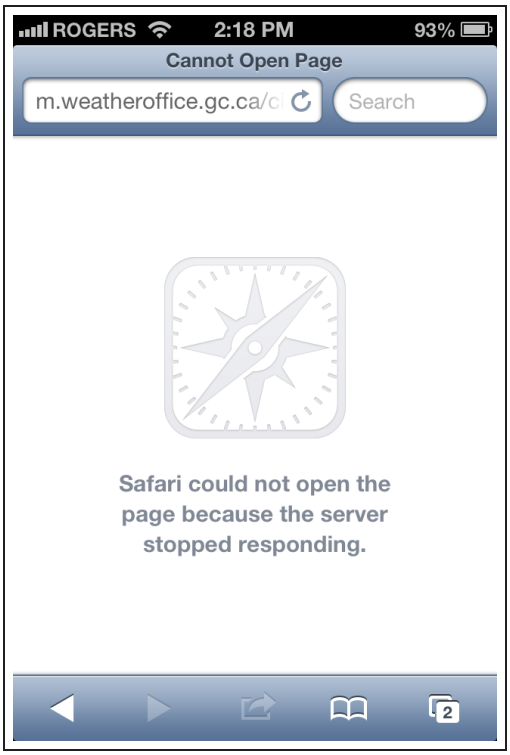
Verify that mobile devices can connect to the Internet outside of class time, when the schedule group is valid.

Go to **Log & Report > Traffic Log > Forward Traffic** to view mobile device traffic.

#	Date/Time	Src	Device	Dst
161	17:00:48	20.10.10.40	Android Phone	8.8.8.8
162	15:00:28	20.10.10.40	Android Phone	216.250.166.65
163	12:58:38	20.10.10.40	Android Phone	65.55.172.252
164	12:48:26	20.10.10.41	iPad	17.172.208.30
165	7:44:46	20.10.10.41	iPad	8.8.8.8

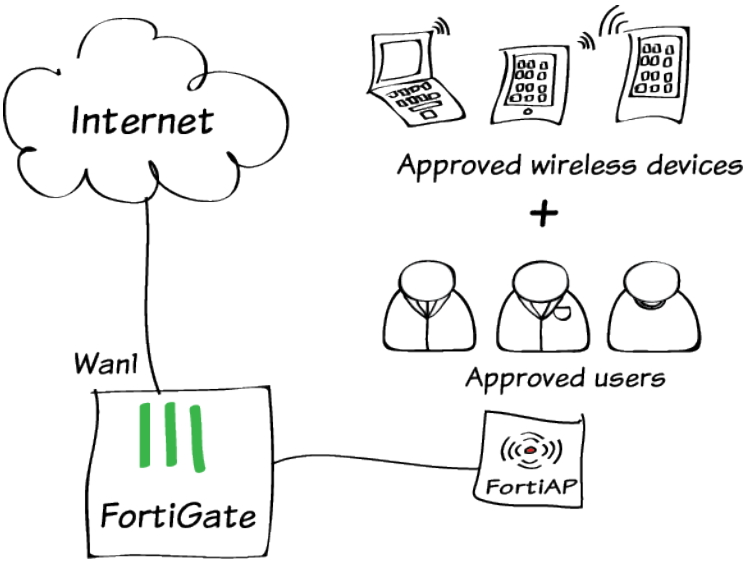
When the time in the schedule is reached, further surfing cannot continue.

This traffic does not appear in the logs, as only allowed traffic is logged.



For further reading, check out Managing "bring your own device" in the FortiOS 5.2 Handbook.

BYOD for a user with multiple wireless devices



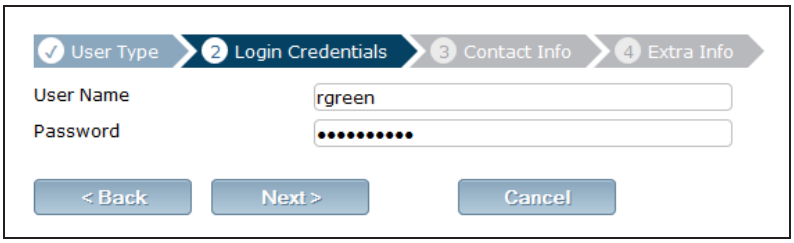
In this example, you will make a FortiOS security policy that requires both user and device authentication, so that known users can only access the network when they are using known devices.

Using a combination of user and device authentication improves security in BYOD environments. Any authenticated user can connect through wireless, using any wireless device that is included in the device group specified in the policy. Thus, the BYOD policy can even support a user with multiple devices.

1. Create users and a user group

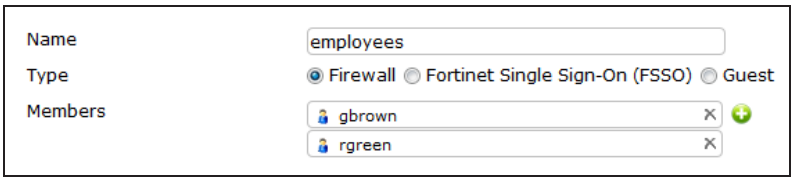
Go to **User & Device > User > User Definition** and create a Local user.

Create additional users as needed. You can use any authentication method.



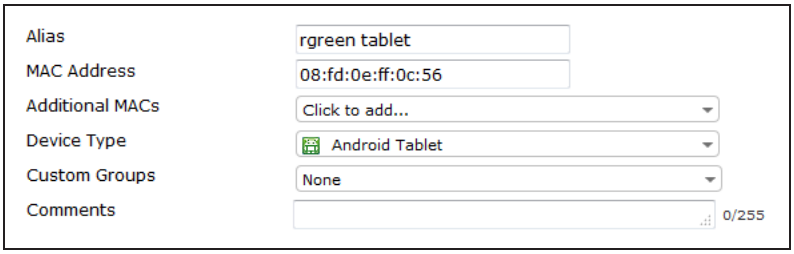
Go to **User & Device > User > User Groups**.

Create a user group for employees and add the new user(s) to the group.



2. Create devices and a device group

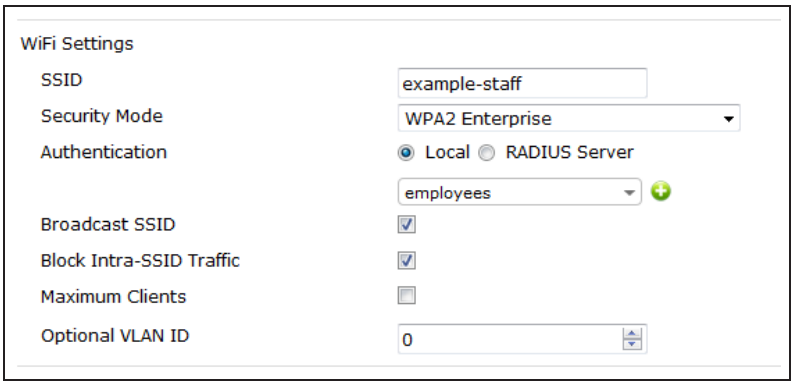
Go to **User & Device > Device > Device Definitions** and enter the user's device information.



Go to **User & Device > Device > Device Groups**. Create a device group and add user's devices to it.

3. Configure WiFi security

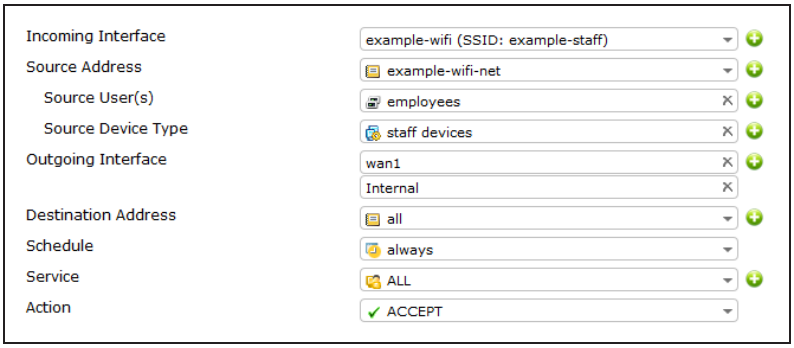
Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network for WPA-Enterprise authentication using the employees user group.



4. Create the security policy

Go to **Policy & Objects > Policy > IPv4** and create a policy to enable traffic from the WiFi interface to the Internet (in the example, *wan1*) and office LAN (in the example, *Internal*) interfaces.

Restrict the policy to allow only the employees user group and device group.



5. Results

User **rgreen** can connect to the Internet using the **rgreen tablet** that belongs to the **staff devices** group.

Go to **Policy & Objects > Monitor > Policy Monitor** to see the security policy in use.

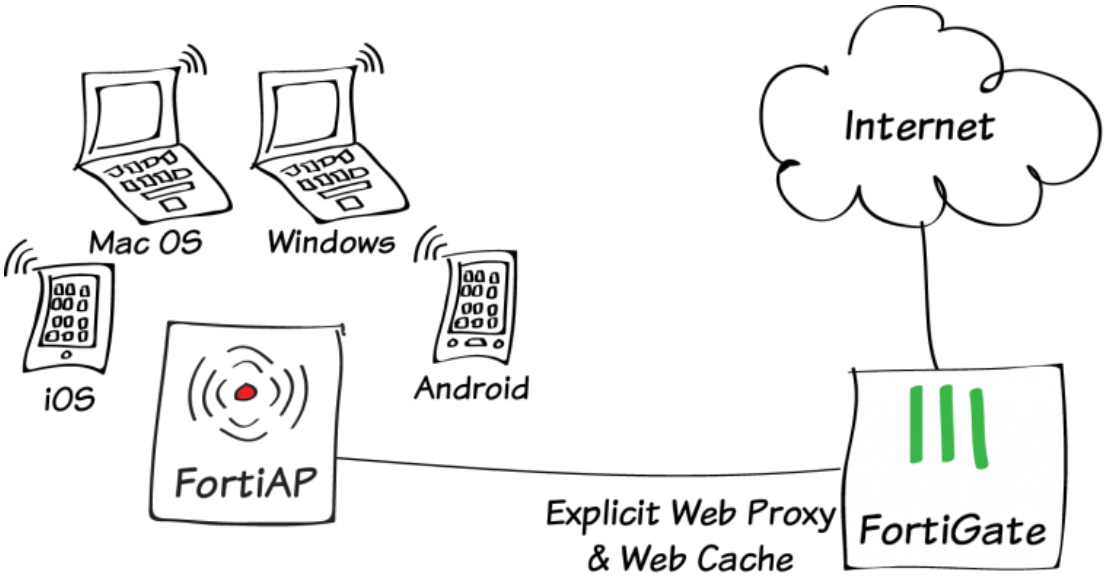
Policy ID	Source Interface/Zone	Destination Interface/Zone	Action	Active Sessions	Bytes	Packets
4	example-wifi	wan1, Internal	✓	30	79.12 MB	124,095

Attempts to access the Internet fail if any of the following are true:

- the user does not belong to the employees user group
- the device does not belong to the staff devices group

For further reading, check out Deploying Wireless Networks in the FortiOS 5.2 Handbook.

Explicit proxy with web caching



In this example, you will add explicit proxy with web caching to your wireless network.

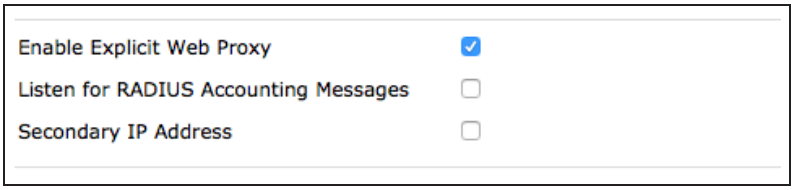
All devices on the wireless network will be required to connect to the proxy at port 8080 before they can browse web pages on the Internet. WAN Optimization web caching is added to reduce the amount of Internet bandwidth used and improve web browsing performance.

A video of this recipe is available here.

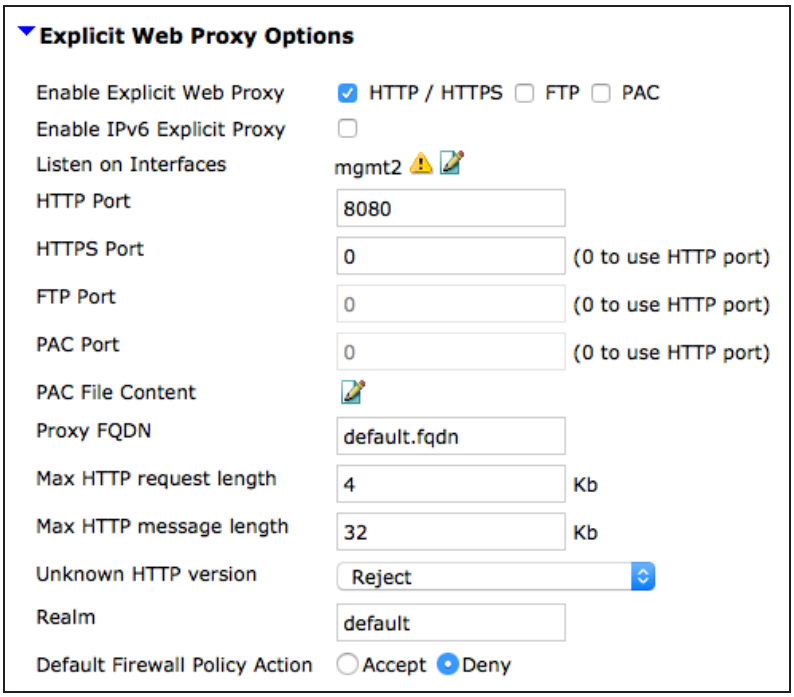
1. Enabling WAN Optimization and configuring the explicit web proxy for the wireless interface

Go to **System > Config > Features**. Ensure that **Explicit Proxy** and **WAN Opt & Cache** are enabled.

Go to **System > Network > Interfaces**, edit the wireless interface and select **Enable Explicit Web Proxy**.

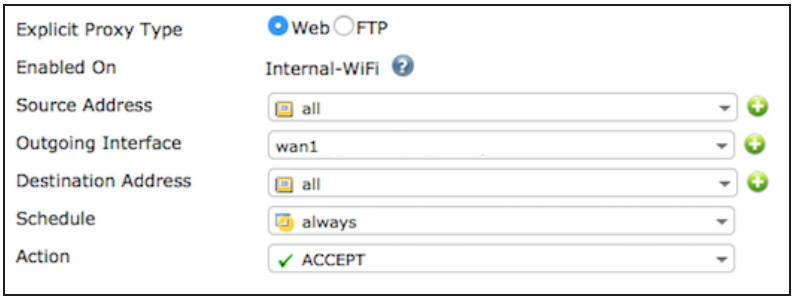


Go to **System > Network > Explicit Proxy**. Select **Enable Explicit Web Proxy** for **HTTP/HTTPS**. Make sure that **Default Firewall Policy Action** is set to **Deny**.



2. Adding an explicit web proxy policy

Go to **Policy & Objects > Policy > Explicit Proxy** and create a new policy. Set **Explicit Proxy Type** to **Web** and the **Outgoing Interface** to the Internet-facing interface.



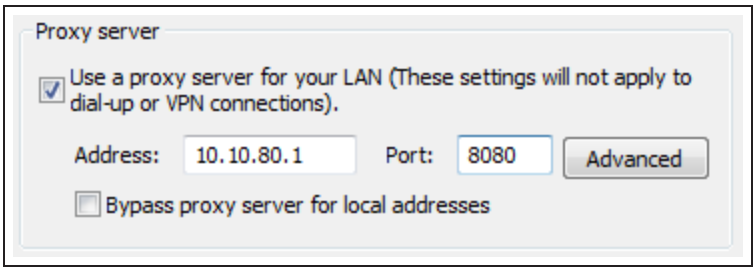
Turn on **Web Cache**.

3. Configuring devices on the wireless network to use the web proxy

To use the web proxy, all devices on the wireless network must be configured to use the explicit proxy server. The IP address of the server is the IP address of the FortiGate's wireless interface (in the example, *10.10.80.1*) and the port is 8080. Some browsers may have to be configured to use the device's proxy settings.

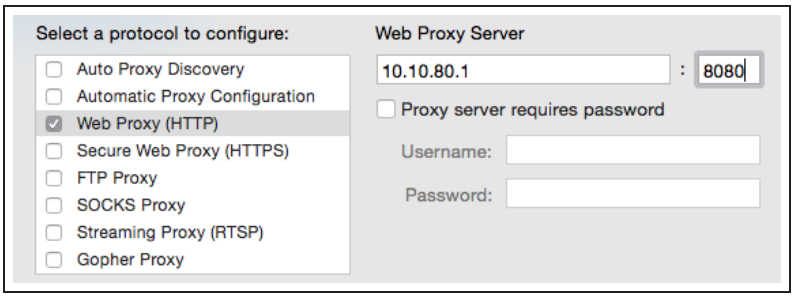
Windows Vista/7/8:

Open **Internet Properties**. Go to **Connections > LAN Settings** and enable and configure the **Proxy Server**.



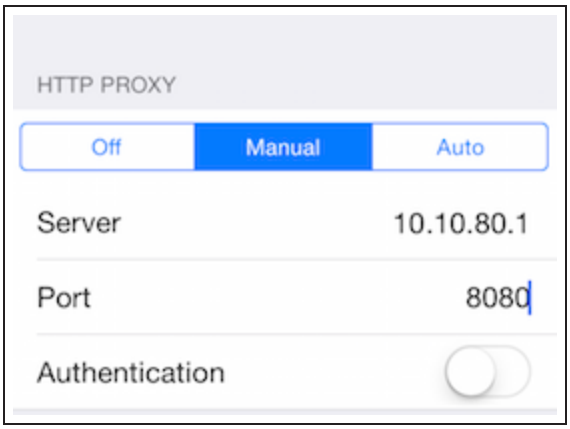
Mac OS X:

Open **Network Preferences > Wi-Fi > Advanced > Proxies**. Select **Web Proxy (HTTP)** and configure the proxy settings.



iOS:

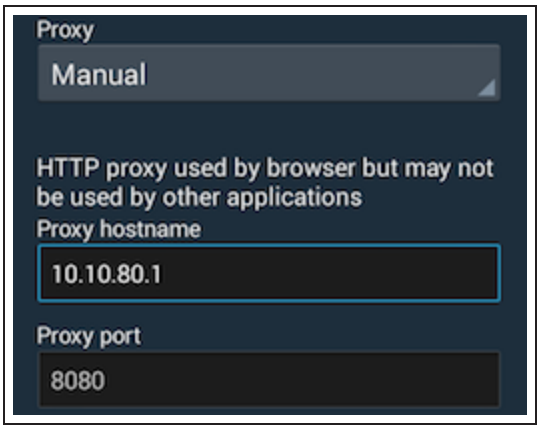
Go to **Settings > Wi-Fi**. Edit the wireless network. Scroll down to **HTTP PROXY** select **Manual** and configure the proxy settings.



Android:

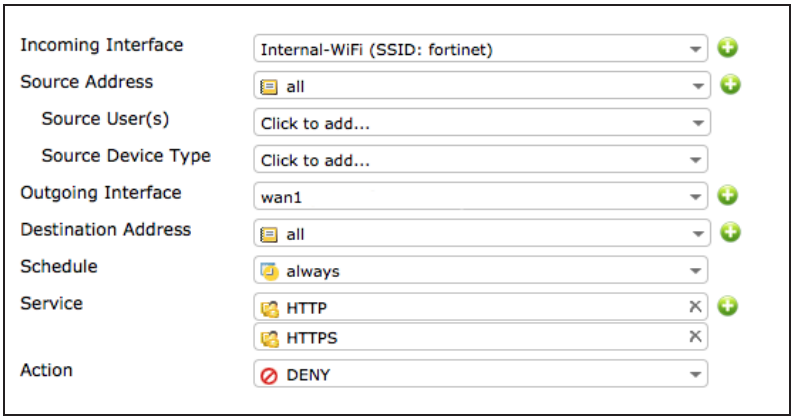
In WiFi network connection settings, edit the wireless network. Select **Show advanced options,** configure a **Manual** proxy and enter the proxy settings.

s



4. Force HTTP and HTTPS traffic to use the Web Proxy

Block HTTP and Replace...HTTPS access to the Internet from the wireless network so that the only path to the Internet is through the explicit proxy. You can edit or delete policies that allow HTTP or HTTPS access. You can also add a policy to the top of the list that **Denies** HTTP and HTTPS traffic.

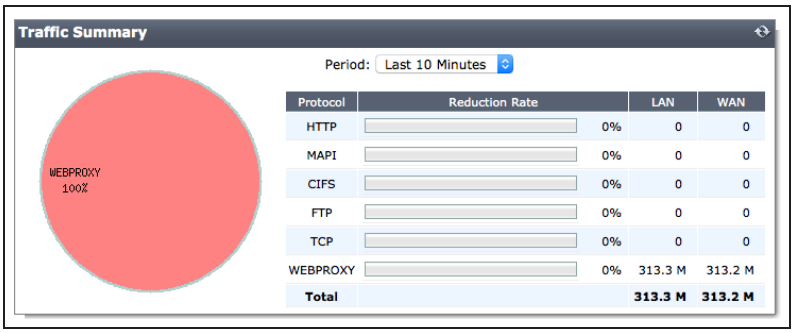


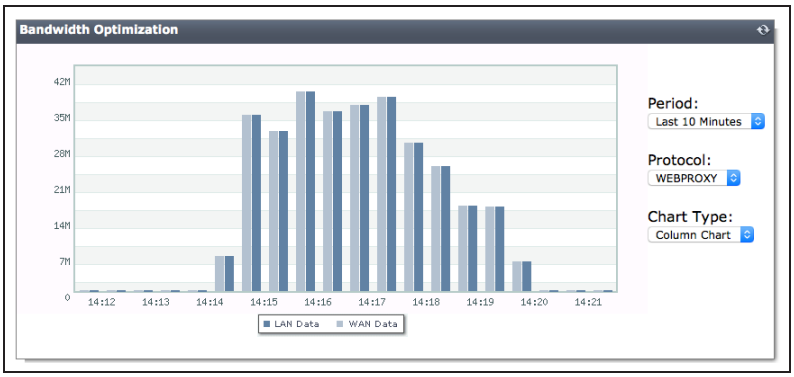
5. Results

To confirm that the proxy is processing traffic, attempt to connect to the Internet from the Wireless network using a device that has not been configured to connect to the proxy. Access should be blocked.

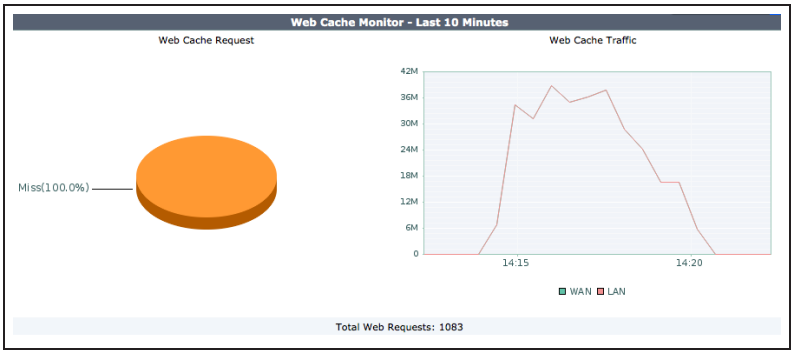
Configure the device to use the proxy. You should now be able to connect to the Internet.

Go to **WAN Opt. & Cache > Monitor > WAN Opt. Monitor** to view **WEBPROXY** traffic in the **Traffic Summary**.Check the **Bandwidth Optimization** graph for WEBPROXY traffic.





Go to **WAN Opt. & Cache > Monitor > Cache Monitor** to view web caching activity.



For further reading, check out The FortiGate explicit web proxy in the FortiOS 5.2 Handbook.

Authentication

This section contains information about authenticating users and devices.

Authentication, the act of confirming the identity of a person or device, is a key part of network security. When authentication is used, the identities of users or host computers must be established to ensure that only authorized parties can access the network.

User accounts and device definitions

- User and device authentication
- Excluding users from security scanning
- MAC access control
- BYOD scheduling
- BYOD for a user with multiple wireless devices
- FSSO in Polling mode

Authentication and security

- Web filtering using quotas
- Blocking and monitoring Tor traffic

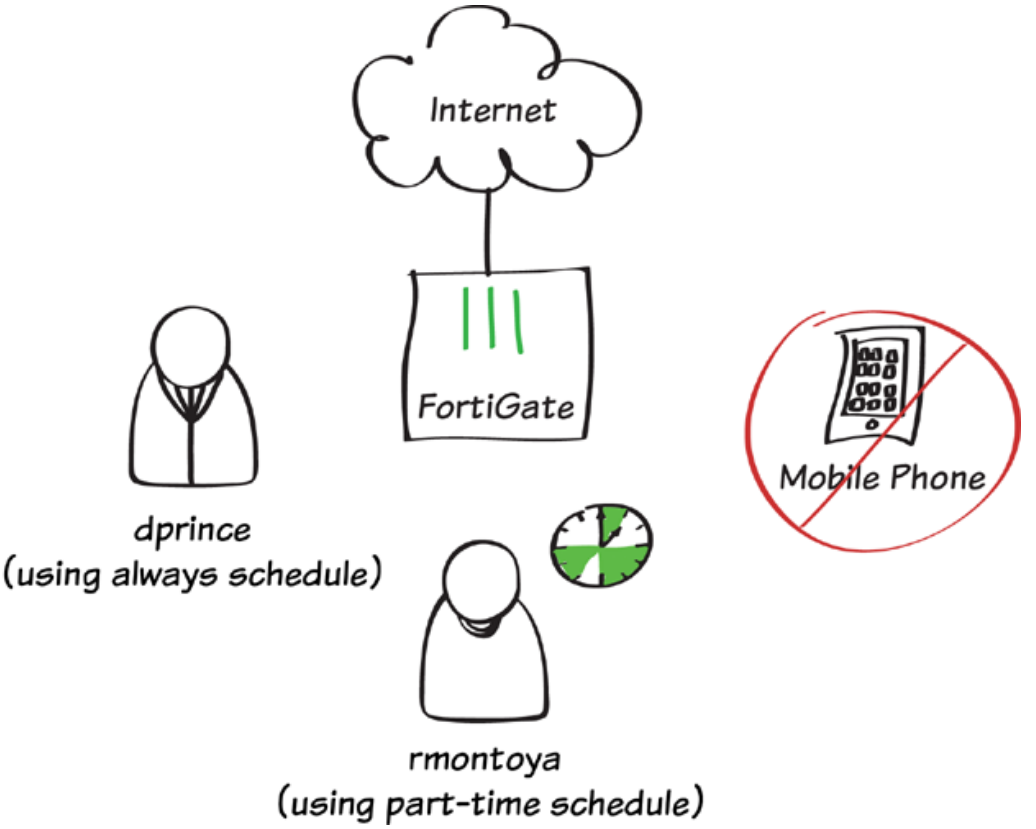
WiFi authentication

- Captive portal WiFi access control
- WP2A WiFi access control
- WiFi with external RADIUS authentication

Authentication with other technologies

- Two-factor authentication with FortiToken Mobile

User and device authentication



In this example, user authentication and device authentication provide different access for staff members based on whether they are full-time or part-time employees, while denying all traffic from mobile phones.

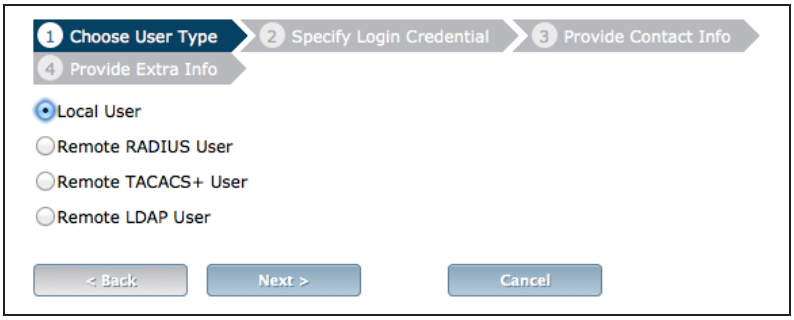
In this example, a wireless network has already been configured that is in the same subnet as the wired LAN. For information about this configuration, see Setting up a WiFi bridge with a FortiAP.

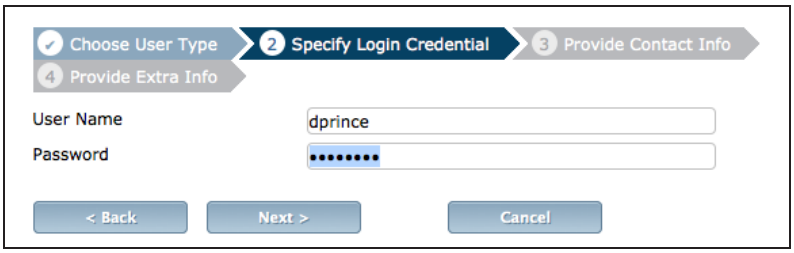
A video of this recipe can be found here.

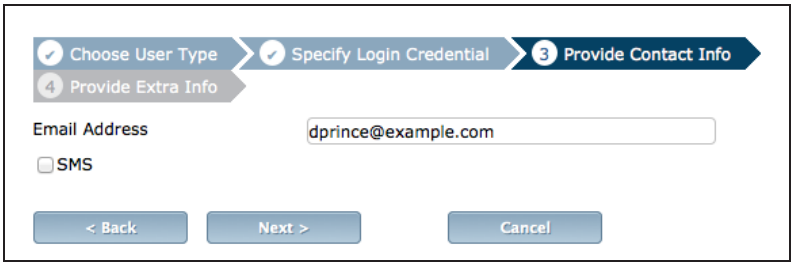
1. Defining two users and two user groups

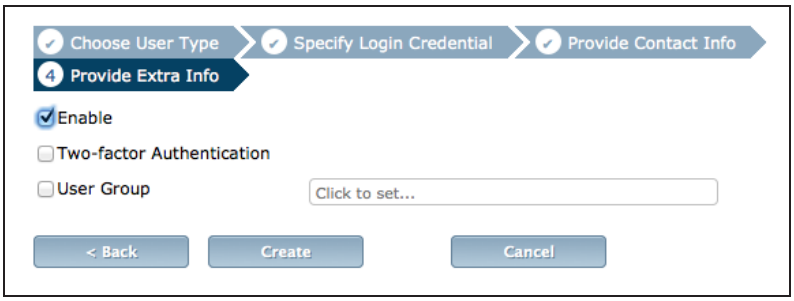
Go to **User & Device > User > User Definitions**.

Create two new users (in the example, *dprince* and *rmontoya*).









Both user definitions now appear in the user list.

User Name	Type	Two-factor Authentication	Ref.
dprince	LOCAL		0
guest	LOCAL		1
rmontoya	LOCAL		0

Go to **User & Device > User > User Groups**.

Create the user group *full-time* and add user *dprince*.

Name: full-time
Type: Firewall / Fortinet Single Sign-On (FSSO) / Guest / RADIUS Single Sign-On (RSSO)
Members: dprince

Create a second user group, *part-time*, and add user *rmontoya*.

Name: part-time
Type: Firewall / Fortinet Single Sign-On (FSSO) / Guest / RADIUS Single Sign-On (RSSO)
Members: rmontoya

2. Creating a schedule for part-time staff

Go to **Policy & Objects > Objects > Schedules** and create a new recurring schedule.

Set an appropriate schedule. In order to get results later, do not select the current day of the week.

Type: Recurring / One-time
Name: part-time
Days: Sunday / Monday / Tuesday / Wednesday / Thursday / Friday / Saturday
Start Time: Hour 0 Minute 0
Stop Time: Hour 0 Minute 0

3. Defining a device group for mobile phones

Go to **User & Device > Device > Device Groups** and create a new group.

Add the various types of mobile phones as **Members**.

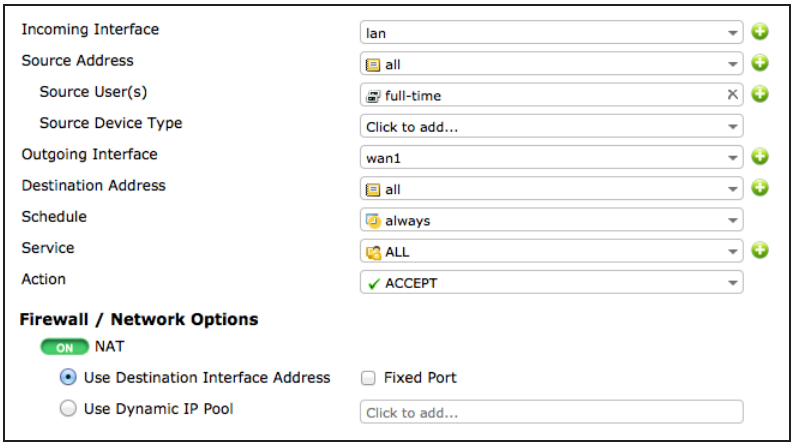
Name: mobile-phones
Members: Android Phone, BlackBerry Phone, Windows Phone, iPhone
Comments: Write a comment... 0/255

4. Creating a policy for full-time staff

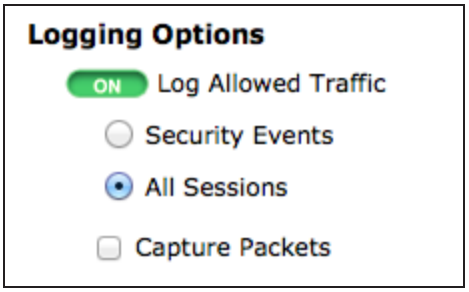
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source User(s)** to the full-time group, **Outgoing Interface** to your Internet-facing interface, and ensure that **Schedule** is set to **always**.

Turn on **NAT**.



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

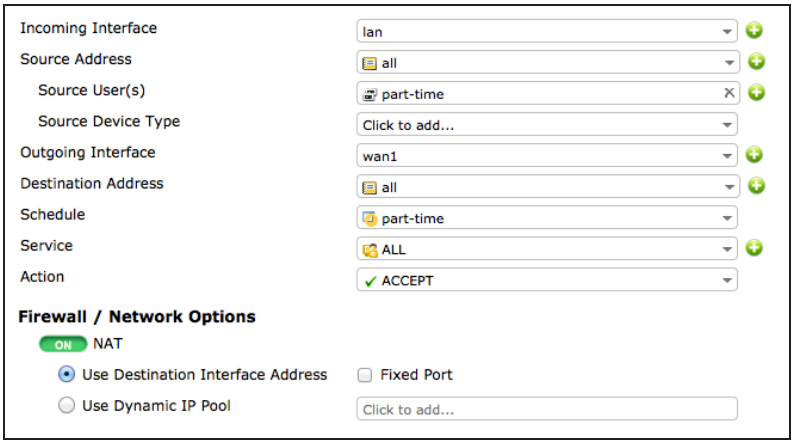


5. Creating a policy for part-time staff that enforces the schedule

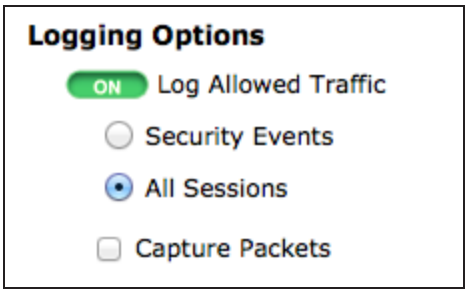
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source User(s)** to the part-time group, **Outgoing Interface** to your Internet-facing interface, and set **Schedule** to use the part-time schedule.

Turn on **NAT**.



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



View the policy list. Click on the title row and select **ID** from the dropdown menu, then select **Apply**. Take note of the ID number that has been given to the part-time policy.

Seq.#	From	To	Schedule	Source	Destination	ID
1	lan	wan1	always	all full-time	all	1
2	lan	wan1	part-time	all part-time	all	2
3	any	any	always	all	all	

Go to **System > Dashboard > Status** and enter the following command into the **CLI Console**, using the ID number of the part-time policy.

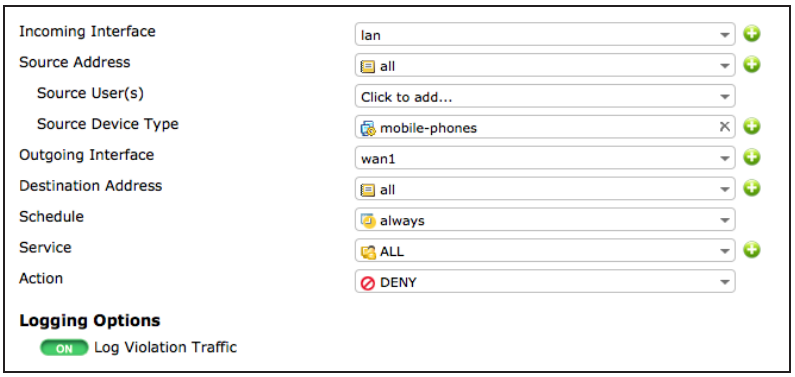
```
config firewall policy
   edit 2
     set schedule-timeout enable
   end
 end
```

This will ensure that part-time users will have their access revoked during days they are not scheduled, even if their current session began when access was allowed.

6. Creating a policy that denies mobile traffic

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source Device** to **Mobile Devices** (a default device group that includes tablets and mobile phones), **Outgoing Interface** to your Internet-facing interface, and set **Action** to **DENY**.



Using a device group will automatically enable device identification on the local

network interface.

Leave **Log Violation Traffic** turned on.

In order for this policy to be used, it must be located at the top of the policy list. Select any area in the far-left column of the policy and drag it to the top of the list.

Seq.#	From	To	Devices	Groups	Action
3	lan	wan1	Mobile Devices		DENY
1	lan	wan1		full-time	✓ ACCEPT
2	lan	wan1		part-time	✓ ACCEPT
4	any	any			DENY

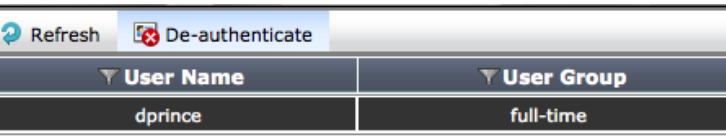
7. Results

Browse the Internet using a computer. You will be prompted to enter authentication credentials.

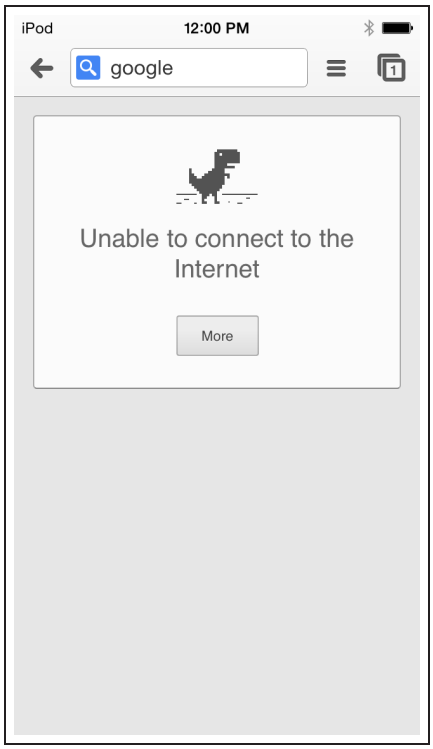
Log in using the *dprince* account. You will be able to access the Internet at any time.

Go to **User & Device > Monitor > Firewall**. Highlight **dprince** and select **De-authenticate**.

Attempt to browse the Internet again. This time, log in using the *rmontoya* account. After authentication occurs, you will not be able to access the Internet.



Attempts to connect to the Internet using any mobile phone will also be denied.



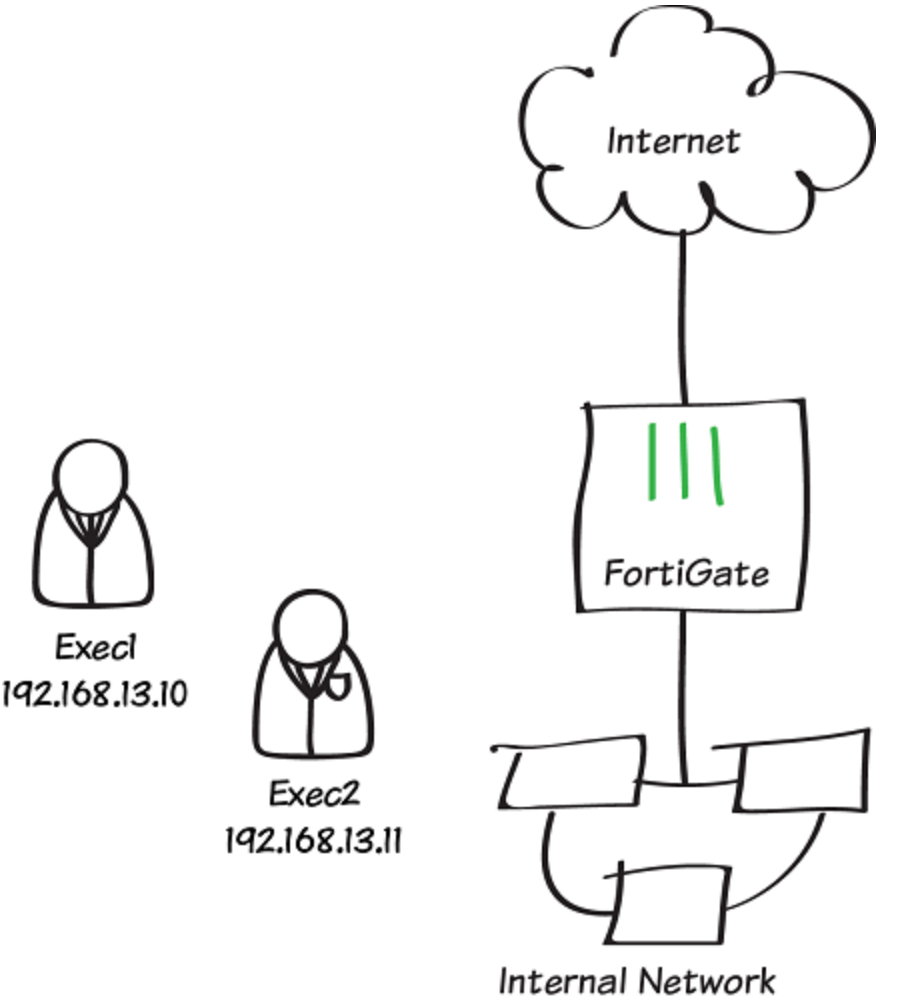
You can view more information about the blocked and allowed sessions by going to **System > FortiView > All Sessions.**

*Sessions that were blocked when you attempted to sign in using the rmontoya account will not have a user account shown in the **User** column.*

Date/Time	User	Device	Destination	Action
09:10:21		iPhone	208.91.112.53	deny
09:10:21		Mac Mini	157.55.56.159	deny
09:10:21		Mac Mini	111.221.74.30	deny
09:10:21		Mac Mini	111.221.77.159	deny
09:10:21		iPhone	208.91.112.52	deny
09:10:20		iPhone	208.91.112.53	deny
09:10:20		iPhone	208.91.112.53	deny
09:10:19		Mac Mini	157.55.56.159	deny
09:10:19		Mac Mini	157.56.52.30	deny
09:10:17		iPhone	208.91.112.52	deny
09:10:17	dprince	Mac Mini	54.231.0.33 (s3-1-w.amazonaws.com)	accept
09:10:16	dprince	Mac Mini	54.231.0.33 (s3-1-w.amazonaws.com)	accept
09:10:16	dprince	Mac Mini	54.231.0.33 (s3-1-w.amazonaws.com)	accept
09:10:15	dprince	Mac Mini	64.94.107.34 (map-pb.quantserve.com.akadns.net)	accept
09:10:15	dprince	Mac Mini	174.36.240.82 (api.mixpanel.com)	accept

For further reading, check out Users and user groups in the FortiOS 5.2 Handbook.

Excluding users from security scanning



In this example, two company executives are excluded from the security scanning that a FortiGate applies to all other staff Internet traffic.

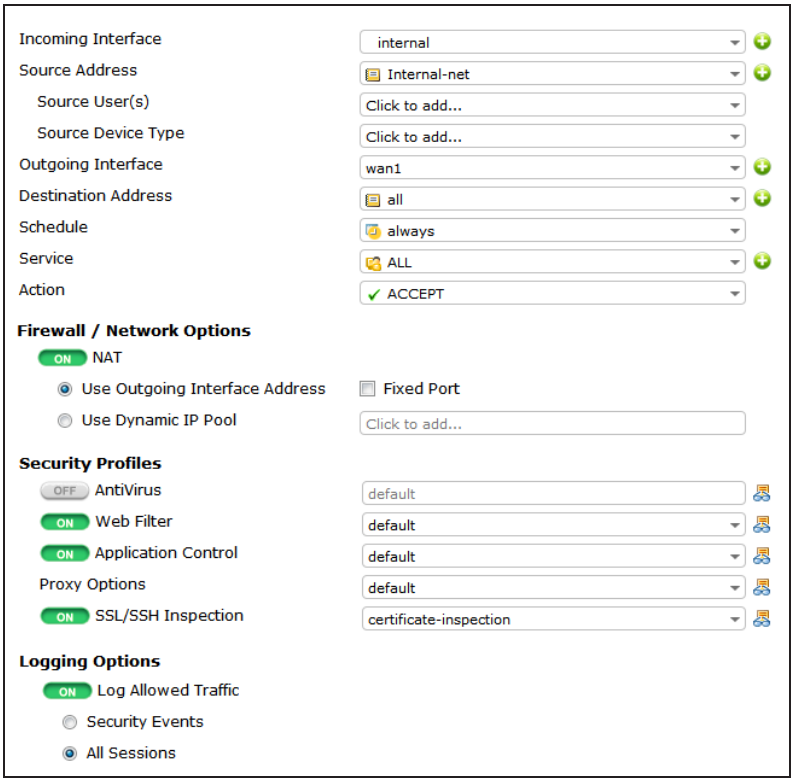
The executives in this example connect to the Internet using PCs with static IP addresses, so these addresses can be used to identify their traffic. If identifying users with a static IP address will not work for your network you can set up authentication or device identification (BYOD).

1. Applying security profiles to the staff policy

Go to **Policy & Objects > Policy > IPv4** and edit the general policy that allows staff to access the Internet.

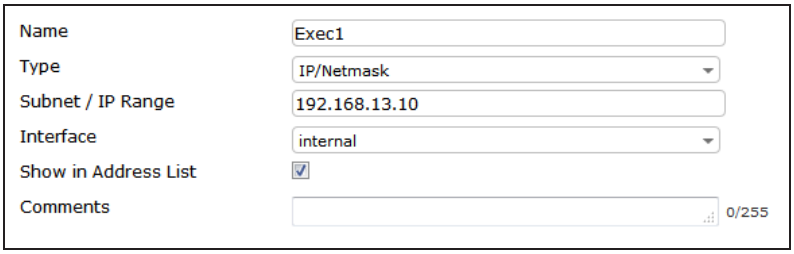
Under **Security Profiles**, enable **Web Filter** and **Application Control**. Set them to use the default profiles. Also set **SSL/SSH Insection** to the **deep-inspection** profile.

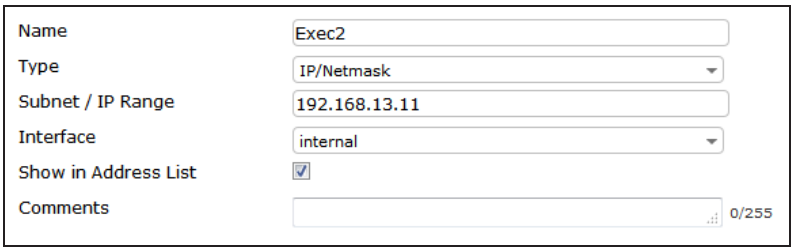
To be able to see results enable logging all sessions.



2. Creating firewall addresses for the executives

Go to **Policy & Objects > Objects > Addresses**. Create an address for each executive. Use /32 as the Netmask to ensure that the firewall address applies only to the specified IP.



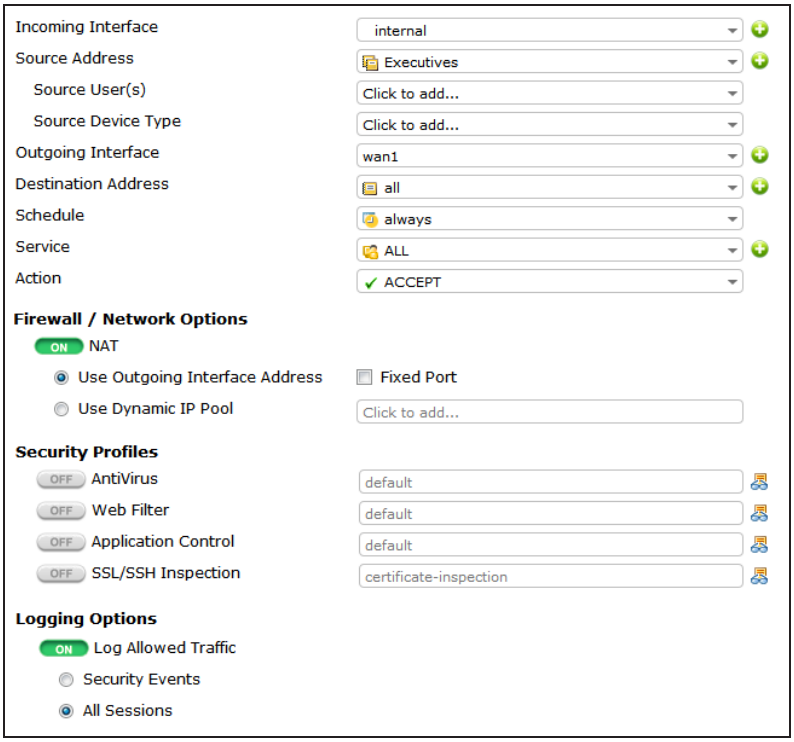


Select **Create New > Address Group** and create an address group for the executive addresses.

3. Creating a security policy for the executives

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing the executives to access the Internet. Set **Source Address** to **Executives**. Enable logging and select Log all Sessions to be able to view results.

Leave all Security Profiles disabled.



In the policy list, the policy for executives (in this example ID=3) must be above the policy for staff (in this example ID=2).

ID	Source	Destination	Schedule	Service	Action	NAT	AV	Web Filter	Application Control
internal - wan1 (2)									
3	Executives	all	always	ALL	✓ ACCEPT	Enable			
2	Internal-net	all	always	ALL	✓ ACCEPT	Enable		default	default

You can re-order policies by hovering your mouse cursor over the borders of the left-most cell of a policy until the cursor changes into crossed arrows and then clicking and dragging that policy up or down into the required order.

Note that in this screen shot the policy ID (**ID**) is shown for each policy and the sequence number (**Seq.#**) is hidden.

4. Results

Connect to the Internet from two computers on the internal network: one from an executive address and one from a staff address.

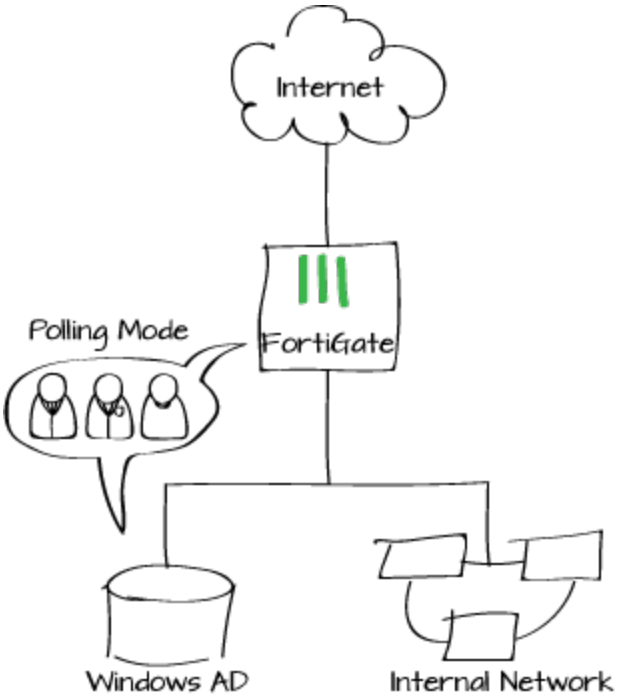
Go to **Log & Report > Traffic Log > Forward Traffic**. Right-click the column headings and make sure that the **Policy ID** column is visible.

In this example output, connections from 192.168.13.10 (an executive address) use policy ID 3 and connections from 192.168.13.144 (a staff address) use policy ID 2.

#	Policy ID	Date/Time	Source	Sent / Received
1	3	07:46:28	192.168.13.10	1.11 KB / 10.99 KB
2	3	07:46:28	192.168.13.10	1.10 KB / 9.13 KB
3	3	07:46:28	192.168.13.10	1.07 KB / 9.51 KB
4	3	07:46:28	192.168.13.10	1.16 KB / 12.48 KB
5	3	07:46:28	192.168.13.10	1.12 KB / 11.14 KB
6	2	07:45:48	192.168.13.144	8.41 KB / 10.79 KB
7	2	07:45:24	192.168.13.144	653 B / 4.99 KB
8	2	07:44:57	192.168.13.144	48 B / 0 B
9	2	07:44:47	192.168.13.144	2.51 KB / 1.28 KB
10	2	07:44:47	192.168.13.144	3.49 KB / 5.99 KB

For further reading, check out Security Profiles in the FortiOS 5.2 Handbook.

FSSO in Polling mode



In this example, you will configure Fortinet Single Sign-On (FSSO) directly in the security policy using the new FSSO wizard introduced in FortiOS 5.2.2.

This recipe requires that your FortiGate's DNS point to a DNS server that can resolve the IP addresses or fully qualified domain names of the users' PCs.

This example uses Active Directory polling to establish FSSO for a Windows AD Domain Controller, without requiring a FortiAuthenticator or a collector agent to act as an intermediary between the FortiGate and the domain. An LDAP server is also used for authentication.

A video of this recipe is available here.

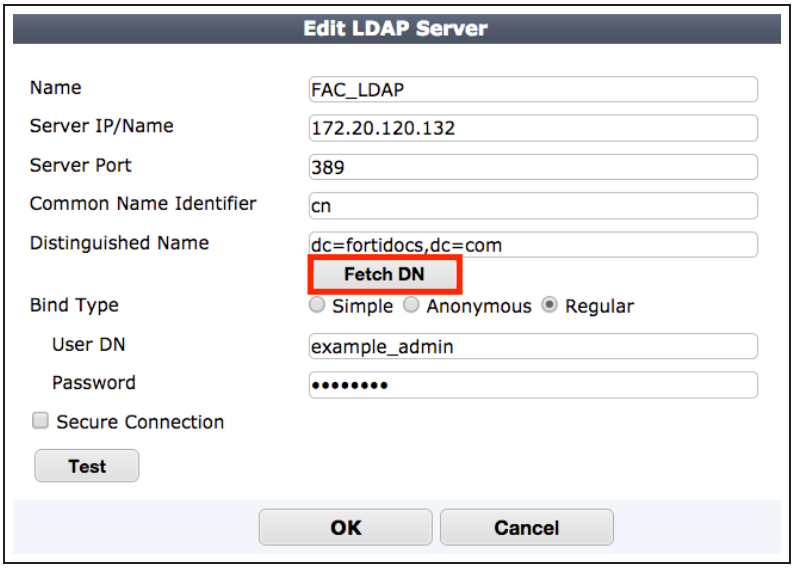
1. Adding the LDAP Server to the FortiGate

In the FortiGate web interface, go to **User & Device > Authentication > LDAP Servers**.

For the **Server IP/Name** enter the LDAP Server's fully qualified domain name or the IP address.

Set the **Bind Type** to **Regular** and enter a **User DN** and **Password**.

Click **Fetch DN** to retrieve your **Distinguished Name**.



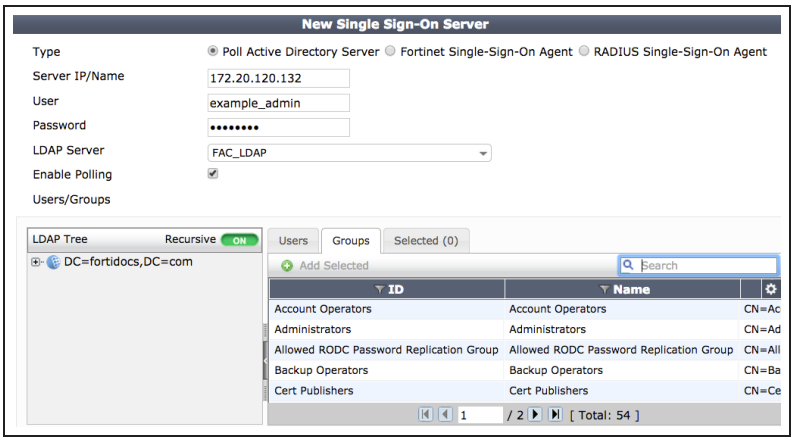
Click **Test** and verify that your connection is successful.

2. Configuring the FortiGate unit to poll the Active Directory

Next, go to **User & Device > Authentication > Single Sign-On** and add a new Single Sign-On Server.

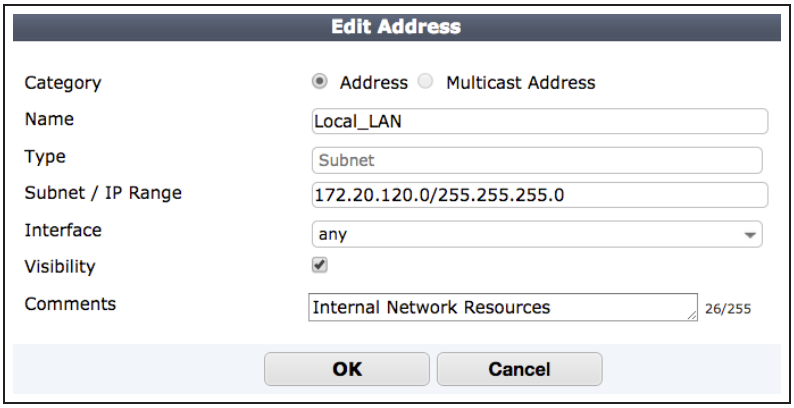
For the **Type**, select **Poll Active Directory Server**. Enter the **Server IP/Name**, **User**, and **Password**, then select the **LDAP Server** you added previously. Make sure **Enable Polling** is checked. Add a test user group of your choice.

You must add at least one user group to create your SSO server.



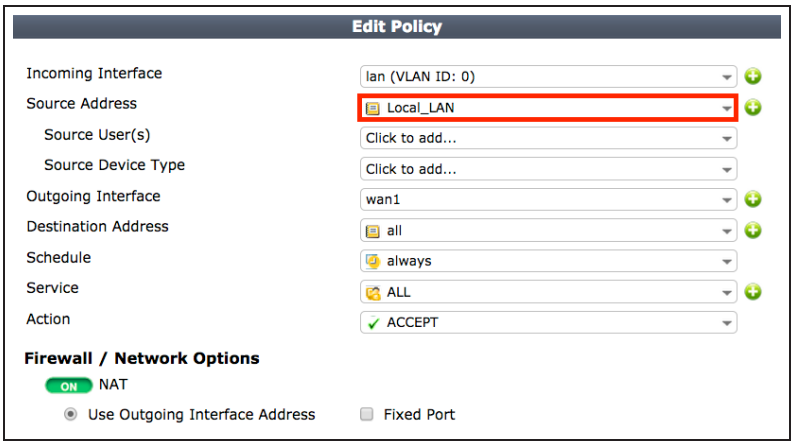
3. Adding a firewall address for the Internal network

Go to **Policy & Objects > Objects > Addresses** and create an internal network address to be used by your security policy.

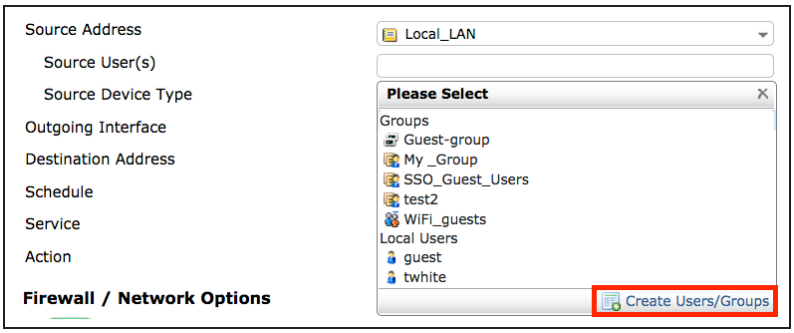


4. One-step FSSO configuration in the security policy

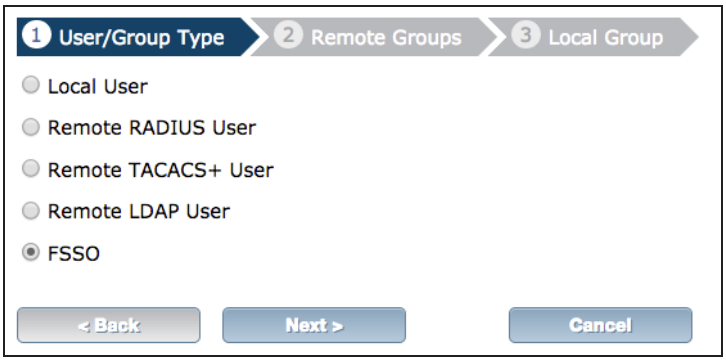
Go to **Policy & Objects > Policy > IPv4** and edit a security policy with access to the Internet. Set the **Source Address** to the **Local_LAN** address created in **Step 3**.



Under **Source User(s)** scroll down past the dropdown menu, and select **Create Users/Groups** wizard.



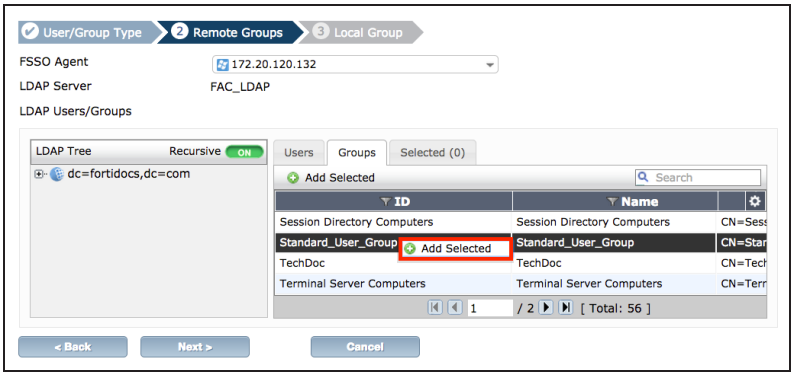
For the **User/Group Type,** select **FSSO** and then click **Next.**



For the **Remote Group**, select the appropriate **FSSO Agent** from the dropdown menu.

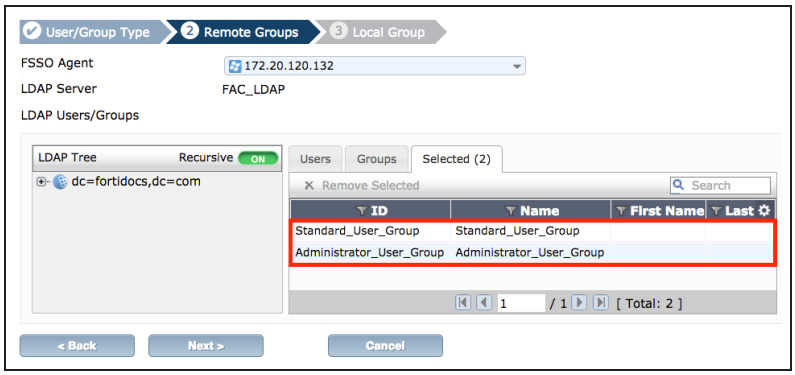
Select the **Groups** tab and right-click on the user groups you would like to add.

To add multiple groups, hold the Shift key and click.



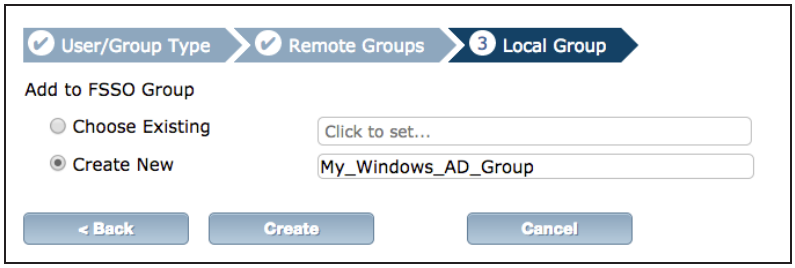
Go to the **Selected** tab. In this example, **Standard_User_Group** and **Admin_User_Group** are shown.

Click **Next**.



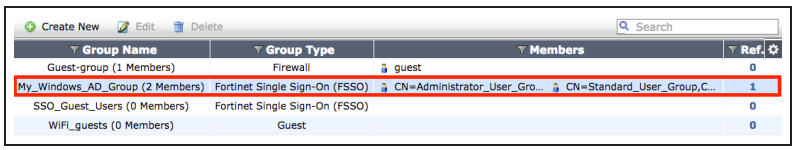
Select **Create New** and name your new FSSO user group.

Click **Create**.



The groups selected have been added to the new FSSO group, **My_Windows_AD_Group**.

*To see these groups go to **User & Device > User > User Groups.***

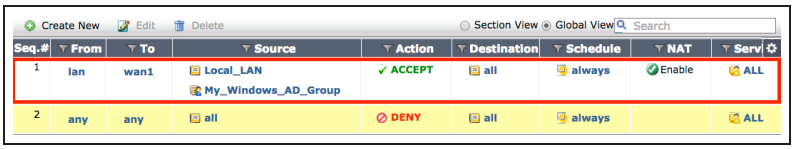


Ensure you enable logging and select **All Sessions**.

In the **Global View** your completed policy should look similar to the screenshot shown on the right.

If necessary, select the policy by clicking on the far left column, and move it as close as possible to the top of the list.

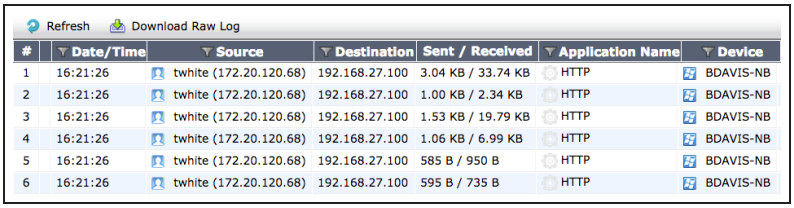
All other policies must deny Internet access in order for the user to be forced to authenticate.



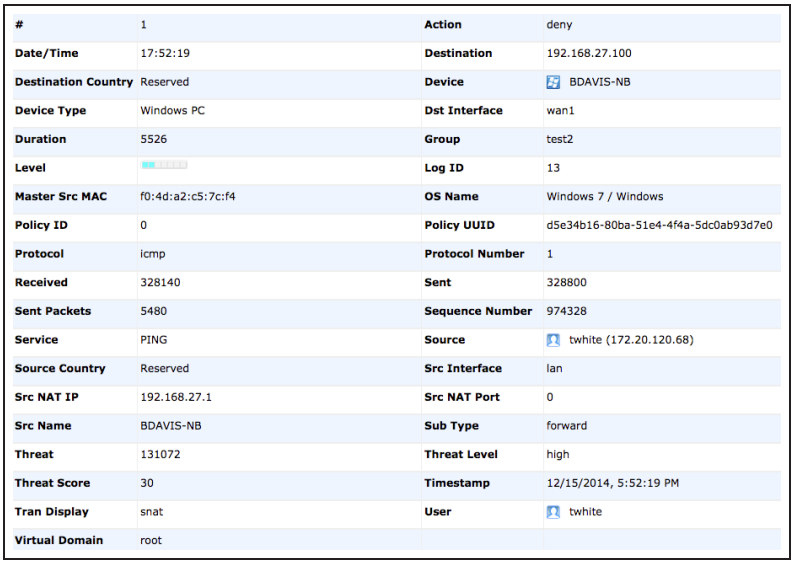
5. Results

Go to **Log & Report > Traffic Log > Forward Traffic**.

When users log into the Windows AD network, the FortiGate will automatically poll the domain for their account information, and record their traffic.

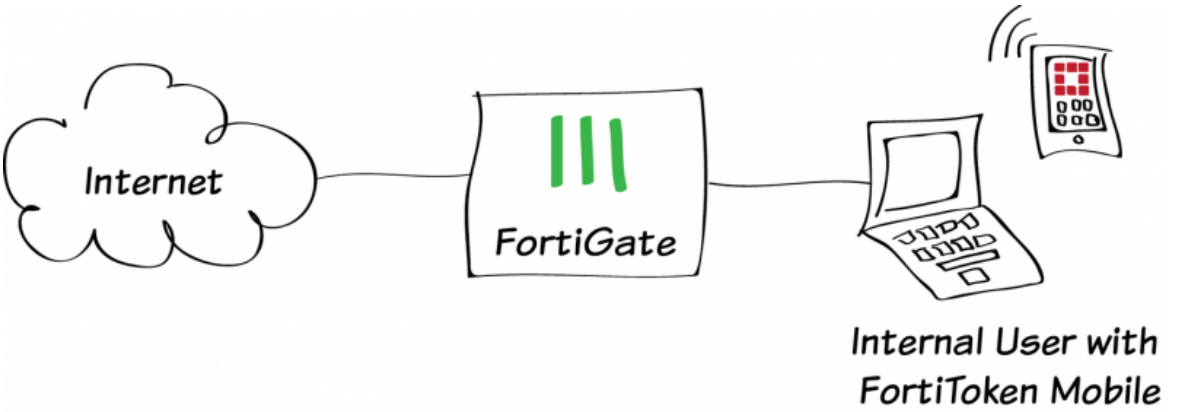


Select an entry for more information.



For further reading, check out Single Sign-On to Windows AD in the FortiOS 5.2 Handbook.

Two-factor authentication with FortiToken Mobile



In this recipe, two-factor authentication is added to a user account to provide extra security to the authentication process.

Two-factor authentication requires a user to provide further means of authentication in addition to their credentials. In this recipe, FortiToken Mobile app for Android will be used to generate a token, also known as a one-time password (OTP), to use in the authentication process.

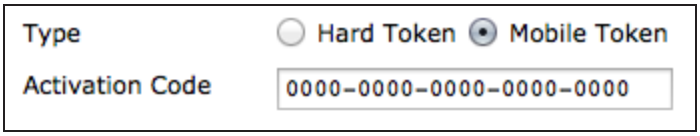
A video of this recipe is available here.

1. Activating your FortiTokens

Ensure that your FortiGate is connected to the Internet. Go to **User & Device > FortiTokens**. Your FortiGate may have two FortiToken Mobile entries listed by default. If so, you may use these tokens and go to step 2.

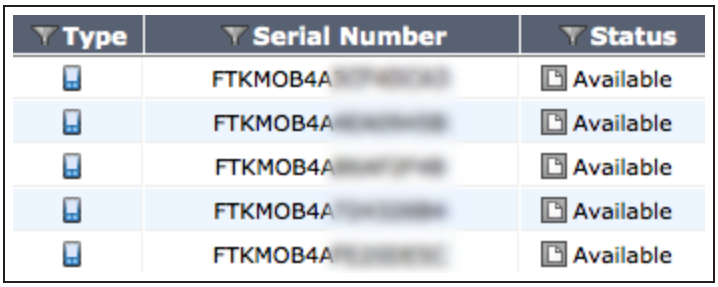
To add new FortiTokens, select **Create New**. Set **Type** to **Mobile Token** and enter your **Activation Code**.

An error stating that the serial number is invalid will appear if you mistyped the code or if it duplicates one you have already entered.



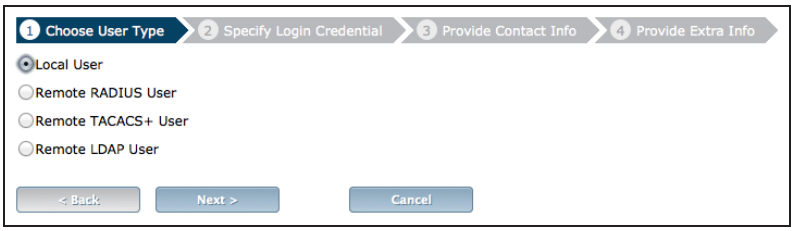
After FortiGuard validates the code, your FortiTokens will appear on the list, with **Status** set to **Available**

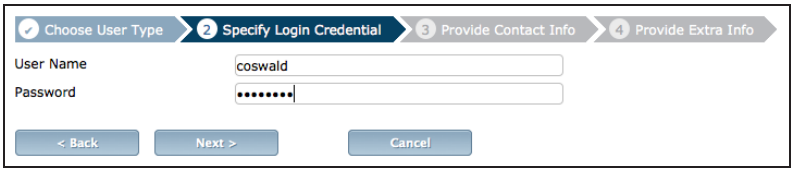
*If the FortiToken has already been registered to another FortiGate, the **Status** will be **Error.***



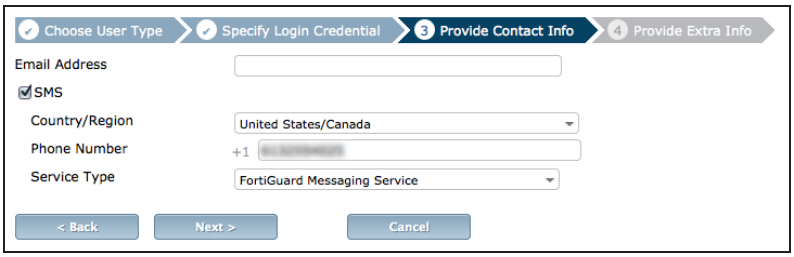
2. Creating a user account with two-factor authentication

Go to **User & Device > User > User Definition** and create a new local user.

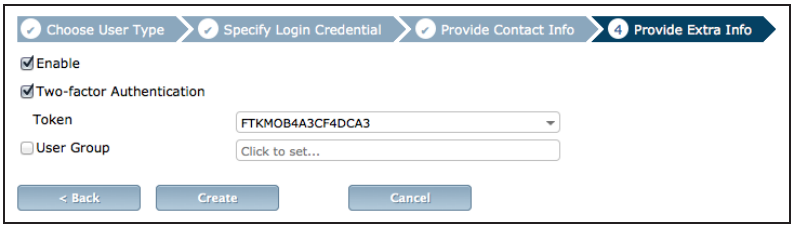




In order to use the FortiToken Mobile, you must enter a mobile number in the third step, **Provide Contact Info**. Select the appropriate **Country/Region** and enter the **Phone Number** without dashes or spaces. Do *not* add an email address.

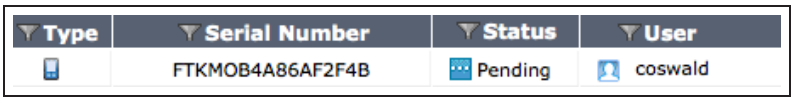


In the fourth step of the User Creation Wizard, **Provide Extra Info**, enable **Two-Factor Authentication** and select an available token.



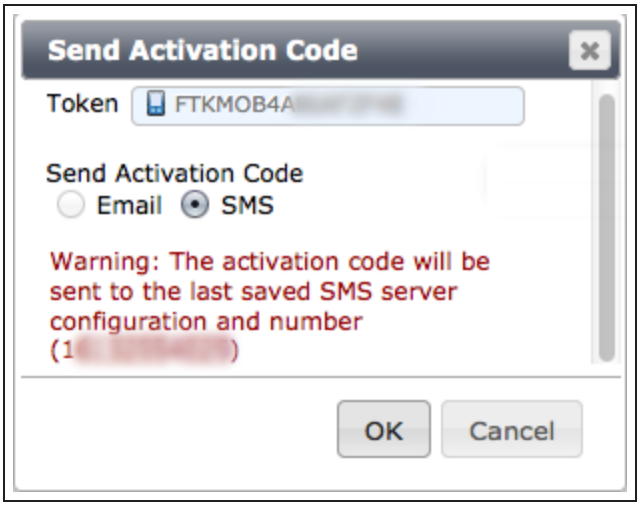
The user list shows the FortiToken in the **Two-factor Authentication** column for the new user account.

Go to **User & Device > FortiTokens**. The FortiToken assigned to the user is now listed as **Pending**, until the user activates the FortiToken.



3. Sending the activation code to the user

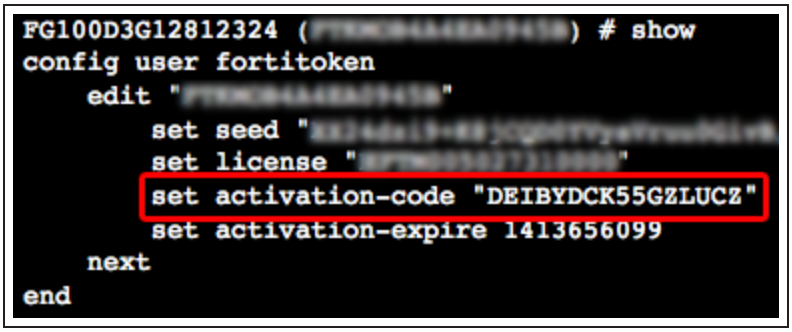
If your FortiGate can send SMS messages, go to **User & Device > User > User Definition** and edit the new user account. Select **Send Activation Code** and send the code by **SMS**.



If your FortiGate cannot send SMS messages, go to **System > Dashboard > Status** and enter the following into the **CLI Console**, substituting the correct serial number:

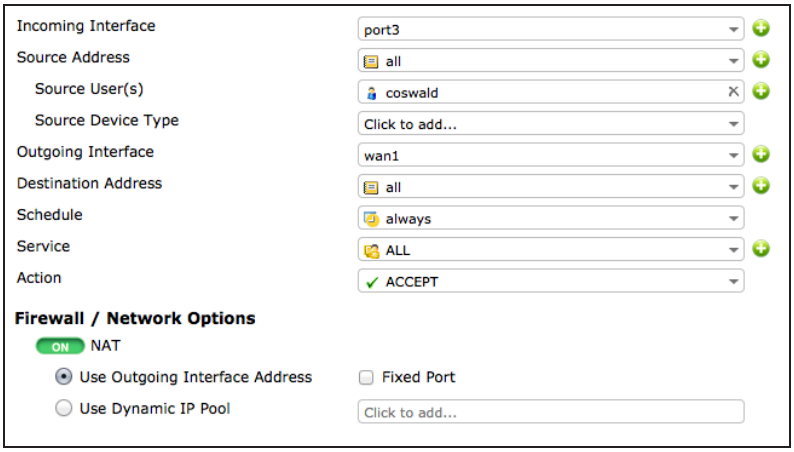
```
config user fortitoken
  edit serial number
  show
```

The activation code will be shown in the output. This code must be given to the user.



4. Adding user authentication to your Internet access policy

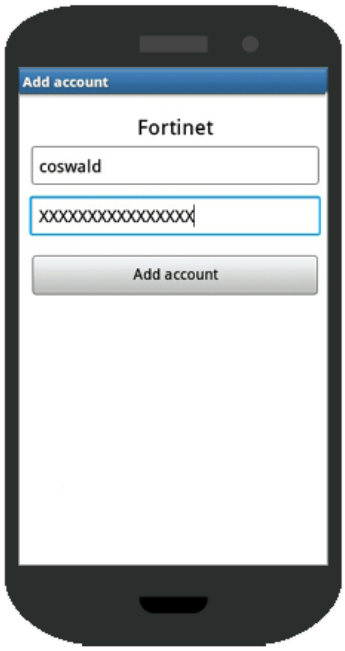
Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet. Set **Source User(s)** to the new user account.



5. Setting up FortiToken Mobile on an Android device

Using your Android device, download and install FortiToken Mobile.

Open the app and add a new account. Select **Enter Manually**. Enter the activation code into FortiToken Mobile.



FortiToken Mobile can now generate a token for use with the FortiGate.

(Optional) For additional security, set a **PIN** for FortiToken Mobile using the app's **Settings** options.

6. Results

Attempt to browse the Internet. An authentication page will appear, requesting a **Username** and **Password**.

After the correct username and password are entered, a FortiToken code will be requested. Enter the code currently shown in the FortiToken Mobile app. Once the token is authenticated, you can connect to the Internet.

For further reading, check out FortiToken in the FortiOS 5.2 Handbook.

VPNs

This section contains information about configuring a variety of different Virtual Private Networks (VPNs), as well as different methods of authenticating VPN users. FortiGates support two types of VPNs: IPsec and SSL.

IPsec VPNs use Internet Protocol Security (IPsec) to create a VPN that extends a private network across a public network, typically the Internet. In order to connect to an IPsec VPN, users must install and configure an IPsec VPN client (such as FortiClient) on their PCs or mobile devices.

SSL VPNs use Secure Sockets Layer (SSL) to create a VPN that extends a private network across a public network, typically the Internet. Connections to an SSL VPN are done through a web browser and do not require any additional applications.

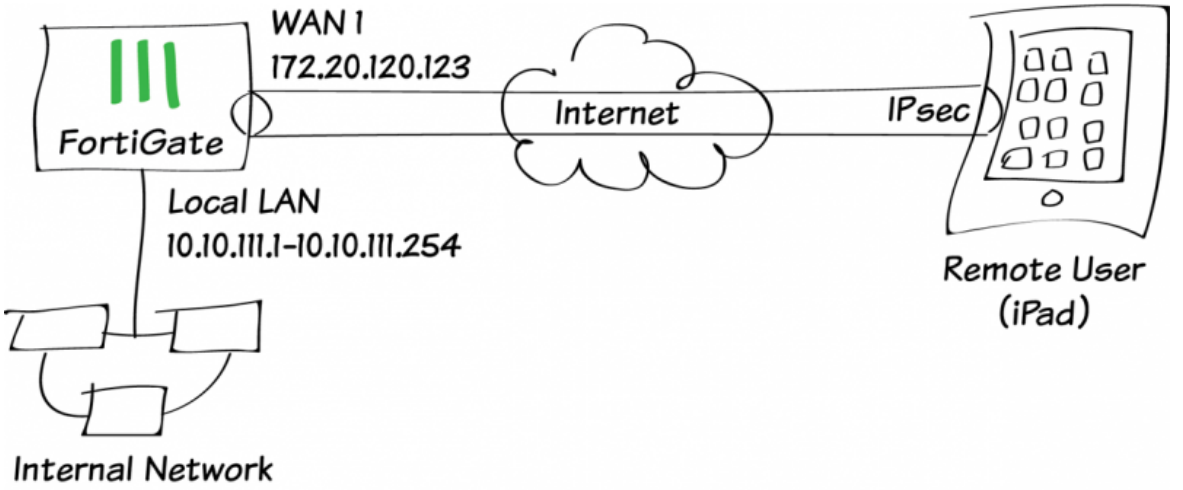
IPsec

- IPsec VPN for iOS devices
- IPsec VPN with FortiClient
- IPsec VPN with the native Mac OS client
- Site-to-site IPsec VPN with two FortiGates
- IPsec VPN to Microsoft Azure
- Remote Internet browsing using a VPN
- Remote browsing using site-to-site IPsec VPN
- IPsec troubleshooting

SSL

- SSL VPN for remote users
- SSL VPN for Windows Phone 8.1
- SSL VPN using FortiClient for iOS
- Remote Internet browsing using a VPN
- SSL VPN troubleshooting

IPsec VPN for iOS devices



This recipe uses the IPsec VPN Wizard to provide a group of remote iOS users with secure, encrypted access to the corporate network. The tunnel provides group members with access to the internal network, but forces them through the FortiGate unit when accessing the Internet.

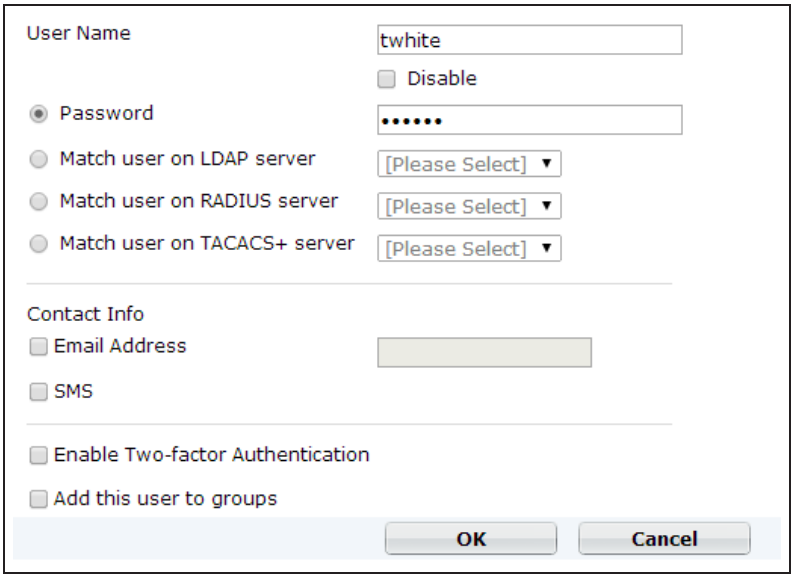
This recipe was tested using an iPad 2 running iOS version 7.1.

A video of this recipe can be found here.

1. Creating a user group for iOS users

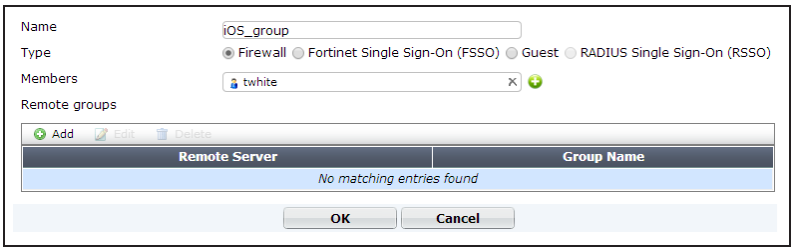
Go to **User & Device > User > User Definition**.

Create a new user.



Go to **User & Device > User > User Groups**.

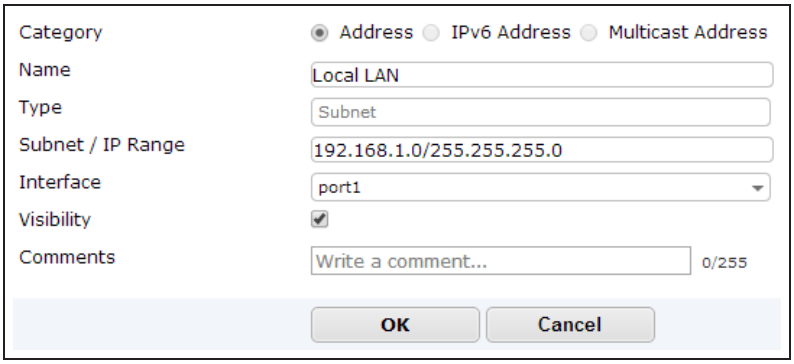
Create a user group for iOS users and add the user you created.



2. Adding a firewall address for the local network

Go to **Policy & Objects > Objects > Addresses**.

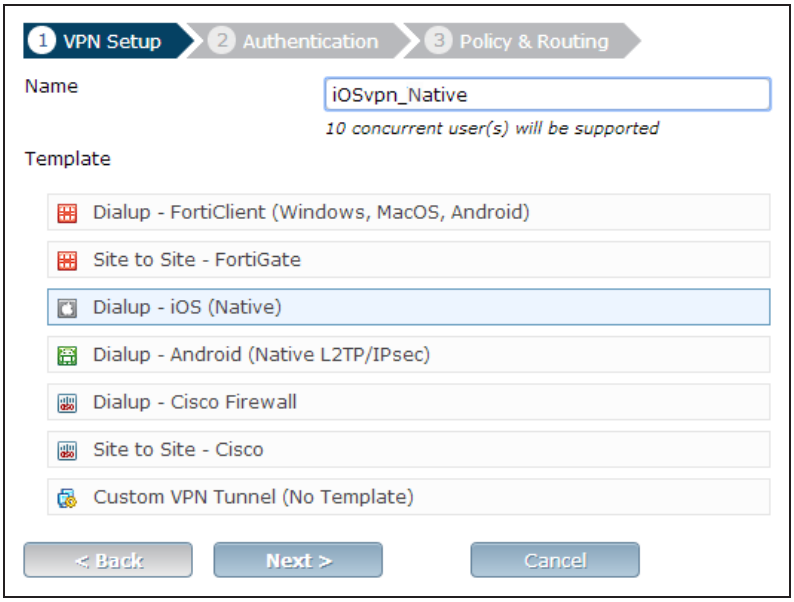
Add a firewall address for the Local LAN, including the subnet and local interface.



3. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to **VPN > IPsec > Wizard**.

Name the VPN connection and select **Dial Up - iOS (Native)** and click **Next**.



Set the **Incoming Interface** to the internet-facing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key and select the iOS user group, then click **Next**.

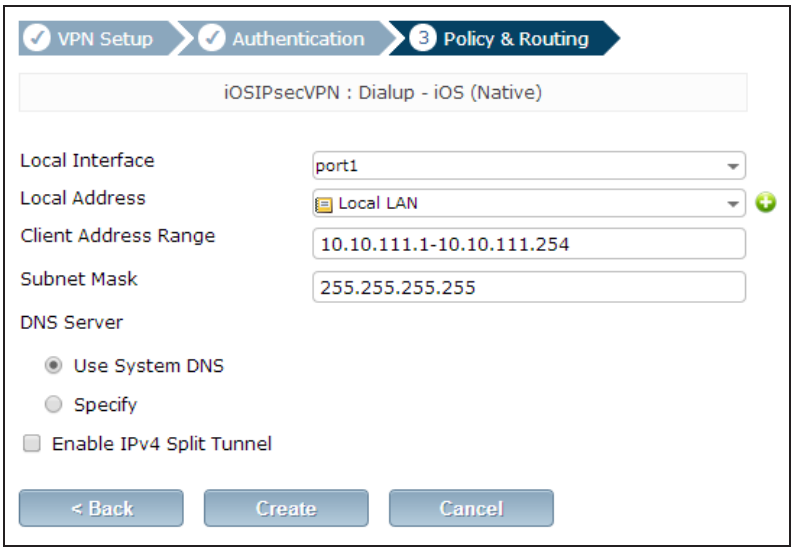
The pre-shared key is a credential for the VPN and should differ from the user's password.

Set **Local Interface** to an internal interface (in the example, port 1) and set **Local Address** to the iOS users address.

Enter an IP range for VPN users in the **Client Address Range** field.

*The IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the **_range** suffix (in this case, **iOSvpn_Native_range**).*

In addition, FortiOS automatically creates a security policy to allow remote users to access the internal network.



4. Creating a security policy for access to the Internet

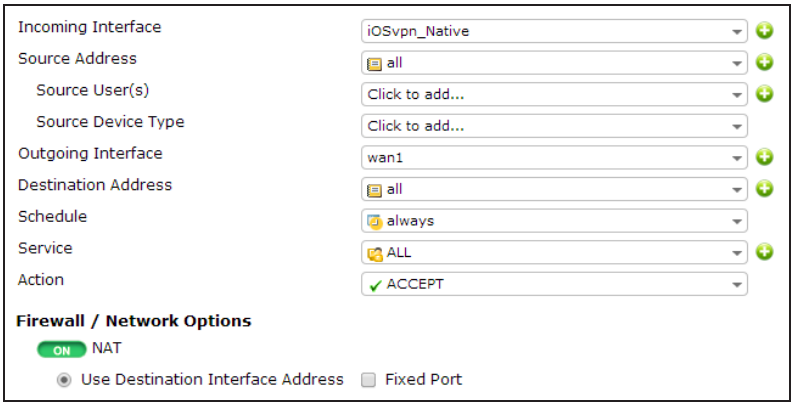
Go to **Policy & Objects > Policy > IPv4**.

Create a security policy allowing remote iOS users to access the Internet securely through the FortiGate unit.

Set **Incoming Interface** to the tunnel interface and set **Source Address** to all.

Set **Outgoing Interface** to **wan1** and **Destination Address** to all.

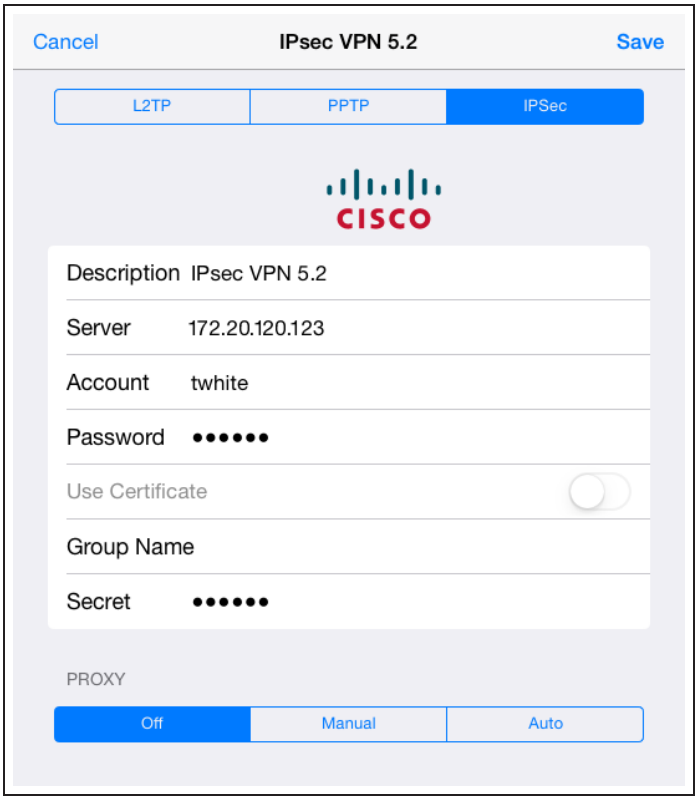
Set **Service** to **all** and ensure that you enable **NAT**.



5. Configuring VPN on the iOS device

On the iPad, go to **Settings > General > VPN** and select **Add VPN Configuration**.

Enter the VPN address, user account, and password in their relevant fields. Enter the pre-shared key in the **Secret** field.



6. Results

On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and view the status of the tunnel.

Name	Ty...	Remote Gatew...	Userna...	Stat...	Incoming D...	Outgoing Data	Phase 2 Proposal
iOSvpn_Native_0	Dialup	172.20.120.16		Up	9.22 K	3.48 K	iOSvpn_Native

Users on the internal network will be accessible using the iOS device.

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

Refresh Download Raw Log

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received
1	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	59 B / 221 B
2	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	60 B / 292 B
3	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	56 B / 288 B
4	11:21:42	port1		192.168.1.117	208.91.113.70	304 B / 304 B

Select an entry to view more information.

Dst	192.168.1.114	**Virtual Domain**	root
Received	72	**Source Country**	Reserved
Sent / Received	72 B / 72 B	**Duration**	63
Sent	72	**Application Details**	
Service	PING	**Protocol**	1
Destination Country	Reserved	**roll**	65428
Status	✓	**Timestamp**	Thu Feb 21 11:20:44 2014
Tran Display	noop	**Sequence Number**	220067
Policy ID	6	**Src Interface**	iOSvpn
Src	10.10.111.16	**VPN**	iOSvpn_Native
Sent Packets	2	**Level**	notice
VPN Type	ipsec-dynamic	**logid**	13
Sub Type	forward	**Threat**	
Received Packets	2	**Date/Time**	11:20:44 (Thu Feb 21 11:20:44 2014)
Dst Interface	port1		

Remote iOS users can also access the Internet securely via the FortiGate unit.

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

Refresh Download Raw Log

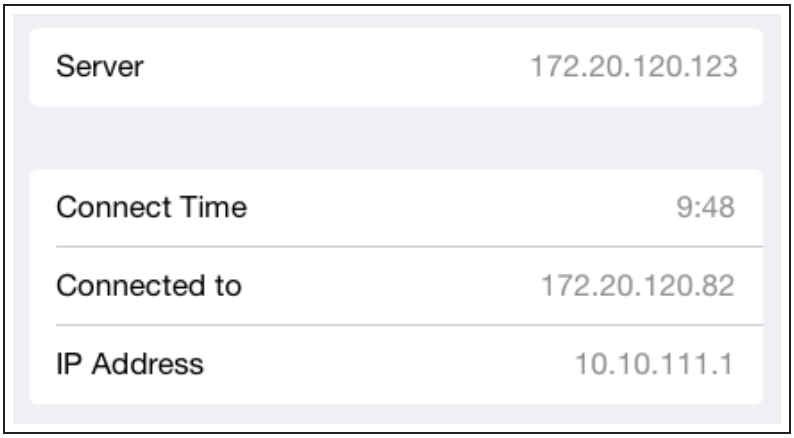
#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received
1	11:28:43	ios_P1	wan1	10.10.111.16	74.121.50.17	1023 B / 579 B
2	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	59 B / 221 B
3	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	60 B / 292 B
4	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	56 B / 288 B
5	11:20:42	iOSvpn_Native	wan1	10.10.111.16	173.194.73.105	812 B / 642 B
6	11:20:42	iOSvpn_Native	wan1	10.10.111.16	74.125.134.102	808 B / 712 B
7	11:20:42	iOSvpn_Native	wan1	10.10.111.16	173.194.73.94	2.96 KB / 23.07 KB
8	11:20:35	iOSvpn_Native	wan1	10.10.111.16	17.149.36.134	104 B / 60 B
9	11:19:15	iOSvpn_Native	wan1	10.10.111.16	204.93.33.67	813 B / 365 B

Select an entry to view more information.

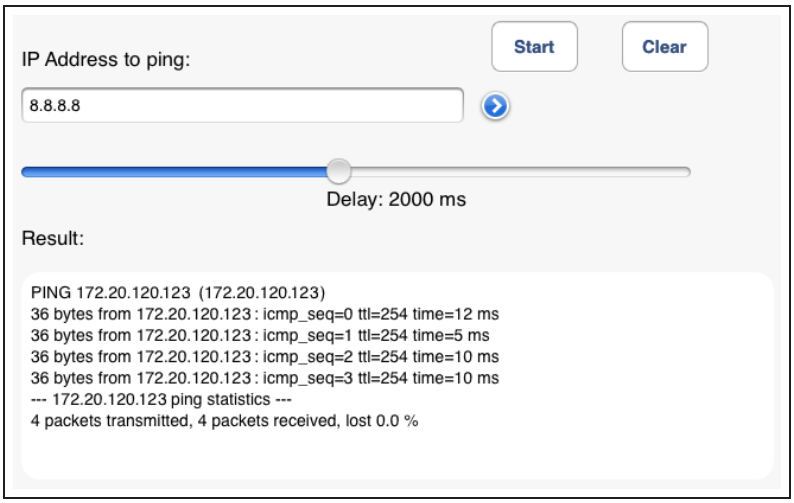
Dst	74.121.50.17	**Virtual Domain**	root
Received	579	**Source Country**	Reserved
Src NAT IP	172.20.120.123	**Sent / Received**	1023 B / 579 B
Duration	2	**Sent**	1023
Src NAT Port	50189	**Application Details**	
Service	HTTP	**Protocol**	6
Destination Country	United States	**Dst Port**	80
roll	65428	**Status**	close
Timestamp	Thu Feb 21 11:28:43 2014	**Tran Display**	snat
Sequence Number	221594	**Policy ID**	7
Src Interface	iOSvpn_Native	**Src**	10.10.111.16
VPN	iOSvpn	**Sent Packets**	6
Level	notice	**VPN Type**	ipsec-dynamic
Src Port	50189	**logid**	13
Sub Type	forward	**Threat**	
Received Packets	4	**Date/Time**	11:28:43 (Thu Feb 21 11:28:43 2014)
Dst Interface	wan1		

You can also view the status of the tunnel on the iOS device itself.

On the device, go to **Settings > VPN > Status** and view the status of the connection.

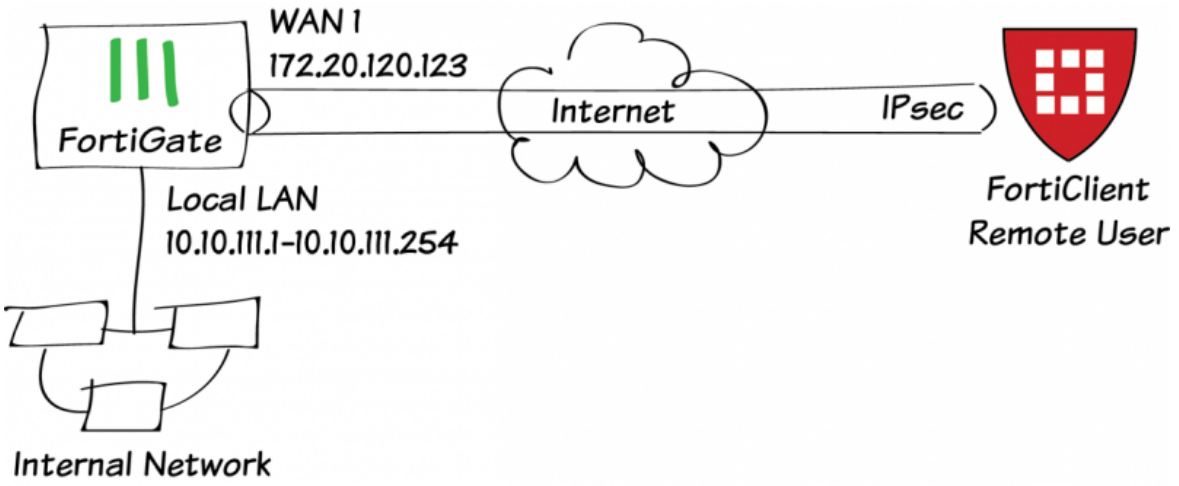


Lastly, using a Ping tool, you can send a ping packet from the iOS device directly to an IP address on the LAN behind the FortiGate unit to verify the connection through the VPN tunnel.



For further reading, check out FortiGate dialup-client configurations in the FortiOS 5.2 Handbook.

IPsec VPN with FortiClient



This recipe uses the IPsec VPN Wizard to provide a group of remote users with secure, encrypted access to the corporate network.

The tunnel provides group members with access to the internal network, but forces them through the FortiGate unit when accessing the Internet. When the tunnel is configured, you will connect using the FortiClient application.

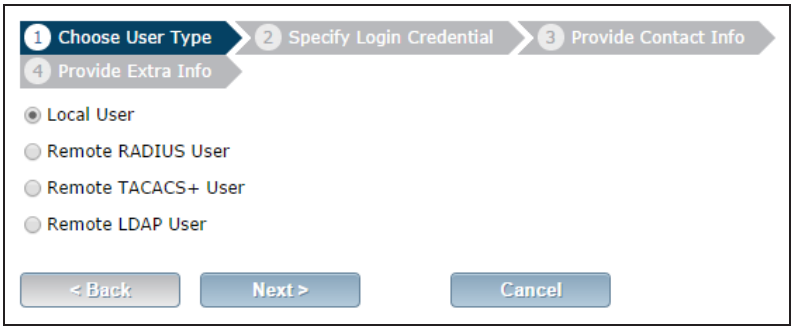
A video of this recipe is available here.

1. Creating a user group for remote users

Go to **User & Device > User > User Definition**.

Create a new **Local User** with the **User Creation Wizard**.

Proceed through each step of the wizard, carefully entering the appropriate information.



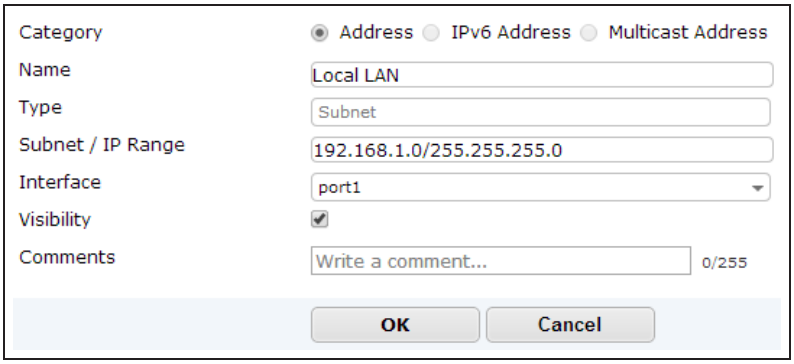
Go to **User & Device > User > User Groups**.

Create a user group for remote users and add the user you created.

2. Adding a firewall address for the local network

Go to **Policy & Objects > Objects > Addresses**.

Add a firewall address for the Local LAN, including the subnet and local interface.

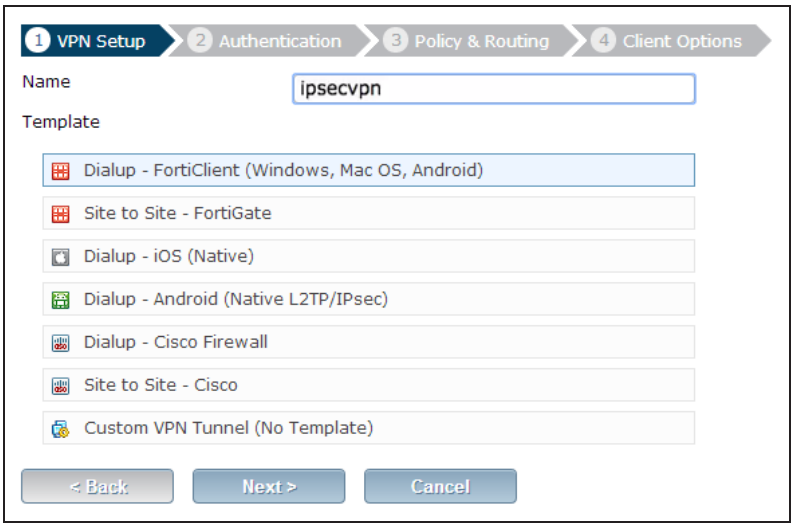


3. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to **VPN > IPSec > Wizard**.

Name the VPN connection and select **Dial Up - FortiClient (Windows, Mac OS, Android)** and click Next.

The tunnel name may not have any spaces in it.

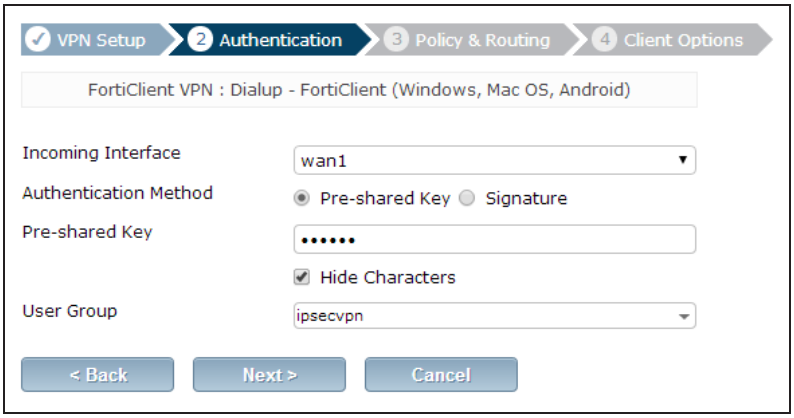


Set the **Incoming Interface** to the internet-facing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key and select the new user group, then click **Next**.

The pre-shared key is a credential for the VPN and should differ from the user's password.

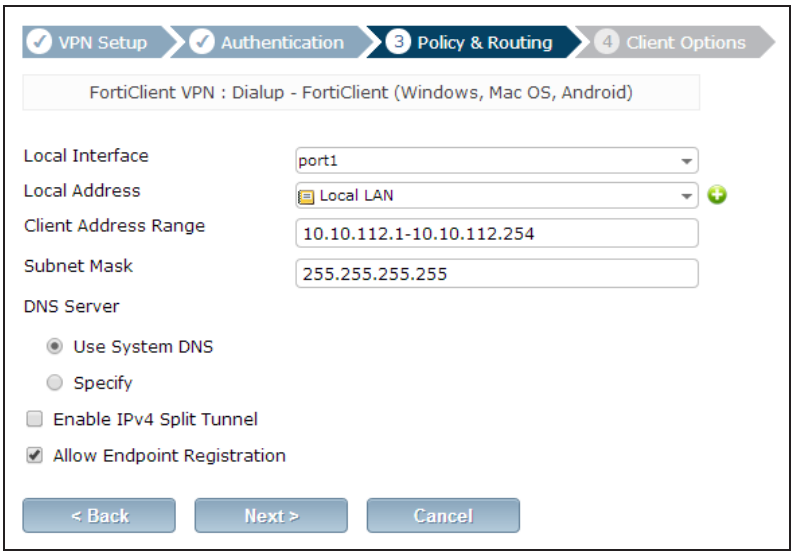


Set **Local Interface** to an internal interface (in the example, port 1) and set **Local Address** to the local LAN address.

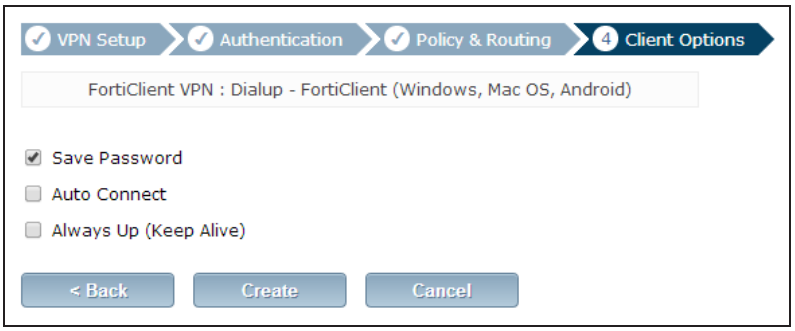
Enter an IP range for VPN users in the **Client Address Range** field.

The IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the _range suffix (in this case, ipsecvpn_range).

In addition, FortiOS automatically creates a security policy to allow remote users to access the internal network.



Click **Next** and select **Client Options** as desired.



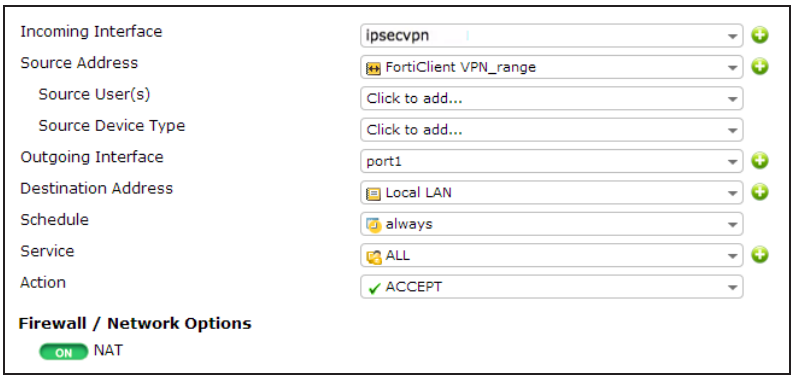
4. Creating a security policy for access to the Internet

Go to **Policy & Objects > Policy > IPv4**.

Create a security policy allowing remote users to access the Internet securely through the FortiGate unit.

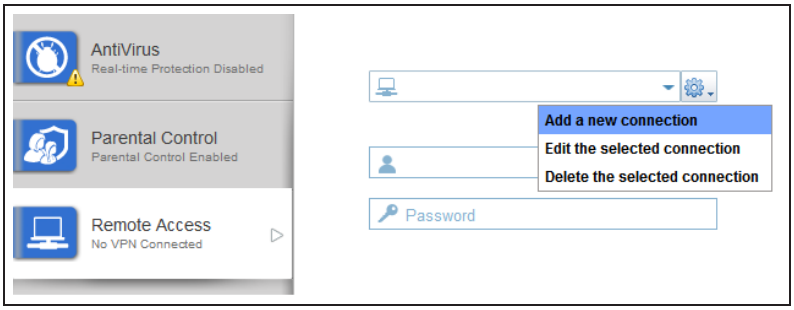
Set **Incoming Interface** to the tunnel interface and set **Source Address** to **all**. Set **Outgoing Interface** to **wan1** and **Destination Address** to **all**.

Set **Service** to **ALL** and ensure that you enable **NAT**.



5. Configuring FortiClient

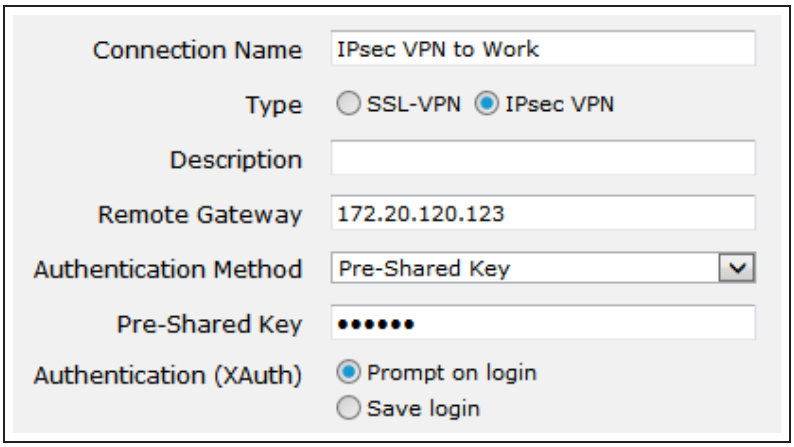
Open FortiClient, go to **Remote Access** and **Add a new connection**.



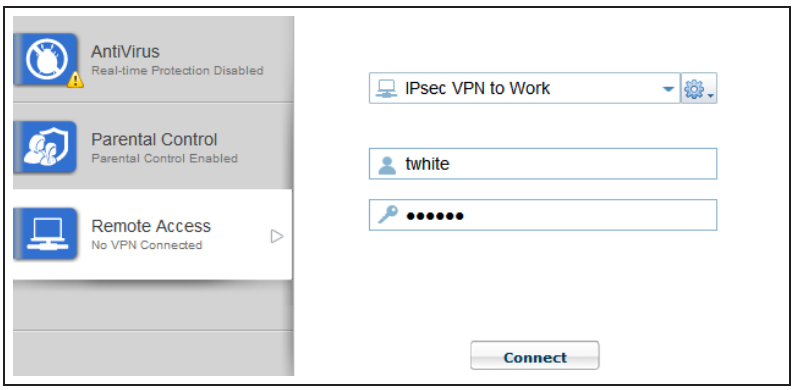
Provide a **Connection Name** and set the **Type** to **IPsec VPN**.

Set **Remote Gateway** to the FortiGate IP address.

Set **Authentication Method** to **Pre-Shared Key** and enter the key below.

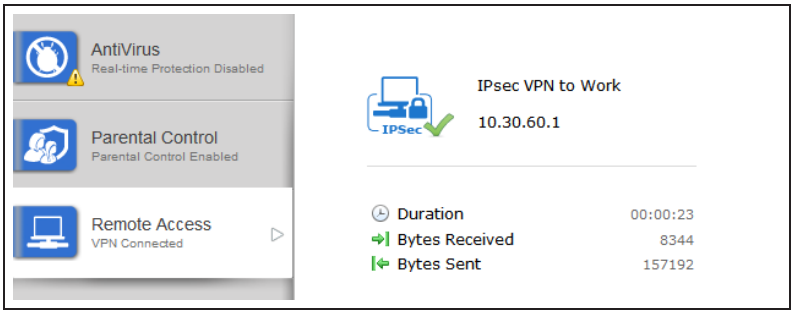


Select the new connection, enter the username and password, and click **Connect**.



6. Results

Once the connection is established, the FortiGate assigns the user an IP address and FortiClient displays the status of the connection, including the IP address, connection duration, and bytes sent and received.



On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and verify that the tunnel **Status** is **Up**.

Name	Ty...	Remote Gatew...	Stat...	Incoming D...	Outgoing Data
ipsec_0	Dialup	172.20.120.16	Up	9.22 K	3.48 K

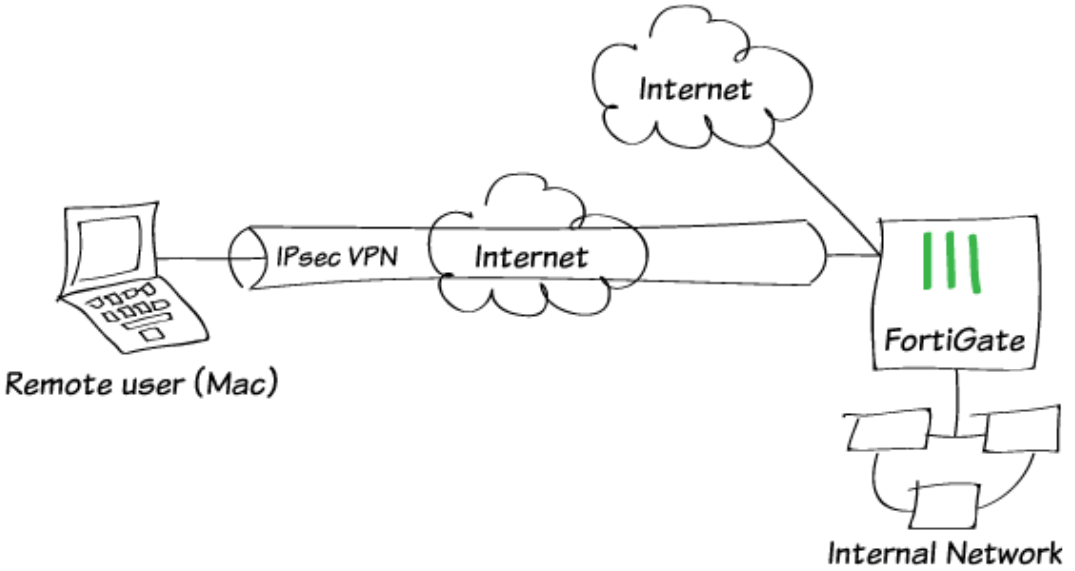
Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

Verify that the **Sent/Received** column displays traffic successfully flowing through the tunnel.

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received
1	11:22:41	ipsecvpn	wan1	10.10.111.16	208.91.112.53	59 B / 221 B
2	11:22:41	ipsecvpn	wan1	10.10.111.16	208.91.112.53	60 B / 292 B
3	11:22:41	ipsecvpn	wan1	10.10.111.16	208.91.112.53	56 B / 288 B

For further reading, check out IPsec VPN in the web-based manager in the FortiOS 5.2 Handbook.

IPsec VPN with the native Mac OS client



In this recipe, you will learn how to create an IPsec VPN on a FortiGate, and connect to it using the default client built into the Mac OS.

This VPN configuration allows Mac users to securely access an internal network as well as browse the Internet through the VPN tunnel.

The recipe assumes that a "mac_users" user group and a Local LAN firewall address have been created.

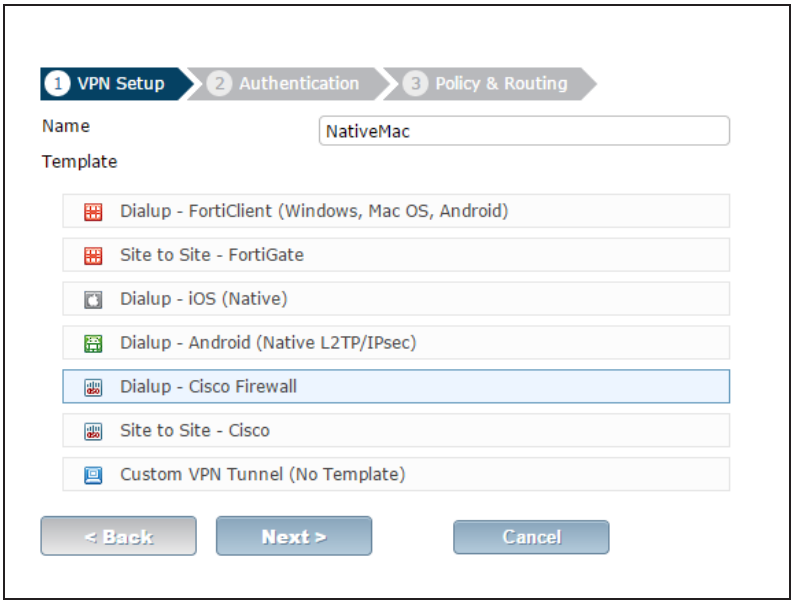
This recipe was tested using Mac OS 10.10.2 (Yosemite).

1. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to **VPN > IPSec > Wizard**.

Name the VPN connection and select **Dial Up - Cisco Firewall** and click **Next**.

The native Mac OS client is a Cisco client, which is why you select Dialup - Cisco Firewall in the VPN Wizard.



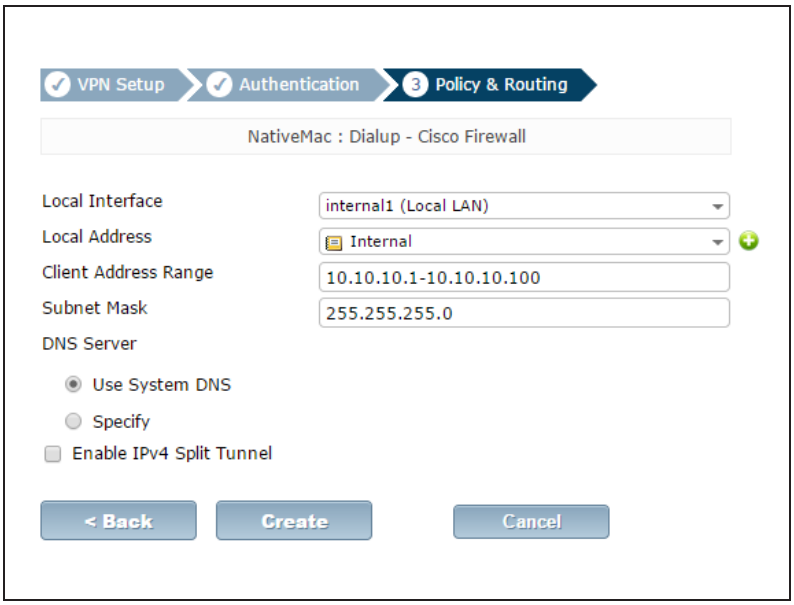
Set the **Incoming Interface** to the internet-facing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key, select the appropriate **User Group**, then click **Next**.

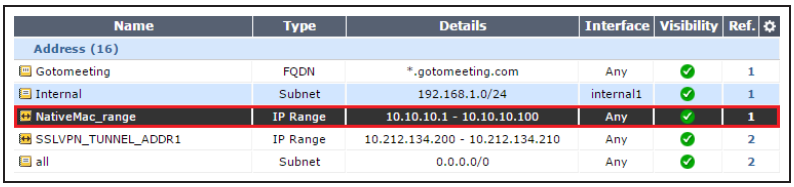
Set **Local Interface** to an internal interface and set **Local Address** to the local LAN address.

Enter an IP address range for VPN users in the **Client Address Range** field then click **Next**.



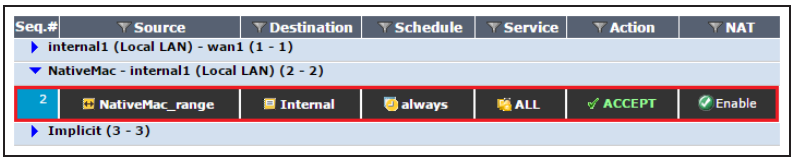
The IPsec VPN Wizard finishes with a summary of created objects.

Go to **Policy & Objects > Objects > Addresses** and confirm that the wizard has created the IPsec VPN firewall address range.



Name	Type	Details	Interface	Visibility	Ref.
Address (16)					
Gotomeeting	FQDN	*.gotomeeting.com	Any	✓	1
Internal	Subnet	192.168.1.0/24	internal1	✓	1
NativeMac_range	IP Range	10.10.10.1 - 10.10.10.100	Any	✓	1
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	Any	✓	2
all	Subnet	0.0.0.0/0	Any	✓	2

Go to **Policy & Objects > Policy > IPv4** and confirm that the wizard has created the policy from the VPN tunnel interface to the internal interface.



2. Creating a security policy for remote access to the Internet

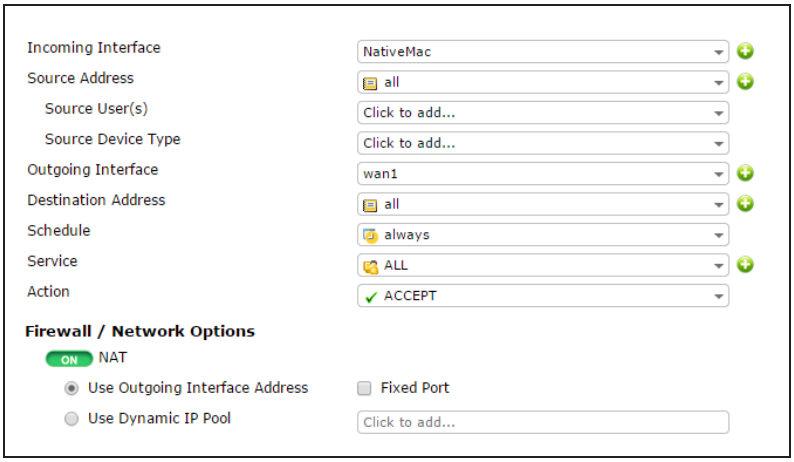
Under **Policy & Objects > Policy > IPv4**, create a security policy

allowing remote users to access the Internet securely through the FortiGate unit.

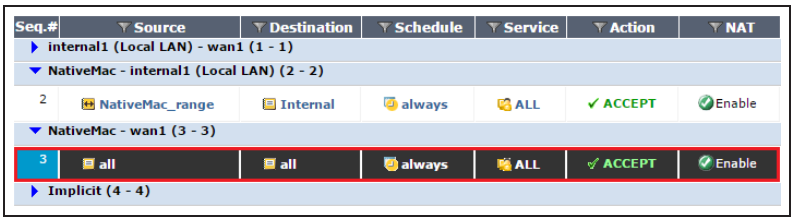
Set **Incoming Interface** to the tunnel interface and set **Source Address** to **all**.

Set **Outgoing Interface** to the Internet-facing interface and **Destination Address** to **all**.

Set **Service** to **ALL** and enable **NAT**.

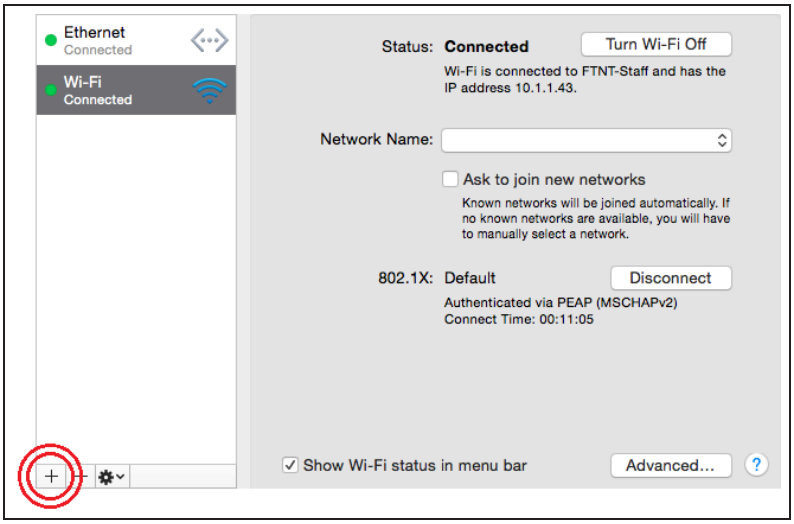


The policy should appear in the policy list at **Policy & Objects > Policy > IPv4**.

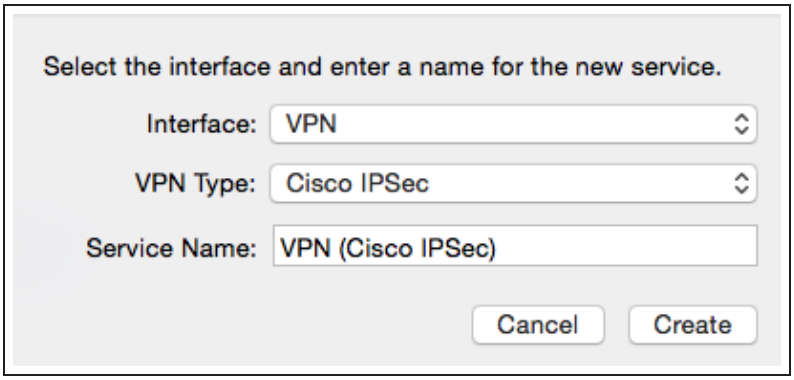


3. Connecting to the IPsec VPN using the native Mac client

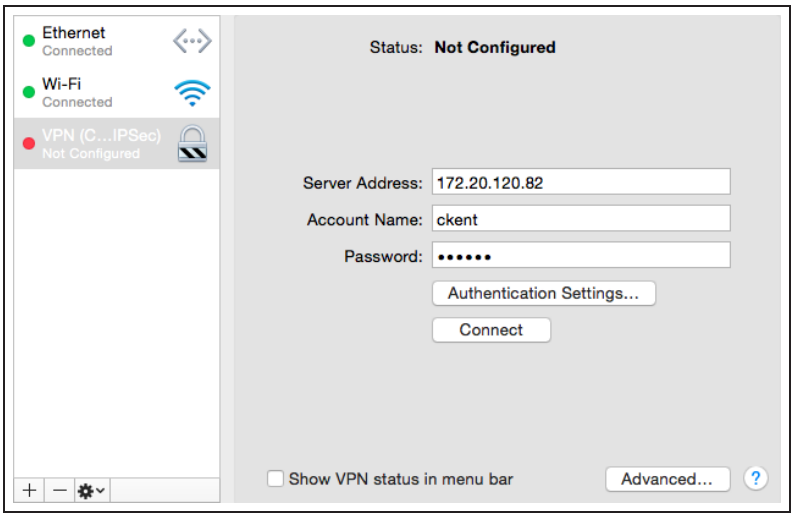
On the Mac, go to **System Preferences > Network** and click the **Plus (+)** button.



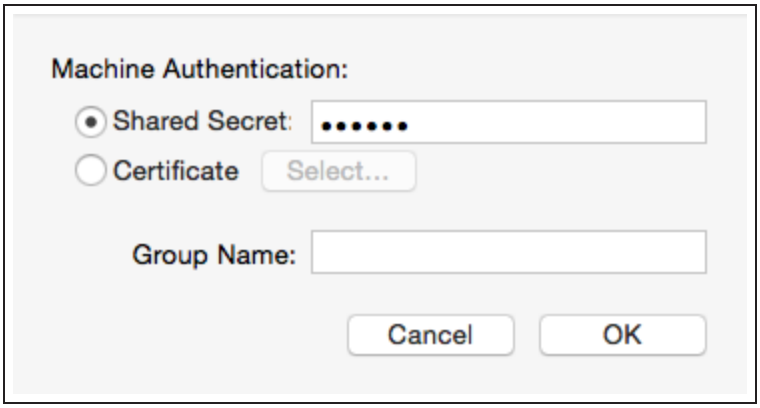
Set **Interface** to **VPN**, set **VPN Type** to **Cisco IPSec**, and click **Create**.



Set the **Server Address** to the FortiGate IP address, configure the network account details for the remote user, then click **Authentication Settings**.



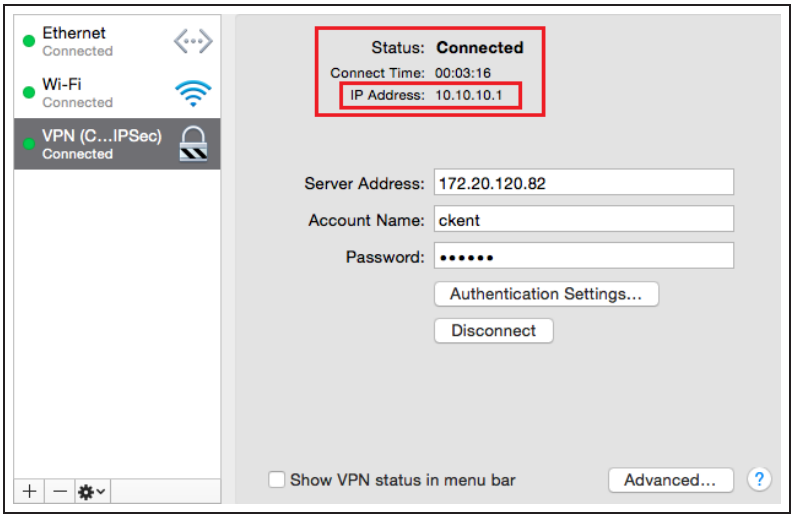
Select **Shared Secret** and enter the pre-shared key you created above, then click **OK**.



4. Results

On the Mac, ensure that the VPN is selected and click **Connect**. The **Status** should change to **Connected** and you should be given an **IP Address** in the range specified above.

You should also be able to browse the Internet, protected by whichever profiles you applied to the security policy created in the above step.

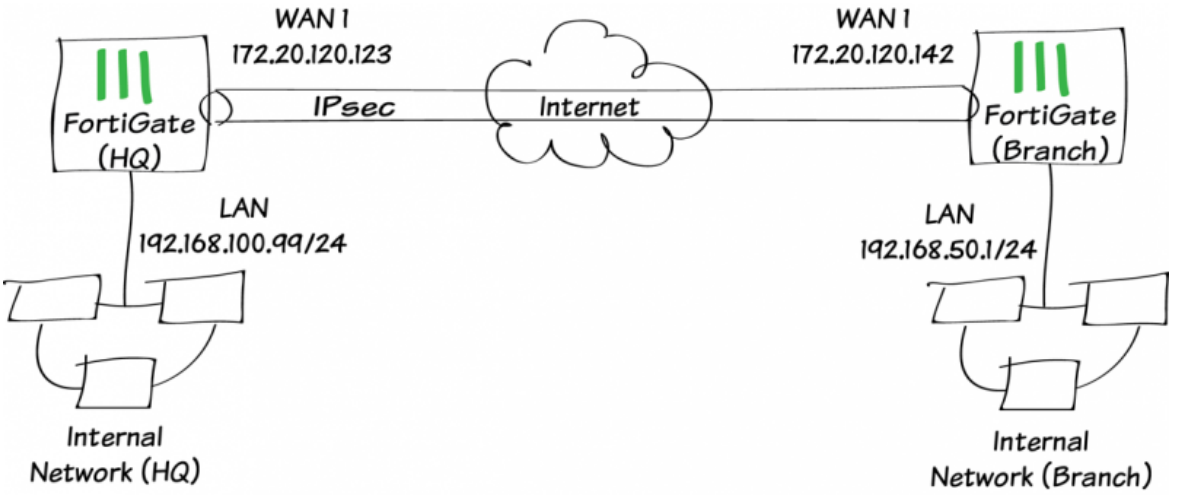


On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and verify that the tunnel **Status** is **Up**, and that there are **Incoming** and **Outgoing Data**.

Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoin
NativeMac_0	Dialup - Cisco Firewall	172.20.120.221		Up	862.49 KB	2.06 MB

For further reading, check out IPsec VPN in the web-based manager in the FortiOS 5.2 Handbook.

Site-to-site IPsec VPN with two FortiGates

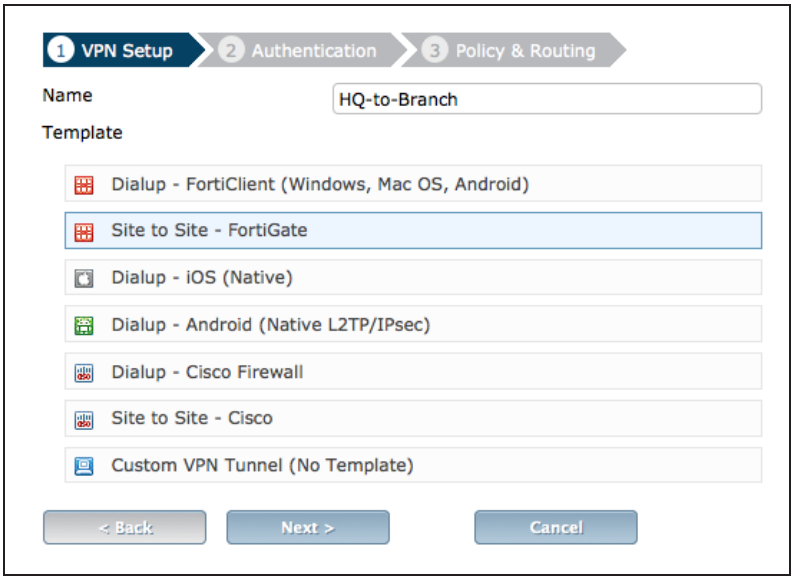


In this example, you will allow transparent communication between two networks that are located behind different FortiGates at different offices using route-based IPsec VPN. The VPN will be created on both FortiGates by using the VPN Wizard's **Site to Site FortiGate** template.

In this example, one office will be referred to as HQ and the other will be referred to as Branch.

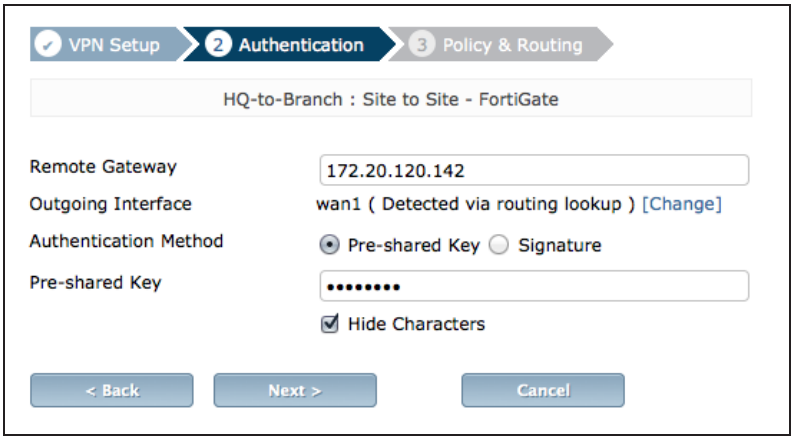
1. Configuring the HQ IPsec VPN

On the HQ FortiGate, go to **VPN > IPsec > Wizard** and select **Site to Site - FortiGate**.

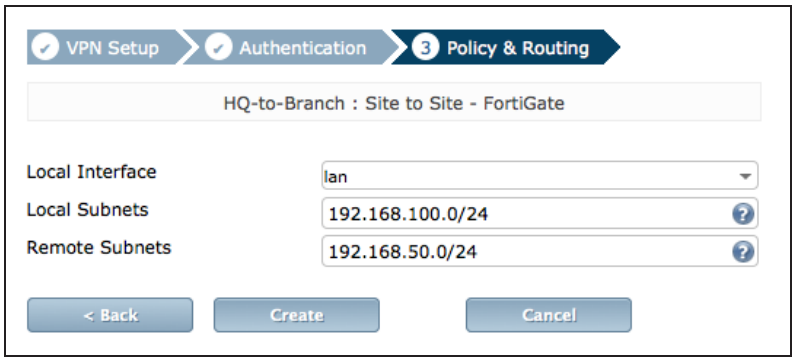


In the **Authentication** step, set the Branch FortiGate's IP as the **Remote Gateway** (in the example, *172.20.120.142*). After you enter the gateway, an available interface will be assigned as the **Outgoing Interface**. If you wish to use a different interface, select **Change**.

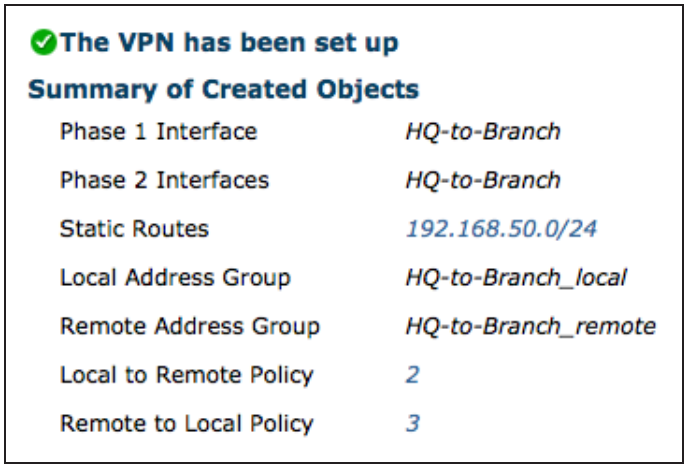
Set a secure **Pre-shared Key**



In the **Policy & Routing** section, set **Local Interface** to your **lan** interface. The **Local Subnet** will be added automatically. Set **Remote Subnets** to the Branch FortiGate's local subnet (in the example, *192.168.50.0/24*).

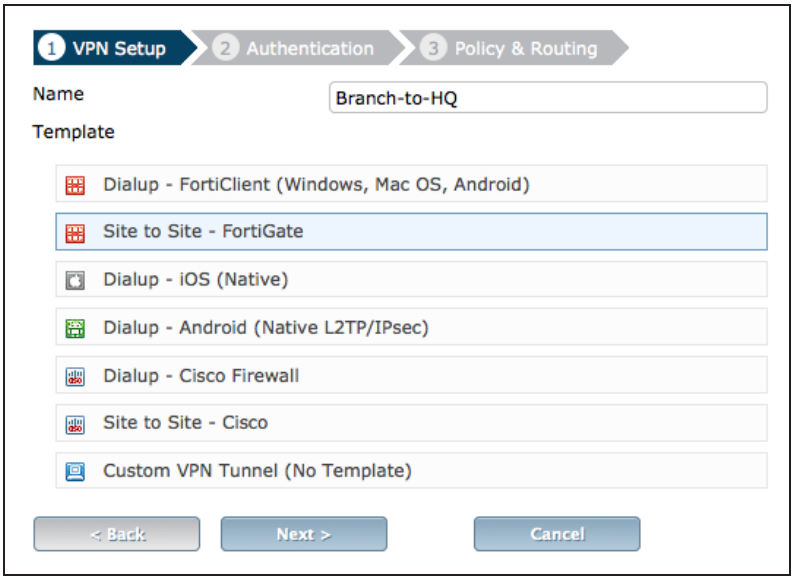


A summary page shows the configuration created by the wizard, including firewall addresses, firewall address groups, a static route, and security policies.



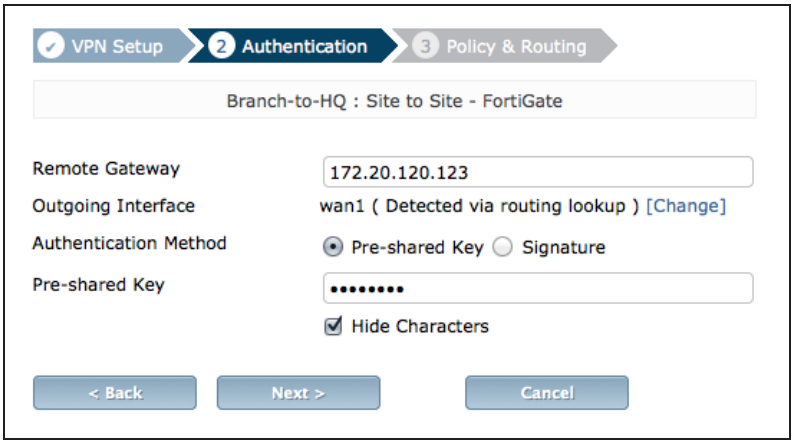
2. Configuring the Branch IPsec VPN

On the Branch FortiGate, go to **VPN > IPsec > Wizard** and select **Site to Site - FortiGate**.

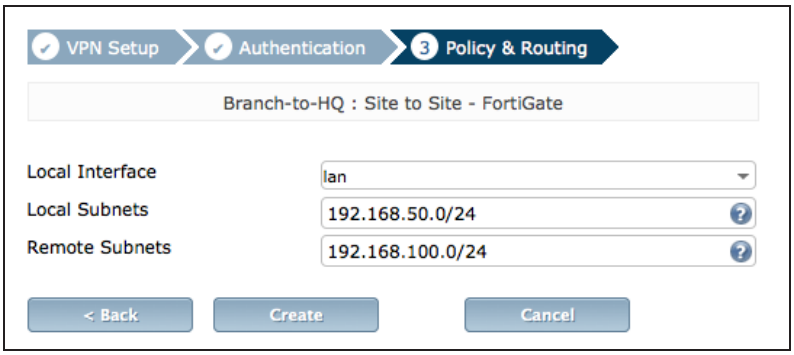


In the **Authentication** step, set the HQ FortiGate's IP as the **Remote Gateway** (in the example, *172.20.120.123*). After you enter the gateway, an available interface will be assigned as the **Outgoing Interface**. If you wish to use a different interface, select **Change**.

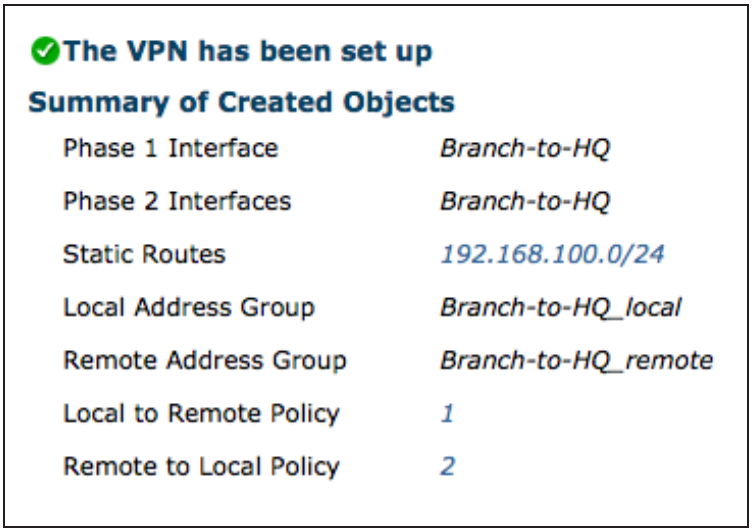
Set the same **Pre-shared Key** that was used for HQ's VPN.



In the **Policy & Routing** section, set **Local Interface** to your **lan** interface. The **Local Subnet** will be added automatically. Set **Remote Subnets** to the HQ FortiGate's local subnet (in the example, *192.168.100.0/24*).



A summary page shows the configuration created by the wizard, including firewall addresses, firewall address groups, a static route, and security policies.

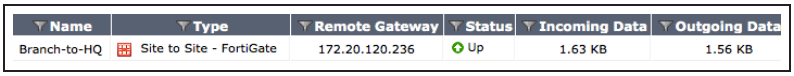


3. Results

A user on either of the office networks should be able to connect to any address on the other office network transparently.

If you need to generate traffic to test the connection, ping the Branch FortiGate's internal interface from the HQ's internal network.

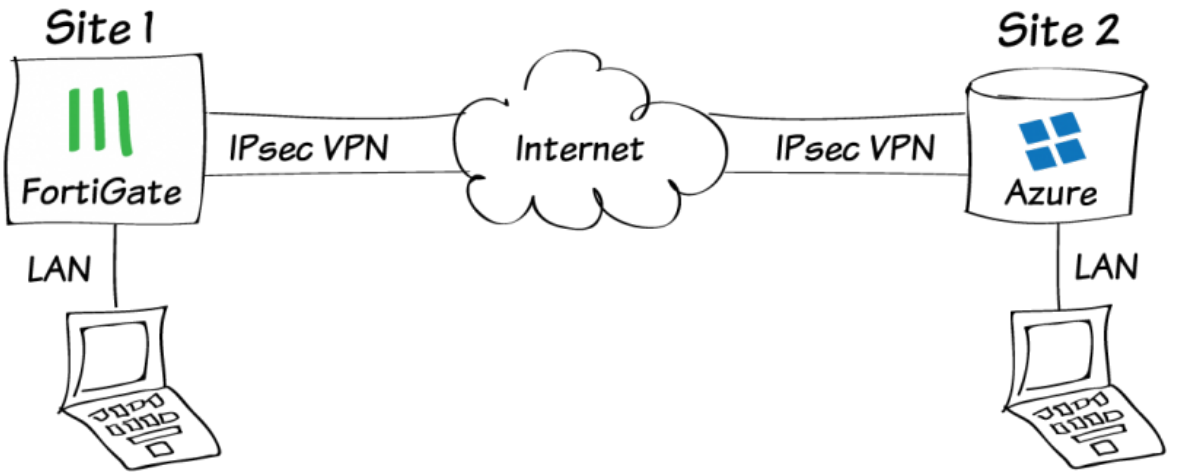
Go to **VPN > Monitor > IPsec Monitor** to verify the status of the VPN tunnel. Ensure that its **Status** is **Up** and that traffic is flowing.



Name	Type	Remote Gateway	Status	Incoming Data	Outgoing Data
Branch-to-HQ	Site to Site - FortiGate	172.20.120.236	Up	1.63 KB	1.56 KB

For further reading, check out Gateway-to-gateway configurations in the FortiOS 5.2 Handbook.

IPsec VPN to Microsoft Azure



The following recipe describes how to configure a site-to-site IPsec VPN tunnel. In this example, one site is behind a FortiGate and another site is hosted on Microsoft Azure™, for which you will need a valid Microsoft Azure profile.

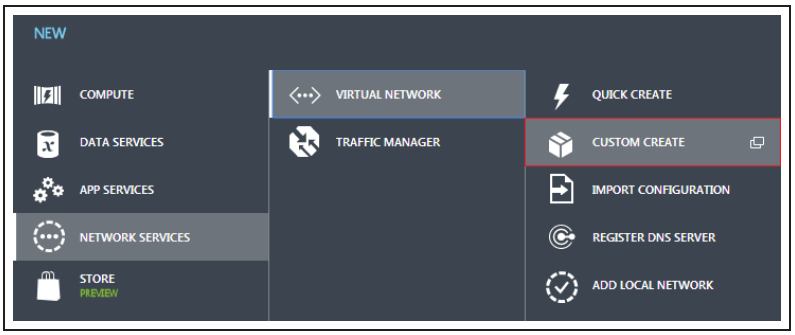
Using FortiOS 5.2, the example demonstrates how to configure the tunnel between each site, avoiding overlapping subnets, so that a secure tunnel can be established with the desired security profiles applied.

A video of this recipe is available here.

1. Configuring the Microsoft Azure™ virtual network

Log into Microsoft Azure and click New in the lower-left corner to add a new service.

From the prompt, select **Network Services > Virtual Network > Custom Create**.



Under 'Virtual Network Details', enter a **Name** for the VPN and a **Location** where you want the VMs to reside, then click the **Next** arrow.

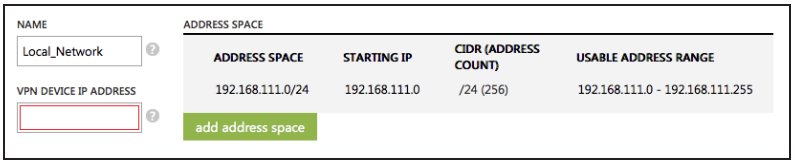
Under 'DNS Servers and VPN Connectivity', enable the **Configure a site-to-site VPN** checkbox and enter DNS server information if required.

Click the **Next arrow.**

Under 'Site-to-Site Connectivity', enter a **Name** and **IP Address** for the FortiGate device.

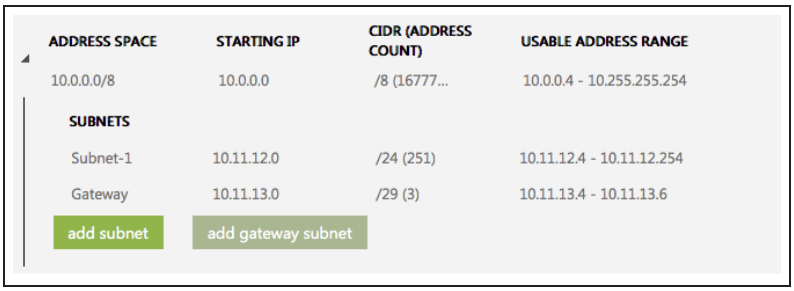
Under Address Space, include a **Starting IP** and **CIDR (Address Count)** for the tunnel, avoiding overlapping subnets.

Click the **Next** arrow.

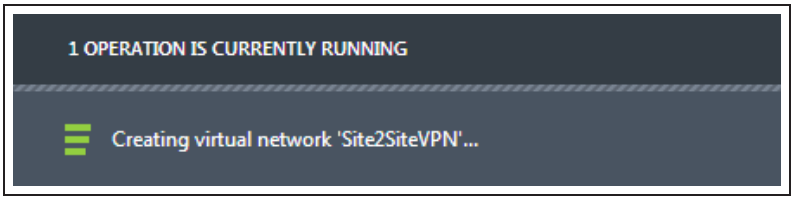


Under 'Virtual Network Address Spaces', configure the desired address space or accept the default settings.

Select **add gateway subnet** to configure a gateway IP and click the Checkmark in the lower-right corner to accept the configuration.

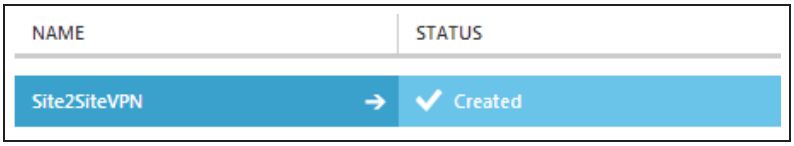


After accepting the configuration, you will have to wait a short period of time for the virtual network to be created, but it shouldn't be long.

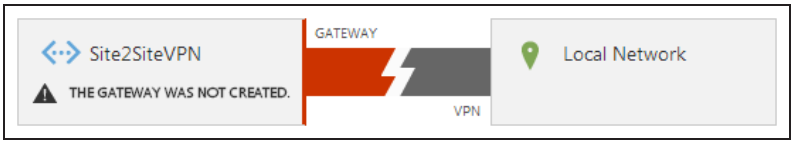


2. Creating the Microsoft Azure™ virtual network gateway

On the 'networks' home screen, click the name of the virtual network you just created.



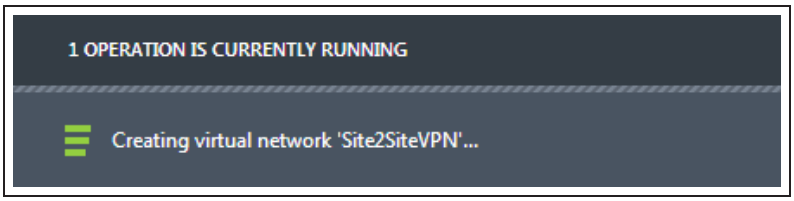
Under this virtual network, go to the **Dashboard**. You will notice that the gateway has not yet been created. You will create the gateway in this step.



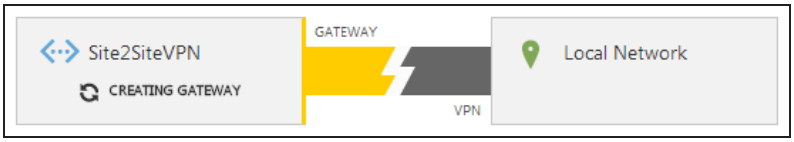
At the bottom of the screen, select **Create Gateway > Dynamic Routing**.

When prompted, select **Yes**.

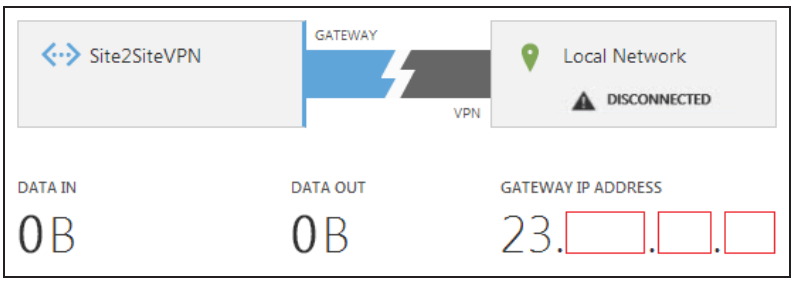
The operation to create the virtual network gateway will run. The process takes a short amount of time.



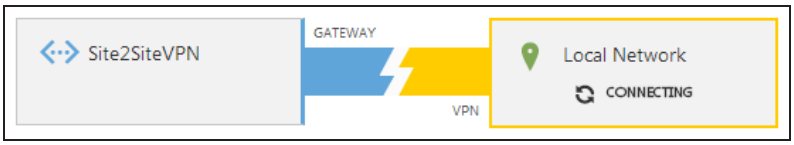
Azure will indicate to you that the gateway is being created. You may wish to leave this running for a few minutes as wait periods in excess of 10 minutes are common.



When the operation is complete, the status changes and you are given a **Gateway IP Address**.



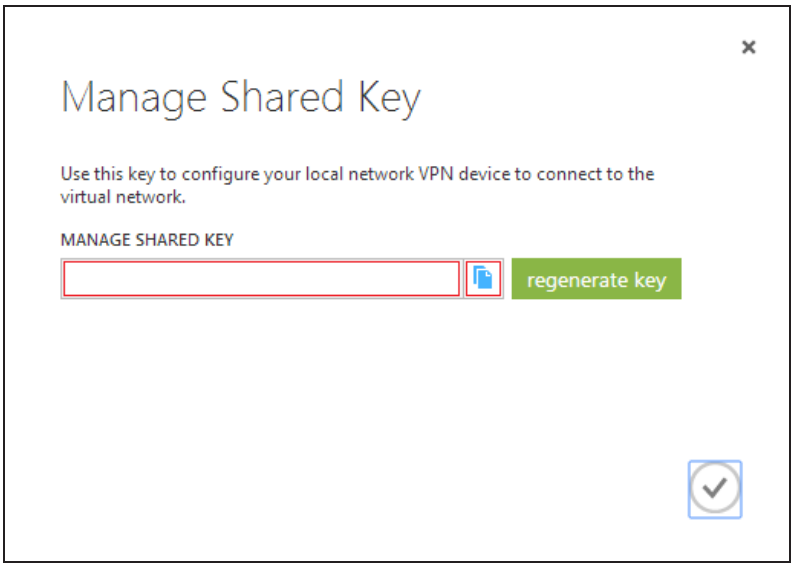
The gateway will then attempt to connect to the Local Network.



At the bottom of the screen, select **Manage Key**.

The 'Manage Shared Key' dialogue appears. **Copy** the key that is shown. You can select **regenerate key** if you want to copy a different key.

Click the **Checkmark** when you are confident that the key is copied.

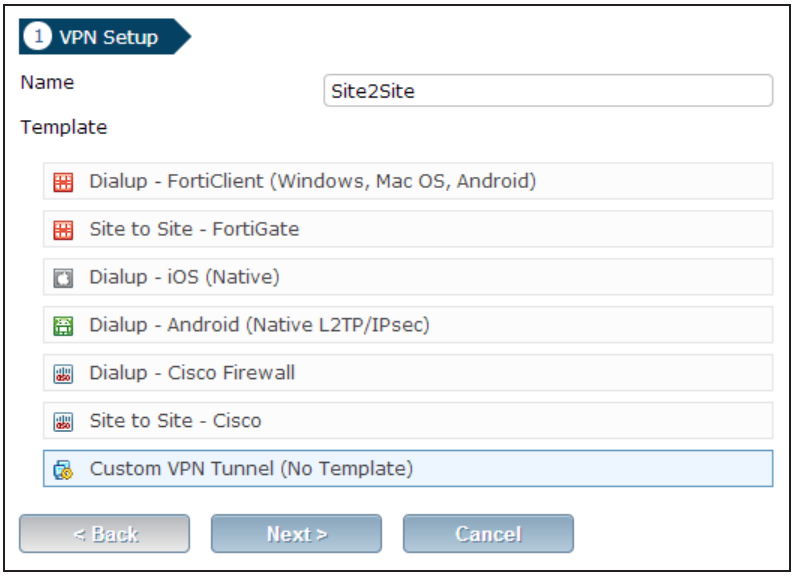


You are now ready to configure the FortiGate endpoint of the tunnel.

3. Configuring the FortiGate tunnel

Go to **VPN > IPsec > Wizard** and select **Custom VPN Tunnel (No Template)**.

Enter a **Name** for the tunnel and click **Next**.

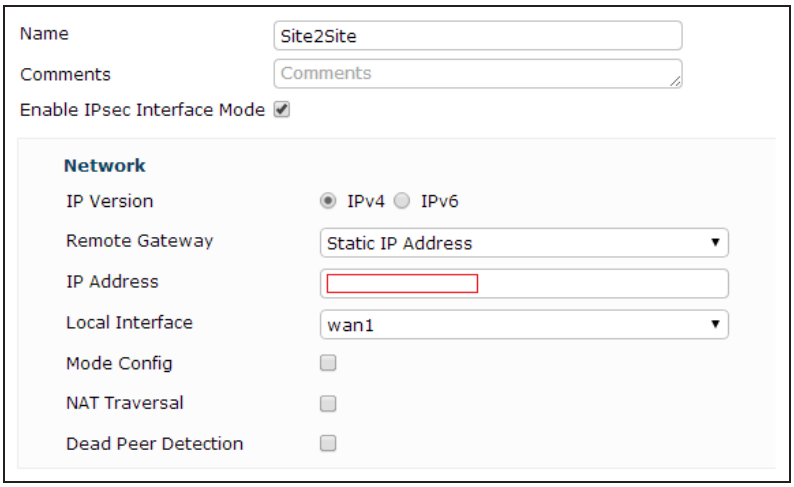


Enter the desired parameters. Set the **Remote Gateway** to **Static IP Address**, and include the gateway **IP Address** provided by Microsoft Azure.

Set the **Local Interface** to **wan1**.

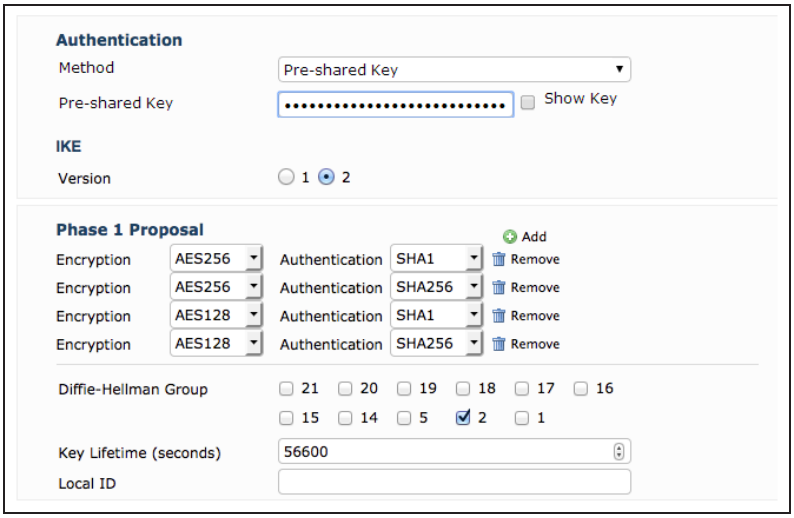
Under **Authentication**, enter the **Pre-shared Key** provided by Microsoft Azure.

Disable **NAT Transversal** and **Dead Peer Detection**.



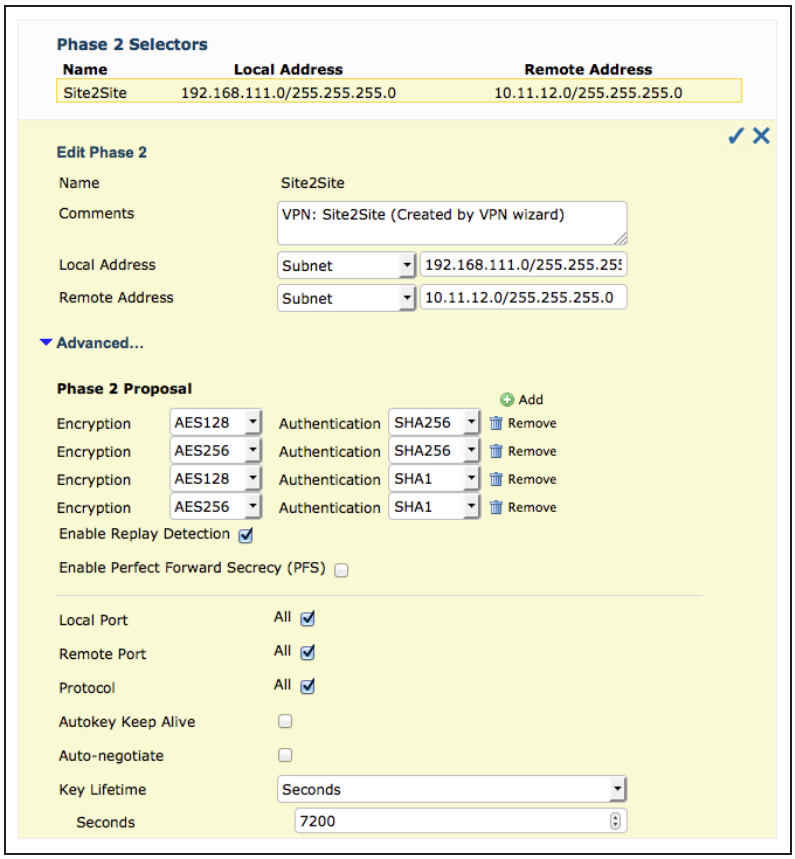
Under **Authentication**, ensure that you enable **IKEv2** and set **DH Group** to **2**.

Enable the encryption types shown and set the **Keylife** to **56660** seconds.



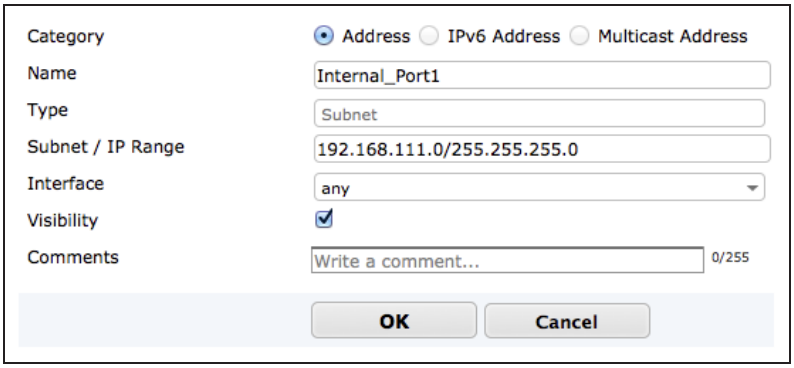
Scroll down to **Phase 2 Selectors** and set **Local Address** to the local subnet and **Remote Address** to the VPN tunnel endpoint subnet (found under 'Virtual Network Address Spaces in Microsoft Azure).

Enable the encryption types to match Phase 1 and set the **Keylife** to **7200 seconds.**

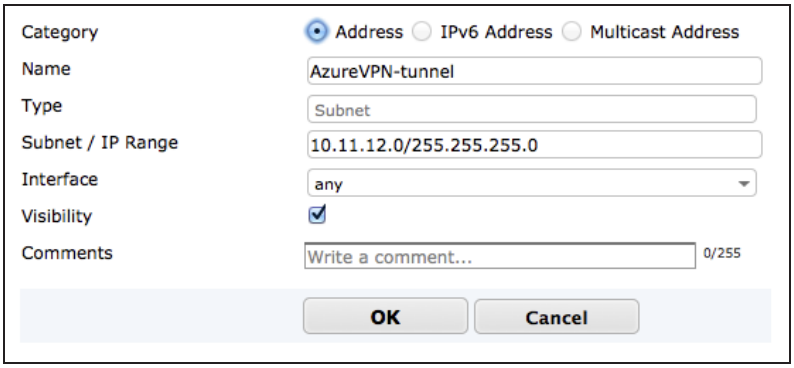


4. Creating the FortiGate firewall addresses

Go to **Policy & Objects> Objects > Addresses** and configure a firewall address for the local network.



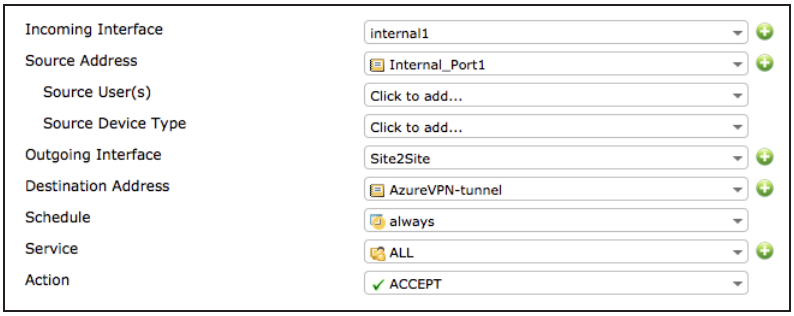
Create another firewall object for the Azure VPN tunnel subnet.



5. Creating the FortiGate firewall policies

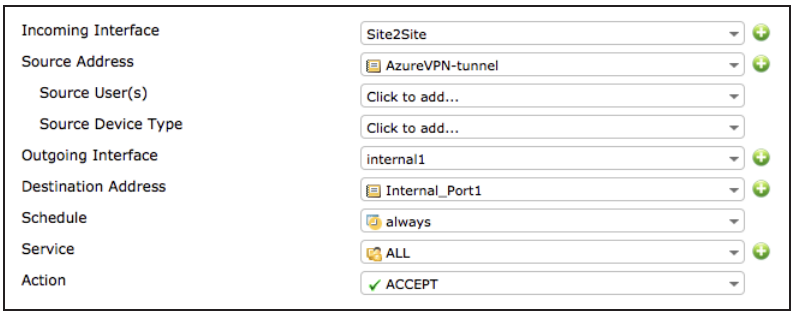
Go to **Policy & Objects > Policy > IPv4** and create a new policy for the site-to-site connection that allows outgoing traffic

Set the **Source Address** and **Destination Address** using the firewall objects you just created.



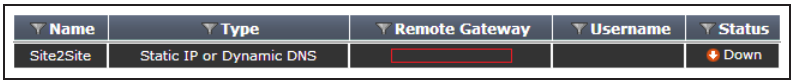
When you are done, create another policy for the same connection to allow incoming traffic.

This time, invert the **Source Address** and **Destination Address**.



6. Results

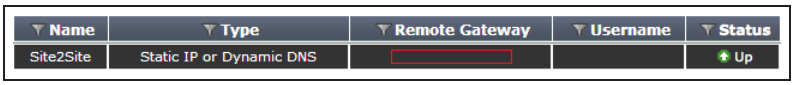
Go to **VPN > Monitor > IPsec > Monitor**. Right-click the tunnel you created and select **Bring Up** to activate the tunnel.



Name	Type	Remote Gateway	Username	Status
Site2Site	Static IP or Dynamic DNS			Down

Go to **Log & Report > Event Log > VPN**.

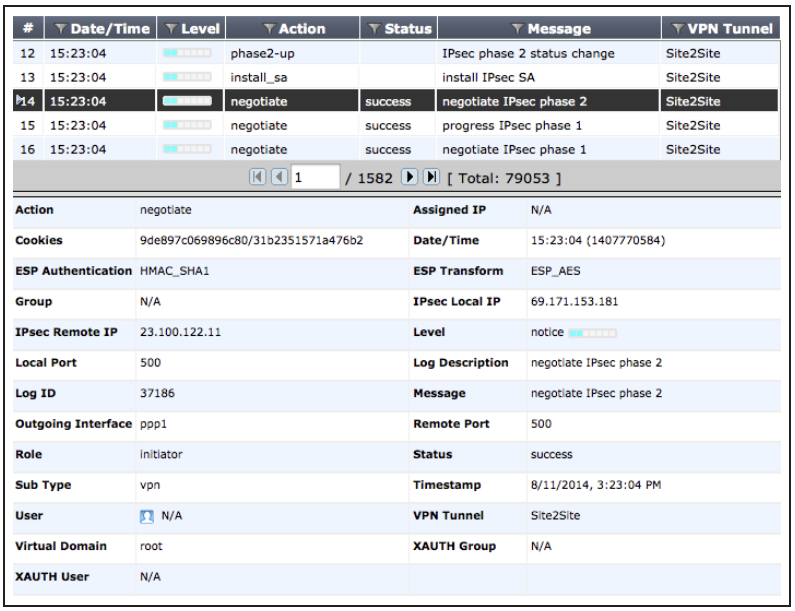
Select an entry to view more information and verify the connection.



Name	Type	Remote Gateway	Username	Status
Site2Site	Static IP or Dynamic DNS			Up

Go to **Log & Report > Event Log > VPN**.

Select an entry to view more information and verify the connection.



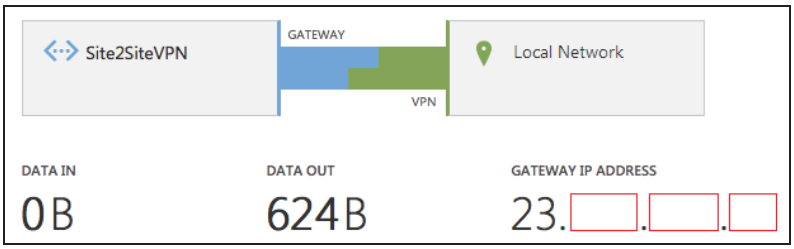
#	Date/Time	Level	Action	Status	Message	VPN Tunnel
12	15:23:04		phase2-up		IPsec phase 2 status change	Site2Site
13	15:23:04		install_sa		install IPsec SA	Site2Site
14	15:23:04		negotiate	success	negotiate IPsec phase 2	Site2Site
15	15:23:04		negotiate	success	progress IPsec phase 1	Site2Site
16	15:23:04		negotiate	success	negotiate IPsec phase 1	Site2Site

1 / 1582 [Total: 79053]

Action	negotiate	**Assigned IP**	N/A
Cookies	9de897c069896c80/31b2351571a476b2	**Date/Time**	15:23:04 (1407770584)
ESP Authentication	HMAC_SHA1	**ESP Transform**	ESP_AES
Group	N/A	**IPsec Local IP**	69.171.153.181
IPsec Remote IP	23.100.122.11	**Level**	notice
Local Port	500	**Log Description**	negotiate IPsec phase 2
Log ID	37186	**Message**	negotiate IPsec phase 2
Outgoing Interface	ppp1	**Remote Port**	500
Role	initiator	**Status**	success
Sub Type	vpn	**Timestamp**	8/11/2014, 3:23:04 PM
User	N/A	**VPN Tunnel**	Site2Site
Virtual Domain	root	**XAUTH Group**	N/A
XAUTH User	N/A		

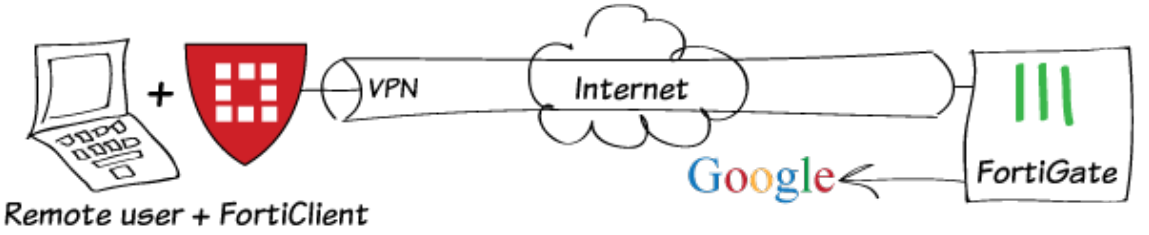
Return to the Microsoft Azure virtual network **Dashboard**. The status of the tunnel will show as **Connected**.

Data In and **Data Out** will indicate that traffic is flowing.



For further reading, check out Gateway-to-gateway configurations in the FortiOS 5.2 Handbook.

Remote Internet browsing using a VPN



In this recipe, you will use remote IPsec and SSL VPN tunnels to bypass Internet access restrictions.

Restricted Internet access is simulated with a Web Filter profile that blocks google.com. You will create FortiClient SSL and IPsec VPN tunnels to bypass the web filter, connect to a remote FortiGate unit, and transparently browse the Internet to google.com.

The recipe assumes that a "vpn_users" user group and a Local LAN firewall address have already been created.

1. Starting point

In this example, we simulate restricted Internet access using a Web Filtering profile to block Google.

With the user situated behind this FortiGate, google.com cannot be accessed, and instead the FortiGuard "Web Page Blocked" message appears.

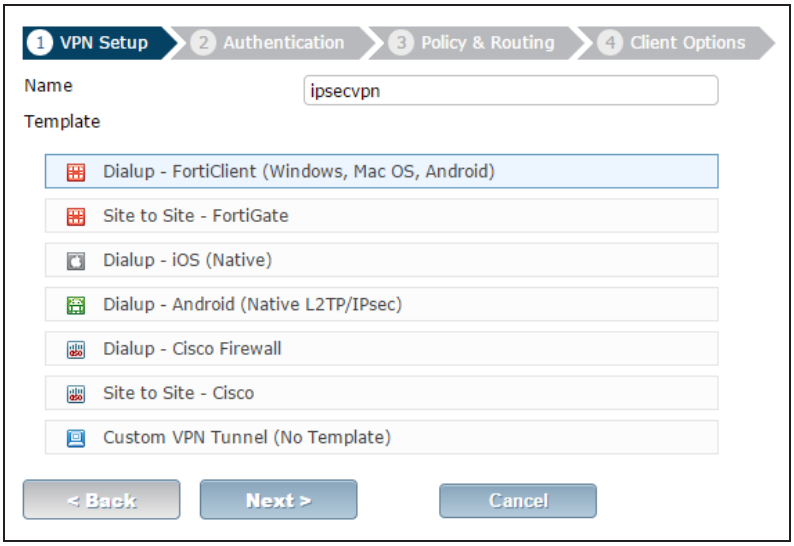
For the user to bypass this Web Filter, the following VPN configurations must be made on a remote FortiGate (which is not blocked by any filter), and the user must connect to it using FortiClient.

2. Configuring the IPsec VPN

On the remote Fortigate, go to **VPN > IPSec > Wizard**.

Name the VPN connection and select **Dial Up - FortiClient (Windows, Mac OS, Android)** and click **Next**.

The tunnel name must not have any spaces in it.

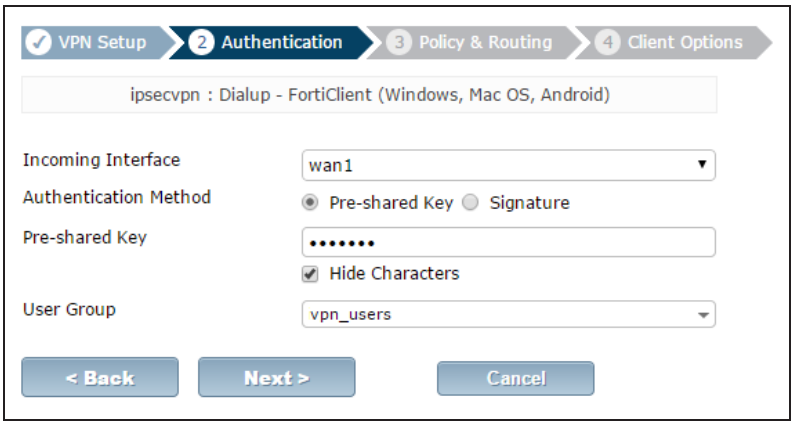


Set the **Incoming Interface** to the internet-facing interface. In this case, **wan1**.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key and select the **vpn_users** user group, then click **Next**.

The pre-shared key is a credential for the VPN and should differ from the user's password.

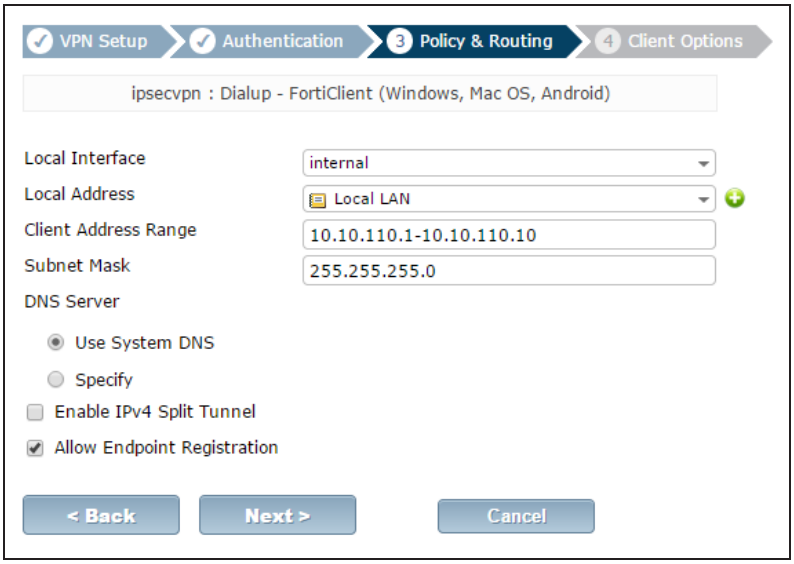


Set **Local Interface** to the internal interface and set **Local Address** to the local LAN address.

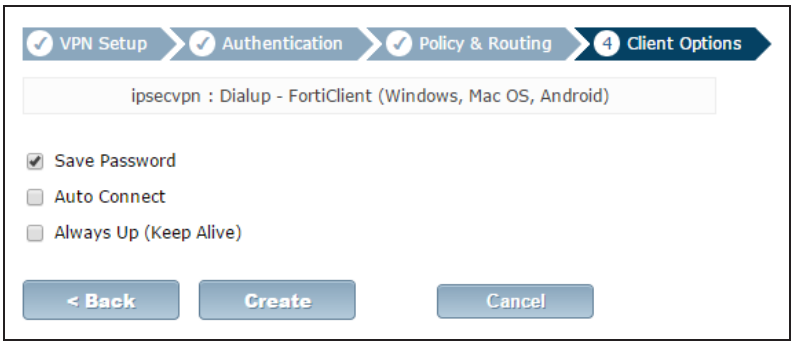
Enter an IP range for VPN users in the **Client Address Range** field.

The IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the _range suffix (in this case, ipsecvpn_range).

In addition, FortiOS automatically creates a security policy to allow remote users to access the internal network.



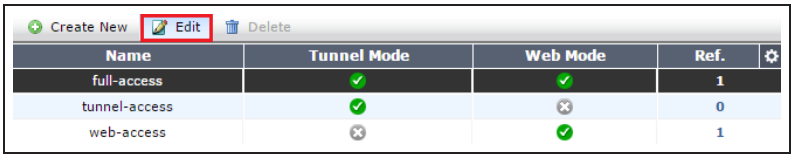
Click **Next** and select **Client Options** as desired.



When using the IPsec VPN Wizard, an IPsec firewall address range is automatically created using the name of the tunnel you entered into the Wizard. The Wizard also creates an **IPsec -> internal** IPv4 policy, so all that is left is to create the Internet access policy. See Step 4.

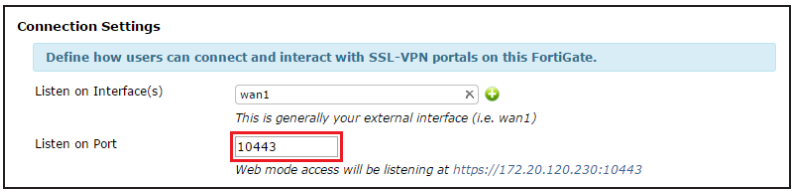
3. Configuring the SSL VPN

Go to **VPN > SSL > Portals**, highlight the **full-access** portal, and select **Edit**.

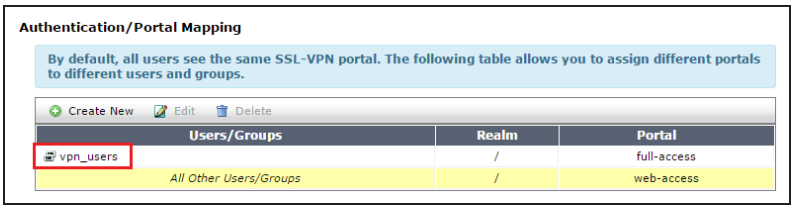


Disable **Split Tunneling** so that all VPN traffic will go through the FortiGate firewall.

Go to **VPN > SSL > Settings**. Under **Connection Settings** set **Listen on Port** to **10443**.



Under **Authentication/Portal Mapping**, assign the **vpn_users** user group to the **full-access** portal, and assign **All Other Users/Groups** to the desired portal.



By default, the FortiGate has an **ssl.root** firewall address. All that is left is to create the Internet access policy, as described in the following step.

4. Creating security policies for VPN access to the Internet

Go to **Policy & Objects > Policy > IPv4**.

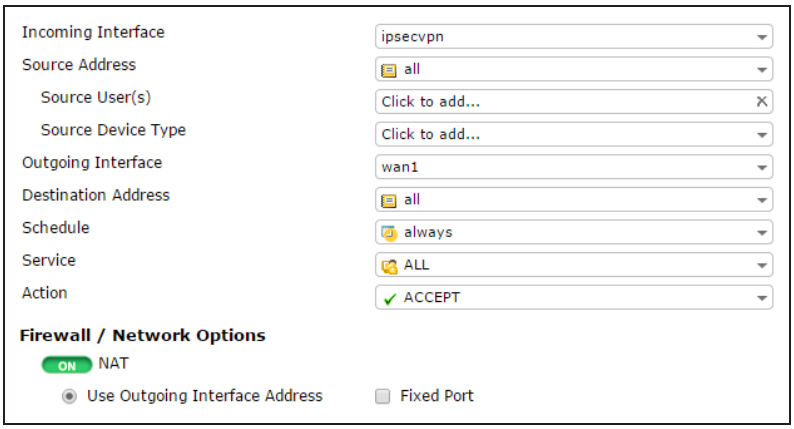
Create two security policies allowing remote users to access the Internet securely through the FortiGate unit; one for each VPN tunnel.

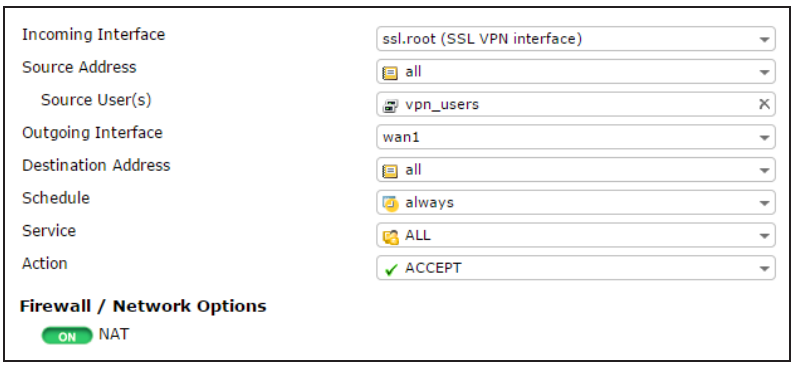
Set **Incoming Interface** to the tunnel interface and set **Source Address** to **all**.

For SSL VPN, set **Source User(s)** to the **vpn_users** user group.

Set **Outgoing Interface** to **wan1** and **Destination Address** to **all**.

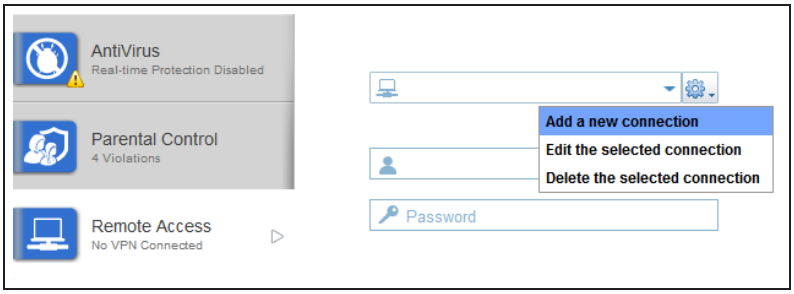
Set **Service** to **ALL** and ensure that you enable **NAT**.





5. Configuring FortiClient for IPsec and SSL VPN

Open FortiClient, go to **Remote Access** and add new connections for both VPNs.

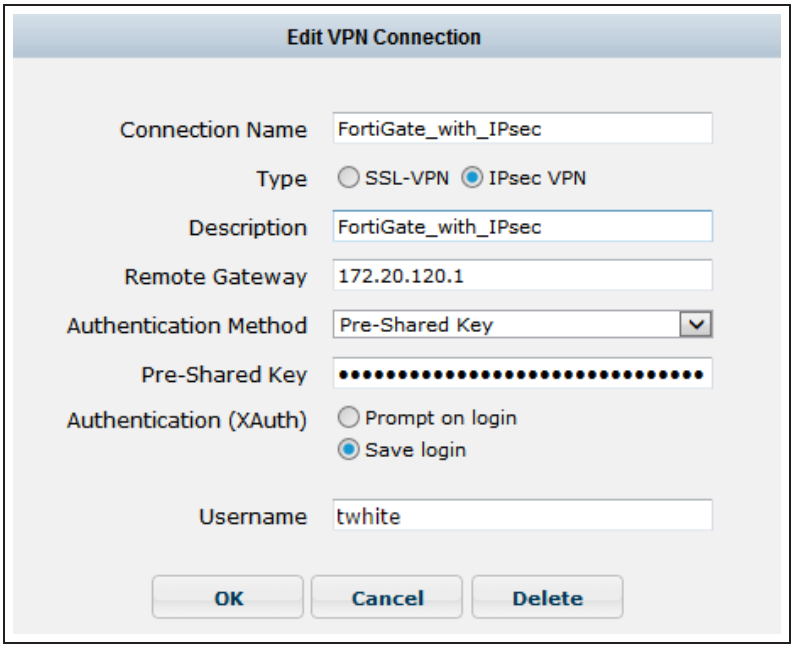


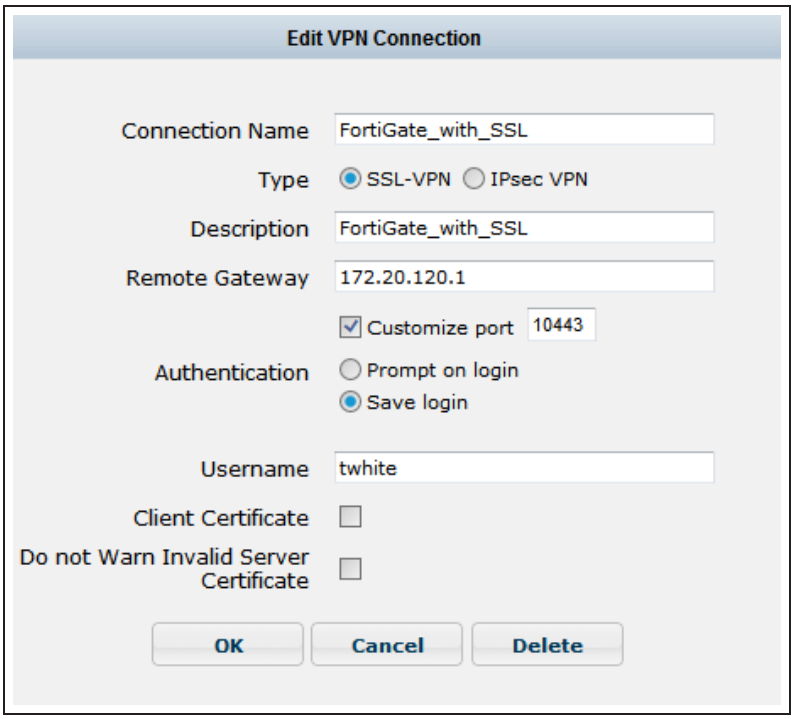
Provide a **Connection Name** and set the **Type** to either **IPsec VPN** or **SSL VPN** depending on the VPN configuration.

Set **Remote Gateway** to the FortiGate IP address.

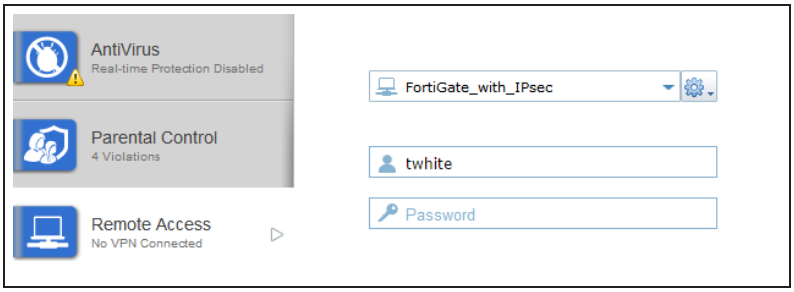
- For IPsec VPN, set **Authentication Method** to **Pre-Shared Key** and enter the key below.
- For SSL VPN, set **Customize Port** to **10443**.

(Optional) For **Username**, enter a username from the **vpn_users** user group.





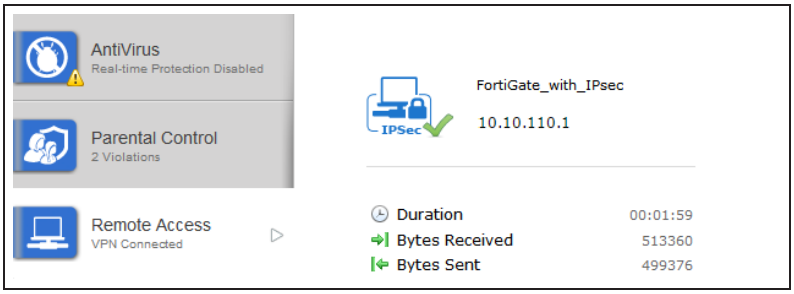
Select the new connection, enter the username and password, and click **Connect**.

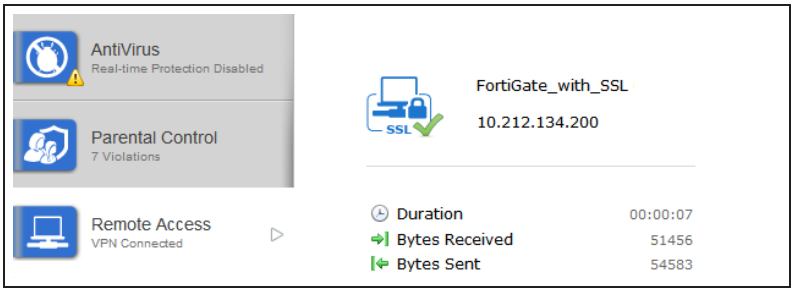


If prompted with a server authentication warning, select **Yes**.

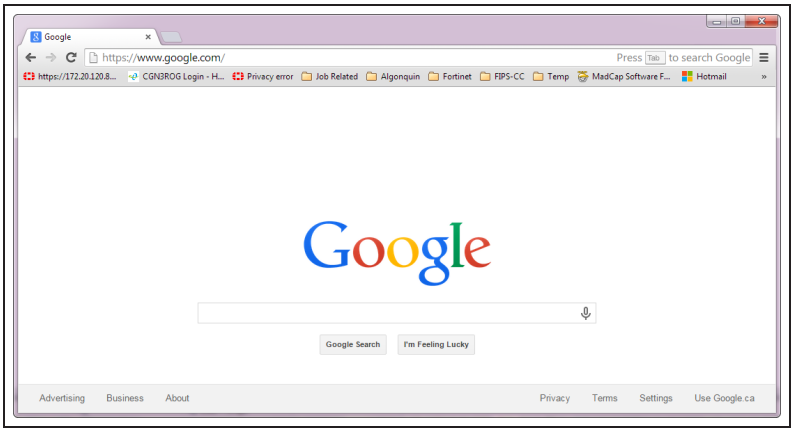
6. Results

From FortiClient start an IPsec or SSL VPN session. Once the connection is established, the FortiGate assigns the user an IP address and FortiClient displays the status of the connection, including the IP address, connection duration, and bytes sent and received.



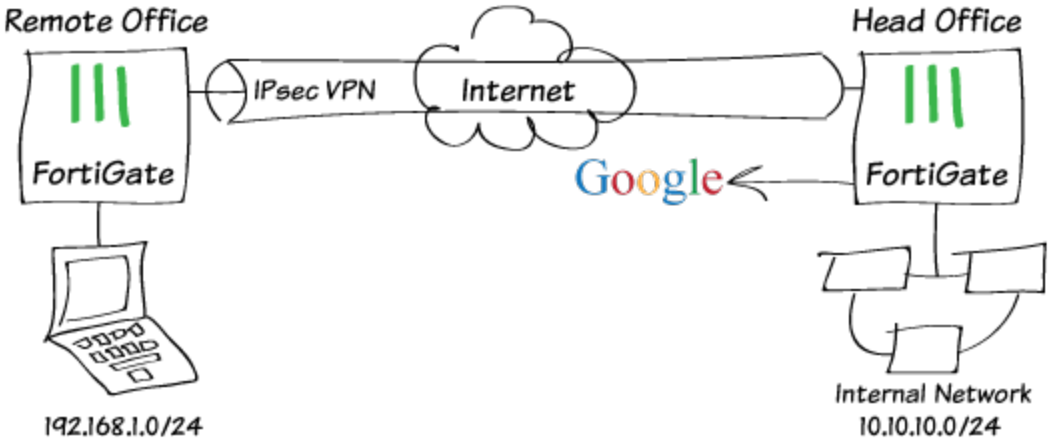


With the tunnel up, you can now visit google.com without being blocked, since the Internet traffic is handled by the remote FortiGate and the web filter on the local FortiGate has been bypassed.



For further reading, check out IPsec VPN in the web-based manager in the FortiOS 5.2 Handbook.

Remote browsing using site-to-site IPsec VPN



In this recipe, you will configure a site-to-site, also called gateway-to-gateway, IPsec VPN between an office with Internet access restrictions (Remote Office) and an office without these restrictions (Head Office) so that the Remote Office can access the Internet through the Head Office, avoiding the restrictions.

To bypass this restriction, this example shows how create a site-to-site VPN to connect the Remote Office FortiGate unit to the Head Office FortiGate unit, and allow Remote Office staff to transparently browse the Internet to google.com using the Head Office's Internet connection.

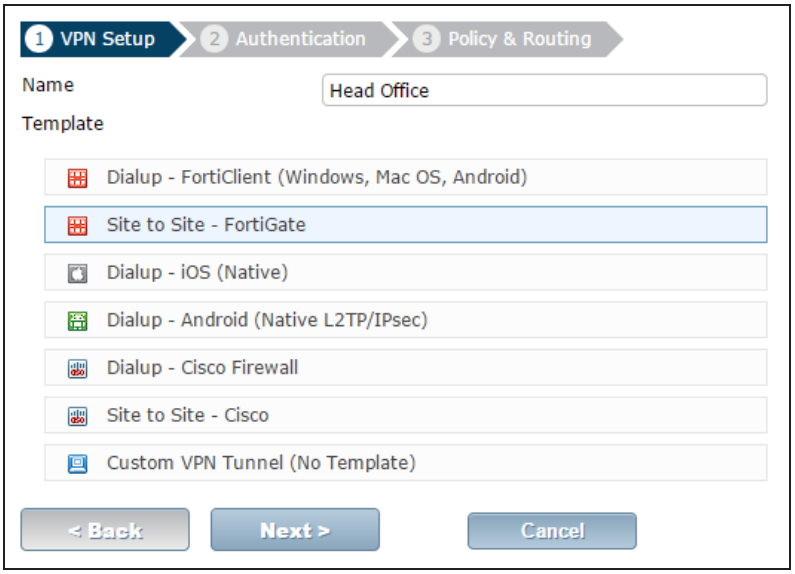
Note that both FortiGates run FortiOS firmware version 5.2.2 and have static IP addresses on Internet-facing interfaces. You will also need to know the Remote Office's gateway IP address.

1. Configuring IPsec VPN on the Head Office FortiGate

In a real world scenario, a Remote Office's ISP or something in their local Internet may be blocking access to Google, or any other site for that matter.

On the Head Office FortiGate, go to **VPN > IPSec > Wizard**.

Name the VPN, select **Site to Site - FortiGate,** and click **Next**.



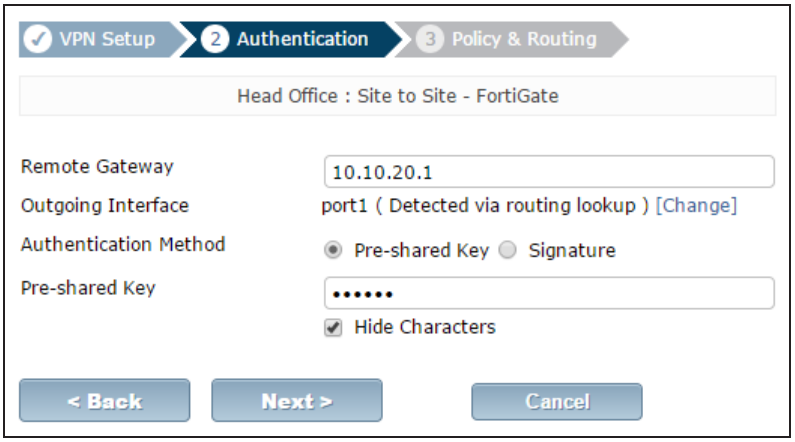
Set the **Remote Gateway** to the Remote Office FortiGate IP address

The Wizard should select the correct **Outgoing Interface** when you click anywhere else in the window. Depending on your configuration, you may have to manually set the outgoing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key then click **Next**.

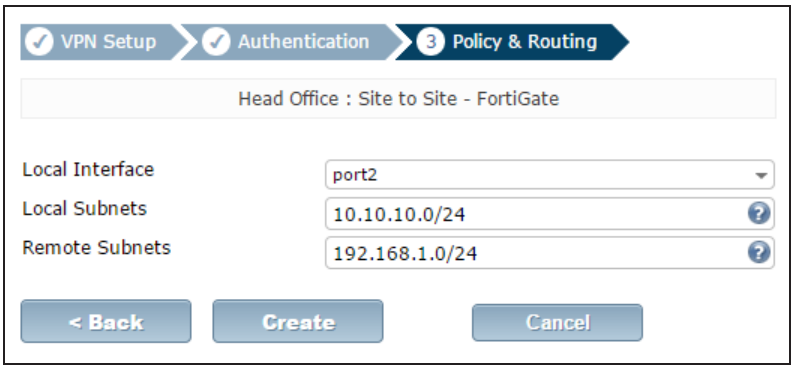
The pre-shared key is a credential for the VPN and should differ from the user's password. Both FortiGate's must have the same pre-shared key.



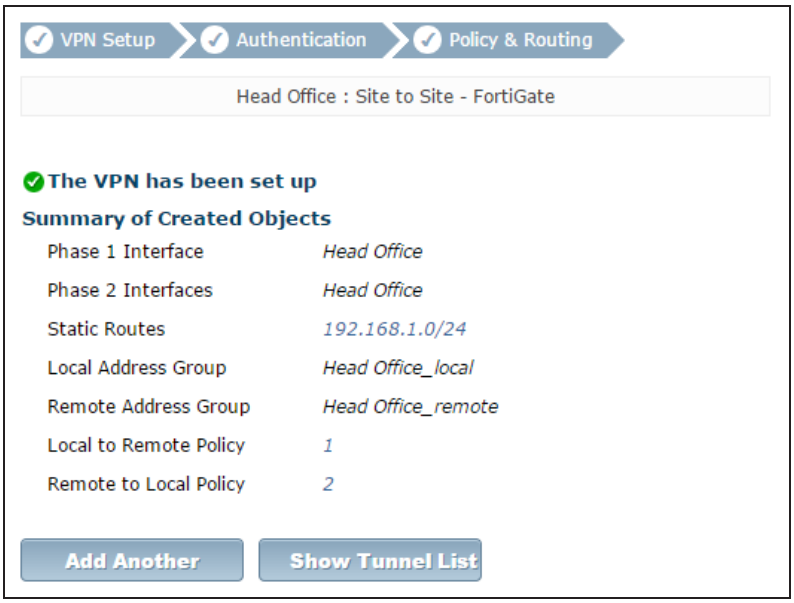
Under **Policy & Routing**, set the **Local Interface** to the interface connected to the Head Office internal network.

For **Local Subnets**, enter the subnet range of the Head Office internal network. Depending on your configuration, this may be set automatically by the wizard.

For **Remote Subnets**, enter the subnet range of the Remote Office internal network then click **Create**.



The VPN Wizard informs you that a static route has been created, as well as two two security policies and two address objects, which are added to two address groups (also created).

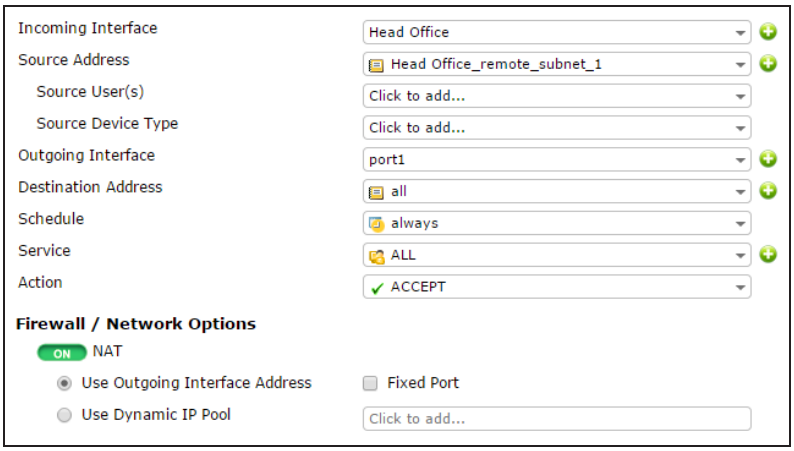


Create a security policy to allow the Remote Office to have Internet access. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.

Set **Incoming Interface** to the VPN interface created by the VPN wizard and set **Source Address** to the remote office address group created by the VPN wizard.

Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **all**.

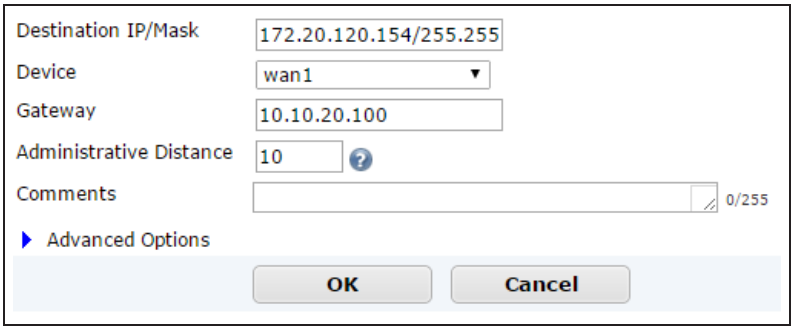
Enable **NAT** and (optionally) enforce any company security profiles.



2. Adding a route on the Remote Office FortiGate

On the Remote Office FortiGate, create a static route that forwards traffic destined for the Head Office FortiGate to the ISP's Internet gateway.

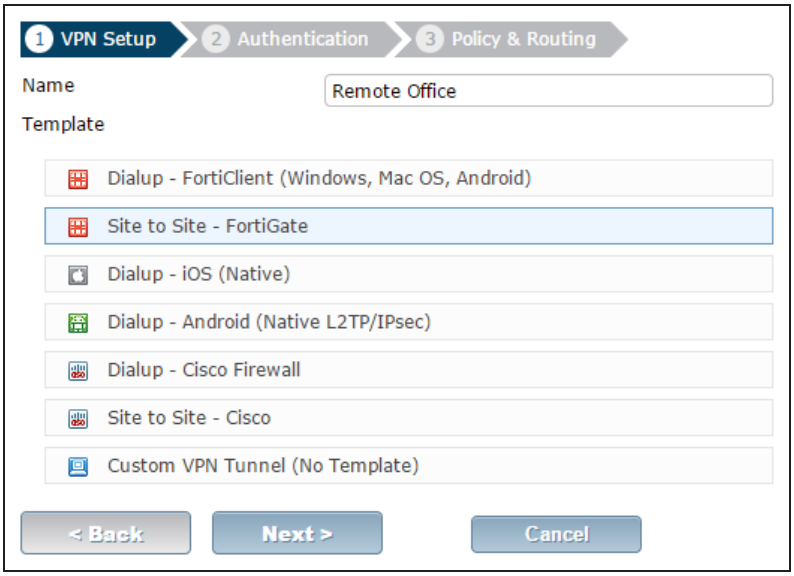
(In this example, the Head Office FortiGate IP address is 172.20.120.154 so the destination IP/Mask is 172.20.120.154/255.255.255.0 and the ISP's gateway IP address is 10.10.20.100.)



3. Configuring IPsec VPN on the Remote Office FortiGate

On the Remote Office FortiGate, go to **VPN > IPSec > Wizard**.

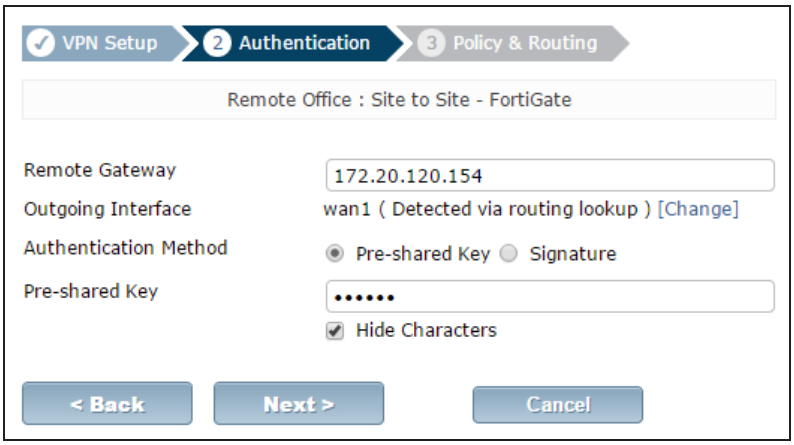
Name the VPN, select **Site to Site - FortiGate,** and click **Next**.



Set the **Remote Gateway** to the Head Office FortiGate IP address.

The Wizard should select the correct **Outgoing Interface**.

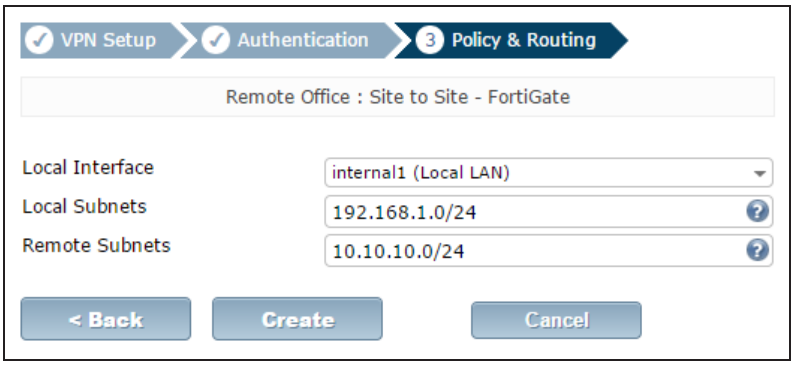
Select **Pre-shared Key** for the **Authentication Method** and enter the same **Pre-shared Key** as you entered in Step 1.



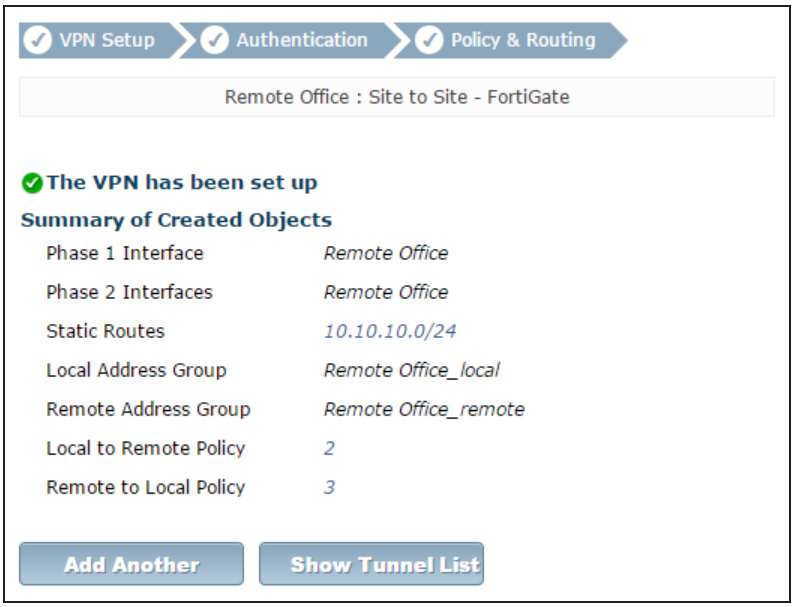
Under **Policy & Routing**, set the **Local Interface** to the interface connected to the Remote Office internal network.

For **Local Subnets**, enter the subnet range of the Remote Office internal network.

For **Remote Subnets**, enter the subnet range of the Head Office internal network then click **Create**.



The VPN Wizard informs you that a static route has been created, as well as two address groups and two security policies.

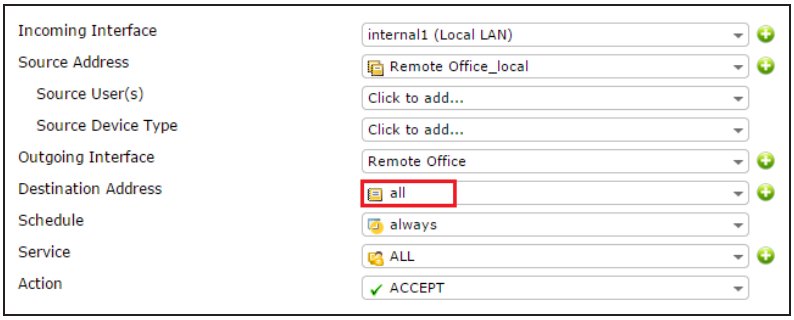


Allow Internet traffic from the remote office to enter the VPN tunnel.

On the Remote Office FortiGate, go to **Policy & Objects > Policy > IPv4**.

Edit the outbound security policy created by the VPN Wizard.

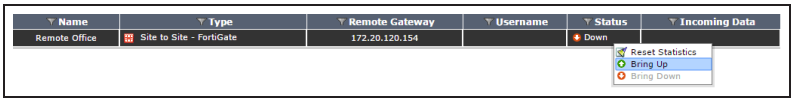
Change the **Destination Address** to **all** so that the policy accepts Internet traffic.



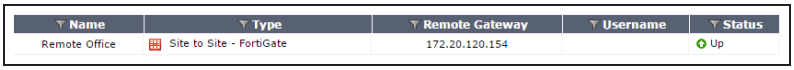
4. Establishing the tunnel

On either FortiGate, go to **VPN > Monitor > IPsec Monitor**.

Right-click the newly created tunnel and select **Bring Up**.

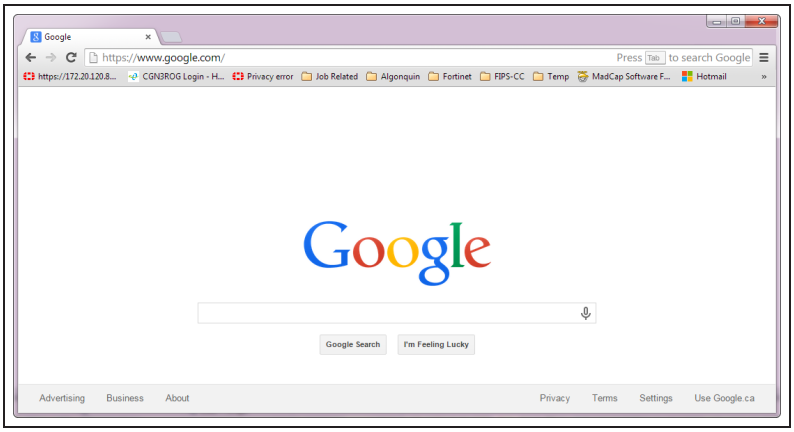


If the tunnel is established, the **Status column** will read **Up** on both of the FortiGates.



6. Results

With the tunnel up, you can now visit google.com without being blocked, since the Internet traffic is handled by the Head Office FortiGate and the access restrictions on the remote FortiGate have been bypassed.



For further reading, check out IPsec VPN in the web-based manager in the FortiOS 5.2 Handbook.

IPsec troubleshooting

This section contains tips to help you with some common challenges of IPsec VPNs.

The options to configure policy-based IPsec VPN are unavailable.

Go to **System > Config > Features**. Select Show More and turn on Policy-based IPsec VPN.

The VPN connection attempt fails.

If your VPN fails to connect, check the following:

- Ensure that the pre-shared keys match exactly.
- Ensure that both ends use the same P1 and P2 proposal settings.
- Ensure that you have allowed inbound and outbound traffic for all necessary network services, especially if services such as DNS or DHCP are having problems.
- Check that a static route has been configured properly to allow routing of VPN traffic.
- Ensure that your FortiGate unit is in NAT/Route mode, rather than Transparent.
- Check your NAT settings, enabling NAT traversal in the Phase 1 configuration while disabling NAT in the security policy.
- Ensure that both ends of the VPN tunnel are using Main mode, unless multiple dial-up tunnels are being used.
- If you have multiple dial-up IPsec VPNs, ensure that the Peer ID is configured properly on the FortiGate and that clients have specified the correct Local ID.
- If you are using FortiClient, ensure that your version is compatible with the FortiGate firmware by reading the FortiOS Release Notes.
- Ensure that the Quick Mode selectors are correctly configured. If part of the setup currently uses firewall addresses or address groups, try changing it to either specify the IP addresses or use an expanded address range.
- If XAUTH is enabled, ensure that the settings are the same for both ends, and that the FortiGate unit is set to Enable as Server.
- If your FortiGate unit is behind a NAT device, such as a router, configure port forwarding for UDP ports 500 and 4500.
- Remove any Phase 1 or Phase 2 configurations that are not in use. If a duplicate instance of the VPN tunnel appears on the IPsec Monitor, reboot your FortiGate unit to try and clear the entry.

If you are still unable to connect to the VPN tunnel, run the diagnostic command in the CLI:

```
diag debug application ike -1
diag debug enable
```

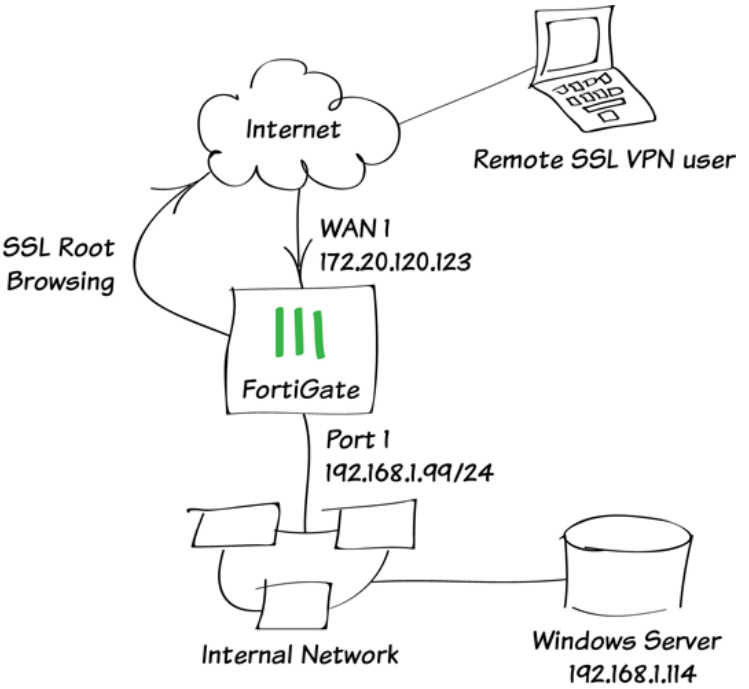
The resulting output may indicate where the problem is occurring. When you are finished, disable the diagnostics by using the following command:

```
diag debug reset
diag debug disable
```

The VPN tunnel goes down frequently.

If your VPN tunnel goes down often, check the Phase 2 settings and either increase the **Keylife** value or enable **Autokey Keep Alive**.

SSL VPN for remote users



This example provides remote users with access to the corporate network using SSL VPN and connect to the Internet through the corporate FortiGate unit. During the connecting phase, the FortiGate unit will also verify that the remote user's antivirus software is installed and current.

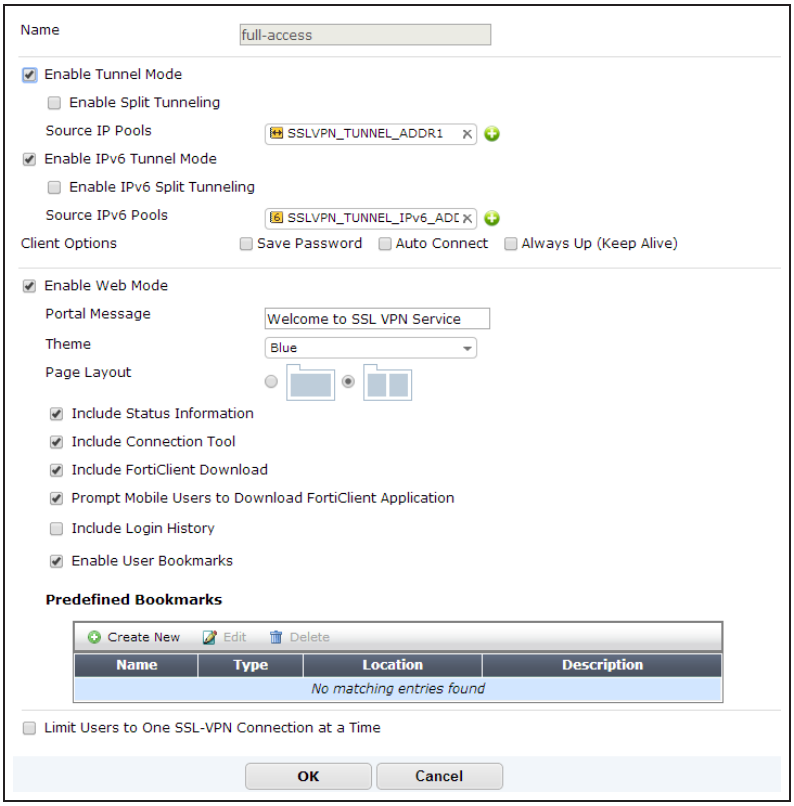
A video of this recipe can be found here.

1. Creating an SSL VPN portal for remote users

Go to **VPN > SSL > Portals**.

Edit the **full-access** portal. The full-access portal allows the use of tunnel mode and/or web mode. In this scenario we are using both modes.

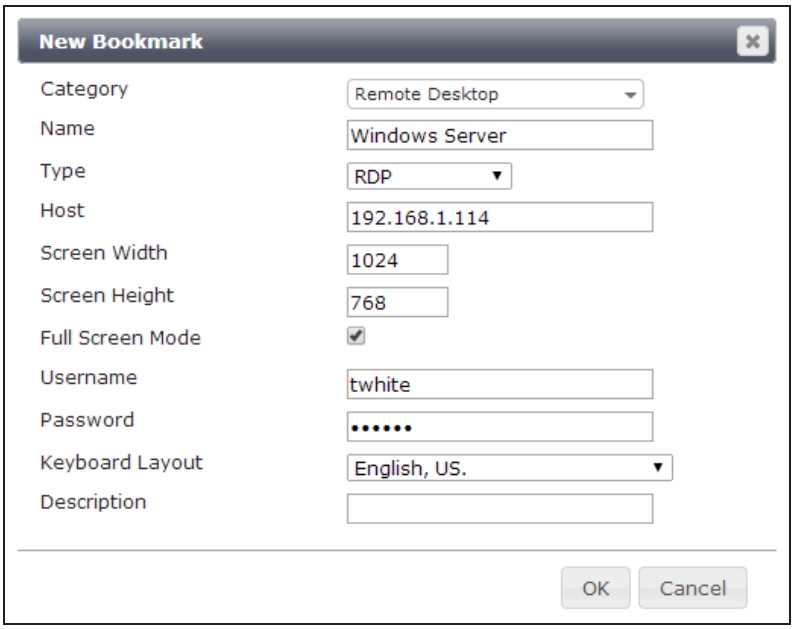
Enable Split Tunneling is *not* enabled so that all Internet traffic will go through the FortiGate unit and be subject to the corporate security profiles.



Select **Create New** in the Predefined Bookmarks area to add a bookmark for a remote desktop link/connection.

Bookmarks are used as links to internal network resources.

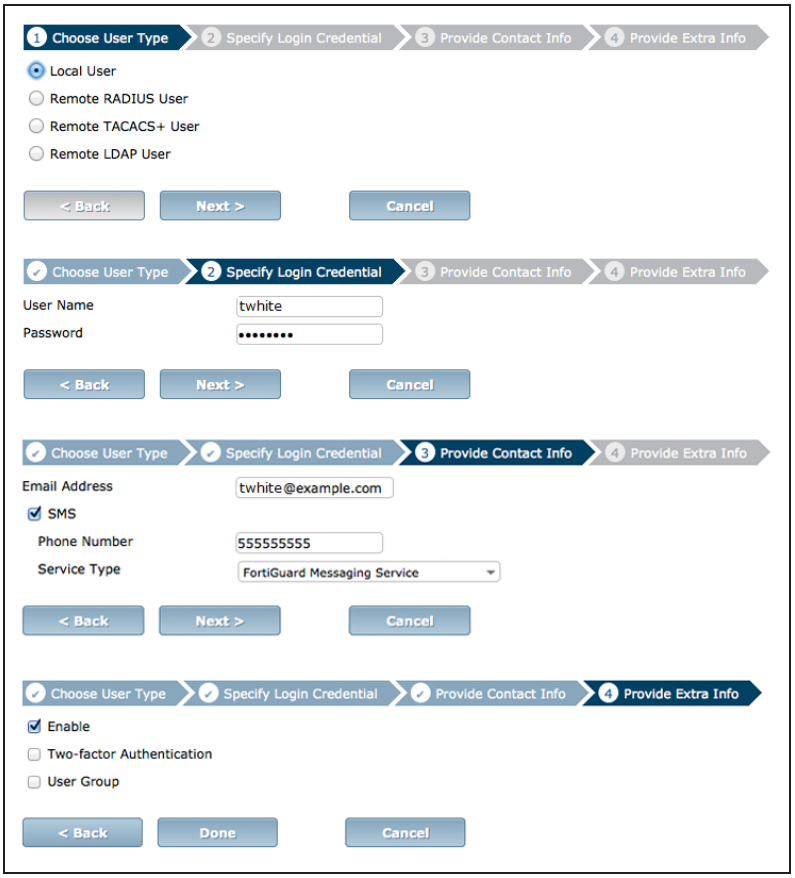
You must include a username and password. You will create this user in the next step, so be sure to use the same credentials.



2. Creating a user and a user group

Go to **User & Device > User > User Definition**.

Add a remote user with the **User Creation Wizard** (in the example, *twhite*, with the same credentials used for the predefined bookmark).



Go to **User & Device > User > User Groups**.

Add the user *twhite* to a user group for SSL VPN connections.

3. Adding an address for the local network

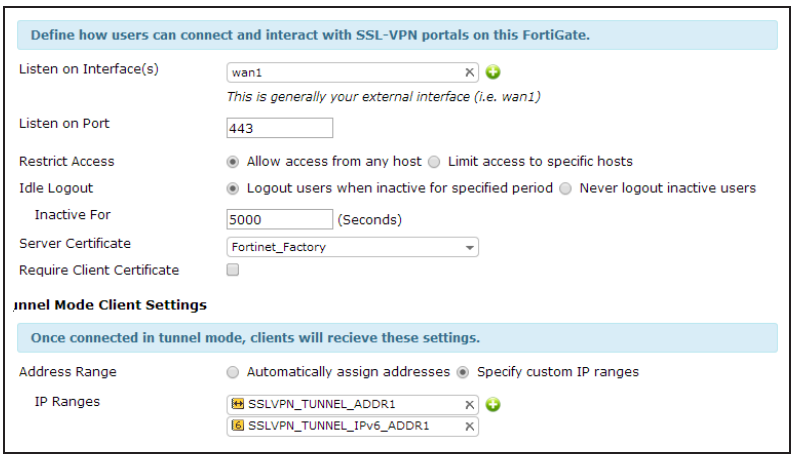
Go to **Policy & Objects > Objects > Addresses**.

Add the address for the local network. Set **Subnet / IP Range** to the local subnet and set **Interface** to an internal port.

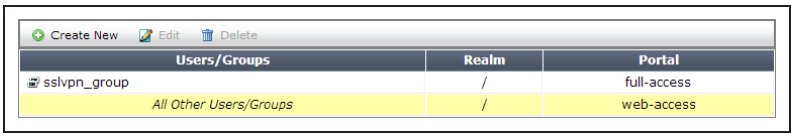
4. Configuring the SSL VPN tunnel

Go to **VPN > SSL > Settings** and set **Listen on Interface(s)** to **wan1**.

Set **Listen on Port** to **443** and **Specify custom IP ranges**.



Under **Authentication/Portal Mapping**, add the SSL VPN user group.



5. Adding security policies for access to the Internet and internal network

Go to **Policy & Objects > Policy > IPv4**.

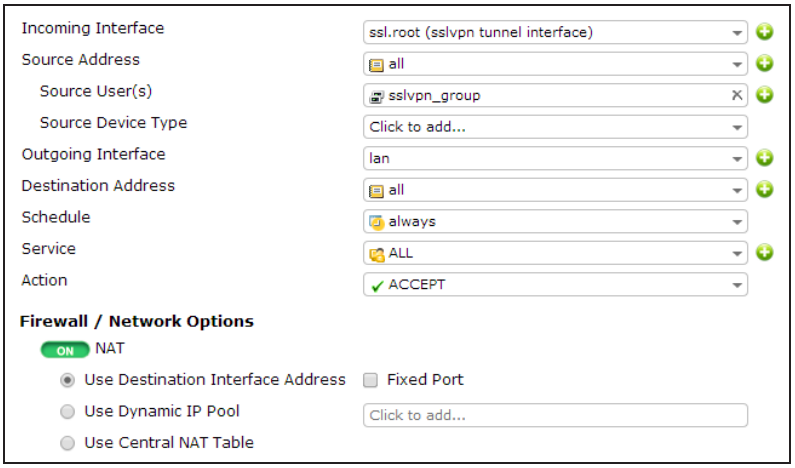
Add a security policy allowing access to the internal network through the *ssl.root* VPN tunnel interface.

Set **Incoming Interface** to **ssl.root**.

Set **Source Address** to **all** and select the **Source User** group you created in step 2.

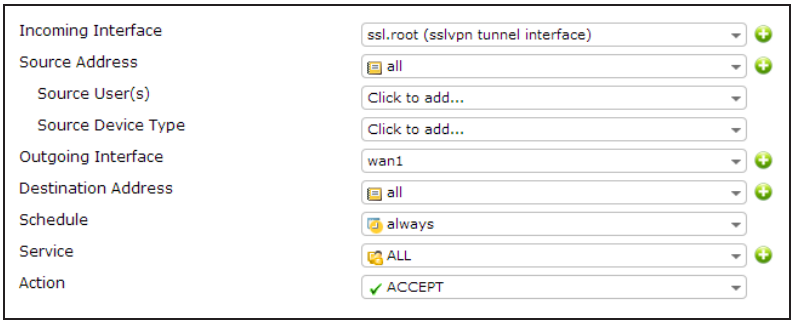
Set **Outgoing Interface** to the local network interface so that the remote user can access the internal network.

Set **Destination Address** to all, enable **NAT**, and configure any remaining firewall and security options as desired.



Add a second security policy allowing SSL VPN access to the Internet.

For this policy, **Incoming Interface** is set to **ssl.root** and **Outgoing Interface** is set to **wan1**.



6. Setting the FortiGate unit to verify users have current AntiVirus software

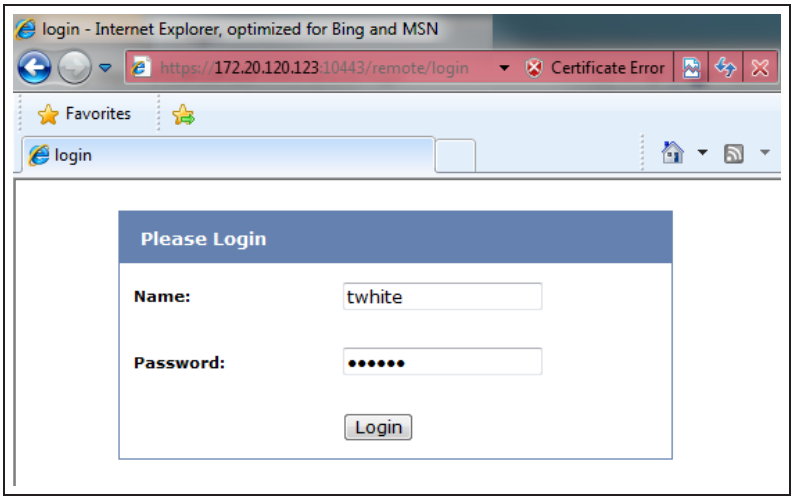
Go to **System > Status > Dashboard**.

In the **CLI Console** widget, enter the commands on the right to enable the host to check for compliant AntiVirus software on the remote user's computer.

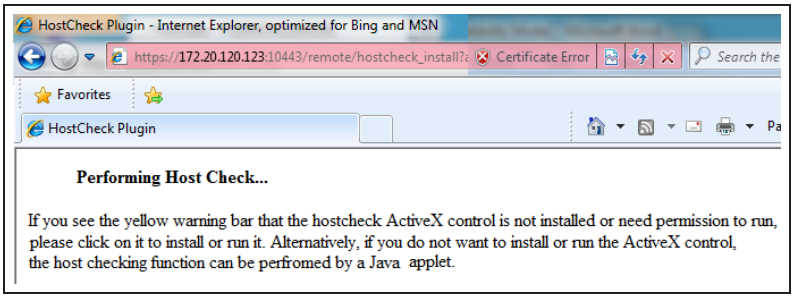
```
config vpn ssl web portal
   edit full-access
     set host-check av
   end
 end
```

7. Results

Log into the portal using the credentials you created in step 2.

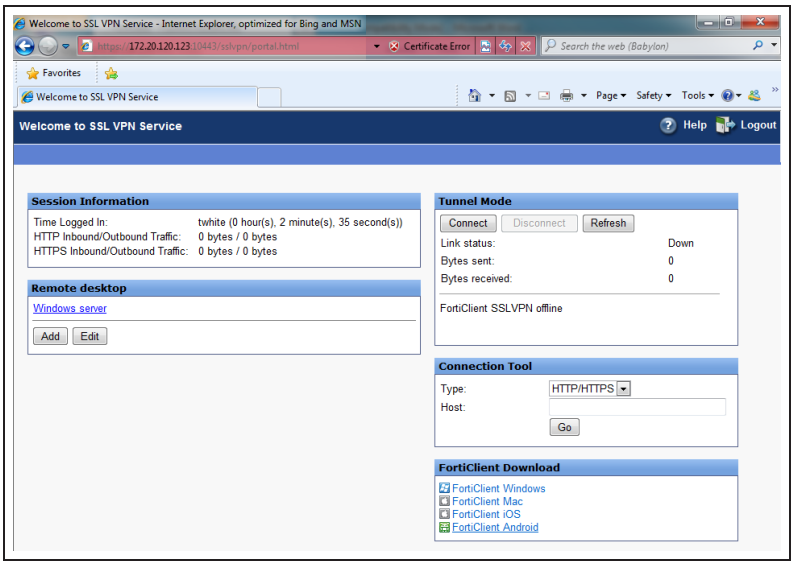


The FortiGate unit performs the host check.

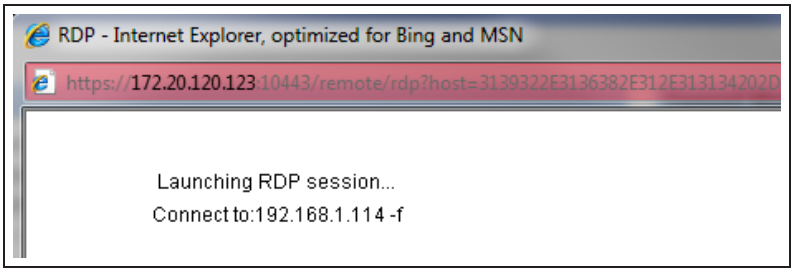


After the check is complete, the portal appears.

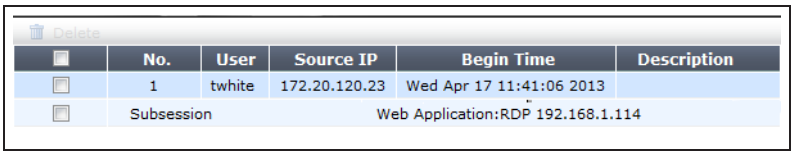
You may need to install the FortiClient application using the available download link.



Select the bookmark **Remote Desktop** link to begin an RDP session.



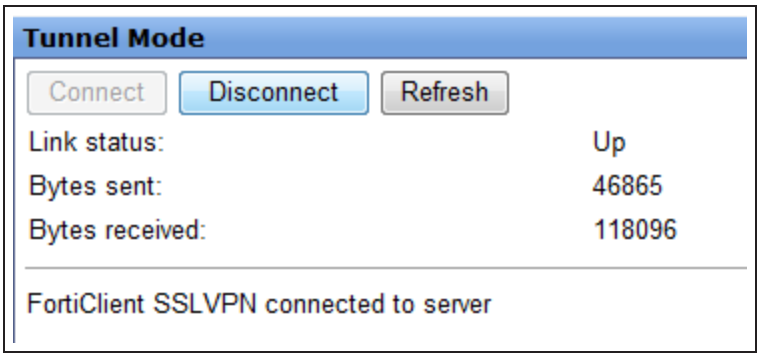
Go to **VPN > Monitor > SSL-VPN Monitor** to verify the list of SSL users. The Web Application description indicates that the user is using web mode.



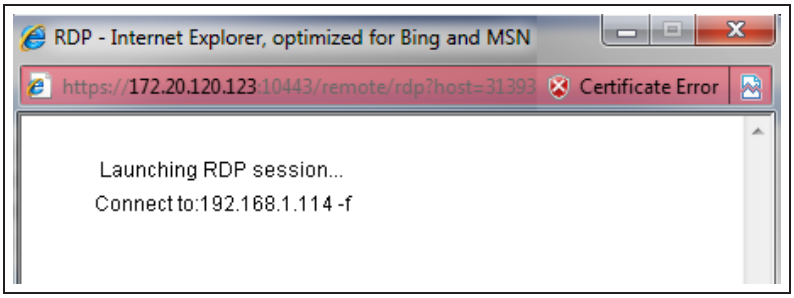
Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.

Dst	192.168.1.114	**Virtual Domain**	root
Received	85591	**Source Country**	Reserved
Sent / Received	8.71 KB / 83.58 KB	**Duration**	36
Sent	8923	**Application Details**	
Group	N/A	**Service**	RDP
Protocol	6	**User**	twhite
Destination Country	Reserved	**Dst Port**	3389
roll	65389	**Status**	✓
Timestamp	Wed Apr 17 14:13:11 2013	**Tran Display**	noop
Sequence Number	2700	**Policy ID**	11
Src Interface	wan1	**Src**	twhite (172.20.120.23)
VPN	sslvpn_web_mode	**Sent Packets**	71
Level	notice	**VPN Type**	sslvpn
Src Port	53712	**Log ID**	13
Sub Type	forward	**Threat**	
Received Packets	98	**Date/Time**	14:13:11 (Wed Apr 17 14:13:11 2013)
Dst Interface	port1		

In the **Tunnel Mode** widget, select **Connect** to enable the tunnel.



Select the bookmark **Remote Desktop** link to begin an RDP session.



Go to **VPN > Monitor > SSL-VPN Monitor** to verify the list of SSL users.

The tunnel description indicates that the user is using tunnel mode.

Delete

	No.	User	Source IP	Begin Time	Description
	1	twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
		Subsession		Tunnel IP:10.212.134.200	

Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.

Dst	192.168.1.114	**Virtual Domain**	root
Received	326664	**Source Country**	Reserved
Sent / Received	54.36 KB / 319.01 KB	**Duration**	83
Sent	55665	**Application Details**	
Group	N/A	**Service**	RDP
Protocol	6	**User**	twhite
Destination Country	Reserved	**Dst Port**	3389
roll	65389	**Status**	✓
Timestamp	Wed Apr 17 14:17:15 2013	**Tran Display**	noop
Sequence Number	3618	**Policy ID**	11
Src Interface	wan1	**Src**	twhite (172.20.120.23)
VPN	sslvpn_web_mode	**Sent Packets**	329
Level	notice	**VPN Type**	sslvpn
Src Port	53820	**Log ID**	13
Sub Type	forward	**Threat**	
Received Packets	407	**Date/Time**	14:17:15 (Wed Apr 17 14:17:15 2013)
Dst Interface	unknown-0		

Go to **Log & Report > Traffic Log > Forward Traffic**.

Internet access occurs simultaneously through the FortiGate unit.

Refresh Download Raw Log Log location: Disk

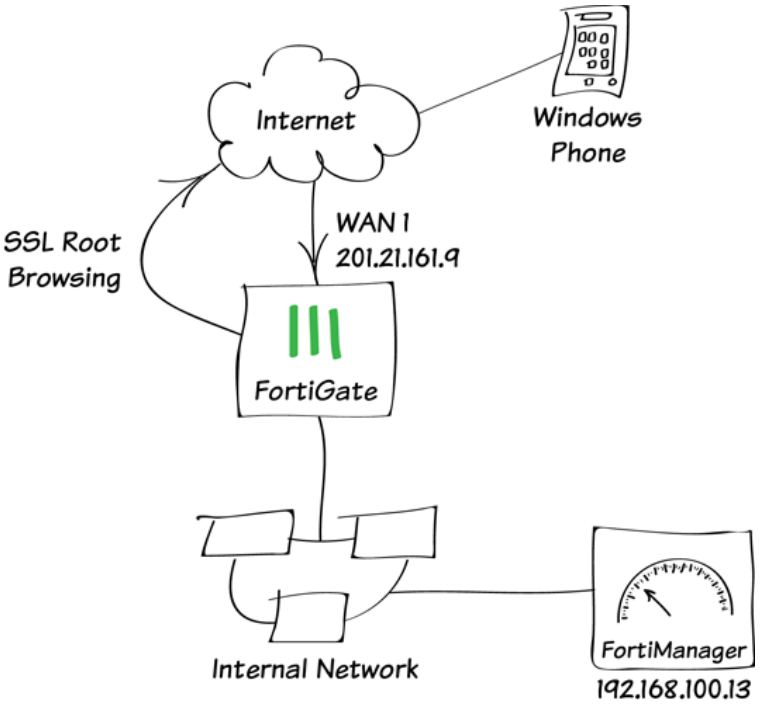
#	Date/Time	Src Interface	Dst Interface	Src	Dst	Service	Policy ID	Sent / Received
1	14:26:05	ssl.root	wan1	10.212.134.200	74.125.133.95	HTTP	8	168 B / 88 B
2	14:26:04	ssl.root	wan1	10.212.134.200	173.194.77.94	HTTP	8	168 B / 88 B
3	14:26:04	ssl.root	wan1	10.212.134.200	173.194.43.79	HTTP	8	168 B / 88 B
4	14:26:03	ssl.root	wan1	10.212.134.200	66.171.121.34 (fortinet.com)	HTTP	8	535 B / 938 B
5	14:25:57	ssl.root	wan1	10.212.134.200	74.121.50.17 (www.pages03.net)	HTTP	8	880 B / 537 B
6	14:25:44	ssl.root	wan1	10.212.134.200	208.91.113.212	HTTPS	8	3.30 KB / 7.44 KB
7	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30	KERBEROS	8	520 B / 1.64 KB
8	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30	KERBEROS	8	1.71 KB / 321 B
9	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30	KERBEROS	8	404 B / 367 B
10	14:24:39	ssl.root	wan1	10.212.134.200	213.199.179.159	40031/tcp	8	512 B / 469 B
11	14:24:37	ssl.root	wan1	10.212.134.200	213.199.179.159	HTTP	8	168 B / 128 B
12	14:24:37	ssl.root	wan1	10.212.134.200	132.246.2.6 (www.msftncsi.com)	HTTP	8	305 B / 387 B

Select an entry to view more information.

Dst	66.171.121.34 (fortinet.com)	**Virtual Domain**	root
Received	938	**Source Country**	Reserved
Src NAT IP	172.20.120.123	**Sent / Received**	535 B / 938 B
Duration	17	**Sent**	535
Src NAT Port	54165	**Application Details**	
Service	HTTP	**Protocol**	6
Destination Country	United States	**Dst Port**	80
roll	65389	**Status**	close
Timestamp	Wed Apr 17 14:26:03 2013	**Tran Display**	snat
Sequence Number	8096	**Policy ID**	8
Src Interface	ssl.root	**Src**	10.212.134.200
Sent Packets	6	**Level**	notice
Src Port	54165	**Log ID**	13
Sub Type	forward	**Threat**	
Received Packets	5	**Date/Time**	14:26:03 (Wed Apr 17 14:26:03 2013)
Dst Interface	wan1		

For further reading, check out Basic SSL VPN configuration in the FortiOS 5.2 Handbook.

SSL VPN for Windows Phone 8.1



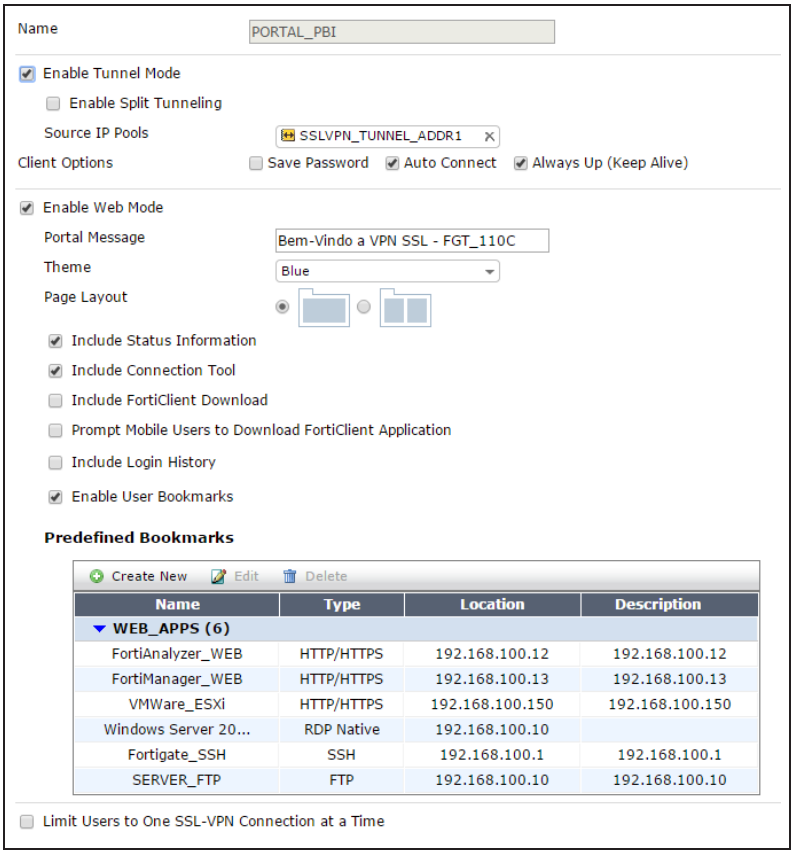
In this example, you will connect to a private network with a Windows Phone, using an SSL VPN.

1. Creating a VPN portal with custom bookmarks

Go to **VPN > SSL > Portals** and create a new portal.

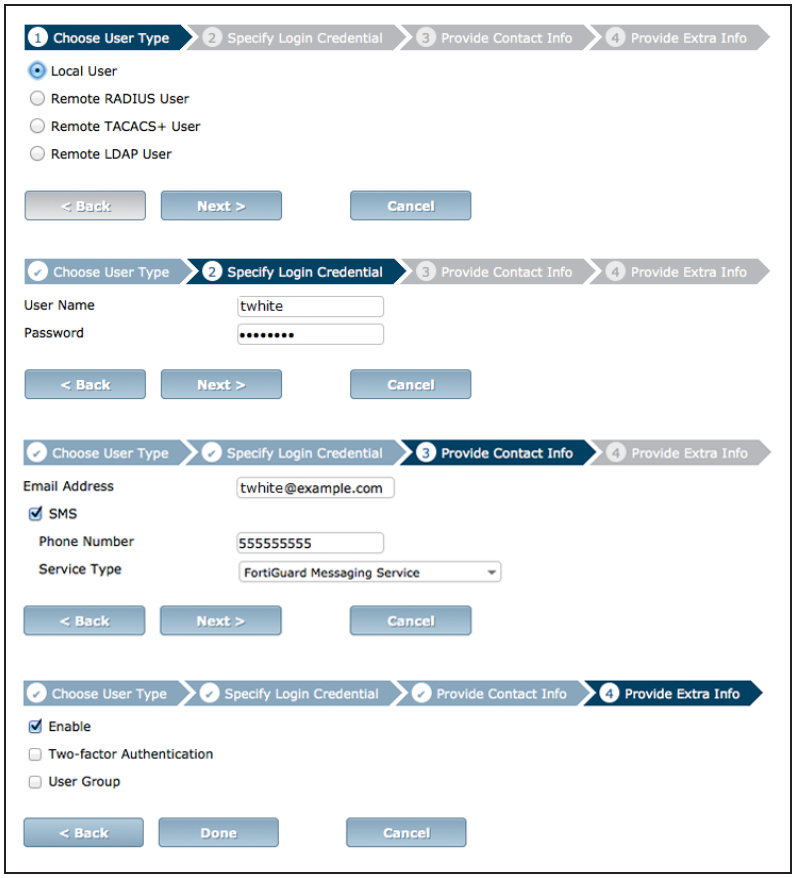
Enable both **Tunnel Mode** and **Web Mode**. Disable **Split Tunneling** and set **Source IP Pools** to use the default SSL VPN tunnel address range.

Under **Predefined Bookmarks**, create bookmarks to access resources on the internal network.



2. Creating a user and user group

Go to **User & Device > User > User Definition** and create a new local user.

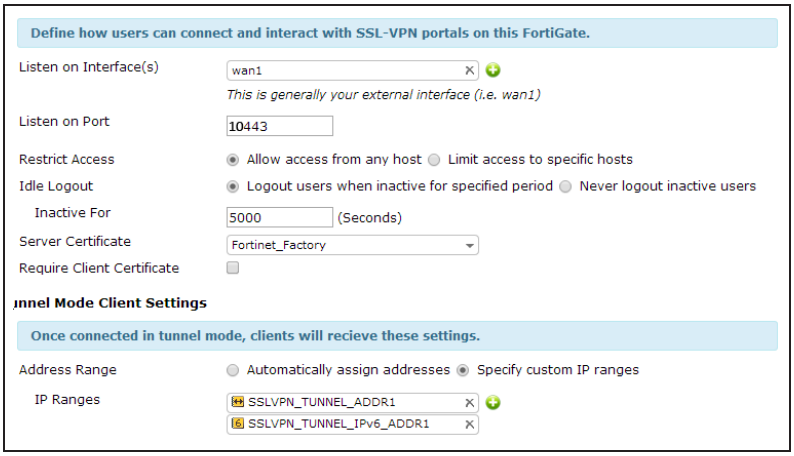


Go **User & Device > User > User Groups** and create a new user group. Set **Members** to include the new user.

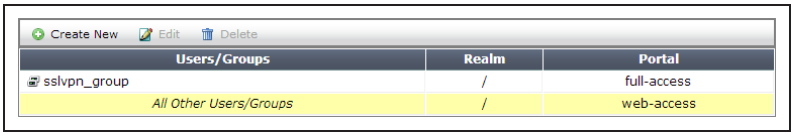
3. Configuring the VPN tunnel

Go to **VPN > SSL > Settings** and set **Listen on Interface(s)** to **wan1**.

Set **Listen on Port** to **10443** and **Specify custom IP ranges** using the default SSL VPN tunnel addresses.



Under **Authentication/Portal Mapping**, add the new user group.



4. Creating security policies

Go to **Policy & Objects > Policy > IPv4**.

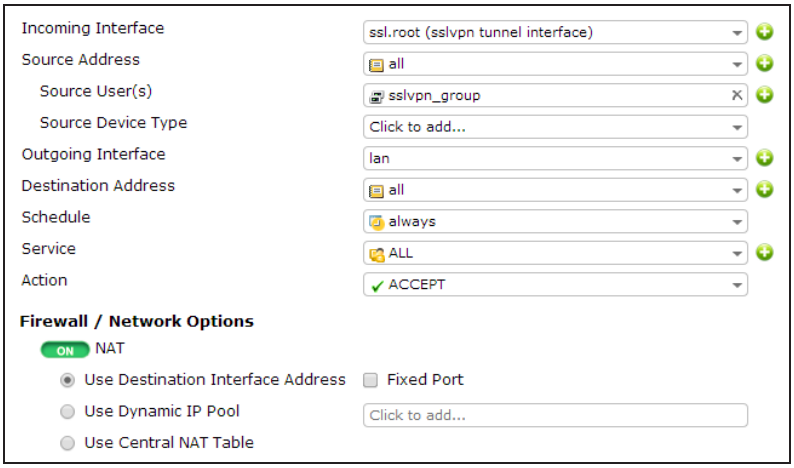
Add a security policy allowing access to the internal network through the *ssl.root* VPN tunnel interface.

Set **Incoming Interface** to **ssl.root**.

Set **Source Address** to **all** and select the **Source User** new user group.

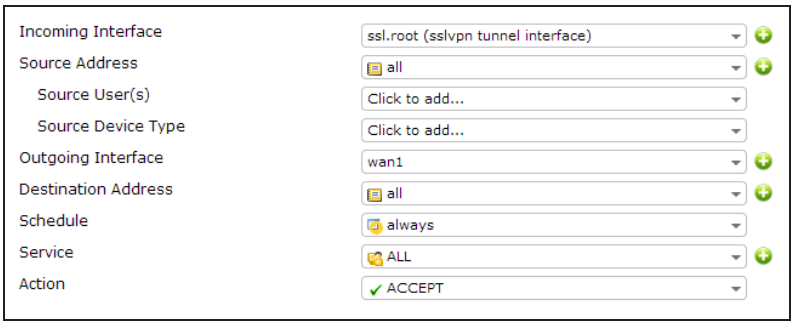
Set **Outgoing Interface** to the local network interface so that the remote user can access the internal network.

Set **Destination Address** to all, enable **NAT**, and configure any remaining firewall and security options as desired.



Add a second security policy allowing SSL VPN access to the Internet.

For this policy, **Incoming Interface** is set to **ssl.root** and **Outgoing Interface** is set to your Internet-facing interface.



3. Results

Using your Window Phone's web browser, access the portal. The portal's address is the IP address of your Internet-facing interface with the port the SSL VPN tunnel is listening to, and it must be accessed using HTTPS (in the example, *https://201.21.161.9:10443*).

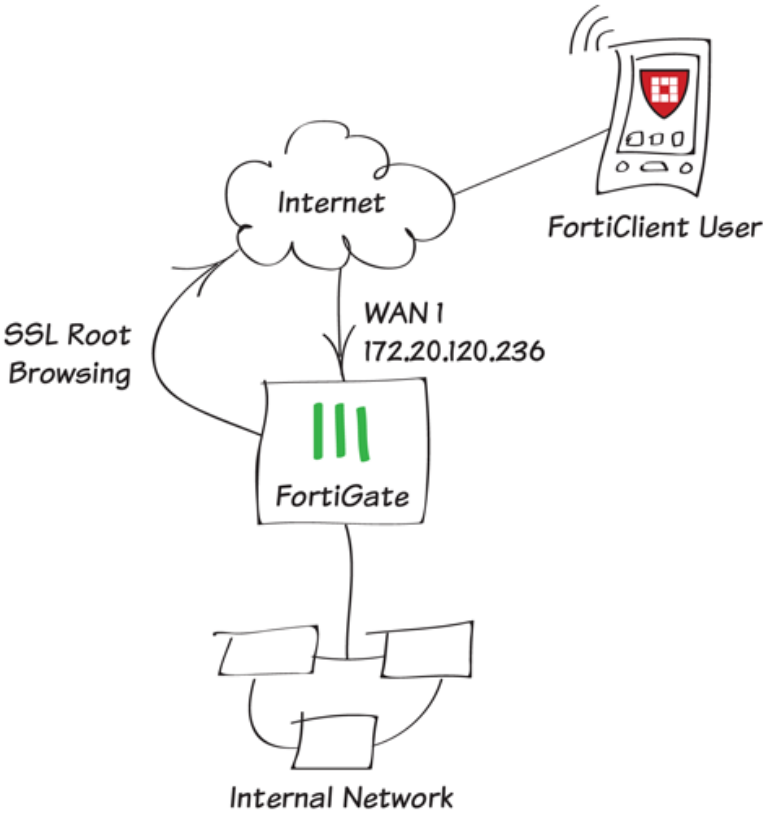
Log in using the credentials for your SSL VPN user.

After your credentials are accepted, you will be able to see the VPN portal.

Select one of the pre-defined bookmarks (in the example, the bookmark for a FortiManager device). You will be able to access the network resource.

For further reading, check out The SSL VPN web portal in the FortiOS 5.2 Handbook.

SSL VPN using FortiClient for iOS



In this recipe, you will create an SSL VPN that remote users connect to using FortiClient running on iOS.

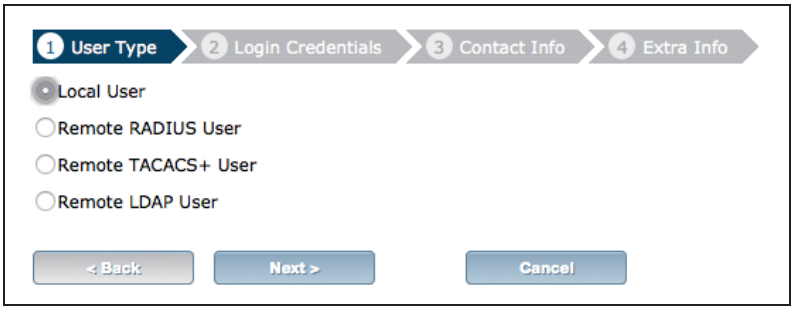
When a user using an iOS device connects to this SSL VPN, they can access servers and data on the internal network. They can also securely browse the Internet using the FortiGate's Internet connection.

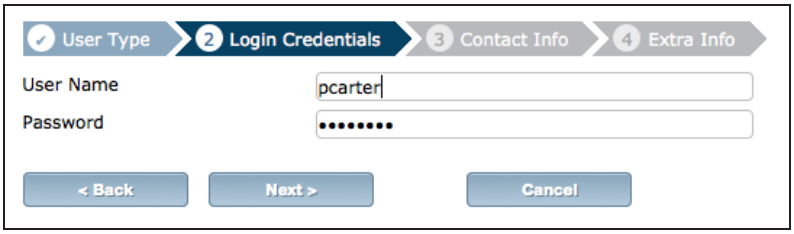
This example uses FortiClient 5.2.0.028 for iOS. FortiClient can be downloaded from www.forticlient.com.

1. Creating users and a user group

Go to **User & Device > User > User Definition**.

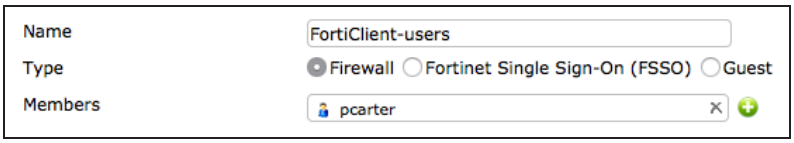
Add as many local users as required with the **User Creation Wizard**.





Go to **User & Device > User > User Groups**.

Create a user group for FortiClient users and add the new user(s) to the group.

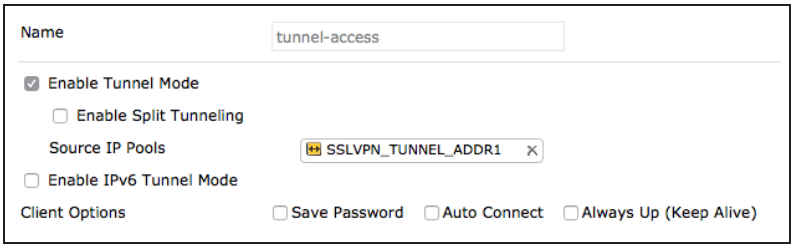


2. Creating an SSL VPN portal

Go to **VPN > SSL > Portals**.

Edit the **tunnel-access** portal. This portal supports tunnel mode by default.

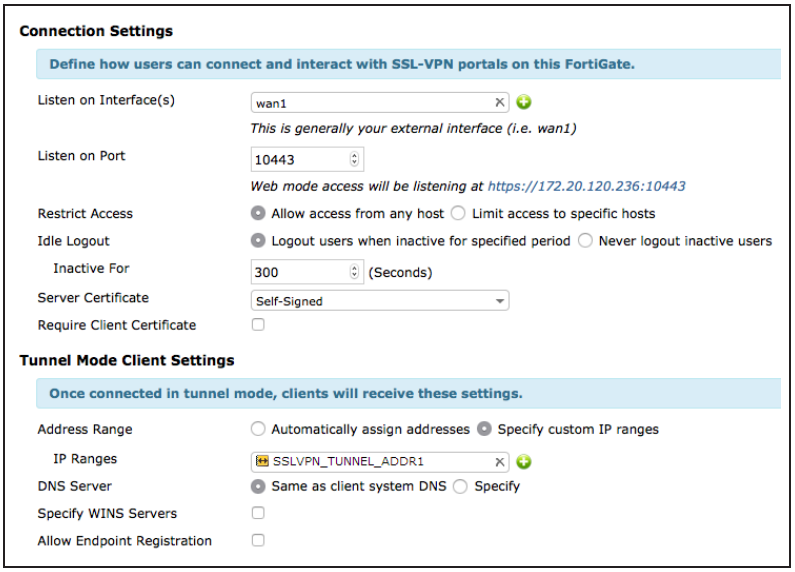
Enable Split Tunneling is *not* enabled so that all SSL VPN traffic will go through the FortiGate unit.



3. Configuring the SSL VPN tunnel

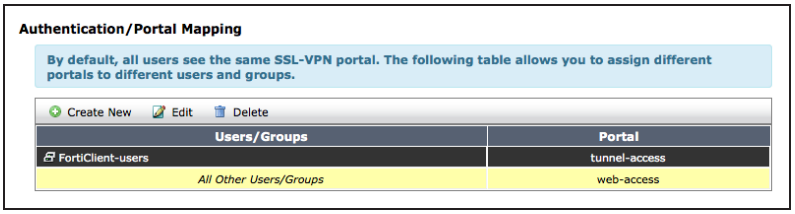
Go to **VPN > SSL > Settings** and set **Listen on Interface(s)** to **wan1**.

Set **Listen on Port** to *10443* and **Specify custom IP ranges**. Use the default **IP Range**, *SSLVPN_TUNNEL_ADDR1*.



At the bottom of the page, under **Authentication/Portal Mapping**, add the FortiClient user group.

If necessary, map a portal for **All Other Users/Groups**.

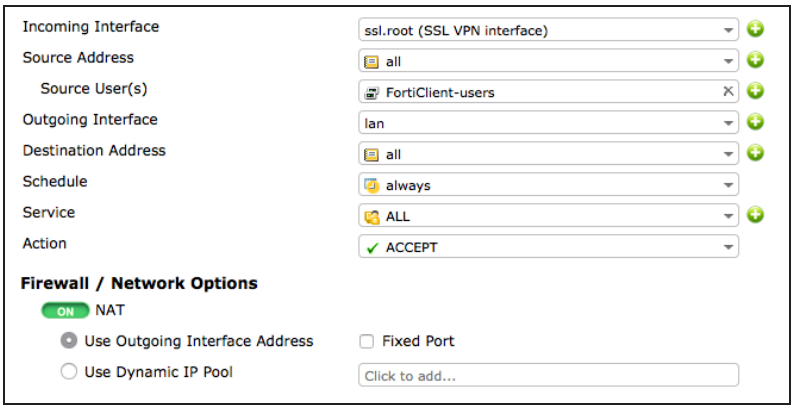


4. Adding security policies for access to the Internet and internal network

Go to **Policy & Objects > Policy > IPv4**. Create a security policy allowing SSL VPN user to access the internal network.

Set **Incoming Interface** to **ssl.root**. Set **Source Address** to **all** and **Source User** to the new user group. Set **Outgoing Interface** to the local network interface so that the remote user can access the internal network.

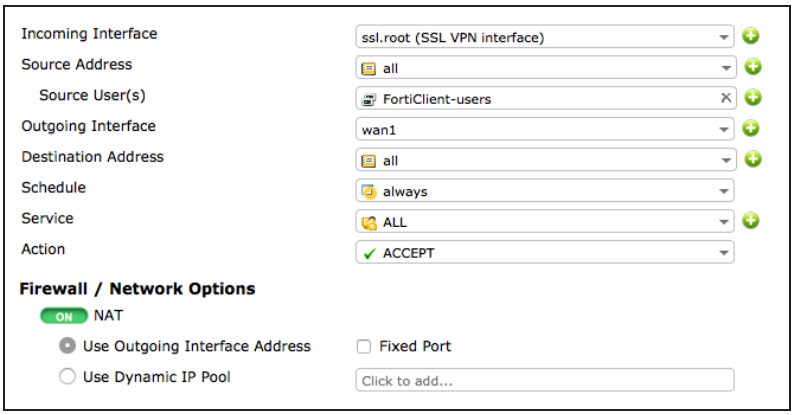
Set **Destination Address** to all, enable **NAT**, and configure any remaining



firewall and security options as desired.

Add a second security policy allowing SSL VPN users to access the Internet.

For this policy, **Incoming Interface** is set to **ssl.root** and **Outgoing Interface** is set to **wan1**.

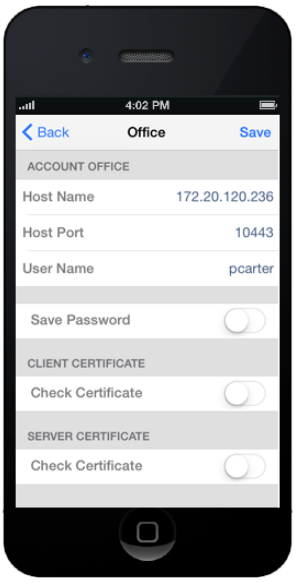


5. Configuring FortiClient for SSL VPN in iOS

Install FortiClient on the iOS device.

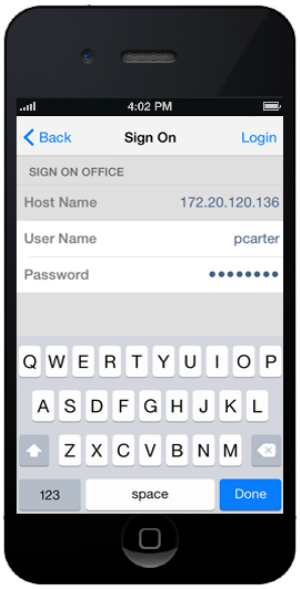
Add a new VPN Gateway.

Set **Host Name** to the FortiGate's IP (in the example, *172.20.120.236*), set **Host Port** to *10443*, and set **User Name** to match the new user account.

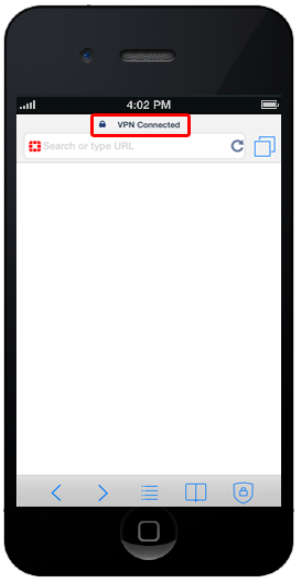


6. Results

Select the VPN in FortiClient. Enter the **Password** and select **Login**.



You will be able to connect to the VPN.



On the FortiGate, go to **VPN > Monitor > SSL-VPN Monitor** to see that the user has connected.

	No.	User	Source IP	Begin Time
☐	1	pcarter	172.20.130.254	Thu Jan 15 10:44:34 2015

For further reading, check out FortiClient in the FortiOS 5.2 Handbook.

SSL VPN troubleshooting

This page contains tips to help you with some common challenges for SSL VPN.

There is no response from the SSL VPN URL.

Go to **VPN > SSL > Settings** and check the SSL VPN port assignment. Also, verify that the SSL VPN policy is configured correctly.

You receive an error stating that the web page cannot be found.

Check the URL you are attempting to connect to. It should follow this pattern:

https:///:/remote/login.

Ensure that you are using the correct port number for the part of the URL.

FortiClient cannot connect.

Read the Release Notes to ensure that the version of FortiClient you are using is compatible with your version of FortiOS.

When you attempt to connect using FortiClient or in Web mode, you receive the following error message: "Unable to logon to the server. Your user name or password may not be configured properly for this connection. (-12)."

Ensure that cookies are enabled in your browser. Also, if you are using a remote authentication server, ensure that the FortiGate is able to communicate with it.

The tunnel connects but there is no communication.

Go to **Router > Static > Static Routes** (or **System > Network > Routing** on some FortiGate models) and ensure that there is a static route to direct packets destined for the tunnel users to the SSL VPN interface.

You can connect remotely to the VPN tunnel but are unable to access the network resources.

Go to **Policy & Objects > Policy > IPv4** and check the policy allowing VPN access to the local network. If the destination address is set to all, create a firewall address for the internal network. Change the destination address and attempt to connect remotely again.

Users are unable to download the SSL VPN plugin.

Go to at **VPN > SSL > Portals** to check the VPN Portal to ensure that the option to **Limit Users to One SSL-VPN Connection at a Time** is disabled. This allows users to connect to the resources on the portal page while also connecting to the VPN through FortiClient.

Users are being assigned to the wrong IP range.

Ensure that the same IP Pool is used in VPN Portal and VPN Settings to avoid conflicts. If there is a conflict, the portal settings will be used.

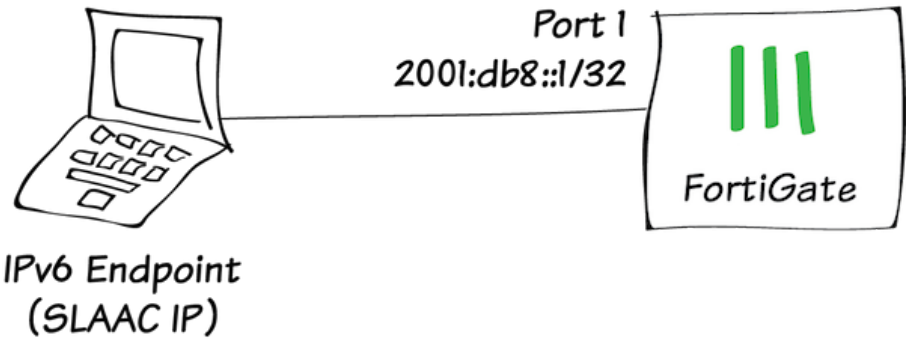
IPv6

Internet Protocol version 6 (IPv6) is the most significant advance in traditional Internet communications protocol. The IPv6 address scheme is based on a 128-bit address, rather than the 32-bit addresses used by IPv4, allowing IPv6 to have a much higher address limit of over 340 undecillion possible addresses (that is 340 followed by 36 zeros).

FortiGates support IPv6 in a wide variety of network configurations.

- Creating an IPv6 interface using SLAAC

Creating an IPv6 interface using SLAAC



In this example you will configure your FortiGate to use Stateless Address Auto Configuration (SLAAC) to assign IPv6 addresses to IPv6-enabled devices on your internal network.

The IPv6 address block used in this recipe (2001:db8::/32) is reserved for documentation purposes and will not work on your network. If you're not sure how to determine the correct IPv6 address for your environment, refer to the FortiOS IPv6 Handbook Chapter.

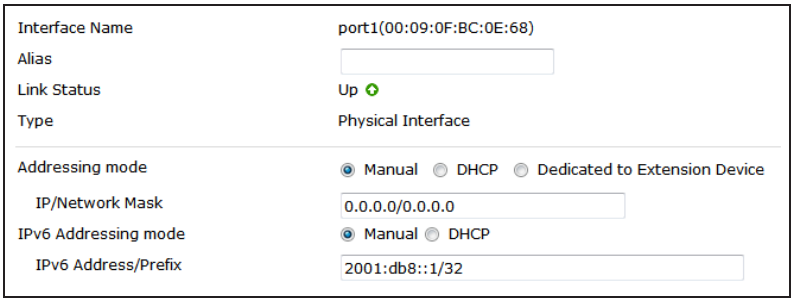
1. Enabling IPv6

Go to **System > Config > Features** and make sure that **IPv6** is turned **ON**.

2. Configuring a FortiGate interface for IPv6

Go to **System > Network > Interfaces** and edit the interface connected to your internal network (in the example, port1).

Set the **IPv6 Addressing mode** to **Manual** and enter the **IPv6 Address/Prefix** for the interface (in this example, 2001:db8::1/32).



The interface can have both IPv4 and IPv6 addressing. This example only includes IPv6 addressing.

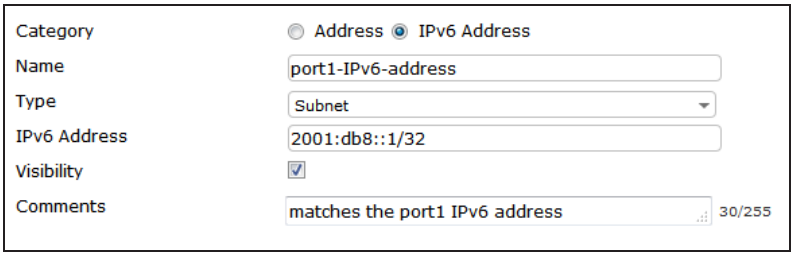
Enter this CLI command to add the router advertisements and specific IPv6 prefixes required to configure SLAAC on the interface.

The `set ip6-address` option is not required since you already added an IPv6 address to the interface from the GUI. But its included in the example to show the complete CLI configuration.

```
config system interface
  edit port1
    config ipv6
      set ip6-address 2001:db8::1/32
      set ip6-send-adv enable
         config ip6-prefix-list
           edit 2001:db8::/32
              set autonomous-flag enable
              set onlink-flag enable
          end
     end
end
```

3. Adding IPv6 firewall addresses

Go to **Policy & Objects > Objects > Addresses > Create New**.
Add an IPv6 firewall address that matches the IPv6 address added to the port1 interface.



4. 'Bouncing' the IPv6 interface

You can now 'bounce' the port1 interface (bring the interface down and then back up). Go to **System > Network > Interfaces**, edit the port1 interface and set the **Administrative Access** to **Down**. Select **OK**, then edit the interface again and set the **Administrative Access** back to **Up**. This causes a router advertisement using the Neighbor Discovery Protocol, which performs address autoconfiguration and determines the reachability of neighboring nodes.

Alternatively, you can reboot the FortiGate or wait for the next router advertisement.

5. Results

Connect a computer to the port1 interface. Configure the computer to get an IPv6 address automatically. Then, from a command prompt or terminal session enter the command `ipconfig` to view the computer's IP configuration.

```
IPv6 Address............: 2001:db8::44d2:ed21:9733:9245
```

You should see that an IPv6 address has been assigned with the prefix advertised on the port1 interface.

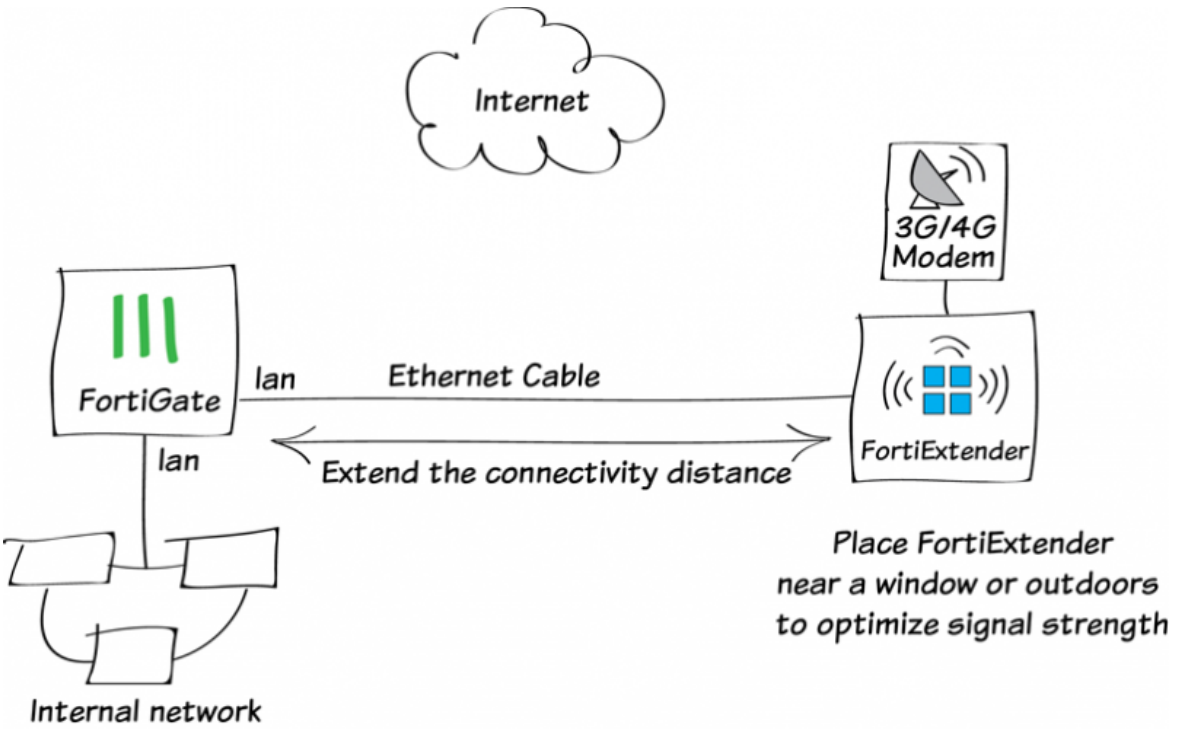
For further reading, check out IPv6 in the FortiOS 5.2 Handbook.

Fortinet Integration

This section contains information about using other Fortinet products alongside a FortiGate. For more information about any of the Fortinet products used in these recipes, go to www.fortinet.com.

- FortiExtender installation
- WiFi with external RADIUS authentication(FortiAuthenticator)
- Remotely accessing FortiRecorder through a FortiGate

FortiExtender installation



This example shows how to set an internet connection using a 3G/4G modem and a FortiExtender. A FortiExtender is used when the FortiGate unit is located in an area without 3G/4G network coverage, the FortiExtender can be placed near a window or outdoors.

For information about the compatibility of FortiExtender and various modems, see the FortiGate and FortiExtender Modem Compatibility Matrix.

1. Installing the 3G/4G modem in the FortiExtender

Remove the housing cover of the FortiExtender and use the provided USB extension cable to connect your 3G/4G modem to the device.

For more information on installing the 3G/4G modem, see the QuickStart Guide.

2. Connecting the FortiExtender

Use an Ethernet cable to connect the FortiExtender to the **lan** interface of a FortiGate unit.

Once connected, FortiGate can control FortiExtender and modem.

Enable FortiExtender in the FortiGate's CLI.

CAPWAP service must be enabled on the port to which FortiExtender is connected, **lan** interface in this example.

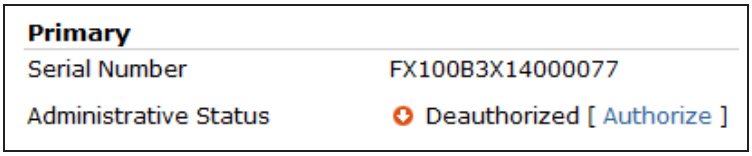
```
config system global
   set fortiextender enable
   set wireless-controller enable
 end

config system interface
   edit lan
   append allowaccess capwap
   end
 end
```

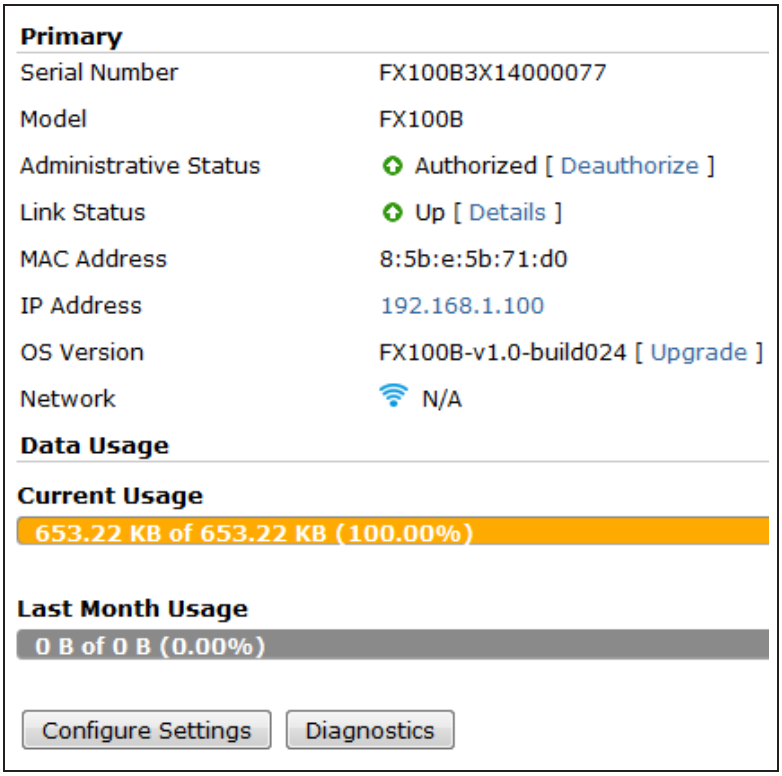
Once enabled, it appears as a virtual WAN interface in the FortiGate, such as **fext-wan1**. Go to **System > Network > Interface** to verify **fext-wan1** interface.

3. Configuring the FortiExtender

Go to **System > Network > FortiExtender** and authorize the FortiExtender.



Once authorized, you can see the status of the FortiExtender.

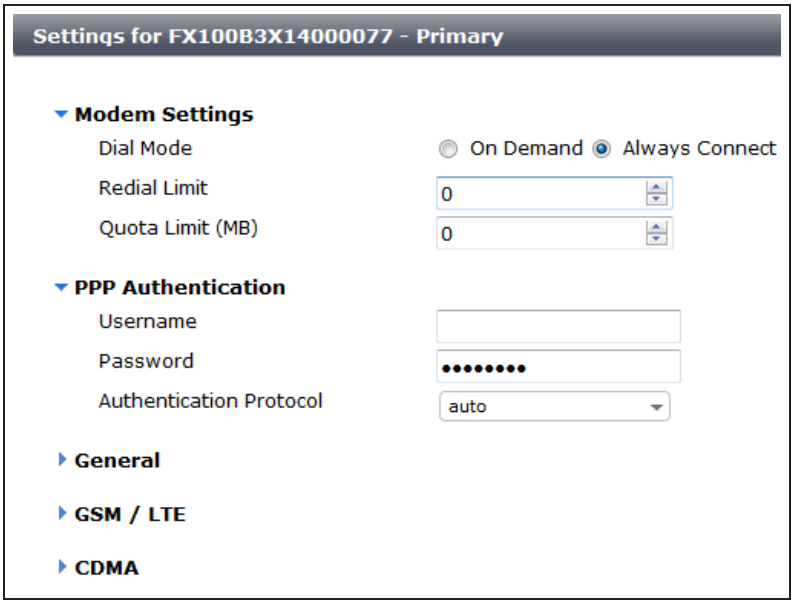


4. Modem settings

The FortiExtender unit allows for two modes of operation for the modem; On Demand and Always Connect.

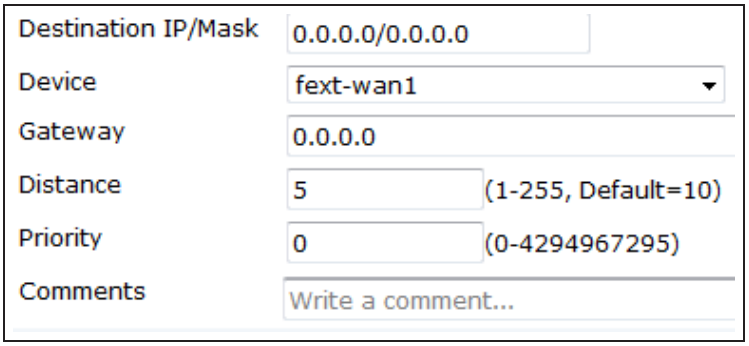
Go to **System > Network > FortiExtender** and click on **Configuring Settings**.

Select **Always Connect** for **Dial Mode** and keep other settings to default.

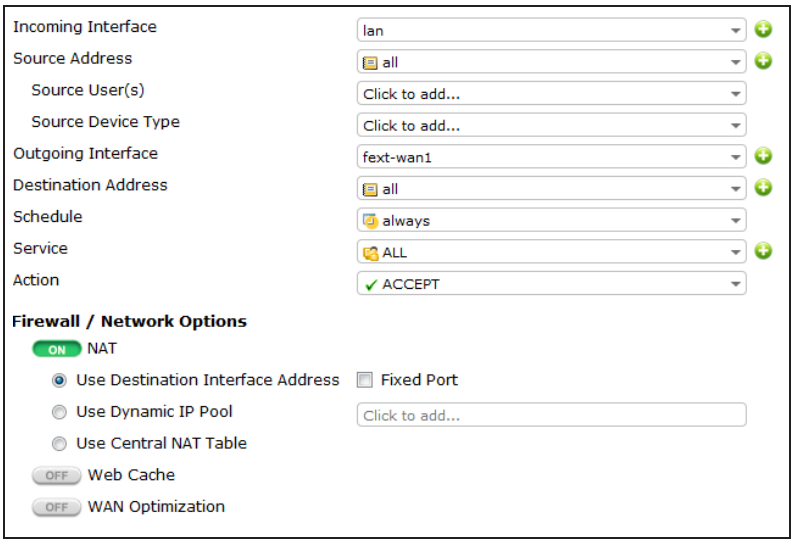


5. Configuring the FortiGate

Go to **Router > Static > Static Routes** and add new route through **fext-wan1** interface.

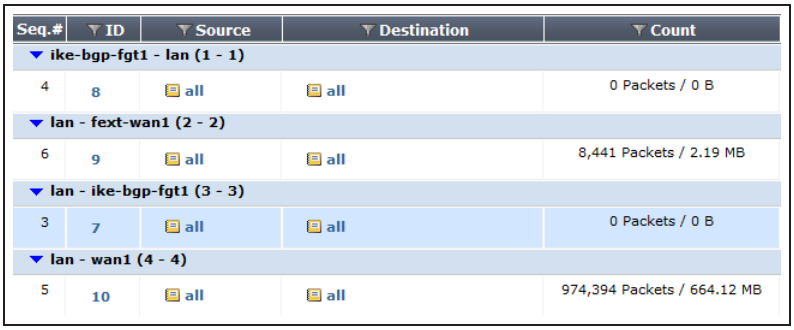


Go to **Policy & Objects > Policy > IPv4** and create a new security policy allowing traffic from **lan** interface to **fext-wan1** interface.



6. Results

Browse the Internet and go to **Policy & Objects > Policy > IPv4** to verify the **Count**.



Seq.#	ID	Source	Destination	Count
ike-bgp-fgt1 - lan (1 - 1)				
4	8	all	all	0 Packets / 0 B
lan - fext-wan1 (2 - 2)				
6	9	all	all	8,441 Packets / 2.19 MB
lan - ike-bgp-fgt1 (3 - 3)				
3	7	all	all	0 Packets / 0 B
lan - wan1 (4 - 4)				
5	10	all	all	974,394 Packets / 664.12 MB

Go to **Log & Report > Traffic Log > Forward Traffic**.

You can see that traffic flowing from **lan** interface to **fext-wan1** interface.

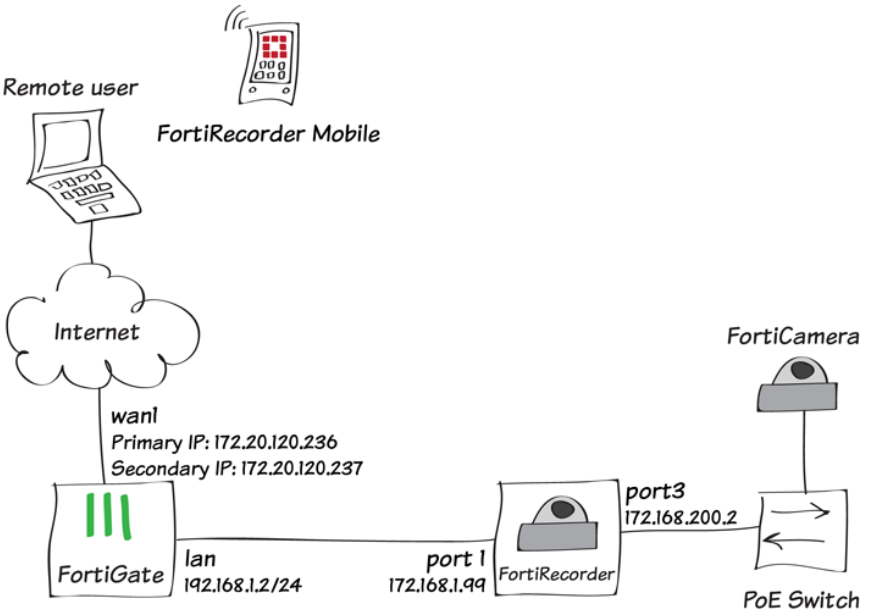
Date...	Policy ...	Src Interface	Dst Interface
15:38:03	9	lan	fext-wan1
15:37:47	9	lan	fext-wan1
15:37:43	9	lan	fext-wan1
15:37:39	9	lan	fext-wan1
15:37:35	9	lan	fext-wan1
15:37:31	9	lan	fext-wan1
15:37:19	9	lan	fext-wan1
15:37:07	9	lan	fext-wan1
15:36:59	9	lan	fext-wan1
15:36:55	9	lan	fext-wan1
15:36:31	9	lan	fext-wan1
15:36:27	9	lan	fext-wan1

Select an entry for details.

Action	ip-conn	**Date/Time**	15:35:51 (1405006551)
Destination	10.10.80.25	**Dst Interface**	fext-wan1
Dst Port	161	**Level**	warning
Log ID	11	**Policy ID**	9
Security Events		**Sent / Received**	N/A / N/A
Sequence Number	10016	**Source**	192.168.1.101
Src Interface	lan	**Src Port**	56442
Sub Type	forward	**Threat**	262144
Threat Score	1375731722	**Timestamp**	7/10/2014, 3:35:51 PM
Virtual Domain	root		

For further reading, check out FortiExtender in the FortiOS 5.2 Handbook.

Remotely accessing FortiRecorder through a FortiGate



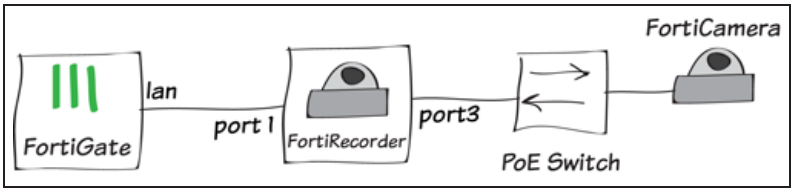
In this recipe, you set up a FortiGate with a secondary IP to provide remote access to a FortiRecorder. This allows you to securely view live FortiCamera video feeds over the Internet, using either the FortiRecorder GUI, FortiRecorder Mobile, or FortiRecorder Central.

This recipe employs a secondary IP and two port forwarding virtual IPs to forward HTTPS and Real Time Streaming Protocol (RTSP) packets from the Internet to the FortiRecorder. To use a secondary IP address you must have a second Internet IP address for your FortiRecorder. Instead of adding this IP address to the FortiRecorder, you add it to your FortiGate and forward traffic for the FortiRecorder IP address through the FortiGate.

1. Connect the hardware

Connect your devices as shown in the diagram.

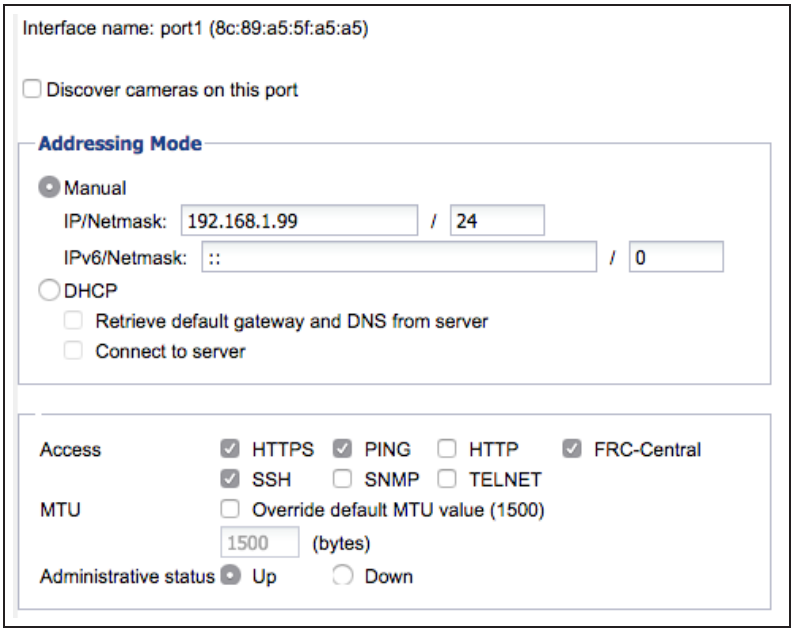
In this example, the FortiCamera connects to a PoE switch, which is then connected to **port3** on the FortiRecorder. The FortiRecorder's **port1** connects to the FortiGate **lan** interface.



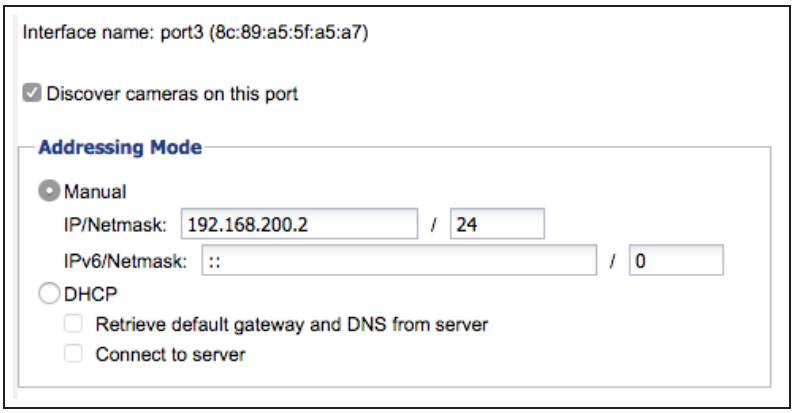
2. Configuring the FortiRecorder and FortiCamera

On the FortiRecorder, go to **System > Network > Interface** and edit **port1**. Set a manual **IP/Netmask** for the interface that is on the same subnet as the FortiGate **lan** interface (in the example, *192.168.1.99*).

Set **Access** to allow HTTPS and any other protocols you require. If you are using FortiRecorder Central, you must enable **FRC-Central**.

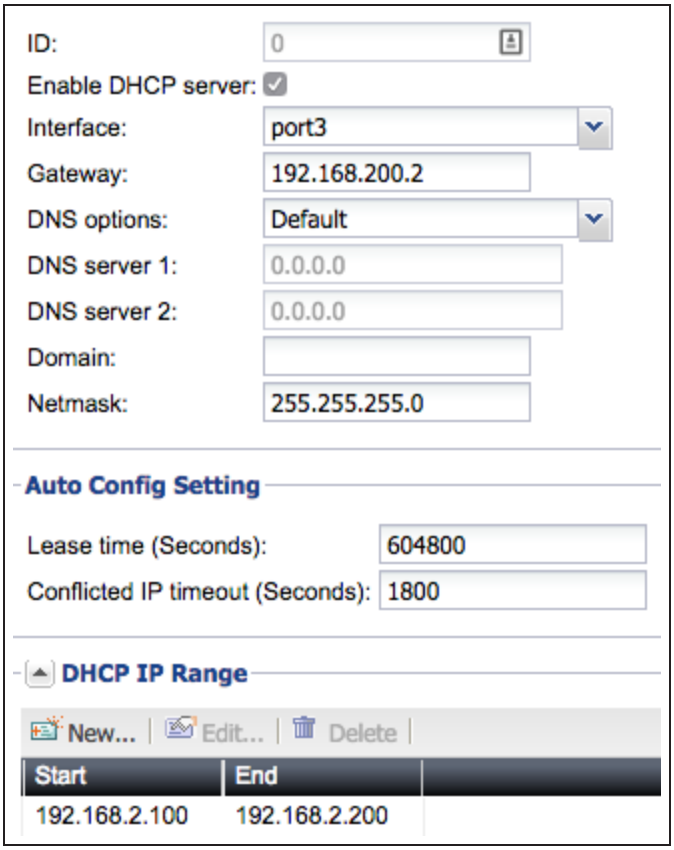


Edit **port3**. Make sure that **Discover cameras on this port** is enabled. Set a manual **IP/Netmask** for the interface.

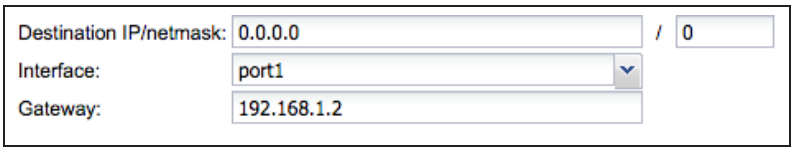


Go to **System > Network > DHCP** and create a new DHCP server. Set **Interface** to **port3** and **Gateway** to port3's IP address (in the example, *192.168.200.2*).

Create a new **DHCP IP Range** that is on the same subnet as port3.

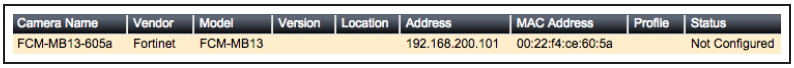


Go to **System > Network > Routing**. Add a default route that uses the IP address of the FortiGate's lan interface (in the example, 192.168.1.2). Set **Interface** to **port1**.



Go to **Camera > Configuration > Camera**. Click on **Force Discover** to have connected cameras displayed.

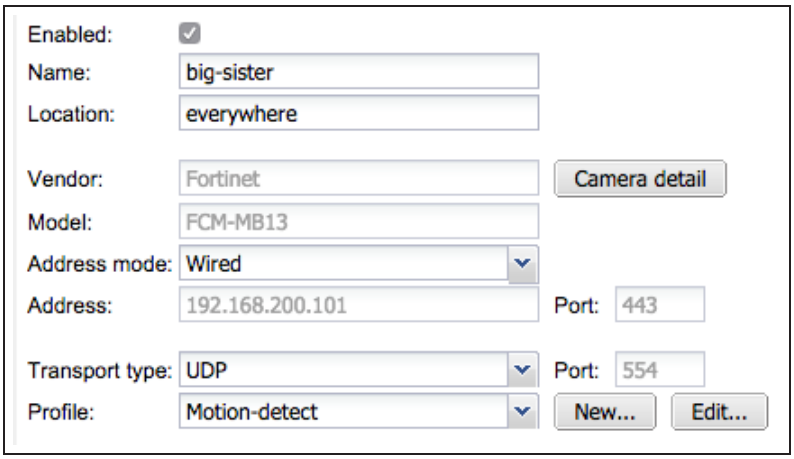
The FortiCamera will appear on the list, with the **Status** column displayed as **Not Configured**.



Camera Name	Vendor	Model	Version	Location	Address	MAC Address	Profile	Status
FCM-MB13-605a	Fortinet	FCM-MB13			192.168.200.101	00:22:f4:ce:60:5a		Not Configured

Select the FortiCamera and select **Configure**. Set the unit's **Name** and **Location**, and **Profile**, as well as any other required configuration settings.

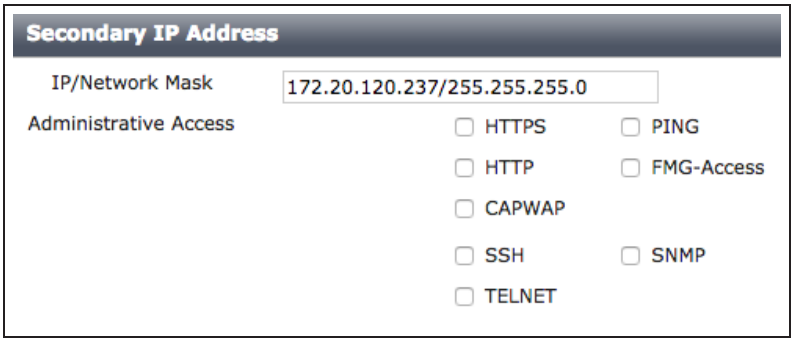
If you do not have any profiles already created, you will have to configure one. For more information, see the FortiRecorder 2.0.0 Administration guide.



3. Adding a secondary IP to the FortiGate

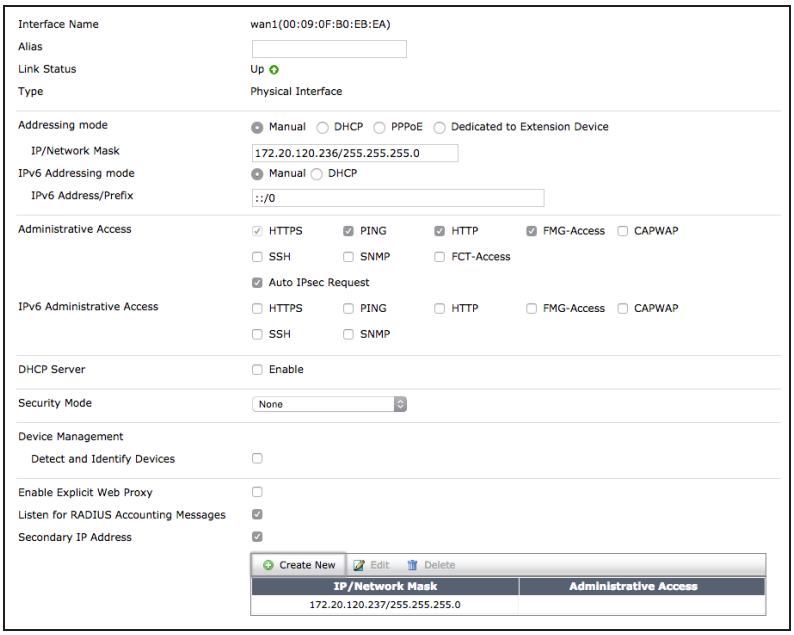
From the FortiGate GUI, go to **System > Network > Interfaces** and edit your Internet-facing interface.

Enable **Secondary IP Address** and create a new **IP/Network Mask** for the interface.



Adding a secondary IP address allows the FortiGate and the network to see two IP addresses, the primary and the secondary, that terminate at the interface.

In this example, the primary IP address is used to connect to the FortiGate, while the secondary IP will be used to connect to the FortiRecorder.

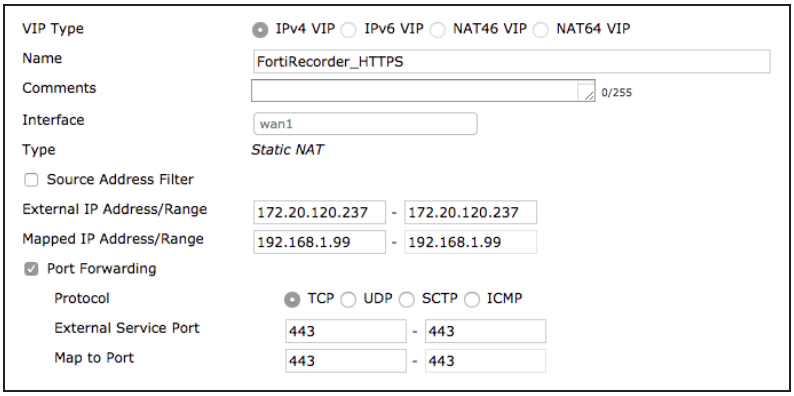


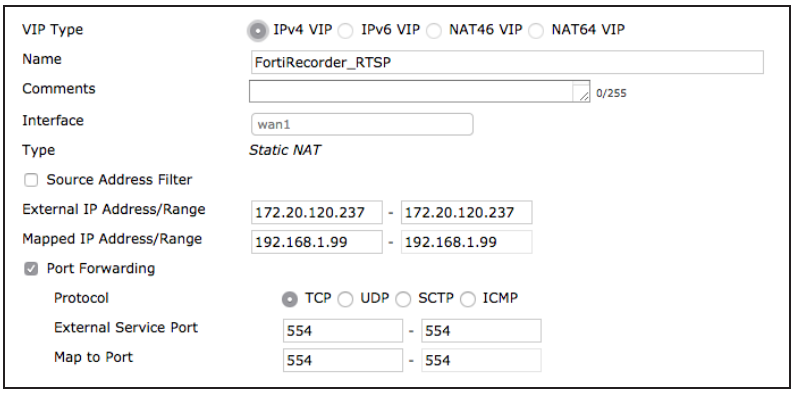
4. Creating virtual IPs

From the FortiGate GUI, go to **Policy & Objects > Objects > Virtual IPs**. Create the two virtual IPs: one for HTTPS traffic and one for RTSP traffic.

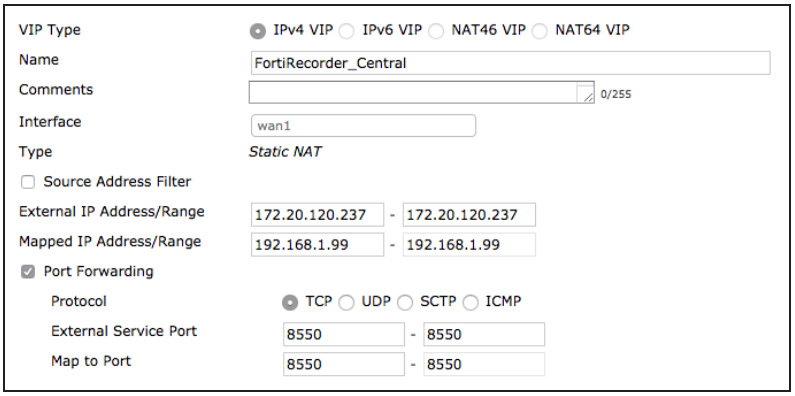
For both virtual IPs, set **External Interface** to your Internet-facing interface, **External IP Address/Range** to the secondary IP of that interface (in the example, *172.20.120.237*) and the **Mapped IP Address/Range** to the IP of port1 on the FortiRecorder unit (in the example, *192.168.1.99*).

Enable **Port Forwarding** and use the standard port for each protocol. HTTPS uses TCP port 443 and RTSP uses TCP port 554.





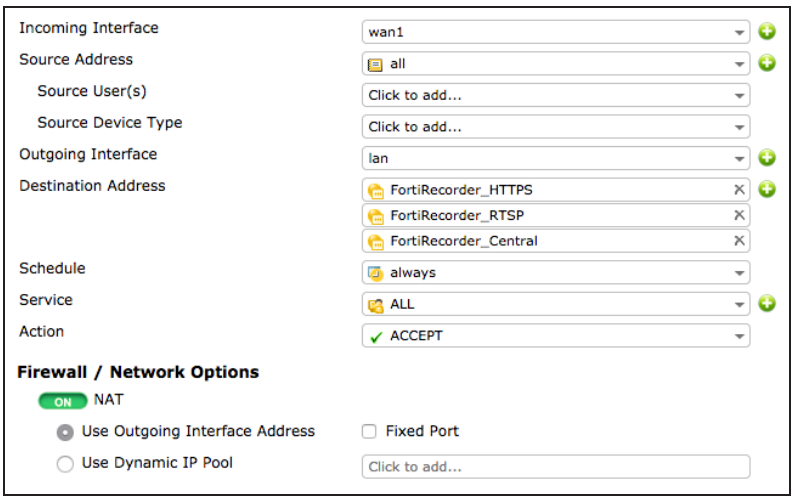
If you are using FortiRecorder Central, you must create a third virtual IP to allow TCP port 8550.



5. Creating a security policy to access to the FortiRecorder

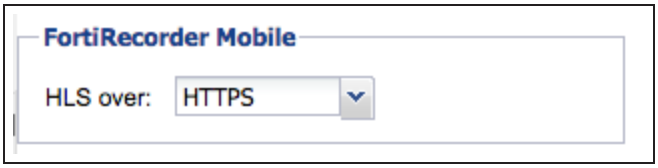
Go to **Policy & Object > Policy > IPv4** and create a new policy that allows access to the FortiRecorder from the Internet.

Set **Incoming Interface** to your Internet-facing interface, **Outgoing Interface** to lan, and **Destination Address** to the new virtual IPs.



6. Configuring FortiRecorder Mobile for iOS

On your FortiRecorder, go to **System > Configuration > Options**.
Set **FortiRecorder Mobile** to use **HLS over HTTPS**.



You can also connect using HLS over HTTP, as long as you add another virtual IP to allow TCP port 80.

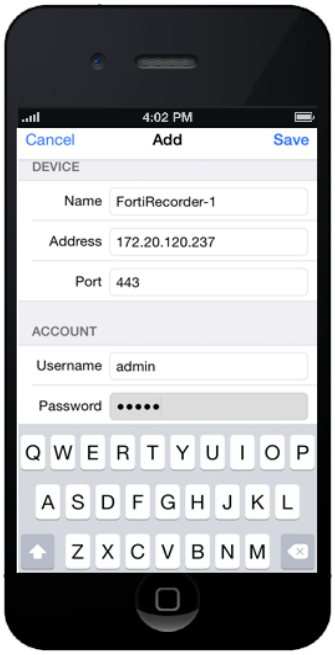
FortiRecorder Mobile for iOS

Download the FortiRecorder Mobile app onto your iOS device.

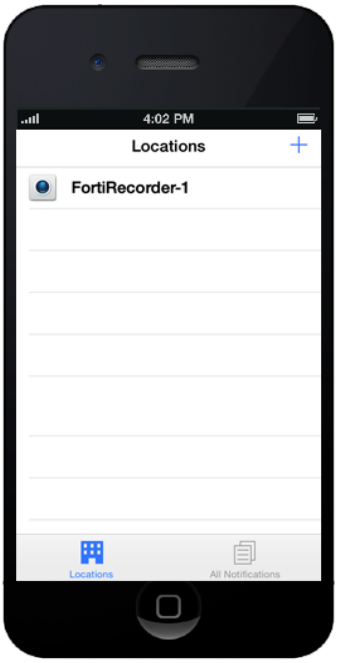
If you will connect using HTTPS, the iOS device must be able to verify the FortiRecorder certificate. To do this, you can either sign the FortiRecorder local certificate with one of the world's largest certificate authorities, whose CA certificate are trusted by the iOS device, or install the CA certificate on the iOS device, if the CA certificate is not trusted by the iOS device. For information about this, see the technical note Provisioning CA Certificate to iOS Devices for FortiRecorder Mobile.

Open FortiRecorder Mobile. Use the **+** to add a new location.

Enter the information for the FortiRecorder device, including the **Address** (in the example, *172.20.120.237*) and the admin account **username** and **password**.



The FortiRecorder is shown in the list of **Locations**.

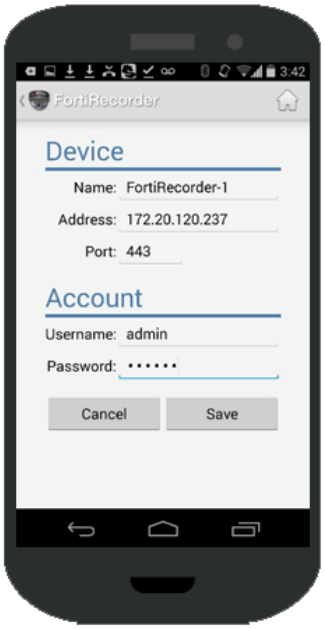


FortiRecorder Mobile for Android

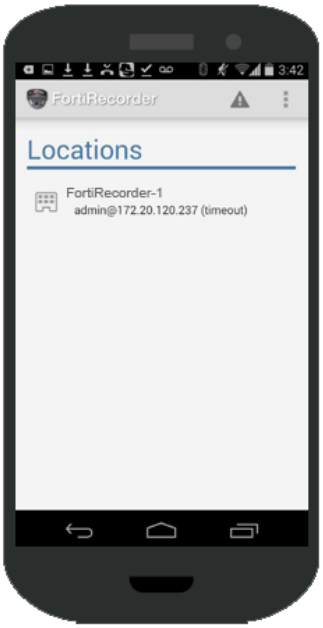
Download the FortiRecorder Mobile app onto your Android device.

Open FortiRecorder Mobile. Select **Add Location**.

Enter the information for the FortiRecorder device, including the **Address** (in the example, *172.20.120.237*) and the admin account **username** and **password**.



The FortiRecorder is shown in the list of **Locations**.



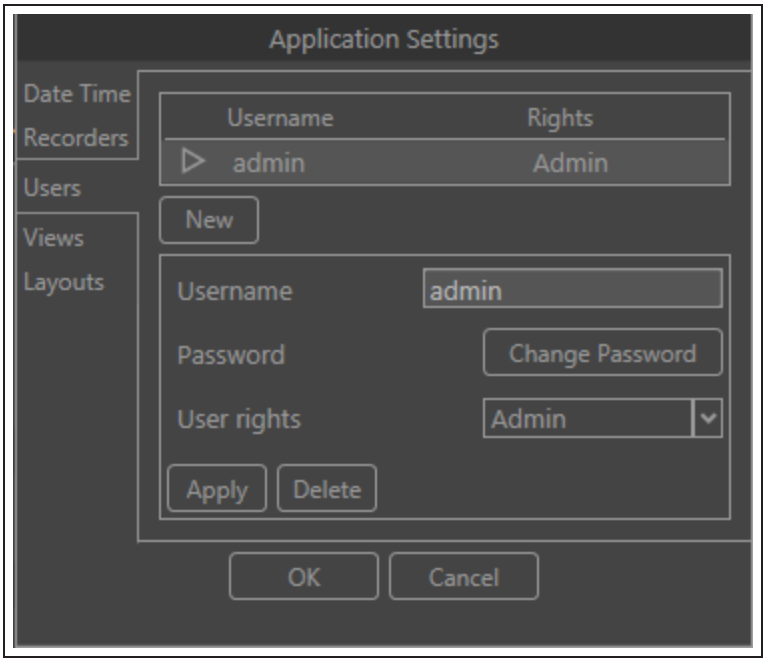
7. Configuring FortiRecorder Central

FortiRecorder Central is a Windows-based video management system that is used to connect and view information from several FortiRecorder units at the same time. It can be downloaded at the Fortinet Support website.

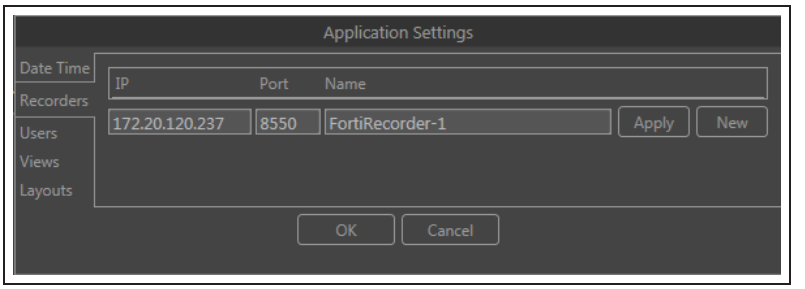
The recipe was written using FortiRecorder Central 1.0.0.

From FortiRecorder Central, use the **Settings** cogwheel in the top right corner to go to **Settings > Users**. Make sure the admin account settings are identical to those on the FortiRecorder because FortiRecorder Central has to be able to log into FortiRecorder using these credentials.

All FortiRecorders must use the same admin credentials in order to be used by FortiRecorder Central.



Go to **Settings > Recorders**. Set the **IP** to the FortiGate's secondary IP (in this example, *172.20.120.237)*.



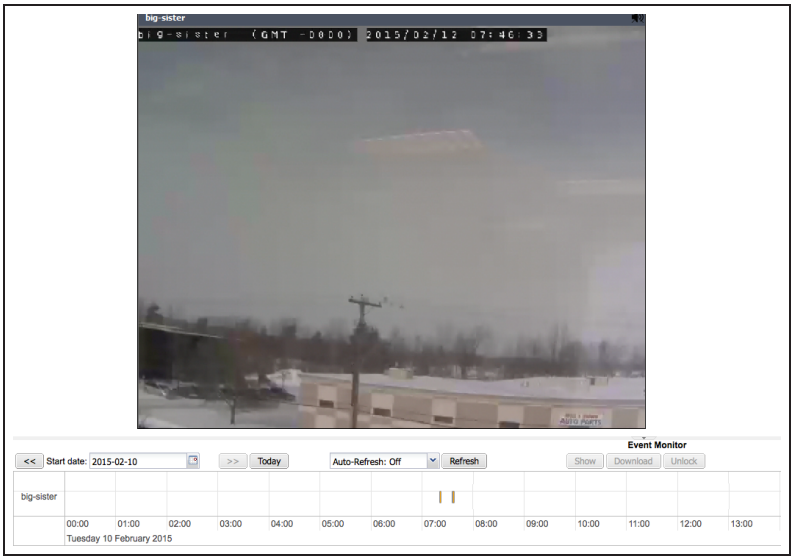
The FortiRecorder will appear in the list of devices, with its connected cameras listed underneath.

8. Results

From the Internet you can browse to the secondary IP address, using HTTPS (in the example, *https://172.20.120.237*). The FortiRecorder GUI login screen appears.

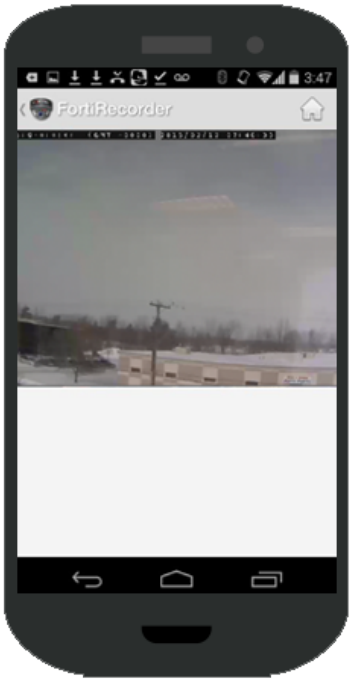
Go to **Monitor > Video Monitor** to see the live video feed from the FortiCamera.

*Quicktime 6.0 or higher is required to view the **Video Monitor**.*

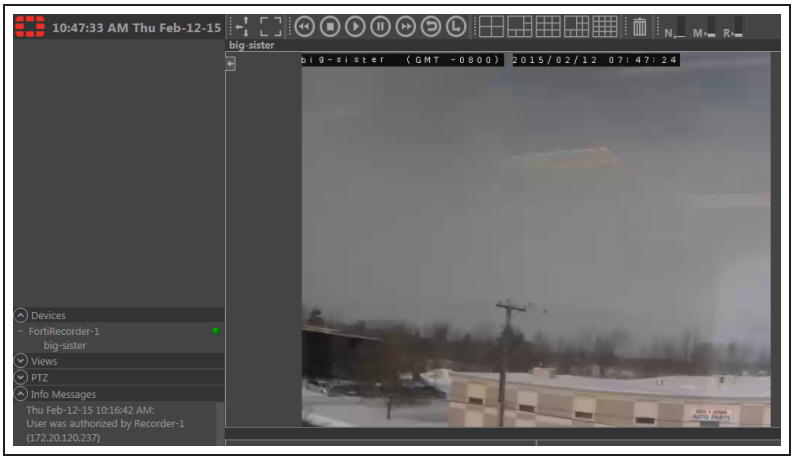


In FortiRecorder Mobile for iOS, go the the **Locations** list and select the FortiRecorder. A list of the available cameras will be shown. Click on the camera you wish to view.

In FortiRecorder Mobile for Android, go the the **Locations** list and select the FortiRecorder, then select **Cameras**. A list of the available cameras will be shown. Click on the camera you wish to view.



In FortiRecorder Central, click on the listing for the FortiCamera and drag it onto a square in the grid. The live video feed will be shown.



Expert

FortiGate units can be deployed in many ways to meet a wide range of advanced requirements. This section contains recipes and articles (which discuss topics in greater depth than a recipe) about a variety of these configurations.

Recipes and articles in this section are intended for users with a high degree of background knowledge about FortiGates and computer networking, such as users who have completed Fortinet's Network Security Expert (NSE) 4 level of training.

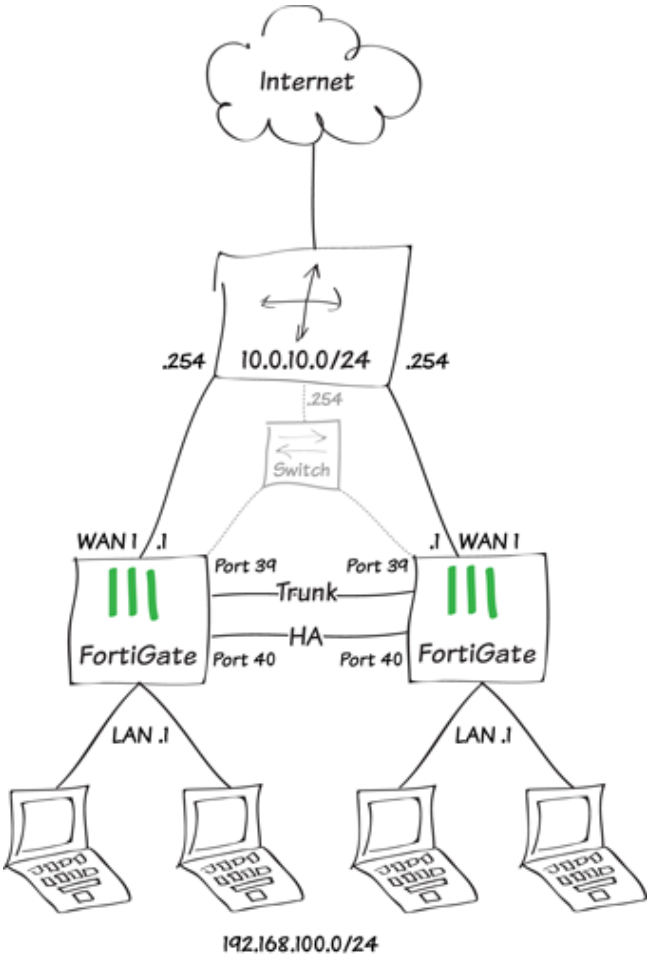
Recipes

- Redundant architecture
- BGP over a dynamic IPsec VPN
- SLBC setup with one FortiController
- SLBC Active-Passive setup with two FortiControllers
- SLBC Active-Passive with two FortiControllers and two chassis
- SLBC Dual Mode setup with two FortiControllers
- SLBC Active-Passive with four FortiControllers and two chassis

Articles

- Hub-and-spoke VPN using quick mode selectors

Redundant architecture



The following recipe provides useful instructions for customers with multi-site architecture and redundant firewalls. It is intended for those customers that want to reduce the number of on-site appliances while increasing network security and decreasing Total Cost of Ownership, where the goal is simple, cost-effective reliability.

FortiOS 5.2 introduced many new features that we will use in this configuration, which is therefore not possible on FortiOS 5.0.x or earlier. The recipe is performed with the FortiGate 1xxD/2xxD series.

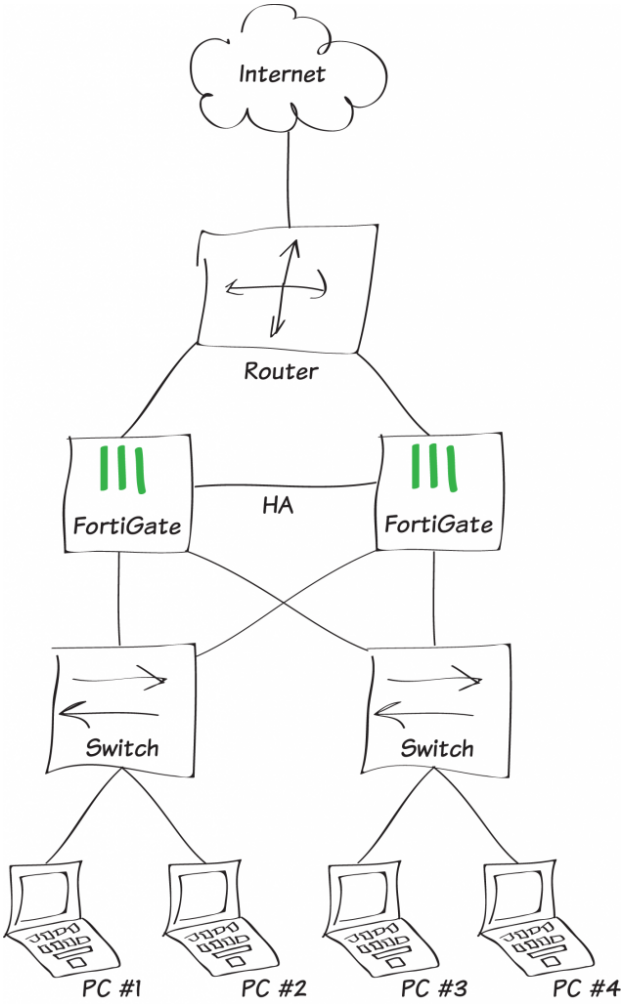
By following the recipe, you will be able to provide your small-site customers with simple, yet secure infrastructure that perfectly matches the UTM approach, where we want to centralize as many security features as possible on a single device or cluster.

The recipe provides task-oriented instructions for administrators to fully complete the installation. It is divided into the following sections:

1. Scenario: This section section explains the problems that this new network topology solves, including the cases in which the topology should be used.
2. Topology: This section includes diagrams of the new topology. It also lists key advantages to this kind of architecture and explains why it solves the problems previously identified in The Scenario.
3. Configuration: This section provides step-by-step instructions for configuring the FortiGates within the new topology.

Scenario

In the standard scenario, we assume the following topology as the starting point:



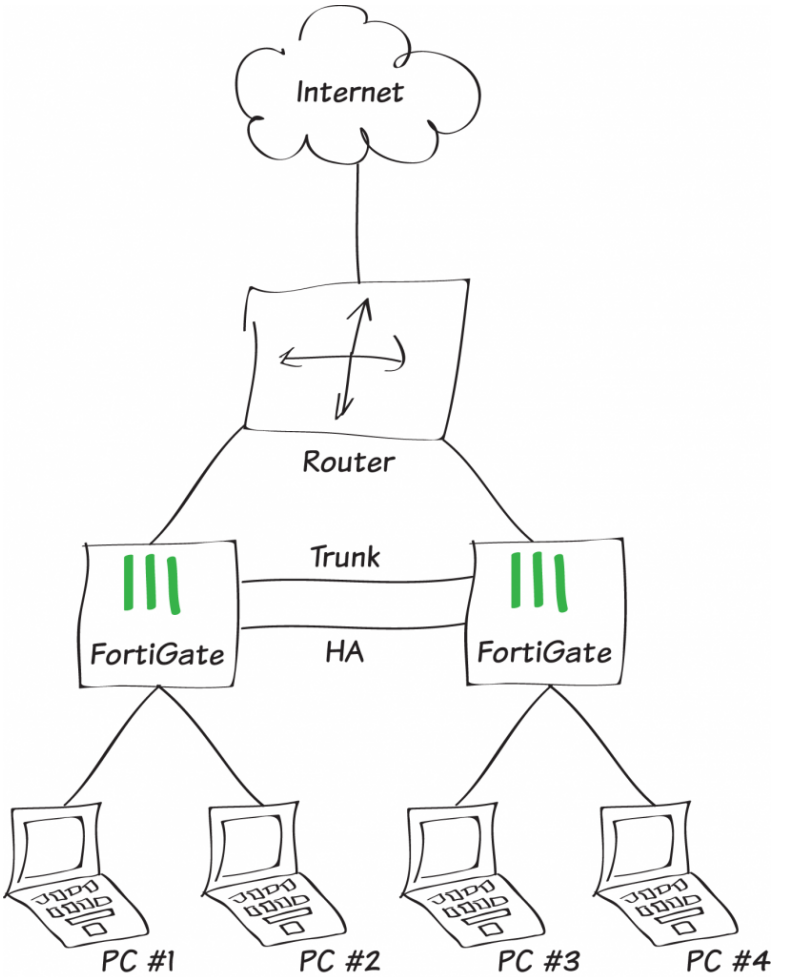
Multi-site customers that want to avoid any “Single Point of Failure” in their remote networks often use this kind of topology. These customers require two FortiGates in Active/Passive mode and therefore two switches on the LAN side to transfer Ethernet payloads to the active FortiGate. There are a few downsides to this approach:

- Four appliances need to be managed and supervised.
- Administrators must know how to work with the Firewall OS and with the Switch OS.
- If one switch fails, the workstations connected won’t be able to reach the Internet.
- Most of the firewall ports are not used.

Topology

In this section, we look at the target topology and the scenarios for FortiGate failover. At the end of the section, we discuss the key advantages of adopting the target topology.

2.1 The Target Topology



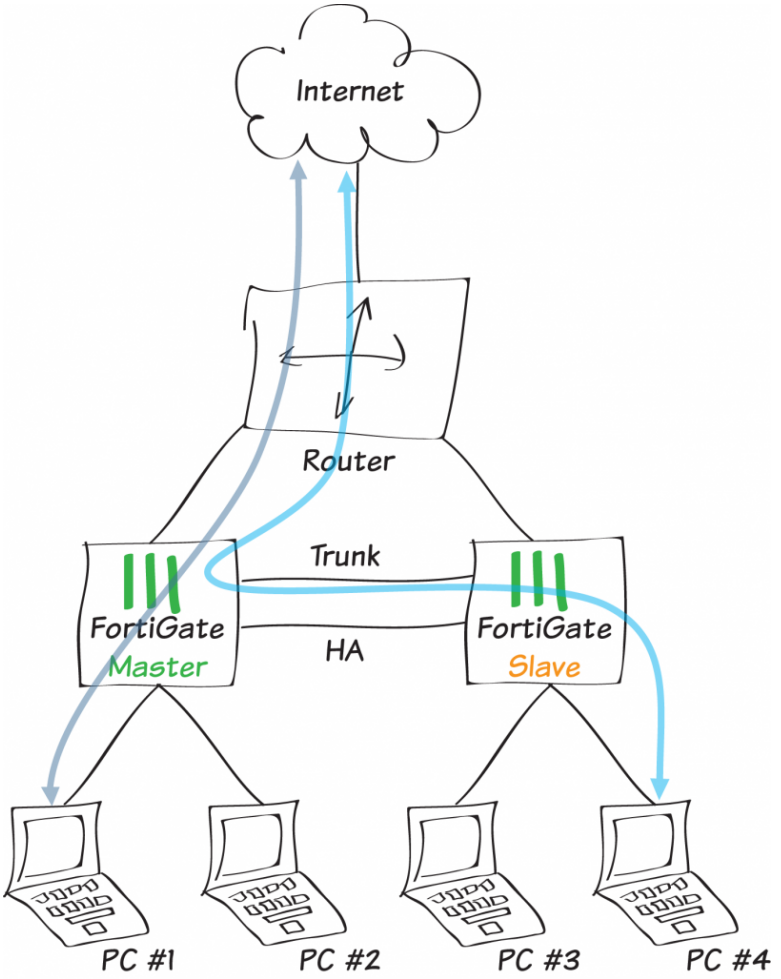
In this new topology, we won't be using additional switches. Instead, we will be using the FortiGate's Integrated Switch Fabric (ISF) solution on both master and slave firewalls.

Note that the target topology uses a FortiGate 2xxD, which has 40 ports. In your configuration, ensure that each FortiGate has enough ports to handle all of the computers in the event of a failover, or switches will still need to be involved.

The administrator will have to configure a trunk link between the two FortiGate physical switches to expand subnets and VLANs from one firewall to the other.

In a FortiGate cluster using FGCP, the slave firewall's ISF can still be used to send traffic destined for the active member across the trunk link.

A representation of the traffic flow appears below:

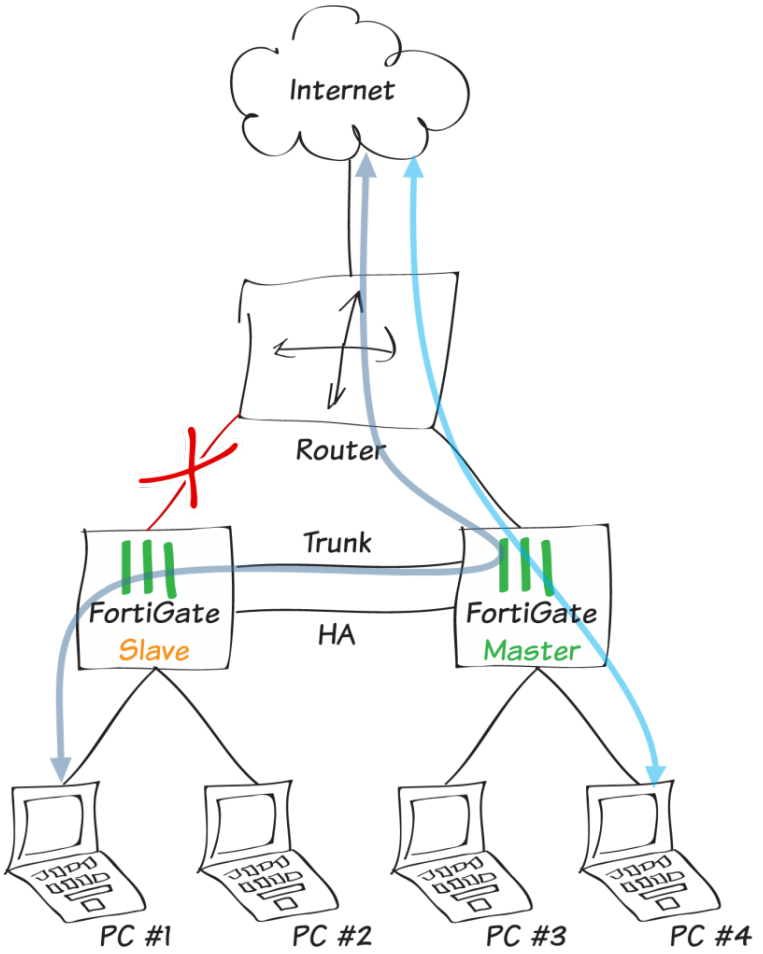


2.2 FortiGate Failover

Case 1: Link failure

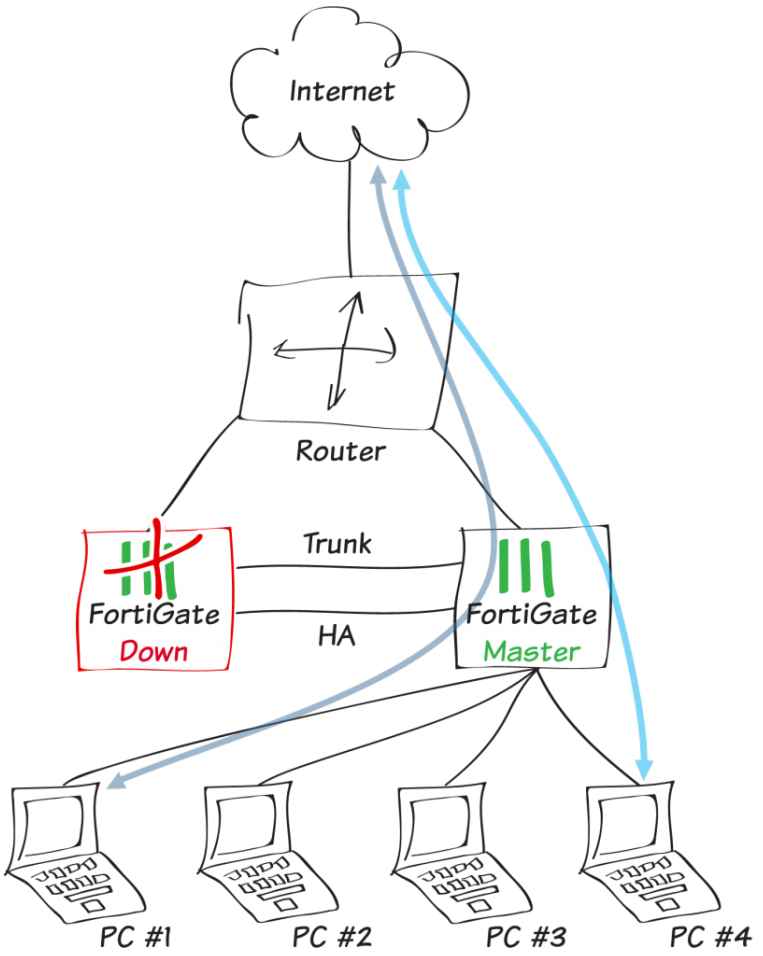
The diagram below represents traffic flow in the event of a failover in the following cases:

- The monitored WAN port, on what was originally the Master FortiGate, fails.
- The link between the router and the original Master FortiGate fails.



Case 2: FortiGate global failure

If the master were to completely fail (including the ISF), the administrator would have to plug the LANsegments into the remaining firewall, just as if one switch were to fail in our standard topology.



2.3 Key Advantages

This new topology offers a few key advantages:

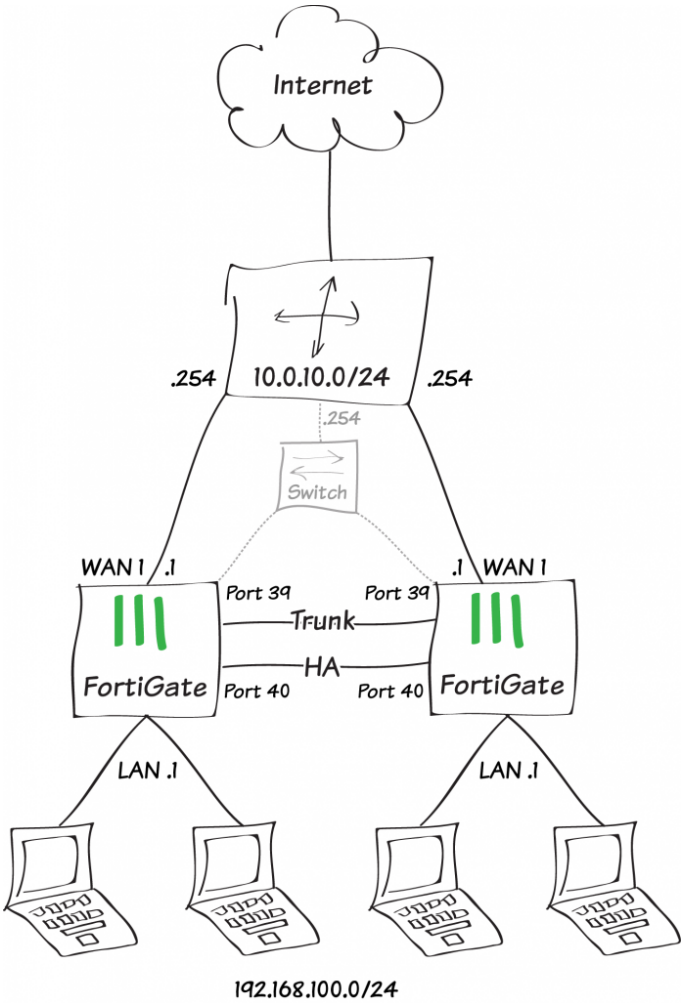
- Only two devices are required, where four are required in the standard topology.
- It is easier for the administrator to manage security and switching on a single device.
- The use of FortiManager simplifies central management.
- There is only one cluster to supervise.

Configuration

In this section, we reproduce the following network topology. Notice how the router has a switch interface.If your router does not have a switch interface, you will have to add an extra switch (noted in gray below), and in the event of a firewall crash, you will have to power cycle the router.

As we will be changing the configuration of the hardware switch, we strongly recommend that you use the management port to follow the steps below.

By default, the FortiGate management IP address is 192.168.1.99/24.



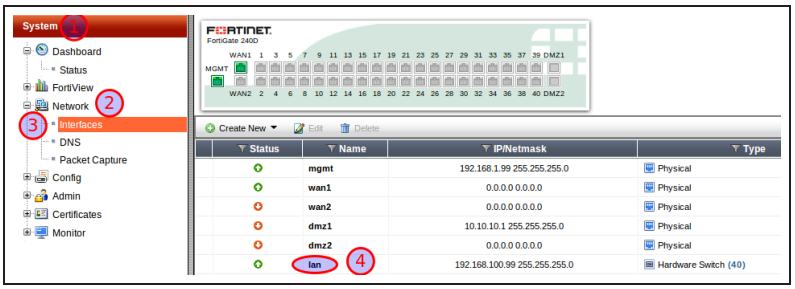
1. Configuring the hardware switch

By default on a FortiGate 1xxD/2xxD, the unit is in Interface mode and all of the internal ports are attached to a hardware switch named **lan**. In this example, we need to use ports 39 and 40 for Trunk and HA respectively.

The first step is to remove ports 39 and 40 from the Hardware Switch lan. Begin by editing the lan interface.

If the unit is in Switch mode, it will have to be reconfigured into Interface mode. For more information, see Choosing your FortiGate's switch mode.

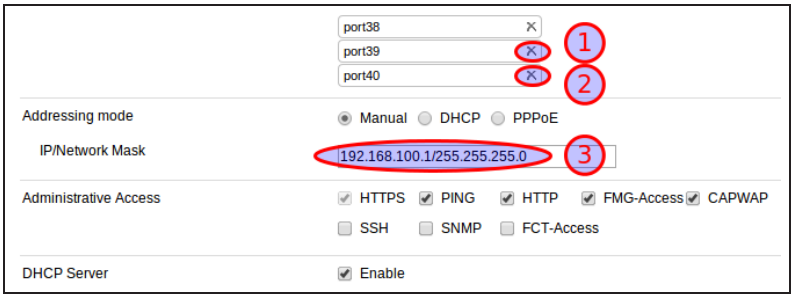
Go to **System > Network > Interfaces** and double-click **lan** in the interface list.



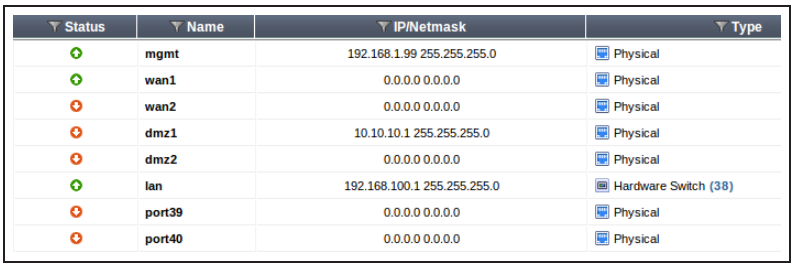
Remove the last two ports in the list, in this case **port39** and **port40**.

Then configure the **IP/Network Mask** with the following address: *192.168.100.1/255.255.255.0*

When you are done, accept the change.



The interface list should now look like this:



Status	Name	IP/Netmask	Type
	mgmt	192.168.1.99 255.255.255.0	Physical
	wan1	0.0.0.0 0.0.0.0	Physical
	wan2	0.0.0.0 0.0.0.0	Physical
	dmz1	10.10.10.1 255.255.255.0	Physical
	dmz2	0.0.0.0 0.0.0.0	Physical
	lan	192.168.100.1 255.255.255.0	Hardware Switch (38)
	port39	0.0.0.0 0.0.0.0	Physical
	port40	0.0.0.0 0.0.0.0	Physical

For the trunk port to work properly, we need to configure a vlan ID on the Virtual Switch. This can only be done in the CLI.

```
FGT1 # config system global
 FGT1 (global) # set virtual-switch-vlan enable
 FGT1 (global) # end
 FGT1 # show system global
```

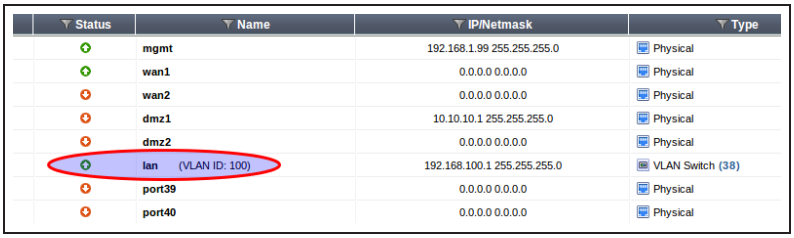
First we need to enable this feature globally. Use the commands shown here:

```
config system global
  set fgd-alert-subscription advisory latest-threat
  set hostname "FGT1"
  set internal-switch-mode interface
  set optimize antivirus
  set timezone 04
  set virtual-switch-vlan enable
end
```

Next, edit the Virtual Switch and set the vlan number:

```
FGT1 # config system virtual-switch
 FGT1 (virtual-switch) # edit lan
 FGT1 (lan) # set vlan 100
 FGT1 (lan) # end
```

You should now be able to see VLAN Switch in the interface list.



Status	Name	IP/Netmask	Type
	mgmt	192.168.1.99 255.255.255.0	Physical
	wan1	0.0.0.0 0.0.0.0	Physical
	wan2	0.0.0.0 0.0.0.0	Physical
	dmz1	10.10.10.1 255.255.255.0	Physical
	dmz2	0.0.0.0 0.0.0.0	Physical
	lan (VLAN ID: 100)	192.168.100.1 255.255.255.0	VLAN Switch (38)
	port39	0.0.0.0 0.0.0.0	Physical
	port40	0.0.0.0 0.0.0.0	Physical

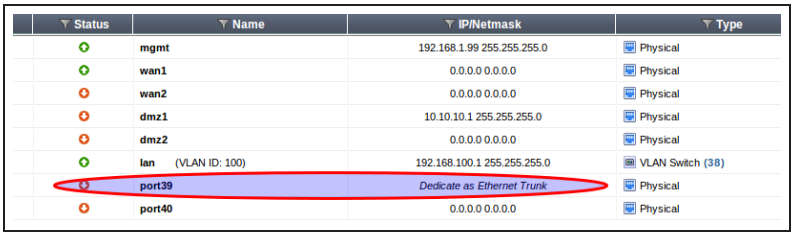
2. Configuring the trunk port

The trunk port will be used to allow traffic to flow between the Virtual Switch of each FortiGate.

Configuring the trunk port is only possible in the CLI:

```
FGT1 # config system interface
 FGT1 (interface) # edit port39
 FGT1 (port39) # set trunk enable
 FGT1 (port39) # end
 FGT1 # show system interface port39
 config system interface
   edit "port39"
     set [glossary_exclude]vdom[/glossary_exclude] "root"
     set type physical
     set trunk enable
     set [glossary_exclude]snmp[/glossary_exclude]-index 10
   next
 end
```

You should now be able to see the trunk port in the interface list.

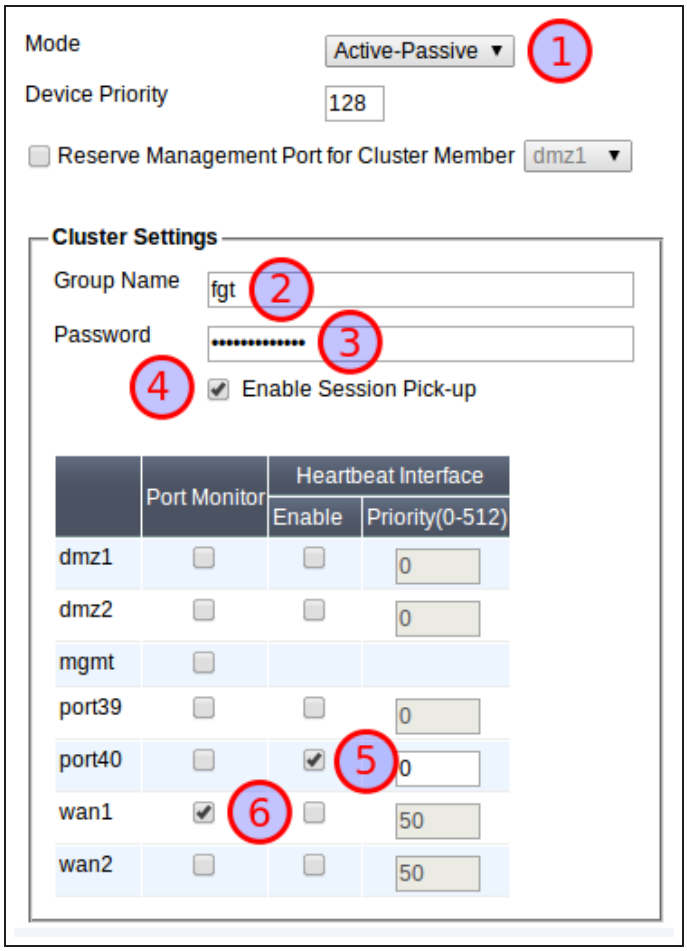


Status	Name	IP/Netmask	Type
	mgmt	192.168.1.99 255.255.255.0	Physical
	wan1	0.0.0.0 0.0.0.0	Physical
	wan2	0.0.0.0 0.0.0.0	Physical
	dmz1	10.10.10.1 255.255.255.0	Physical
	dmz2	0.0.0.0 0.0.0.0	Physical
	lan (VLAN ID: 100)	192.168.100.1 255.255.255.0	VLAN Switch (38)
	port39	*Dedicate as Ethernet Trunk*	Physical
	port40	0.0.0.0 0.0.0.0	Physical

3. Configuring HA

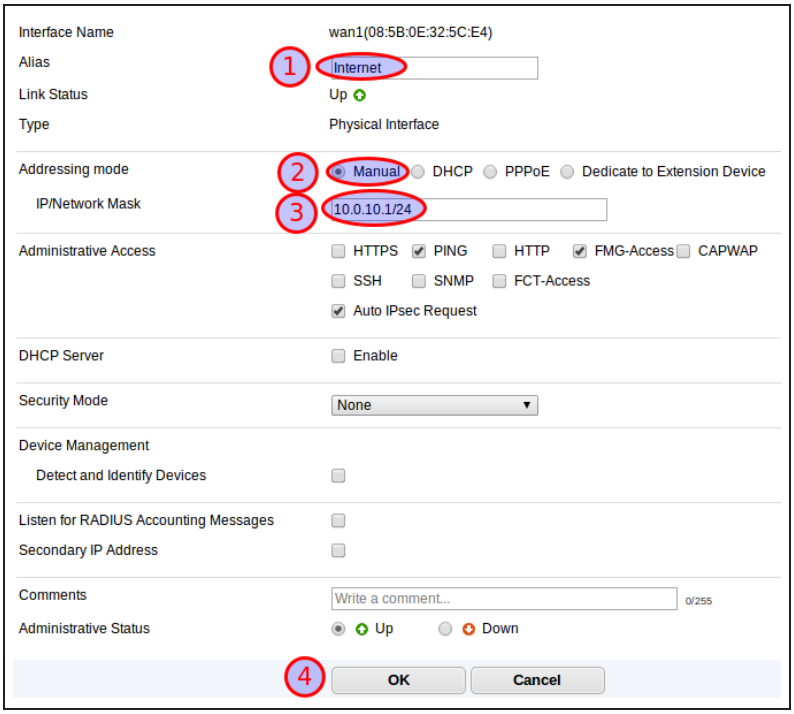
We will now configure High Availability. Port 40 will be used for HeartBeat/Sync communications between cluster members. Port Wan1 will be monitored.

Go to **System > Config > HA** and configure High Availability as shown:

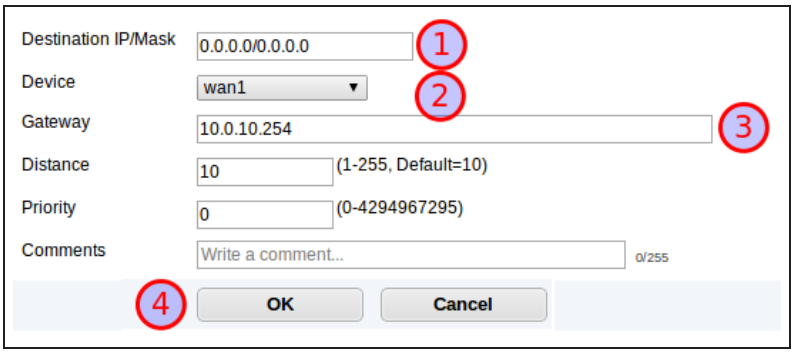


4. Configuring WAN1 IP routing

Go to **System > Network > Interfaces** and edit **wan1** as shown.



Go to **Router > Static > Static Routes** and create a new route as shown:

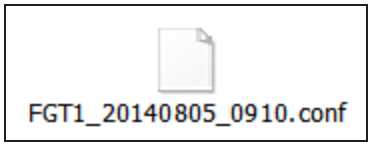


5. Configuring your firewall policies

Go to **Policy & Objects > Policy > IPv4** and configure firewall policies as desired.

6. Replicate the entire configuration on the second device

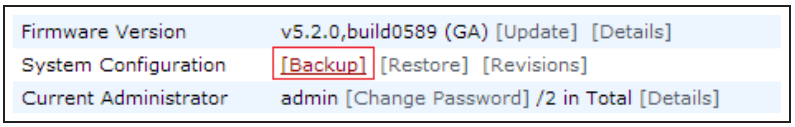
Once the first FortiGate is configured, the easiest way to configure the second one is to backup the configuration file of the first FortiGate and restore it on the second.



You can change the hostname and HA priority lines directly in the configuration file prior to restoring it on the second FortiGate.

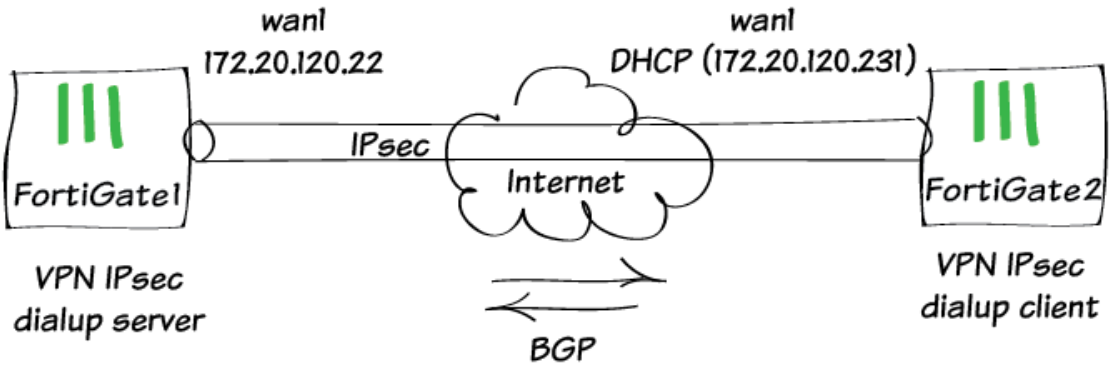
Do not use a text editor, like Notepad or Word, to do this editing. Instead, use a code editor, like Notepad++ or TextWrangler, that won't add unintended content to the file.

Go to **System > Dashboard > Status** and select **Backup** next to **System Configuration** in the **System Information** widget.



For further reading, check out High Availability in the FortiOS 5.2 Handbook.

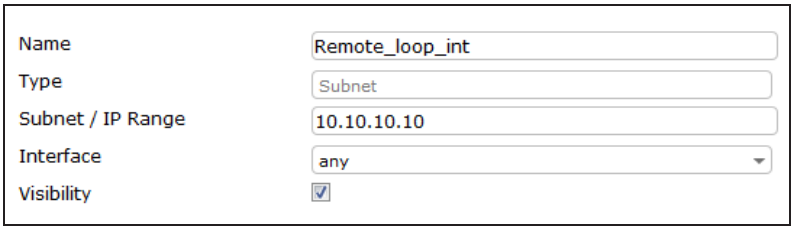
BGP over a dynamic IPsec VPN



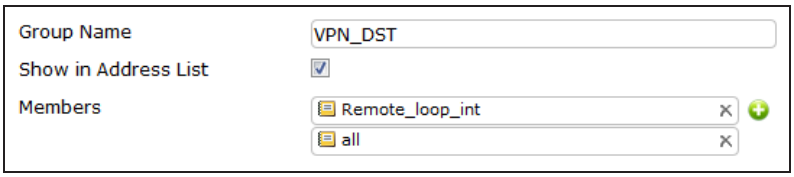
This example shows how to create a dynamic IPsec VPN tunnel and allowing BGP peering through it.

1. Configuring IPsec in FortiGate1

Go to **Policy & Objects > Objects > Addresses** and select create new **Address.**



Then create **Address Group.**



Go to **System > Status** to look for **CLI Console** widget and create phase 1.

```
 config vpn ipsec phase1-interface
    edit Dialup
        set type dynamic
        set interface wan1
        set mode aggressive
        set peertype one
        set mode-cfg enable
        set proposal 3des-sha1 aes128-sha1
        set peerid dial
        set assign-ip disable
        set psksecret
    next
end
```

Create phase 2.

```
config vpn ipsec phase2-interface
    edit dial_p2
        set phase1name Dialup
        set proposal 3des-sha1 aes128-sha1
        set src-addr-type name
        set dst-addr-type name
        set src-name all
        set dst-name VPN_DST
    next
end
```

2. Configuring BGP in FortiGate1

Go to **System > Network > Interfaces** and create a **Loopback** interface.

Interface Name	loop
Type	Loopback Interface
IP/Network Mask	20.20.20.20/255.255.255.255

Go to **System > Status** to look for **CLI Console** widget and create BGP route.

```
 config router bgp
    set as 100
    set router-id 1.1.1.1
        config neighbor
            edit 10.10.10.10
                set ebgp-enforce-multihop enable
                set remote-as 200
                set update-source loop
            next
        end
        config redistribute connected
            set status enable
        end
end
```

3. Adding policies in FortiGate1

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **Dialup** to **loop** interfaces.

Incoming Interface	Dialup
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	loop
Destination Address	all
Schedule	always
Service	BGP
Action	✓ ACCEPT

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **loop** to **Dialup** interfaces.

4. Configuring IPSec in FortiGate 2

Go to **System > Status** to look for **CLI Console** widget and create phase 1.

```
config vpn ipsec phase1-interface
 edit Dialup
 set interface wan1
 set mode aggressive
 set mode-cfg enable
 set proposal 3des-sha1 aes128-sha1
 set localid dial
 set remote-gw 172.20.120.22
 set assign-ip disable
 set psksecret
 next
 end
```

Create phase 2.

```
config vpn ipsec phase2-interface
    edit dial_p2
        set phase1name Dialup
        set proposal 3des-sha1 aes128-sha1
        set keepalive enable
    next
end
```

5. Configuring BGP in FortiGate 2

Go to **System > Network > Interfaces** and create a **Loopback** interface.

Interface Name	loop
Type	Loopback Interface
IP/Network Mask	10.10.10.10/255.255.255.255

Go to **System > Status** to look for **CLI Console** widget and create BGP route.

```
config router bgp
    set as 200
    set router-id 1.1.1.2
        config neighbor
            edit 20.20.20.20
                set ebgp-enforce-multihop enable
                set remote-as 100
                set update-source loop
            next
        end
        config redistribute connected
            set status enable
        end
end
```

6. Adding policies in FortiGate 2

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **Dialup** to **loop** interfaces.

Incoming Interface	Dialup
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	loop
Destination Address	all
Schedule	always
Service	BGP
Action	✓ ACCEPT

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **loop** to **Dialup** interfaces.

Incoming Interface	loop
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	Dialup
Destination Address	all
Schedule	always
Service	BGP
Action	✓ ACCEPT

7. Adding a static route in FortiGate 2

Go to **Router > Static > Static Routes** and add a route to the remote Loopback interface via **Dialup** interface.

Destination IP/Mask	20.20.20.20/255.255.25
Device	Dialup
Administrative Distance	10

8. Verifying tunnel is Up

Go to **VPN > Monitor > IPsec Monitor** to verify that the tunnel is **Up**.

Name	Remote Gateway	Status	Incoming Data	Outgoing Data
Dialup_0	172.20.120.231	Up	82.99 MB	987.89 KB

9. Results

From FortiGate 1, Go to **Router > Monitor > Routing Monitor** and verify that routes from FortiGate 2 were successfully advertised to FortiGate 1 via BGP.

Type	Network	Gateway	Interface
Static	0.0.0.0/0	172.20.120.2	wan1
Static	10.10.10.10/32	0.0.0.0	Dialup_0
BGP	10.10.80.0/24	10.10.10.10	
BGP	10.10.100.0/24	10.10.10.10	
Connected	20.20.20.20/32	0.0.0.0	loop
Connected	172.20.120.0/24	0.0.0.0	wan1
Connected	192.168.100.0/24	0.0.0.0	lan

From FortiGate 1, go to **System > Status** to look for **CLI Console** widget and type this command to verify BGP neighbors.

```
get router info bgp summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 8
2 BGP AS-PATH entries
0 BGP community entries
Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd

10.10.10.10     4         200     8257     8237
7     0     0 5d00h01m         4
Total number of neighbors 1
```

From FortiGate 2, go to **Router > Monitor > Routing Monitor** and verify that routes from FortiGate 1 were successfully advertised to FortiGate 2 via BGP.

Type	Network	Gateway	Interface
Static	0.0.0.0/0	0.0.0.0	Dialup
Connected	10.10.10.10/32	0.0.0.0	loop
Connected	10.10.80.0/24	0.0.0.0	lan
Connected	10.10.100.0/24	0.0.0.0	dmz
Static	20.20.20.20/32	0.0.0.0	Dialup
Connected	172.20.120.0/24	0.0.0.0	wan1
BGP	192.168.100.0/24	20.20.20.20	

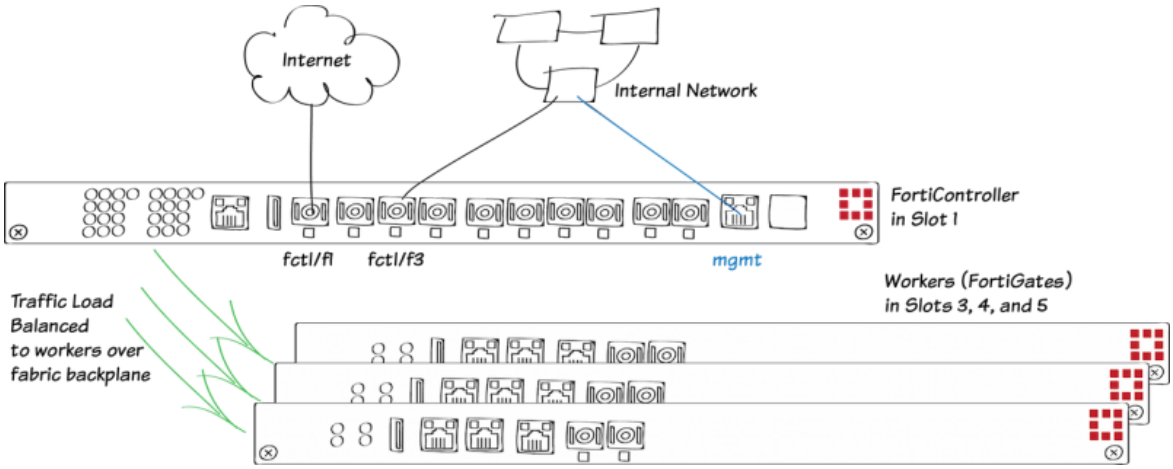
From FortiGate 2, go to **System > Status** to look for **CLI Console** widget and type this command to verify BGP neighbors.

```
get router info bgp summary
BGP router identifier 1.1.1.2, local AS number 200
BGP table version is 11
2 BGP AS-PATH entries
0 BGP community entries
Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd

20.20.20.20     4         100     8341     8361
10    0     0 5d01h32m         3
Total number of neighbors 1
```

For further reading, check out IPsec VPN and Border Gateway Protocol (BGP) in the FortiOS 5.2 Handbook.

SLBC setup with one FortiController



This example describes the basics of setting up a Session-aware Load Balancing Cluster (SLBC) that consists of one FortiController-5103B, installed in chassis slot 1, and three FortiGate-5001C workers, installed in chassis slots 3, 4, and 5. This SLBC configuration can have up to eight 10Gbit network connections.

For more information about SLBC go here.

1. Hardware setup

Install a FortiGate-5000 series chassis and connect it to power. Install the FortiController in slot 1. Install the workers in slots 3, 4, and 5. Power on the chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally. (To check normal operation LED status see the FortiGate-5000 series documents available here.)

Check the FortiSwitch-ATCA release notes and install the latest supported firmware on the FortiController and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

2. Configuring the FortiController

Connect to the FortiController GUI (using HTTPS) or CLI (using SSH) with the default IP address (http://192.168.1.99) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None). Login using the admin administrator account and no password.

Add a password for the admin administrator account. From the GUI use the **Administrators** widget or from the CLI enter this command.

```
config admin user
  edit admin
      set password <password>
  end
```

Change the FortiController mgmt interface IP address. From the GUI use the **Management Port** widget or from the CLI enter this command.

```
config system interface
  edit mgmt
      set ip 172.20.120.151/24
   end
```

If you need to add a default route for the management IP address, enter this command.

```
config route static
   edit route 1
       set gateway 172.20.120.2
   end
```

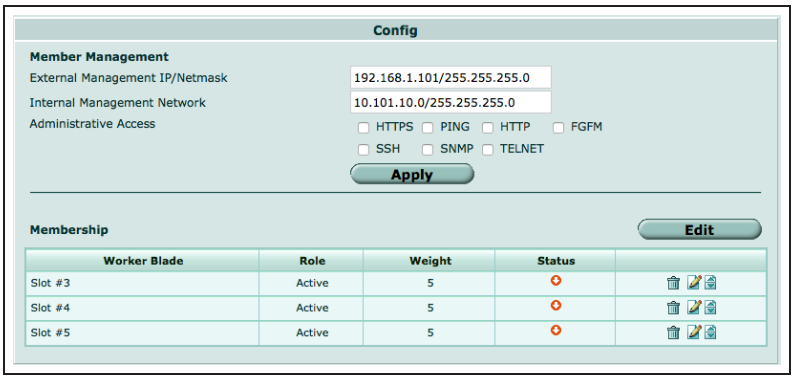
Set the chassis type that you are using.

```
config system global
   set chassis-type fortigate-5140
end
```

Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. Since the workers have not been configured yet their status is **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure them.



You can also enter the following CLI command to add slots 3, 4, and 5 to the cluster:

```
config load-balance setting
  config slots
    edit 3
    next
    edit 4
    next
    edit 5
  end
end
```

You can also enter the following CLI command to configure the external management IP/Netmask and management access to this address:

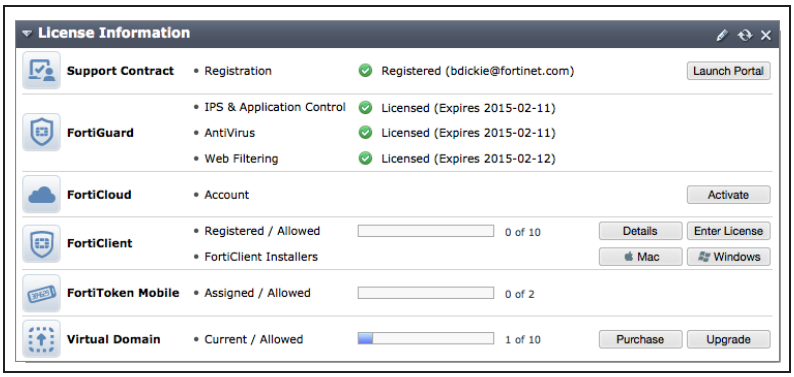
```
config load-balance setting
  endset base-mgmt-external-ip 172.20.120.100 255.255.255.0
  endset base-mgmt-allowaccess https ssh ping
end
```

3. Adding the workers

Enter this command to reset the workers to factory default settings.

```
execute factoryreset
```

Register and apply licenses to each worker before adding the workers to the SLBC. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**.

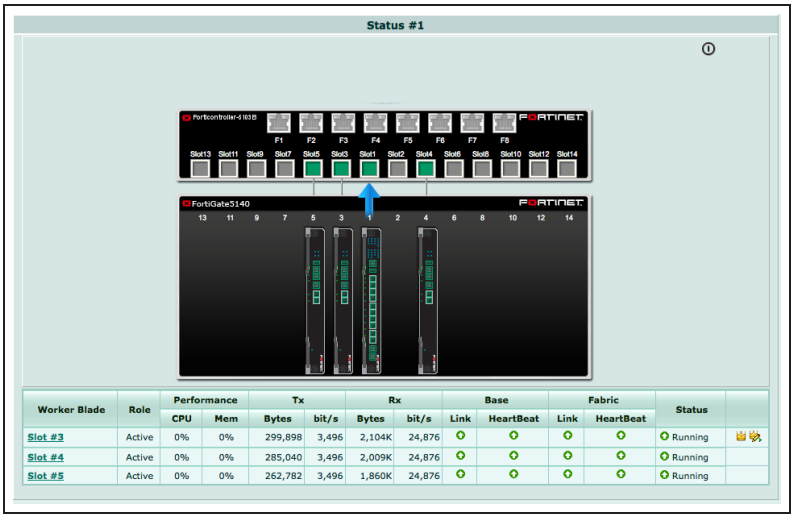


Log into the CLI of each worker and enter this CLI command to set the worker to operate in FortiController mode.

```
config system elbc
  set mode forticontroller
end
```

The worker restarts and joins the cluster. On the FortiController GUI go to **Load Balance > Status**. As the workers restart they should appear in their appropriate slots.

The worker in the lowest slot number usually becomes the primary unit.



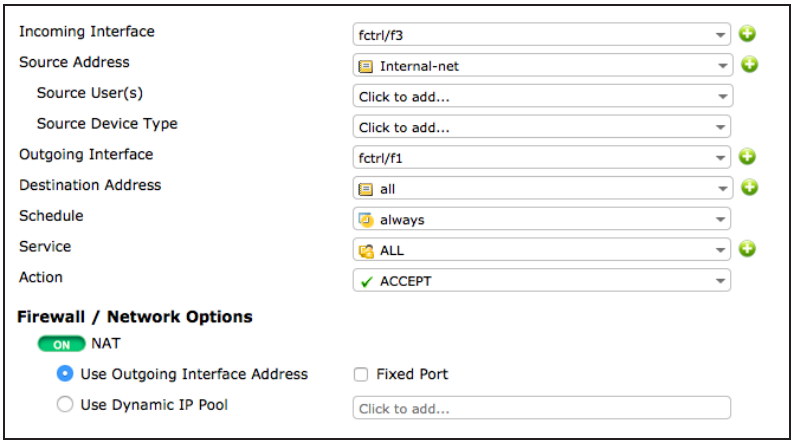
4. Results

You can now manage the workers in the same way as you would manage a standalone FortiGate. You can connect to the worker GUI or CLI using the **External Management IP**. If you had configured the worker mgmt1 or mgmt2 interfaces you can also connect to one of these addresses to manage the cluster.

To operate the cluster, connect networks to the FortiController front panel interfaces and connect to a worker GUI or CLI to configure the workers to process the traffic they receive. When you connect to the External Management IP you connect to the primary worker. When you make configuration changes they are synchronized to all workers in the cluster.

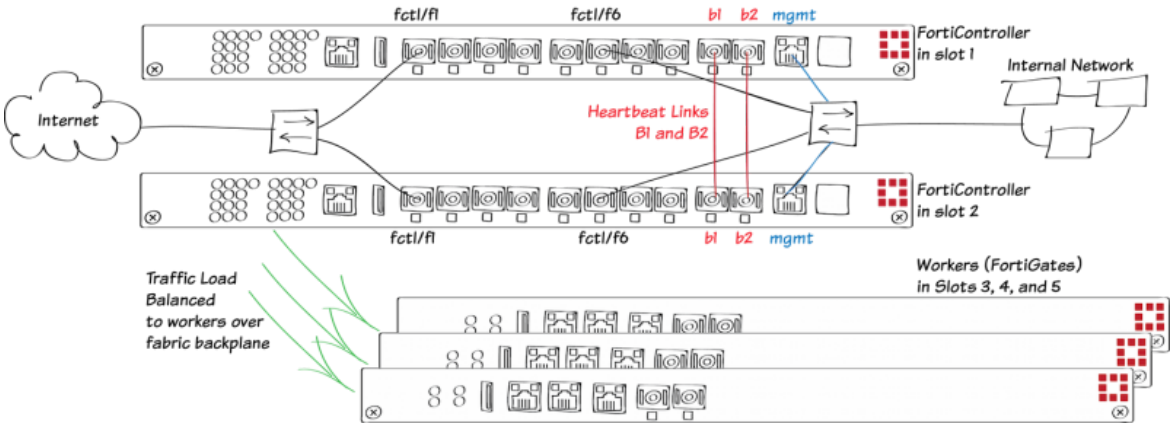
By default on the workers, all FortiController front panel interfaces are in the root VDOM. You can configure the root VDOM or create additional VDOMs and move interfaces into them.

For example, you could connect the Internet to FortiController front panel interface 4 (fctrl/f4 on the worker GUI and CLI) and an internal network to FortiController front panel interface 2 (fctrl/f2 on the worker GUI and CLI) . Then enter the root VDOM and add a policy to allow users on the Internal network to access the Internet.



For further reading, check out the FortiController Session-aware Load Balancing Guide.

SLBC Active-Passive setup with two FortiControllers



This example describes the basics of setting up an active-passive Session-aware Load Balancing Cluster (SLBC) that consists of two FortiController-5103Bs, installed in chassis slots 1 and 2, and three FortiGate-5001C workers, installed in chassis slots 3, 4, and 5. This SLBC configuration can have up to eight redundant 10Gbit network connections.

The FortiControllers in the same chassis to operate in active-passive HA mode for redundancy. The FortiController in slot 1 becomes the primary unit actively processing sessions. The FortiController in slot 2 becomes the subordinate unit, sharing the primary unit's session table. If the primary unit fails the subordinate unit resumes all active sessions.

All networks have redundant connections to both FortiControllers. You also create heartbeat links between the FortiControllers and management links from the FortiControllers to an internal network.

For more information about SLBC go here.

1. Hardware setup

Install a FortiGate-5000 series chassis and connect it to power. Install the FortiControllers in slots 1 and 2. Install the workers in slots 3, 4, and 5. Power on the chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally (to check normal operation LED status, see the FortiGate-5000 series documents available here).

Create duplicate connections from the FortiController front panel interfaces to the Internet and to the internal network.

Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a backup heartbeat link by connecting the FortiController B2 interfaces together. You can directly connect the interfaces with a patch cable or connect them together through a switch. If you use a switch, it must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301 and 101). These connections establish heartbeat, base control, and base management communication between the FortiControllers. Only one heartbeat connection is required but redundant connections are recommended.

Connect the mgmt interfaces of the both FortiControllers to the internal network or any network from which you want to manage the cluster.

Check the FortiSwitch-ATCA release notes and install the latest supported firmware on the FortiController and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

2. Configuring the FortiControllers

Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in slot 1 with the default IP address (http://192.168.1.99) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None).

Add a password for the admin administrator account. You can either use the GUI **Administrators** widget or enter this CLI command.

```
config admin user
  edit admin
      set password <password>
   end
```

Change the FortiController mgmt interface IP address. Use the **Management Port** widget in the GUI or enter this command. Each FortiController should have a different Management IP address.

```
config system interface
  edit mgmt
      set ip 172.20.120.151/24
   end
```

If you need to add a default route for the

```
config route static
```

management IP address, enter this command.

```
edit 1
    set gateway 172.20.120.2
end
```

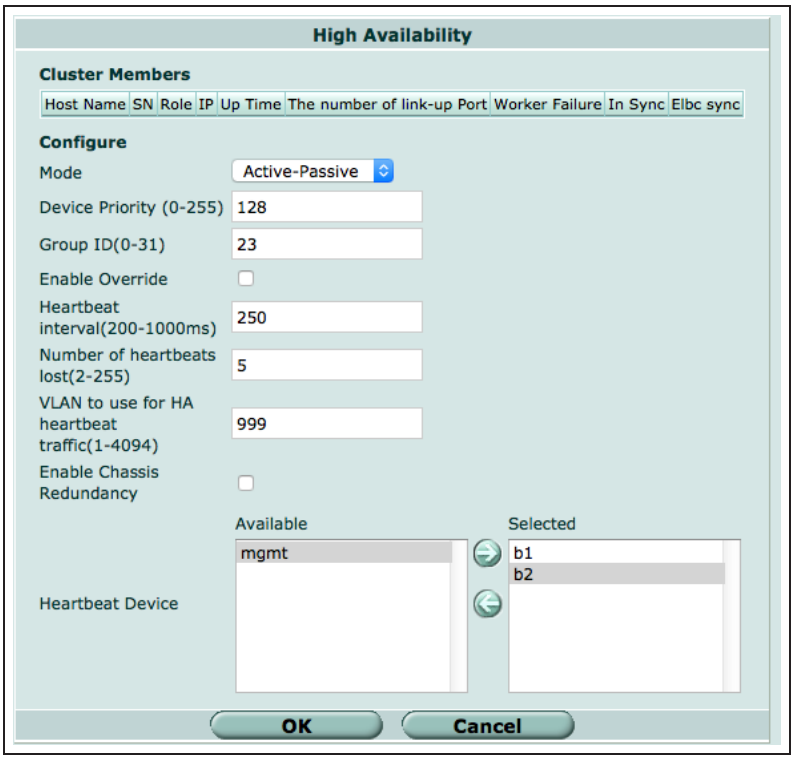
Set the chassis type that you are using.

```
config system global
   set chassis-type fortigate-5140
end
```

Configure active-passive HA on the FortiController in slot 1.

From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

Set **Mode** to **Active-Passive**, change the **Group ID**, and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.



You can also enter this command:

```
config system ha
   set mode a-p
   set groupid 23
   set hbdev b1 b2
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 setting causes a

MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

You can also adjust other HA settings. For example, you could increase the **Device Priority** of the FortiController that you want to become the primary unit, enable **Override** to make sure the FortiController with the highest device priority becomes the primary unit, and change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on your network.

You would only select **Enable chassis redundancy** if your cluster has more than one chassis.

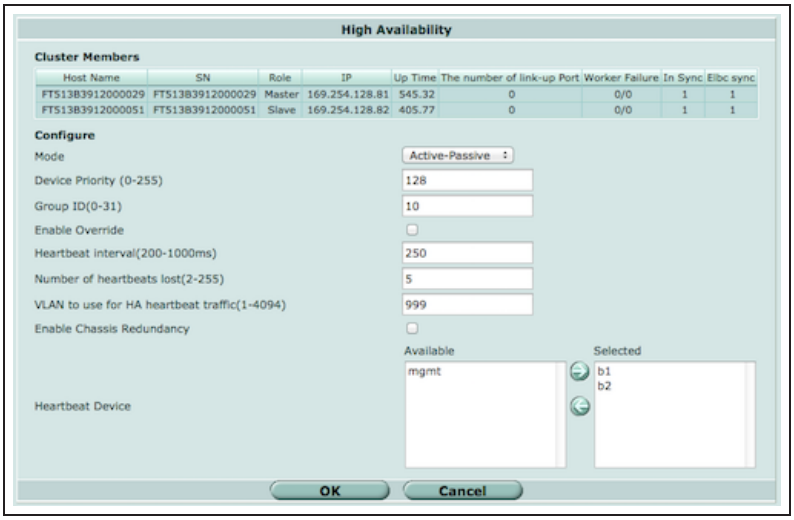
Log into the web-based manager of the FortiController in slot 2 and duplicate the HA configuration of the FortiController in slot 1, except for the Device Priority and override setting, which can be different on each FortiController.

After a short time, the FortiControllers restart in HA mode and form an active-passive cluster. Both FortiControllers must have the same HA configuration and at least one heartbeat link must be connected.

Normally the FortiController in slot 1 is the primary unit, and you can log into the cluster using the management IP address you assigned to this FortiController.

You can confirm that the cluster has been formed by viewing the HA configuration from the the FortiController web-based manager. The display should show both FortiControllers in the cluster.

Since the configuration of all FortiControllers is synchronized, you can complete the configuration of the cluster from the primary FortiController.



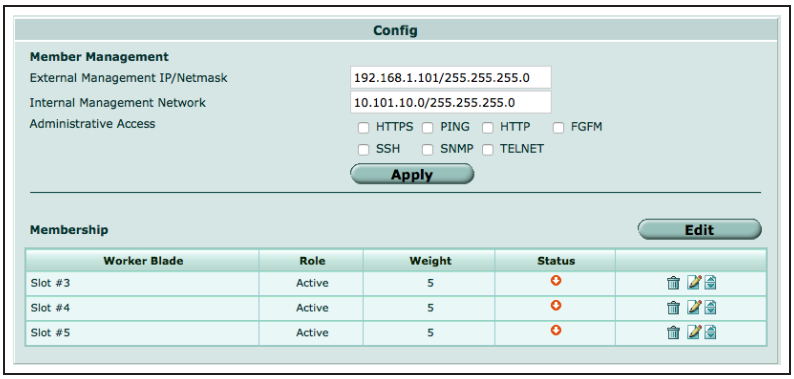
You can also go to **Load Balance > Status** to see the status of the cluster. This page should show both FortiControllers in the cluster.

The FortiController in slot 1 is the primary unit (slot icon colored green) and the FortiController in slot 2 is the backup unit (slot icon colored yellow).

Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured yet their status will be **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure them.



You can also enter this command to add slots 3, 4, and 5 to the cluster:

```
config load-balance setting
  config slots
    edit 3
    next
    edit 4
    next
    edit 5
  end
end
```

You can also enter this command to set the external management IP/Netmask and configure management access.

```
config load-balance setting
 set base-mgmt-external-ip 172.20.120.100 255.255.255.0
 set base-mgmt-allowaccess https ssh ping
 end
```

Enable base management traffic between FortiControllers.

```
config load-balance setting
 config base-mgmt-interfaces
 edit b1
 next
 edit b2
 end
 end
```

Enable base control traffic between FortiControllers.

```
 config load-balance setting
 config base-ctrl-interfaces
 edit b1
 next
 edit b2
```

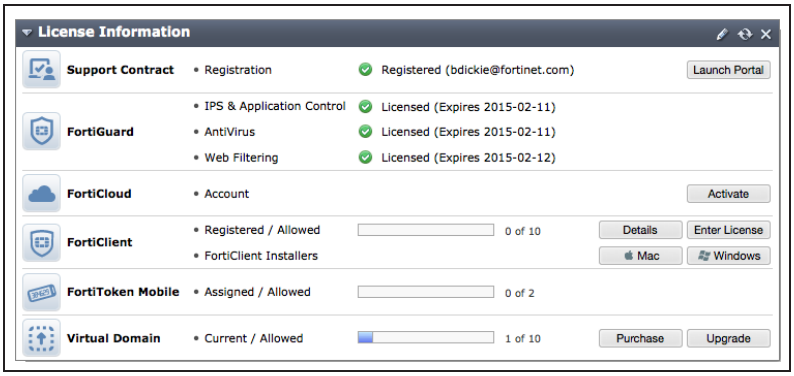
```
end
end
```

3. Adding the workers to the cluster

Reset the workers to factory default settings.

```
execute factoryreset
```

Register and apply licenses to each worker before adding the workers to the SLBC. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**.



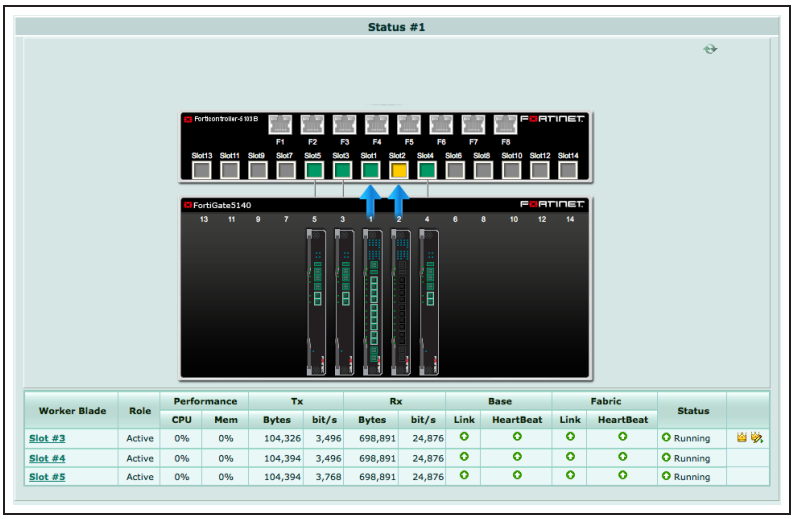
Optionally give the mgmt1 and or mgmt2 interfaces of each worker IP addresses and connect them to your network. When a cluster is created, the mgmt1 and mgmt2 IP addresses are not synchronized, so you can connect to and manage each worker separately.

Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

Log into the CLI of each worker and enter this command to set the worker to operate in FortiController mode.

```
config system elbc
set mode forticontroller
end
```

The worker restarts and joins the cluster. On the FortiController GUI go to **Load Balance > Status**. As the workers restart they should appear in their appropriate slots.

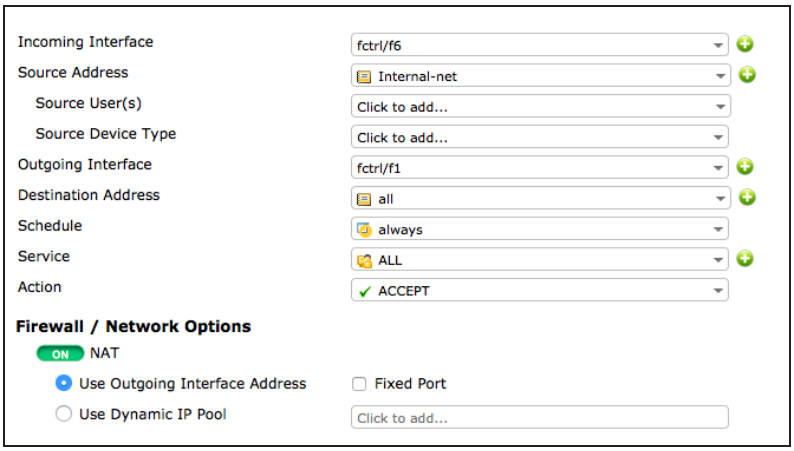


4. Results

You can now connect to the worker GUI or CLI using the **External Management IP** and manage the workers in the same way as you would manage a standalone FortiGate. If you configured the worker mgmt1 or mgmt2 interfaces you can also connect to these interfaces to configure the workers. Configuration changes made to any worker are synchronized to all workers.

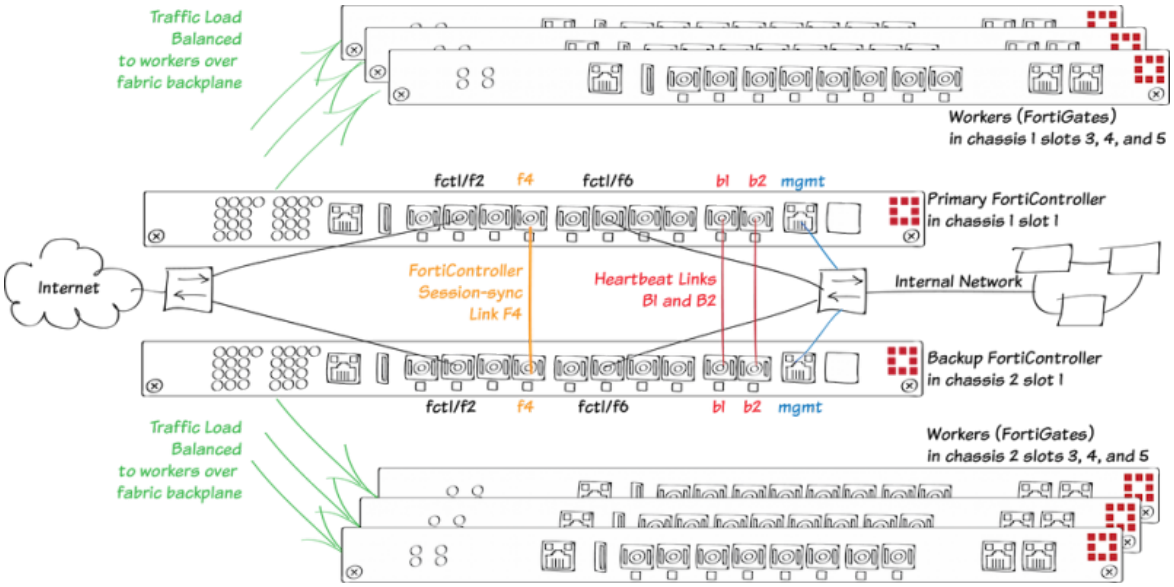
Configure the workers to process the traffic they receive from the FortiController front panel interfaces. By default all FortiController front panel interfaces are in the root VDOM. You can keep them in the root VDOM or create additional VDOMs and move interfaces into them.

For example, if you connect the Internet to FortiController front panel interface 1 (fctrl/f1 on the worker GUI and CLI) and the internal network to FortiController front panel interface 6 (fctrl/f6 on the worker GUI and CLI) you would access the root VDOM and add this policy to allow users on the Internal network to access the Internet.



For further reading, check out the FortiController Session-aware Load Balancing Guide.

SLBC Active-Passive with two FortiControllers and two chassis



This example describes how to setup an active-passive session-aware load balancing cluster (SLBC) consisting of two FortiGate-5000 chassis, two FortiController-5103Bs, and six FortiGate-5001Bs acting as workers, three in each chassis. This SLBC configuration can have up to seven redundant 10Gbit network connections.

The FortiControllers operate in active-passive HA mode for redundancy. The FortiController in chassis 1 slot 1 will be configured to be the primary unit, actively processing sessions. The FortiController in chassis 2 slot 1 becomes the subordinate unit. If the primary unit fails the subordinate unit resumes all active sessions.

All networks in this example have redundant connections to both FortiControllers and redundant heartbeat and base control and management links are created between the FortiControllers using their front panel B1 and B2 interfaces.

This example also includes a FortiController session sync connection between the FortiControllers using the FortiController F4 front panel interface (resulting in the SLBC having a total of seven redundant 10Gbit network connections). (You can use any fabric front panel interface.)

Heartbeat and base control and management traffic uses VLANs and specific subnets. So the switches and network components used must be configured to allow traffic on these VLANs and you should be aware of the subnets used in case they conflict with any connected networks.

This example sets the device priority of the FortiController in chassis 1 higher than the device priority of the FortiController in chassis 2 to make sure that the FortiController in chassis 1 becomes the primary FortiController for the cluster.

For more information about SLBC go here.

1. Hardware setup

Install two FortiGate-5000 series chassis and connect them to power. Ideally each chassis should be connected to a separate power circuit. Install a FortiController in slot 1 of each chassis. Install the workers in slots 3, 4, and 5 of each chassis. The workers must be installed in the same slots in both chassis. Power on both chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally (to check normal operation LED status, see the FortiGate-5000 series documents available here).

Create duplicate connections from both FortiController front panel interfaces to the Internet and to the internal network.

Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a backup heartbeat link by connecting the FortiController B2 interfaces together. You can directly connect the interfaces with a patch cable or connect them together through a switch. If you use a switch, it must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301 and 101). These connections establish heartbeat, base control, and base management communication between the FortiControllers. Only one heartbeat connection is required but redundant connections are recommended.

Create a FortiController session sync connection between the chassis by connecting the FortiController F4 interfaces. If you use a switch it must allow traffic on the FortiController session sync VLAN (2000). You can use any of the F1 to F8 interfaces. We chose F4 in this example to make the diagram easier to understand.

Connect the mgmt interfaces of the both FortiControllers to the internal network or any network from which you want to manage the cluster.

Check the FortiSwitch-ATCA release notes and install the latest supported firmware on the FortiController and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

2. Configuring the FortiController in Chassis 1

Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in chassis 1 with the default IP address (http://192.168.1.99) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None).

From the Dashboard System Information widget, set the **Host Name** to ch1-slot1. Or enter this command.

```
config system global
   set hostname ch1-slot1
end
```

Add a password for the admin administrator account. You can either use the **Administrators** widget on the

```
config admin user
   edit admin
     set password
```

GUI or enter this command.

```
end
```

Change the FortiController mgmt interface IP address. Use the GUI **Management Port** widget or enter this command.

```
config system interface
 edit mgmt
     set ip 172.20.120.151/24
 end
```

If you need to add a default route for the management IP address, enter this command.

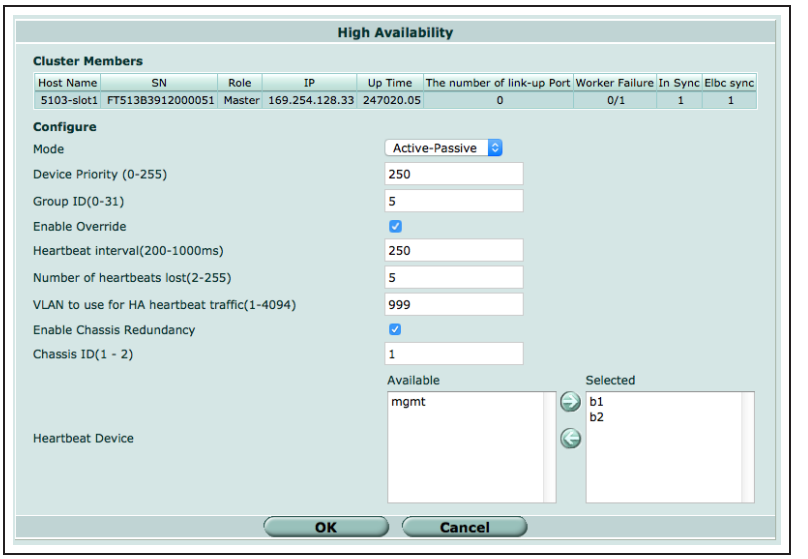
```
config route static
 edit 1
     set gateway 172.20.120.2
 end
```

Set the chassis type that you are using.

```
config system global
 set chassis-type fortigate-5140
end
```

Configure Active-Passive HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

Set **Mode** to **Active-Passive**, set the **Device Priority** to 250, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 1 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.



Enter this command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
   set session-sync-port f4
 end
```

You can also enter the complete HA

```
config system ha
```

configuration with this command.

```
 set mode active-passive
set groupid 5
 set priority 250
 set override enable
 set chassis-redundancy enable
 set chassis-id 1
 set hbdev b1 b2
 set session-sync-port f4
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 setting causes a MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

Enable Override is selected to make sure the FortiController in chassis 1 always becomes the primary unit. Enabling override could lead to the cluster renegotiating more often, so once the chassis is operating you can disable this setting.

You can also adjust other HA settings. For example, you could change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on your network. You can also adjust the **Heartbeat Interval** and **Number of Heartbeats** lost to adjust how quickly the cluster determines one of the FortiControllers has failed.

3. Configuring the FortiController in Chassis 2

Log into the FortiController in chassis 2.

Enter these commands to set the host name to ch2-slot1 and duplicate the HA configuration of the FortiController in chassis 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10), and set the **Chassis ID** to 2.

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

```
config system global
   set hostname ch2-slot1
end

config system ha
   set mode active-passive
   set groupid 5
   set priority 10
   set chassis-redundancy enable
   set chassis-id 2
   set hbdev b1 b2
   set session-sync-port f4
 end
```

4. Configuring the cluster

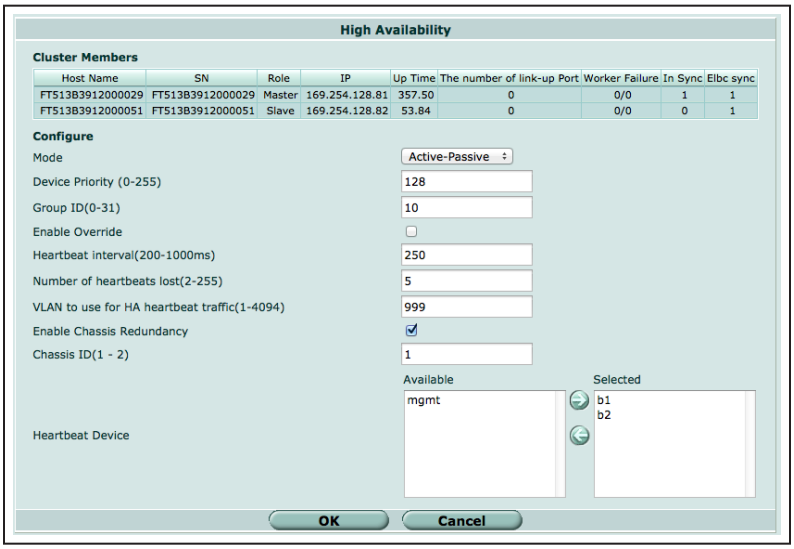
After a short time the FortiControllers restart in HA mode and form an active-passive SLBC. Both FortiControllers must have the same HA configuration and at least one heartbeat link (the B1 and B2 interfaces) must be connected. If the FortiControllers are unable to form a cluster, check to make sure that they both have the same HA configuration. Also they can't form a cluster if the heartbeat interfaces (B1 and B2) are not connected.

With the configuration described in the previous steps, the FortiController in chassis 1 should become the primary unit and you can log into the cluster using the management IP address that you assigned to the FortiController in chassis 1.

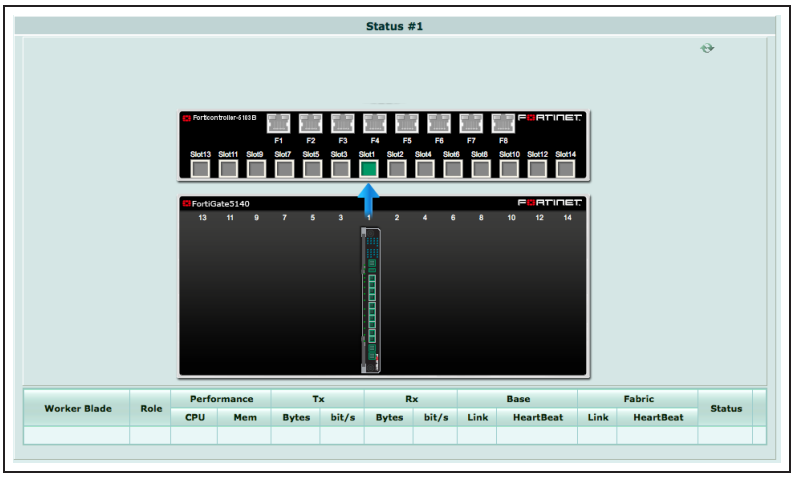
The FortiController in chassis 2 becomes the backup FortiController. You cannot log into or manage the backup FortiController until you configure the cluster External Management IP and add workers to the cluster. Once you do this you can use the External Management IP address and a special port number to manage the backup FortiController. This is described below. (You can also connect to the backup FortiController CLI using the console port.)

You can confirm that the cluster has been formed by viewing the FortiController HA configuration. The display should show both FortiControllers in the cluster.

Note in some of the screen images in this example the host names shown on the screen images may not match the host names used in the example configuration.



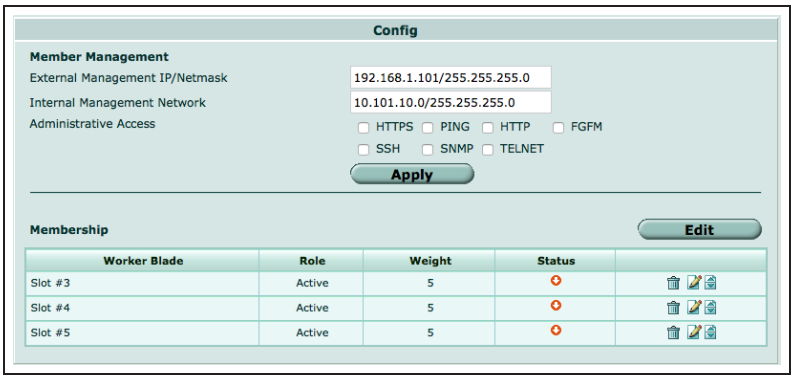
You can also go to **Load Balance > Status** to see the status of the primary FortiController (slot icon colored green).



Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured their status will be **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure all of the devices in the cluster.



You can also enter this command to add slots 3, 4, and 5 to the cluster.

```
config load-balance setting
 config slots
 edit 3
 next
 edit 4
 next
 edit 5
 end
 end
```

You can also enter this command to set the External Management IP and

```
config load-balance setting
 set base-mgmt-external-ip 172.20.120.100 255.255.255.0
```

configure management access.

```
 set base-mgmt-allowaccess https ssh ping
 end
```

Enable base management traffic between FortiControllers.

```
config load-balance setting
 config base-mgmt-interfaces
  edit b1
  next
  edit b2
 end
 end
```

Enable base control traffic between FortiControllers.

```
config load-balance setting
 config base-ctrl-interfaces
   edit b1
   next
   edit b2
 end
 end
```

5. Adding the workers to the cluster

Reset each worker to factory default settings.

```
execute factoryreset
```

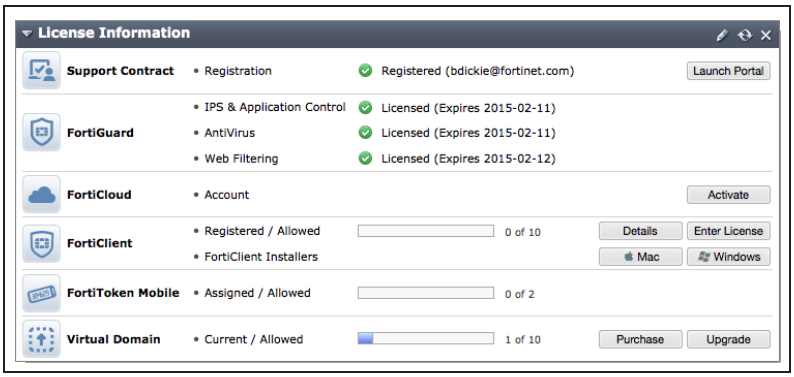
Give the mgmt1 or mgmt2 interface of each worker an IP address and connect these interfaces to your network. This step is optional but useful because when the workers are added to the cluster, these IP addresses are not synchronized, so you can connect to and manage each worker separately.

```
config system interface
 edit mgmt1
 set ip 172.20.120.120
 end
```

Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

```
config system global
   set hostname worker-chassis-1-slot-3
end
```

Register and apply licenses to each worker before adding the workers to the cluster. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**.



Log into the CLI of each worker and enter this command to set the worker to operate in FortiController mode. The worker restarts and joins the cluster.

```
config system elbc
set mode forticontroller
end
```

6. Managing the cluster

After the workers have been added to the cluster you can use the External Management IP to manage the the primary worker. This includes access to the primary worker GUI or CLI, SNMP queries to the primary worker, and using FortiManager to manage the primary worker. As well SNMP traps and log messages are sent from the primary worker with the External Management IP as their source address. And finally connections to FortiGuard for updates, web filtering lookups and so on, all originate from the External Management IP.

You can use the external management IP followed by a special port number to manage individual devices in the cluster. The special port number identifies the protocol (80 for HTTP, 443 for HTTPS, 22 for SSH, 23 for Telnet, 161 for SNMP) and the chassis and slot number of the device you want to connect to. In fact this is the only way to manage the backup FortiController. Some examples:

- To use HTTP to connect to the GUI of the FortiController in chassis 1 slot 1, browse to: **https://172.20.120.100:44311**
- To use HTTP to connect to the GUI of the FortiController in chassis 2 slot 1, (the backup FortiController) browse to: **https://172.20.120.100:44321**
- To use Telnet to connect to the CLI of the worker in chassis 1 slot 4: **telnet 172.20.120.100 2314**
- To use SSH to connect to the CLI the worker in chassis 2 slot 5: **ssh admin@172.20.120.100 -p2225**
- To use SNMP to query the FortiController in chassis 2 slot 1 (the backup FortiController) use port **16121** in the SNMP query.

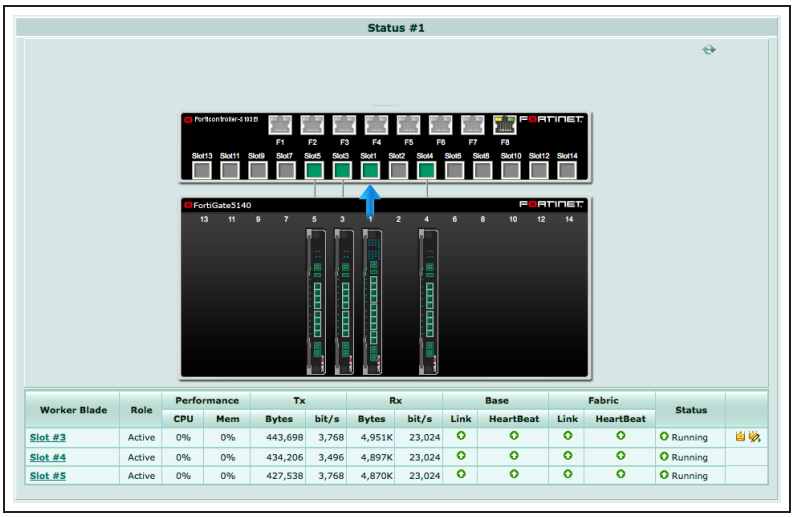
You can also manage the primary FortiController using the IP address of its mgmt interface, set up when you first configured the primary FortiController. You can also manage the workers by connecting directly to their mgmt1 or mgmt2 interfaces if you set them up. However, the only way to manage the backup FortiController is by using its special port number.

To manage a FortiController using SNMP you need to load the FORTINET-CORE-MIB.mib file into your SNMP

manager. You can get this MIB file from the Fortinet support site, in the same location as the current FortiController firmware (select the FortiSwitchATCA product).

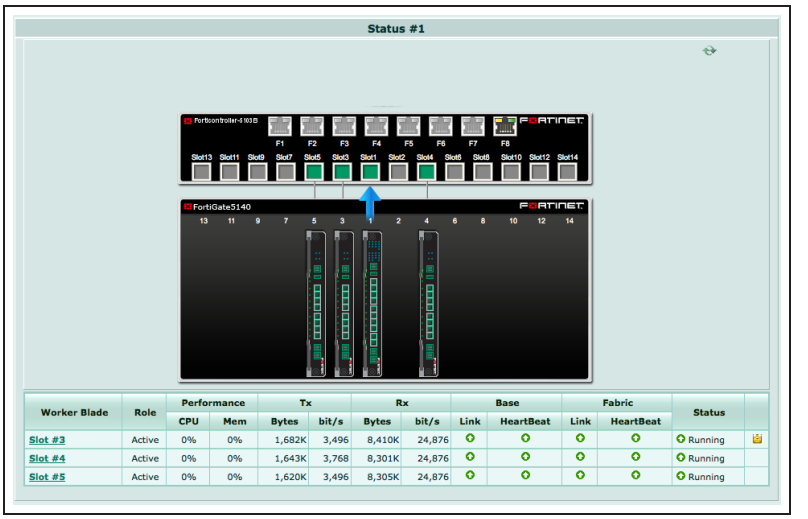
On the primary FortiController GUI go to **Load Balance > Status**. As the workers in chassis 1 restart they should appear in their appropriate slots.

The primary FortiController should be the FortiController in chassis 1 slot 1. The primary FortiController status display includes a **Config Master** link that you can use to connect to the primary worker.



Log into the backup FortiController GUI (for example by browsing to https://172.20.120.100:44321) and go to **Load Balance > Status**. As the workers in chassis 2 restart they should appear in their appropriate slots.

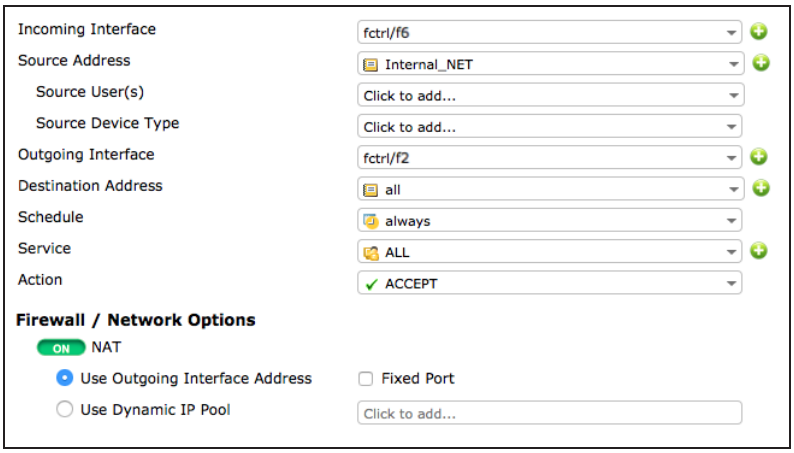
The backup FortiController Status page shows the status of the workers in chassis 2 and does not include the **Config Master** link.



7. Results - Configuring the workers

Configure the workers to process the traffic they receive from the FortiController front panel interfaces. By default all FortiController front panel interfaces are in the worker root VDOM. You can keep them in the root VDOM or create additional VDOMs and move interfaces into them.

For example, if you connect the Internet to FortiController front panel 2 interfaces (fctrl/f2 on the worker GUI and CLI) and the internal network to FortiController front panel 6 interfaces (fctrl/f6) you would access the root VDOM and add this policy to allow users on the Internal network to access the Internet.



8. Results - Checking the cluster status

You can use the following get and diagnose commands to show the status of the cluster and all of the devices in it.

Log into the **primary FortiController** CLI and enter this command to view the system status of the primary FortiController.

For example, you can use SSH to log into the primary FortiController CLI using the external management IP:

```
ssh admin@172.20.120.100 -p2211

get system status
Version: FortiController-5103B
v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000029
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: ch1-slot1
Current HA mode: a-p, master
System time: Sat Sep 13 06:51:53 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)
```

Enter this command to view the load balance status of the primary FortiController and its workers. The command output shows the workers in slots 3, 4, and 5, and status information about each one.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
   Working:  3 [  3 Active  0 Standby]
   Ready:    0 [  0 Active  0 Standby]
   Dead:     0 [  0 Active  0 Standby]
```

```
Total:     3 [  3 Active  0 Standby]

Slot 3: Status:Working  Function:Active
  Link:      Base: Up         Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
Slot 4: Status:Working  Function:Active
  Link:      Base: Up          Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
Slot 5: Status:Working  Function:Active
  Link:      Base: Up         Fabric: Up
  Heartbeat: Management: Good Data: Good
  Status Message:"Running"
```

Enter this command from the primary FortiController to show the HA status of the primary and backup FortiControllers. The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (this case 0 for each FortiController) the number of failed workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (status=alive) and the B2 interfaces are not (status=dead). The cluster can still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch1-slot1(FT513B3912000029), Master(priority=0),  ip=169.254.128.41,
uptime=62581.81, chassis=1(1)
   slot: 1
   sync: conf_sync=1, elbc_sync=1
   session: total=0, session_sync=in sync
   state: worker_failure=0/3, intf_state=(port up:)=2
force-state(0:none) hbdevs: local_interface=         b1 best=yes
            local_interface=     b2 best=no

ch2-slot1(FT513B3912000051), Slave(priority=1),  ip=169.254.128.42,
uptime=1644.71, chassis=2(1)
   slot: 1
   sync: conf_sync=0, elbc_sync=1, conn=3(connected)
   session: total=0, session_sync=in sync
   state: worker_failure=0/3, intf_state=(port up:)=2
force-state(0:none) hbdevs: local_interface=    b1 last_hb_time=66430.35
status=alive
```

```
local_interface= b2 last_hb_time= 0.00   status=dead
```

Log into the **backup FortiController** CLI and enter this command to view the status of the backup FortiController.

To use SSH:

```
ssh admin@172.20.120.100 -p2221
```

```
get system status
 Version: FortiController-5103B
v5.0,build0020,131118 (Patch 3)
 Branch Point: 0020
 Serial-Number: FT513B3912000051
 BIOS version: 04000009
 System Part-Number: P08442-04
 Hostname: ch2-slot1
 Current HA mode: a-p, backup
 System time: Sat Sep 13 07:29:04 2014
 Daylight Time Saving: Yes
 Time Zone: (GMT-8:00)Pacific Time(US&Canada)
```

Enter this command to view the status of the backup FortiController and its workers.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: N/A
Blades:
   Working:  3 [  3 Active  0 Standby]
   Ready:    0 [  0 Active  0 Standby]
   Dead:     0 [  0 Active  0 Standby]
  Total:     3 [  3 Active  0 Standby]

    Slot  3: Status:Working   Function:Active
      Link:      Base: Up          Fabric: Up
      Heartbeat: Management: Good   Data: Good
      Status Message:"Running"
    Slot  4: Status:Working   Function:Active
      Link:      Base: Up          Fabric: Up
      Heartbeat: Management: Good   Data: Good
      Status Message:"Running"
    Slot  5: Status:Working   Function:Active
      Link:      Base: Up          Fabric: Up
      Heartbeat: Management: Good   Data: Good
      Status Message:"Running"
```

Enter this command from the backup FortiController to show the HA status of the backup and primary FortiControllers. Notice that the backup FortiController is shown first. The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (this case 0 for each FortiController) the number of failed

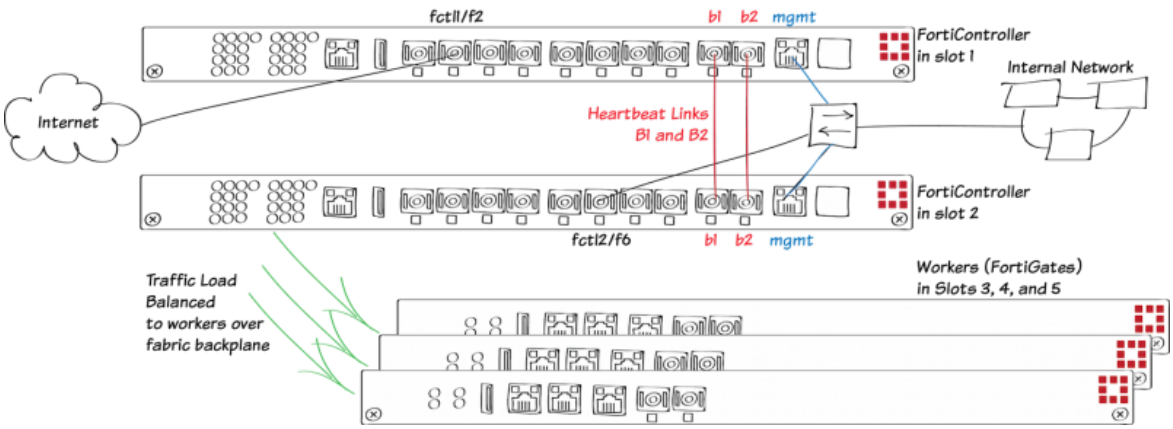
workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (status=alive) and the B2 interfaces are not (status=dead). The cluster can still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch2-slot1(FT513B3912000051), Slave(priority=1), ip=169.254.128.42,
uptime=3795.92, chassis=2(1)
    slot: 1
    sync: conf_sync=0, elbc_sync=1
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 best=yes
    local_interface=        b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.41,
uptime=64732.98, chassis=1(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)  hbdevs: local_interface=      b1 last_hb_time=68534.90
status=alive
    local_interface=        b2 last_hb_time=    0.00   status=dead
```

For further reading, check out the FortiController Session-aware Load Balancing Guide.

SLBC Dual Mode setup with two FortiControllers



This example describes the basics of setting up a dual mode Session-aware Load Balancing Cluster (SLBC) that consists of two FortiController-5103Bs, installed in chassis slots 1 and 2, and three FortiGate-5001C workers, installed in chassis slots 3, 4, and 5. This SLBC configuration can have up to 16 10Gbit network connections.

The two FortiControllers in the same chassis to operate in dual mode to double the number of network interfaces available. In dual mode, two FortiControllers load balance traffic to multiple workers. Traffic can be received by both FortiControllers and load balanced to all of the workers in the chassis. In dual mode configuration the front panel interfaces of both FortiControllers are active.

In a dual FortiController-5103B cluster this means up to 16 10Gbyte network interfaces are available. The interfaces of the FortiController in slot 1 are named fctrl/f1 to fctrl/f8 and the interfaces of the FortiController in slot 2 are named fctr2/f1 to fctrl2/f8.

All networks have single connections to the first or second FortiController. One or more heartbeat links are created between the FortiControllers. Redundant heartbeat links are recommended. The heartbeat links use the front panel B1 and B2 interfaces.

If one of the FortiControllers fails, the remaining FortiController keeps processing traffic received by its front panel interfaces. Traffic to and from the failed FortiController is lost.

For more information about SLBC go here.

1. Hardware setup

Install a FortiGate-5000 series chassis and connect it to power. Install the FortiControllers in slots 1 and 2. Install the workers in slots 3, 4, and 5. Power on the chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally (to check normal operation LED status, see the FortiGate-5000 series documents available here).

Create connections from the FortiController front panel interfaces to the Internet and to the internal network.

Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a backup heartbeat link by connecting the FortiController B2 interfaces together. You can directly connect the interfaces with a patch cable or connect them together through a switch. If you use a switch, it must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301 and 101). These connections establish heartbeat, base control, and base management communication between the FortiControllers. Only one heartbeat connection is required but redundant connections are recommended.

Connect the mgmt interfaces of the both FortiControllers to the internal network or any network from which you want to manage the cluster.

Check the FortiSwitch-ATCA release notes and install the latest supported firmware on the FortiController and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

2. Configuring the FortiControllers

Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in slot 1 with the default IP address (http://192.168.1.99) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None).

Add a password for the admin administrator account. You can either use the **Administrators** widget in the GUI or enter the following command in the CLI.

```
config admin user
  edit admin
      set password password
   end
```

Change the FortiController mgmt interface IP address. Use the **Management Port** widget in the GUI or enter the following command in the CLI.

```
config system interface
  edit mgmt
      set ip 172.20.120.151/24
   end
```

If you need to add a default route for the management IP address, enter this command.

```
config route static
   edit 1
       set gateway 172.20.120.2
   end
```

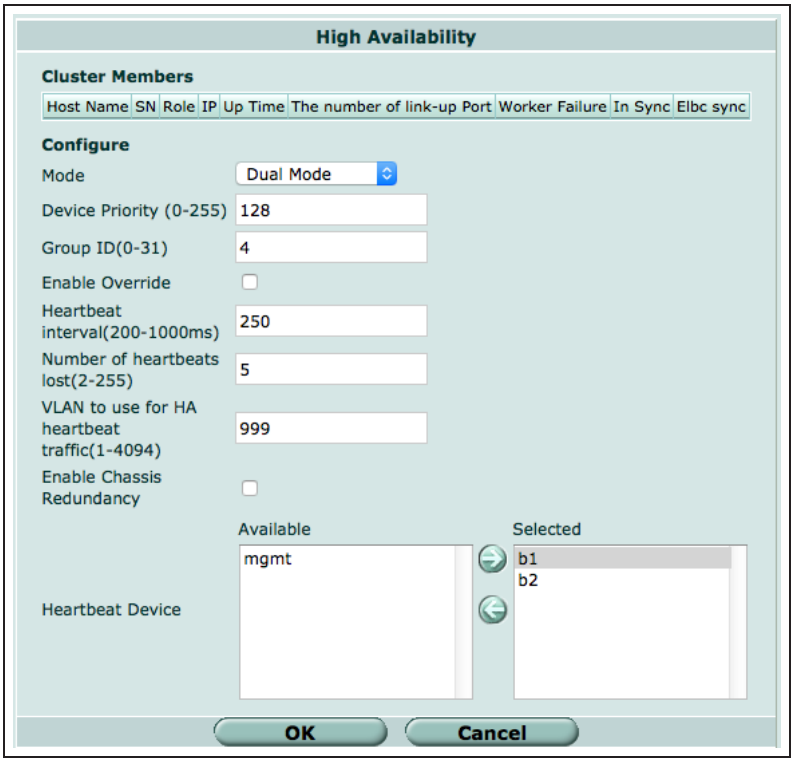
Set the chassis type that you are using.

```
config system global
   set chassis-type fortigate-5140
end
```

Configure dual Mode HA on the FortiController in slot 1.

From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

Set **Mode** to **Dual Mode**, change the **Group ID**, and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.



You can also enter this CLI command:

```
config system ha
   set mode dual
   set groupid 4
   set hbdev b1 b2
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 setting causes a MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

You can also adjust other HA settings. For example, you could increase the **Device Priority** of the FortiController that you want to become the primary unit, enable **Override** to make sure the FortiController with the highest device priority becomes the primary unit, and change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on your network.

You would only select **Enable chassis redundancy** if your cluster has more than one chassis.

Log into the web-based manager of the FortiController in slot 2 and duplicate the HA configuration of the FortiController in slot 1, except for the Device Priority and override setting, which can be different on each FortiController.

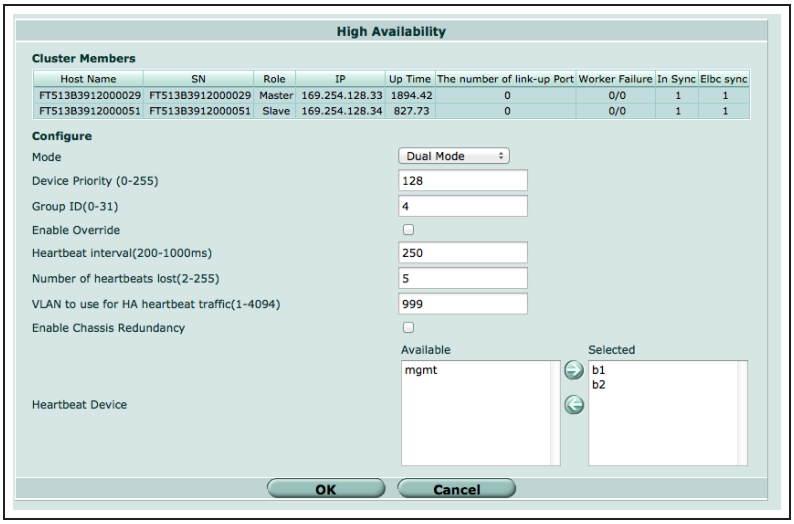
After a short time, the FortiControllers restart in HA mode and form a dual mode cluster. Both FortiControllers must have the same HA configuration and at least one heartbeat link must be connected.

Normally the FortiController in slot 1 is the primary unit, and you can log into the cluster using the management IP address you assigned to this FortiController.

If the FortiControllers are unable to form a cluster, check to make sure that they both have the same HA configuration. Also they can't form a cluster if the heartbeat interfaces (B1 and B2) are not connected.

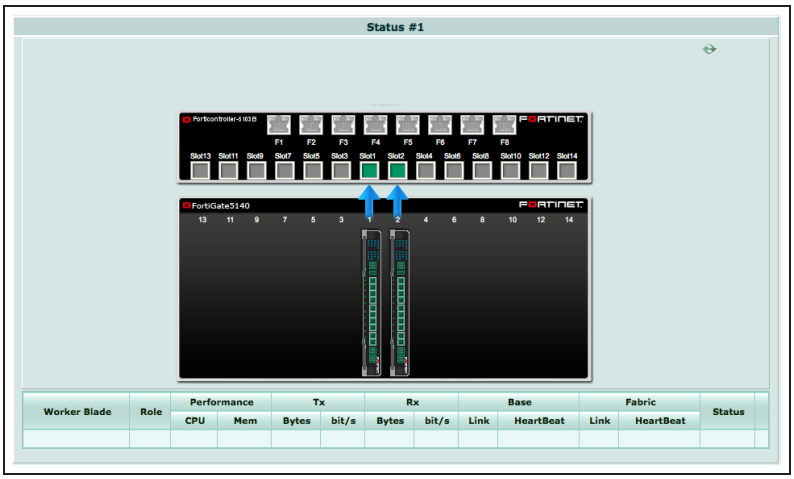
You can confirm that the cluster has been formed by viewing the HA configuration from the the FortiController web-based manager. The display should show both FortiControllers in the cluster.

Since the configuration of the FortiControllers is synchronized, you can complete the configuration of the cluster from the primary FortiController.



You can also go to **Load Balance > Status** to see the status of the cluster. This page should show both FortiControllers in the cluster.

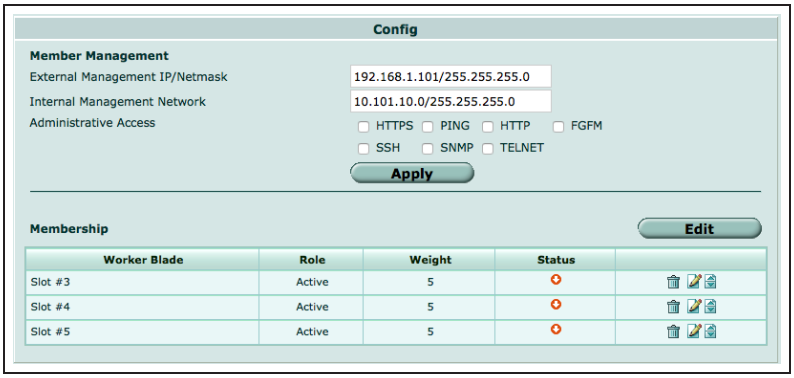
Since both FortiControllers are active their slot icons are both colored green.



Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured yet their status will be **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure them.



You can also enter this command to add slots 3, 4, and 5 to the cluster.

```
config load-balance setting
  config slots
     edit 3
     next
     edit 4
     next
     edit 5
     end
  end
```

You can also enter this command to configure the external management IP/Netmask and management access to

```
config load-balance setting
  set base-mgmt-external-ip 172.20.120.100 255.255.255.0
   set base-mgmt-allowaccess https ssh ping
```

this address.

```
end
```

Enable base management traffic between FortiControllers.

```
config load-balance setting
 config base-mgmt-interfaces
    edit b1
    next
    edit b2
    end
 end
```

Enable base control traffic between FortiControllers.

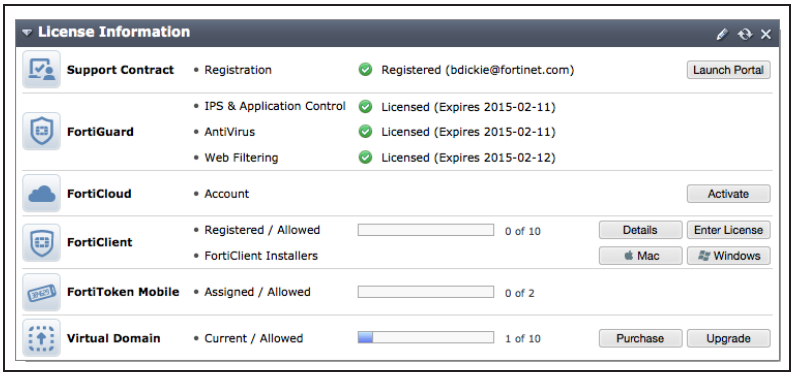
```
config load-balance setting
 config base-ctrl-interfaces
    edit b1
    next
    edit b2
    end
 end
```

3. Adding the workers to the cluster

Reset the workers to factory default settings.

```
execute factoryreset
```

Register and apply licenses to each worker before adding the workers to the SLBC. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**.



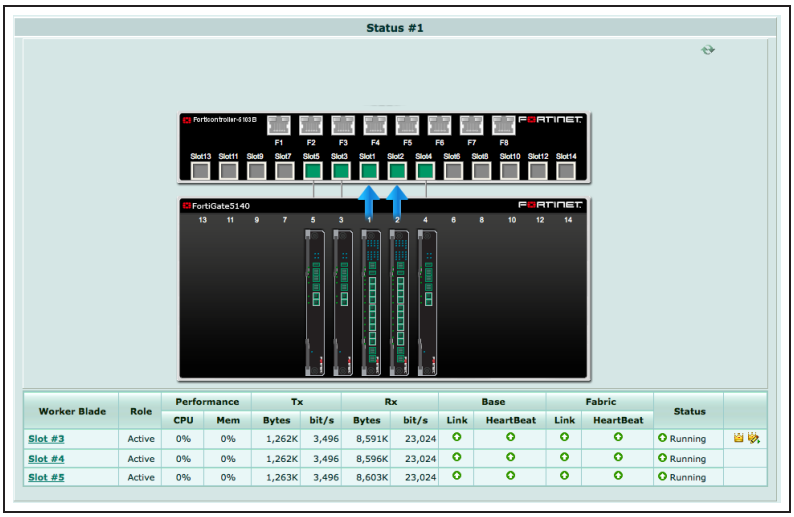
Optionally give the mgmt1 and or mgmt2 interfaces of each worker IP addresses and connect them to your network. When a cluster is created, the mgmt1 and mgmt2 IP addresses are not synchronized, so you can connect to and manage each worker separately.

Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

Log into the CLI of each worker and enter this command to set the worker to operate in FortiController mode.

```
config system elbc
  set mode dual-forticontroller
end
```

The worker restarts and joins the cluster. On the FortiController GUI go to **Load Balance > Status**. As the workers restart they should appear in their appropriate slots.

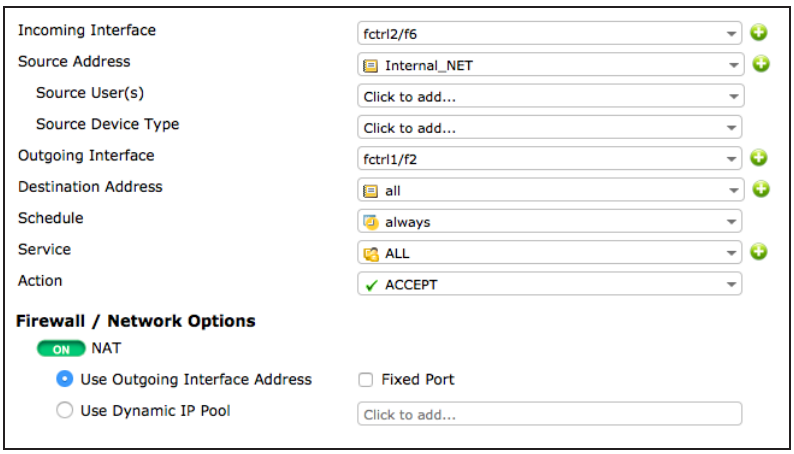


4. Results

You can now connect to the worker GUI or CLI using the **External Management IP** and manage the workers in the same way as you would manage a standalone FortiGate. If you configured the worker mgmt1 or mgmt2 interfaces you can also connect to these interfaces to configure the workers. Configuration changes made to any worker are synchronized to all workers.

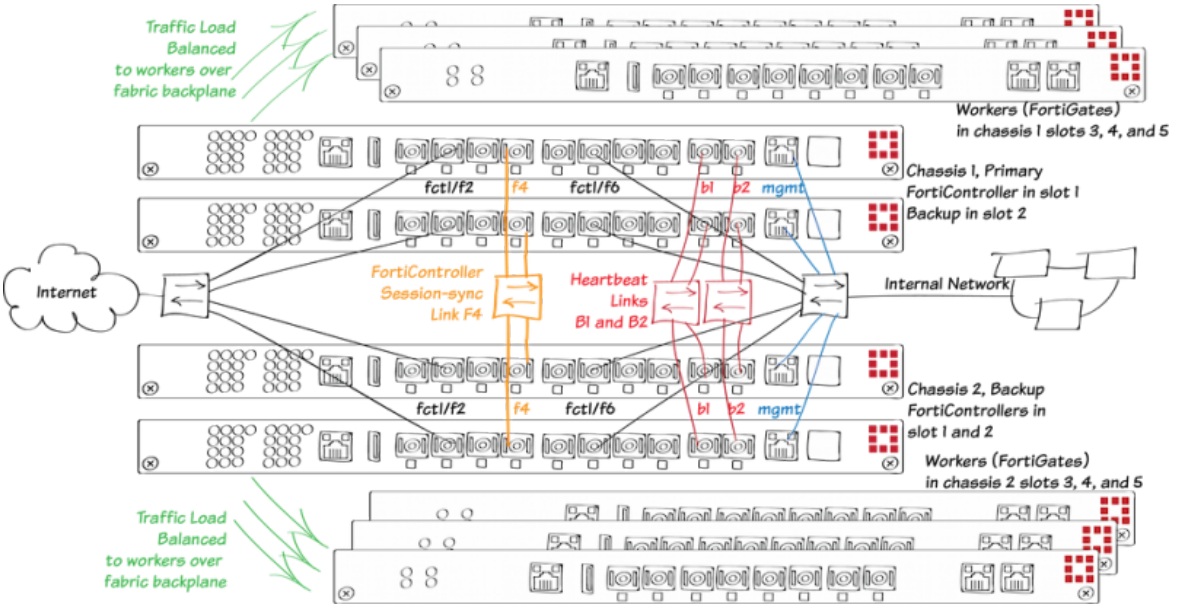
Configure the workers to process the traffic they receive from the FortiController front panel interfaces. By default all FortiController front panel interfaces are in the root VDOM. You can keep them in the root VDOM or create additional VDOMs and move interfaces into them.

For example, if you connect the Internet to FortiController front panel interface 2 of the FortiController in slot 1 (fctrl1/f2 on the worker GUI and CLI) and the internal network to FortiController front panel interface 6 of the FortiController in slot 2 (fctrl2/f6 on the worker GUI and CLI) you would access the root VDOM and add this policy to allow users on the Internal network to access the Internet.



For further reading, check out the FortiController Session-aware Load Balancing Guide.

SLBC Active-Passive with four FortiControllers and two chassis



This example describes how to setup an active-passive session-aware load balancing cluster (SLBC) consisting of two FortiGate-5000 chassis, four FortiController-5103Bs two in each chassis, and six FortiGate-5001Bs acting as workers, three in each chassis. This SLBC configuration can have up to seven redundant 10Gbit network connections.

The FortiControllers operate in active-passive HA mode for redundancy. The FortiController in chassis 1 slot 1 will be configured to be the primary unit, actively processing sessions. The other FortiControllers become the subordinate units.

In active-passive HA with two chassis and four FortiControllers, both chassis have two FortiControllers in active-passive HA mode and the same number of workers. Network connections are duplicated to the redundant FortiControllers in each chassis and between chassis for a total of four redundant data connections to each network.

All traffic is processed by the primary unit. If the primary unit fails, all traffic fails over to the chassis with two functioning FortiControllers and one of these FortiControllers becomes the new primary unit and processes all traffic. If the primary unit in the second chassis fails as well, one of the remaining FortiControllers becomes the primary unit and processes all traffic.

Heartbeat and base control and management communication is established between the chassis using the FortiController B1 and B2 interfaces. Only one heartbeat connection is required but redundant connections are recommended. Connect all of the B1 and all of the B2 interfaces together using switches. This example shows using one switch for the B1 connections and another for the B2 connections. You could also use one switch for both the B1 and B2 connections but using separate switches provides more redundancy.

The following VLAN tags and subnets are used by traffic on the B1 and B2 interfaces:

- Heartbeat traffic uses VLAN 999.
- Base control traffic on the 10.101.11.0/255.255.255.0 subnet uses VLAN 301.
- Base management on the 10.101.10.0/255.255.255.0 subnet uses VLAN 101

This example also includes a FortiController session sync connection between the FortiControllers using the FortiController F4 front panel interface (resulting in the SLBC having a total of seven redundant 10Gbit network connections). (You can use any fabric front panel interface, F4 is used in this example to make the diagram clearer.) FortiController-5103B session sync traffic uses VLAN 2000.

This example sets the device priority of the FortiController in chassis 1 slot 1 higher than the device priority of the other FortiControllers to make sure that the FortiController in chassis 1 slot 1 becomes the primary FortiController for the cluster. Override is also enabled on the FortiController in chassis 1 slot 1. Override may cause the cluster to negotiate more often to select the primary unit. This makes it more likely that the unit that you select to be the primary unit will actually be the primary unit; but enabling override can also cause the cluster to negotiate more often.

For more information about SLBC go here.

1. Hardware setup

Install two FortiGate-5000 series chassis and connect them to power. Ideally each chassis should be connected to a separate power circuit. Install FortiControllers in slot 1 and 2 of each chassis. Install the workers in slots 3, 4, and 5 of each chassis. The workers must be installed in the same slots in both chassis. Power on both chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally (to check normal operation LED status, see the FortiGate-5000 series documents available here).

Create redundant connections from all four FortiController front panel interfaces to the Internet and to the internal network.

Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a backup heartbeat link by connecting the FortiController B2 interfaces together.

Create a FortiController session sync connection between the chassis by connecting the FortiController F4 interfaces together.

Connect the mgmt interfaces of all of the FortiControllers to the internal network or any network from which you want to manage the cluster.

Check the FortiSwitch-ATCA release notes and install the latest supported firmware on the FortiControllers and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

2. Configuring the FortiController in Chassis 1 Slot 1

This will become the primary FortiController. To make sure this is the primary FortiController it will be assigned the highest device priority and override will be enabled. Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in chassis 1 slot 1 with the default IP address (http://192.168.1.99) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None).

From the Dashboard System Information widget, set the **Host Name** to ch1-slot1. Or enter this command.

```
config system global
  set hostname ch1-slot1
end
```

Add a password for the admin administrator account. You can either use the **Administrators** widget on the GUI or enter this command.

```
config admin user
  edit admin
  set password
end
```

Change the FortiController mgmt

```
config system interface
```

interface IP address. Use the GUI **Management Port** widget or enter this command.

```
 edit mgmt
 set ip 172.20.120.151/24
end
```

If you need to add a default route for the management IP address, enter this command.

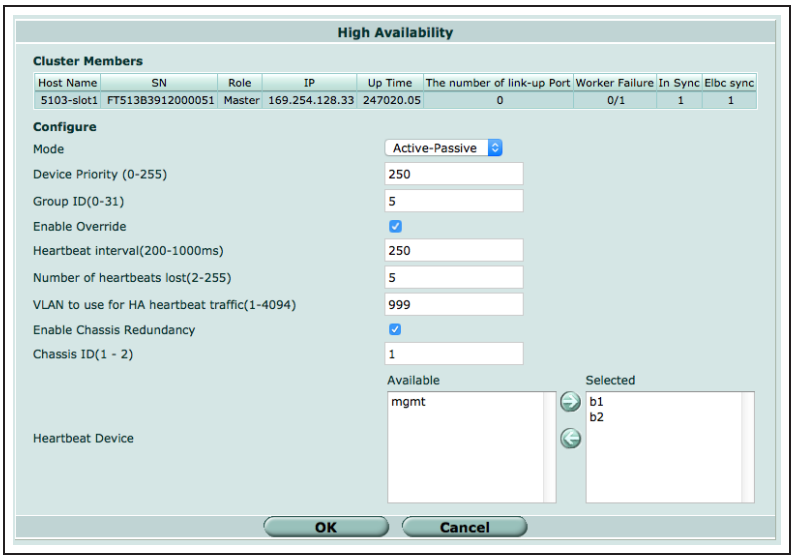
```
config route static
  edit 1
  set gateway 172.20.120.2
 end
```

Set the chassis type that you are using.

```
 config system global
  set chassis-type fortigate-5140
 end
```

Configure Active-Passive HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

Set **Mode** to **Active-Passive**, set the **Device Priority** to 250, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 1 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.



Enter this command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
  set session-sync-port f4
 end
```

You can also enter the complete HA configuration with this command.

```
 config system ha
  set mode active-passive
  set groupid 15
  set priority 250
```

```
  set override enable
  set chassis-redundancy enable
  set chassis-id 1
  set hbdev b1 b2
  set session-sync-port f4
 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 setting causes a MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

You can also adjust other HA settings. For example, you could change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on your network. You can also adjust the **Heartbeat Interval** and **Number of Heartbeats** lost to adjust how quickly the cluster determines one of the FortiControllers has failed.

3. Configuring the FortiController in Chassis 1 Slot 2

Log into the FortiController in chassis 1 slot 2.

Enter these commands to set the host name to ch1-slot2, to configure the mgmt interface, and to duplicate the HA configuration of the FortiController in slot 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10).

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

```
config system global
  set hostname ch1-slot2
end

config system interface
  edit mgmt
  set ip 172.20.120.152/24
 end

config system ha
  set mode active-passive
  set groupid 15
  set priority 10
  set chassis-redundancy enable
  set chassis-id 1
  set hbdev b1 b2
  set session-sync-port f4
 end
```

4. Configuring the FortiController in Chassis 2 Slot 1

Log into the FortiController in chassis 2 slot 1.

Enter these commands to set the host

```
config system global
  set hostname ch2-slot1
end
```

name to ch2-slot1, to configure the mgmt interface, and to duplicate the HA configuration of the FortiController in chassis 1 slot 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10), and set the **Chassis ID** to 2.

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

```
config system interface
  edit mgmt
  set ip 172.20.120.251/24
 end

config system ha
  set mode active-passive
  set groupid 15
  set priority 10
  set chassis-redundancy enable
  set chassis-id 2
  set hbdev b1 b2
  set session-sync-port f4
 end
```

5. Configuring the FortiController in Chassis 2 Slot 2

Log into the FortiController in chassis 2 slot 2.

Enter these commands to set the host name to ch2-slot2, to configure the mgmt interface, and to duplicate the HA configuration of the FortiController in chassis 1 slot 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10), and set the **Chassis ID** to 2.

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

```
config system global
  set hostname ch2-slot2
end

config system interface
  edit mgmt
  set ip 172.20.120.252/24
 end

config system ha
  set mode active-passive
  set groupid 15
  set priority 10
  set chassis-redundancy enable
  set chassis-id 2
  set hbdev b1 b2
  set session-sync-port f4
 end
```

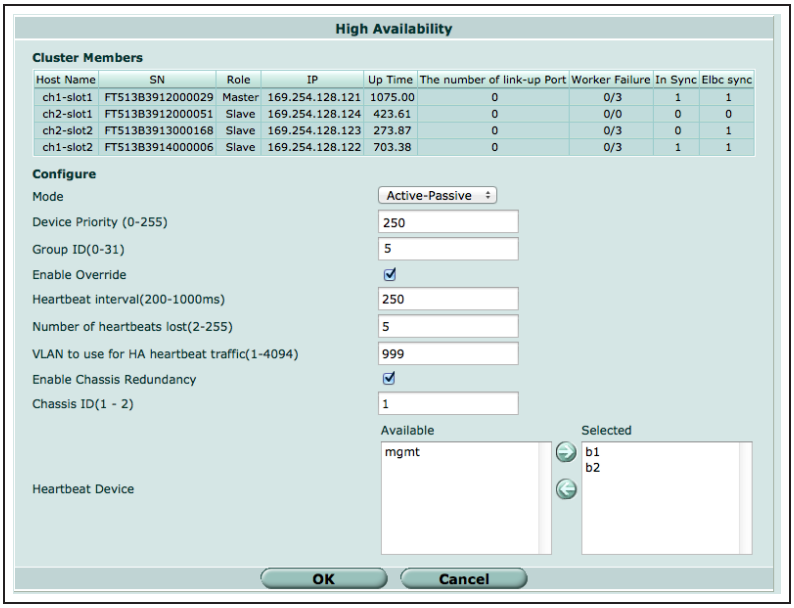
6. Configuring the cluster

After a short time the FortiControllers restart in HA mode and form an active-passive SLBC. All of the FortiControllers must have the same HA configuration and at least one heartbeat link (the B1 and B2 interfaces) must be connected. If the FortiControllers are unable to form a cluster, check to make sure that they all have the same HA configuration. Also they can't form a cluster if the heartbeat interfaces (B1 and B2) are not connected.

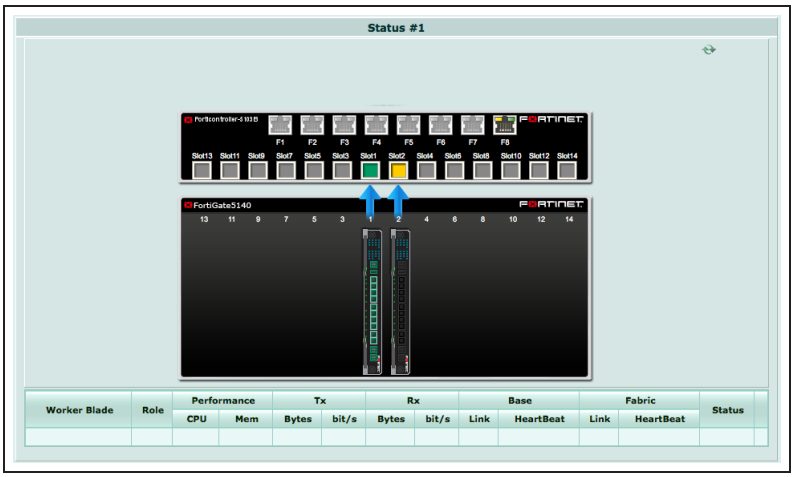
With the configuration described in the previous steps, the FortiController in chassis 1 slot 1 should become the primary unit and you can log into the cluster using the management IP address that you assigned to this FortiController.

The other FortiControllers become backup FortiControllers. You cannot log into or manage the backup FortiControllers until you configure the cluster External Management IP and add workers to the cluster. Once you do this you can use the External Management IP address and a special port number to manage the backup FortiControllers. This is described below. (You can also connect to any backup FortiController CLI using their console port.)

You can confirm that the cluster has been formed by viewing the FortiController HA configuration. The display should show both FortiControllers in the cluster.



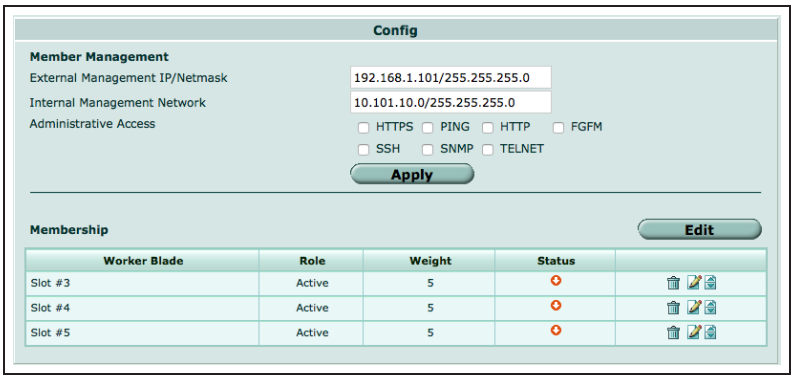
You can also go to **Load Balance > Status** to see the status of the primary FortiController (slot icon colored green).



Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured for SLBC operation their status will be **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure all of the devices in the cluster.



You can also enter this command to add slots 3, 4, and 5 to the cluster.

```
config load-balance setting
 config slots
   edit 3
   next
   edit 4
   next
   edit 5
   end
 end
```

You can also enter this command to set the External Management IP and configure management access.

```
config load-balance setting
 set base-mgmt-external-ip 172.20.120.100 255.255.255.0
 set base-mgmt-allowaccess https ssh ping
end
```

Enable base management traffic between FortiControllers.

```
config load-balance setting
 config base-mgmt-interfaces
   edit b1
   next
   edit b2
   end
 end
```

Enable base control traffic between FortiControllers.

```
config load-balance setting
 config base-ctrl-interfaces
   edit b1
   next
   edit b2
```

```
    end
  end
```

7. Adding the workers to the cluster

Reset each worker to factory default settings.

```
execute factoryreset
```

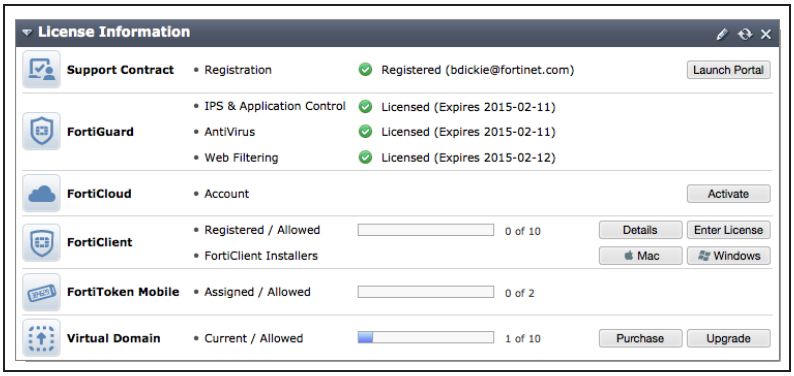
Give the mgmt1 or mgmt2 interface of each worker an IP address and connect these interfaces to your network. This step is optional but useful because when the workers are added to the cluster, these IP addresses are not synchronized, so you can connect to and manage each worker separately.

```
config system interface
  edit mgmt1
    set ip 172.20.120.120
  end
```

Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

```
config system global
  set hostname worker-chassis-1-slot-3
end
```

Register each worker and apply licenses to each worker before adding the workers to the cluster. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**.



Log into the CLI of each worker and enter this command to set the worker to operate in FortiController mode. The worker restarts and joins the cluster.

```
config system elbc
 set mode forticontroller
end
```

8. Managing the cluster

After the workers have been added to the cluster you can use the External Management IP to manage the the primary worker. This includes access to the primary worker GUI or CLI, SNMP queries to the primary worker, and using FortiManager to manage the primary worker. As well SNMP traps and log messages are sent from the primary worker with the External Management IP as their source address. And finally connections to FortiGuard for updates, web filtering lookups and so on, all originate from the External Management IP.

You can use the external management IP followed by a special port number to manage individual devices in the cluster. The special port number identifies the protocol (80 for HTTP, 443 for HTTPS, 22 for SSH, 23 for Telnet, 161 for SNMP) and the chassis and slot number of the device you want to connect to. In fact this is the only way to manage the backup FortiControllers. Some examples:

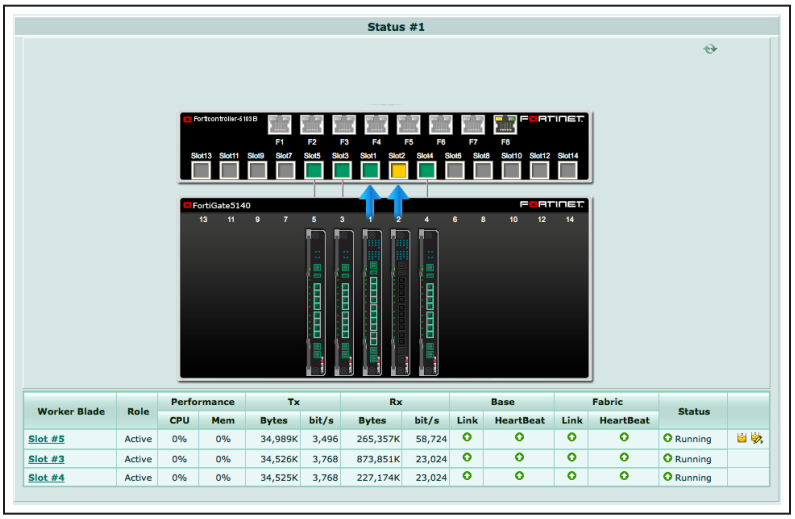
- To use HTTP to connect to the GUI of the FortiController in chassis 1 slot 2, browse to: **https://172.20.120.100:44312**
- To use HTTP to connect to the GUI of the FortiController in chassis 2 slot 1, browse to: **https://172.20.120.100:44321**
- To use Telnet to connect to the CLI of the worker in chassis 2 slot 4: **telnet 172.20.120.100 2324**
- To use SSH to connect to the CLI the worker in chassis 1 slot 5: **ssh admin@172.20.120.100 -p2215**
- To use SNMP to query the FortiController in chassis 1 slot 2 use port **16112** in the SNMP query.

You can also manage the primary FortiController using the IP address of its mgmt interface, set up when you first configured the primary FortiController. You can also manage the workers by connecting directly to their mgmt1 or mgmt2 interfaces if you set them up. However, the only way to manage the backup FortiControllers is by using its special port number (or a serial connection to the Console port).

To manage a FortiController using SNMP you need to load the FORTINET-CORE-MIB.mib file into your SNMP manager. You can get this MIB file from the Fortinet support site, in the same location as the current FortiController firmware (select the FortiSwitchATCA product).

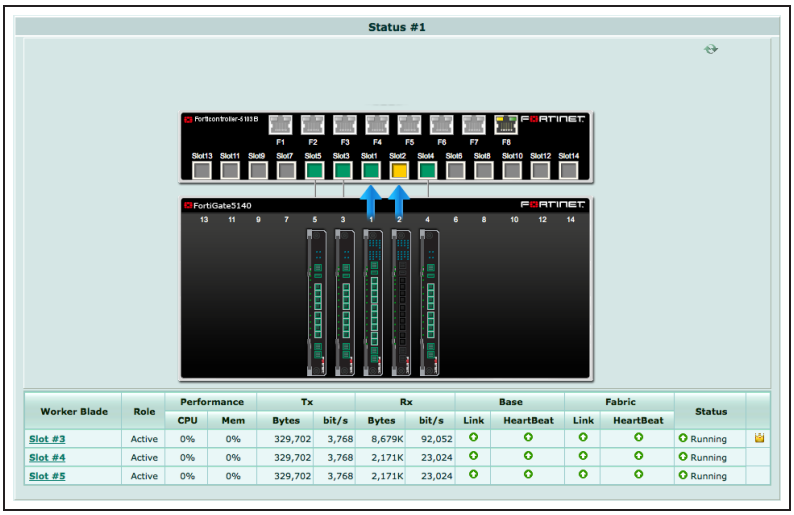
On the primary FortiController GUI go to **Load Balance > Status**. As the workers in chassis 1 restart they should appear in their appropriate slots.

The primary FortiController should be the FortiController in chassis 1 slot 1. The primary FortiController status display includes a **Config Master** link that you can use to connect to the primary worker.



Log into a backup FortiController GUI (for example by browsing to https://172.20.120.100:44321 to log into the FortiController in chassis 2 slot 1) and go to **Load Balance > Status**. If the workers in chassis 2 are configured correctly they should appear in their appropriate slots.

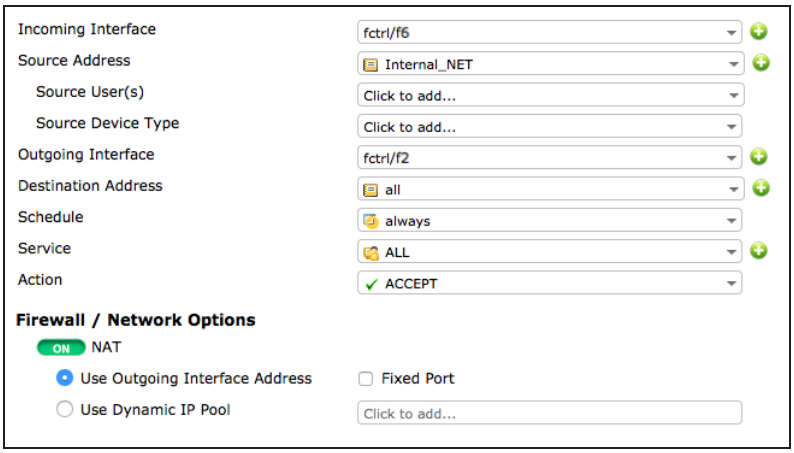
The backup FortiController Status page shows the status of the workers in chassis 2 and does not include the **Config Master** link.



9. Results - Configuring the workers

Configure the workers to process the traffic they receive from the FortiController front panel interfaces. By default all FortiController front panel interfaces are in the worker root VDOM. You can keep them in the root VDOM or create additional VDOMs and move interfaces into them.

For example, if you connect the Internet to FortiController front panel interface 2 (fctrl/f2 on the worker GUI and CLI) and the internal network to FortiController front panel interface 6 (fctrl/f6) you can access the root VDOM and add a policy to allow users on the Internal network to access the Internet.



10. Results - Primary FortiController cluster status

Log into the **primary FortiController** CLI and enter this command to view the system status of the primary FortiController.

For example, you can use SSH to log into the primary FortiController CLI using the external management IP:

```
ssh admin@172.20.120.100 -p2211

get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000029
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: ch1-slot1
Current HA mode: a-p, master
System time: Sun Sep 14 08:16:25 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)
```

Enter this command to view the load balance status of the primary FortiController and its workers. The command output shows the workers in slots 3, 4, and 5, and status information about each one.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
   Working: 3 [ 3 Active 0 Standby]
   Ready:   0 [ 0 Active 0 Standby]
   Dead:    0 [ 0 Active 0 Standby]
  Total:   3 [ 3 Active 0 Standby]

 Slot 3: Status:Working   Function:Active
   Link:     Base: Up        Fabric: Up
   Heartbeat: Management: Good  Data: Good
   Status Message:"Running"
 Slot 4: Status:Working   Function:Active
   Link: Base: Up            Fabric: Up
   Heartbeat: Management: Good  Data: Good
   Status Message:"Running"
 Slot 5: Status:Working   Function:Active
   Link: Base: Up            Fabric: Up
   Heartbeat: Management: Good  Data: Good
   Status Message:"Running"
```

Enter this command from the primary FortiController to show the HA status of the FortiControllers. The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (this case 0 for each FortiController) the number of failed workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (status=alive) and the B2 interfaces are not (status=dead). The cluster can

still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=4416.18, chassis=1(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 best=yes
            local_interface=        b2 best=no

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123, uptime=1181.62, chassis=2(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 last_hb_time= 4739.97   status=alive
            local_interface=        b2 last_hb_time=    0.00   status=dead

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=335.79, chassis=2(1)
    slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 last_hb_time= 4739.93   status=alive
            local_interface=        b2 last_hb_time=    0.00   status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4044.46, chassis=1(1)
    slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 last_hb_time= 4740.03   status=alive
            local_interface=        b2 last_hb_time=    0.00   status=dead
```

11. Results – Chassis 1 Slot 2 FortiController status

Log into the **chassis 1 slot 2 FortiController** CLI and enter this command to view the status of this backup FortiController.

To use SSH:

```
ssh admin@172.20.120.100 -p2212
```

```
get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3914000006
BIOS version: 04000010
System Part-Number: P08442-04
Hostname: ch1-slot2
Current HA mode: a-p, backup
System time: Sun Sep 14 12:44:58 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)
```

Enter this command to view the status of this backup FortiController and its workers.

```
get load-balance status
  ELBC Master Blade: slot-3
  Confsync Master Blade: slot-3
  Blades:
     Working:  3 [  3 Active  0 Standby]
     Ready:    0 [  0 Active  0 Standby]
     Dead:     0 [  0 Active  0 Standby]
    Total:     3 [  3 Active  0 Standby]

     Slot  3: Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
     Slot  4: Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
     Slot  5: Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
```

Enter this command from the FortiController in chassis 1 slot 2 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 1 slot 2 is shown first.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4292.69, chassis=1(1)
    slot: 2
    sync: conf_sync=1, elbc_sync=1
    session: total=0,  session_sync=in sync
```

```
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 best=yes
            local_interface=        b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=4664.49, chassis=1(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 last_hb_time= 4958.88   status=alive
            local_interface=        b2 last_hb_time=    0.00   status=dead

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123, uptime=1429.99, chassis=2(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 last_hb_time= 4958.88   status=alive
            local_interface=        b2 last_hb_time=    0.00   status=dead

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=584.20, chassis=2(1)
    slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 last_hb_time= 4958.88   status=alive
            local_interface=        b2 last_hb_time=    0.00   status=dead
```

12. Results - Chassis 2 Slot 1 FortiController status

Log into the **chassis 2 slot 1 FortiController** CLI and enter this command to view the status of this backup FortiController.

To use SSH:

```
ssh admin@172.20.120.100 -p2221

get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000051
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: ch2-slot1
Current HA mode: a-p, backup
System time: Sun Sep 14 12:53:09 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)
```

Enter this command to view the status of this backup FortiController and its workers.

```
get load-balance status
  ELBC Master Blade: slot-3
  Confsync Master Blade: N/A
  Blades:
     Working:  3 [  3 Active  0 Standby]
     Ready:    0 [  0 Active  0 Standby]
     Dead:     0 [  0 Active  0 Standby]
    Total:     3 [  3 Active  0 Standby]

     Slot  3: Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
     Slot  4: Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
     Slot  5: Status:Working   Function:Active
       Link:      Base: Up          Fabric: Up
       Heartbeat: Management: Good   Data: Good
       Status Message:"Running"
```

Enter this command from the FortiController in chassis 2 slot 1 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 2 slot 1 is shown first.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123, uptime=1858.71, chassis=2(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 best=yes
            local_interface=        b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=5093.30, chassis=1(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 last_hb_time= 2074.15   status=alive
            local_interface=        b2 last_hb_time=    0.00   status=dead
```

```
ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=1013.01, chassis=2(1)
    slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 last_hb_time= 2074.15   status=alive
            local_interface=        b2 last_hb_time=    0.00   status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4721.60, chassis=1(1)
    slot: 2
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 last_hb_time= 2074.17   status=alive
            local_interface=        b2 last_hb_time=    0.00   status=dead
```

13. Results - Chassis 2 Slot 2 FortiController status

Log into the **chassis 2 slot 2 FortiController** CLI and enter this command to view the status of this backup FortiController.

To use SSH:

```
ssh admin@172.20.120.100 -p2222

get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3913000168
BIOS version: 04000010
System Part-Number: P08442-04
Hostname: ch2-slot2
Current HA mode: a-p, backup
System time: Sun Sep 14 12:56:45 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)
```

Enter this command to view the status of the backup FortiController and its workers.

```
get load-balance status
  ELBC Master Blade: slot-3
  Confsync Master Blade: N/A
  Blades:
     Working:  3 [  3 Active  0 Standby]
     Ready:    0 [  0 Active  0 Standby]
     Dead:     0 [  0 Active  0 Standby]
    Total:     3 [  3 Active  0 Standby]

     Slot  3: Status:Working   Function:Active
```

```
  Link:      Base: Up          Fabric: Up
  Heartbeat: Management: Good   Data: Good
  Status Message:"Running"
Slot  4: Status:Working   Function:Active
  Link:      Base: Up          Fabric: Up
  Heartbeat: Management: Good   Data: Good
  Status Message:"Running"
Slot  5: Status:Working   Function:Active
  Link:      Base: Up          Fabric: Up
  Heartbeat: Management: Good   Data: Good
  Status Message:"Running"
```

Enter this command from the FortiController in chassis 2 slot 2 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 2 slot 2 is shown first.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=1276.77, chassis=2(1)
    slot: 2
    sync: conf_sync=1, elbc_sync=1
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 best=yes
            local_interface=        b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=5356.98, chassis=1(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 last_hb_time= 1363.89   status=alive
            local_interface=        b2 last_hb_time=    0.00   status=dead

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123, uptime=2122.58, chassis=2(1)
    slot: 1
    sync: conf_sync=1, elbc_sync=1, conn=3(connected)
    session: total=0,  session_sync=in sync
    state: worker_failure=0/3, intf_state=(port up:)=0
 force-state(0:none)    hbdevs: local_interface=        b1 last_hb_time= 1363.97   status=alive
            local_interface=        b2 last_hb_time=    0.00   status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4985.27, chassis=1(1)
    slot: 2
```

```
   sync: conf_sync=1, elbc_sync=1, conn=3(connected)
   session: total=0,  session_sync=in sync
   state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)    hbdevs: local_interface=        b1 last_hb_time= 1363.89   status=alive
           local_interface=        b2 last_hb_time=    0.00   status=dead
```

For further reading, check out the FortiController Session-aware Load Balancing Guide.

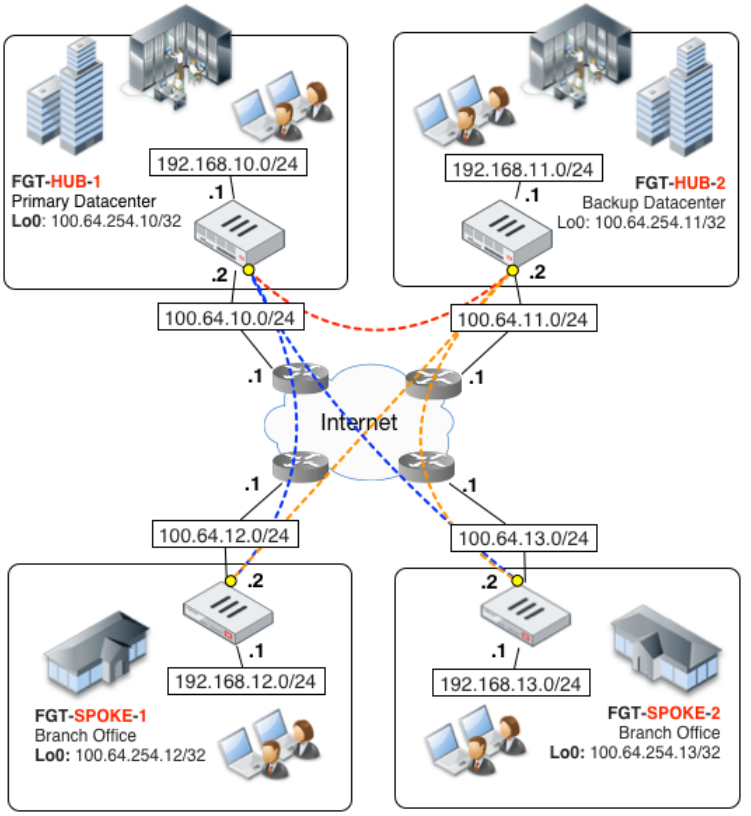
Hub-and-spoke VPN using quick mode selectors

In this expert cookbook article and an included example recipe, we will explore a scalable approach to setting up a large number of spoke VPNs by using quick mode selector source definitions on the spoke FortiGates and the dialup VPN configurations on the hub FortiGates.

We will also explore how redundant spoke VPN tunnels can be configured in order to offer maximum redundancy for environments with critical availability requirements. We will be authenticating the VPN tunnels using X-Auth in order to ensure separate credentials for each spoke.

This recipe is based on FortiOS firmware version 5.2, so some of the steps shown may not be the same as with other versions of the firmware.

The sample topology for this advanced cookbook article follows:



This topology consists of 2 hub networks and 2 spoke networks, using private IP ranges, separated by a simulated Internet, with 100.64.0.0/16 representing the Internet. Each FortiGate also has a loopback interface that is routable across the VPN.

The diagram topology shows the VPN tunnels along with their redundant links:

- The **red** dotted line showing the VPN tunnel connection between the primary and backup data centers; in this case, our two hubs.
- The **blue** dotted line showing the VPN tunnel connection between the primary datacenter and the branch offices; the spokes in the scenario.
- The **orange** dotted line shows the VPN tunnel connection between the backup datacenter and the branch offices.

While the topology shown in the diagram can be built using individual static tunnels between each site, this would not scale well if addition spokes grow to a significant number. There would also be limited support for dynamically addressed sites. This strategy put forth by this article offers a solution to these issues by using a single phase 1 dialup definition on the hub FortiGates with additional spoke tunnels being added, without any changes to the hubs beyond that of adding additional user accounts for each additional spoke.

Spoke authentication is maintained by with X-Auth, which keeps the authentication of the individual tunnels separate in such a way that the use of a Pre-Shared Key alone is insufficient to authenticate a tunnel. A Public Key Infrastructure can also be used, provided that separate key-pairs are used for each VPN tunnel to maintain the segregation of the spokes.

The key points of this design are:

- Each hub FortiGate is configured with a dialup interface-mode Phase1 using X-Auth.
- Each spoke has its own user account on the hub FortiGates. In this example, local accounts are used on each hub, but a RADIUS or LDAP authentication server could be used on the back end, eliminating the need to managed the accounts on the FortiGates.
- Spoke FortiGates are configured to propagate their local subnets using quick mode selectors (specifically, a source object).
- When a new spoke tunnel is connected, the hub FortiGate validates the shared secret along with the X-Auth credentials provided by the spoke FortiGate.
- Spokes FortiGates can have dynamically assigned IP addresses such as those given out by DSL or cable ISPs.
- The hub FortiGates each insert a reverse route pointing to newly established tunnel interfaces, for any of the subnets provided by the spoke FortiGate's source quick mode selectors.
- Each spoke FortiGate uses configured static routes to direct traffic that needs to go to the datacenter(s) through the VPN tunnels destined for the hubs. The static route to the backup hub is set to a higher priority number value, making it the less preferred route. There is also an option where you can send all of your traffic from the spokes through the VPN tunnel by default. This can be done by configuring the WAN interface to route all traffic through the public IP address of the hub FortiGate. This is what our example configuration is set to do.
- We need to aware of any potential points where asymmetrical routing could occur as it relates to traffic

returning to the spokes (This is essentially the response to a request coming back through a different route than it took to get there). This can be a potential problem especially when communicating to hosts that are connected to both data centers and we happen to be redistributing spoke routes using a dynamic routing protocol with hub sites using OSI Layer 3 networking devices. In this case, we would ensure that the backup hub's redistributed routes are less preferred than the primary hub's routes. In all cases, it is important to have a clear view of the routing flows between each endpoint and to keep "diag debug flow" in our toolbox to diagnose those potential asymmetric routing issues. In our example, we would want to route traffic destined to resources in each respective hub directly to that hub, rather than have it cross the inter-datacenter VPN tunnel, and have default routing flow to the primary hub under normal circumstances.

The Hub FortiGates

Let's look at the relevant configuration points of the hub FortiGates (These will be identical on each hub FortiGate:

While the GUI can be used for these steps, we are going to use the CLI to keep things simple and avoid potential confusion that may be caused by changes in the GUI's layout.

Create the IPsec tunnel:

```
config vpn ipsec phase1-interface
   edit "SPOKES"
   set type dynamic
   set interface "port1"
   set mode aggressive
   set peertype one
   set proposal aes256-sha256
   set xauthtype auto
   set authusrgrp "SPOKE-GRP"
   set peerid "SPOKES"
   set psksecret SuperSecretSpokeSecret
   next
end

config vpn ipsec phase2-interface
   edit "SPOKES-P2"
   set phase1name "SPOKES"
   set proposal aes256-sha256
   set keepalive enable
   next
end
```

Create a user for each of the spokes:

```
config user local
   edit "SPOKE1"
   set type password
```

```
   set passwd Spoke1SuperSecret
   next
   edit "SPOKE2"
   set type password
   set passwd Spoke2SuperSecret
   next
end
```

Create a user group and include the spoke members:

```
config user group
   edit "SPOKE-GRP"
   set member "SPOKE1" "SPOKE2"
   next
end
```

Create the firewall policies

```
config firewall policy
   edit 1
   set srcintf "port2" "loop0"
   set dstintf "SPOKES"
   set srcaddr "all"
   set dstaddr "all"
   set action accept
   set schedule "always"
   set service "ALL"
   next
   edit 2
   set srcintf "SPOKES"
   set dstintf "port2" "loop0"
   set srcaddr "all"
   set dstaddr "all"
   set action accept
   set schedule "always"
   set service "ALL"
   next
end
```

A few of the above configuration aspects require further explanation:

- **Aggressive mode**: We are using this mode in order to ensure that these dialup spokes are terminated on the right dialup phase1. If the hub unit has other dialup phase1 (for FortiClient VPN users, for instance), the hub would otherwise be unable to distinguish between each dialup phase1.A few of the above configuration aspects require further explanation:

- **X-Auth**: As previously stated, this allows us to authenticate each connecting spoke unit to a local group, which is defined in the above configuration as currently containing two user accounts (our example has two spokes). Provisioning additional spokes on the hub would simply involve adding additional user accounts.
- **Policies**: As usual, we must always configure policies in order for traffic to flow. IPsec Phase1 follows a special rule in which tunnels will not even attempt to come up unless they have at least one policy referring to them (this happens to be a good trick to know when you want to disable an IPsec VPN tunnel without deleting its configuration).

The Spoke FortiGates

With the hub FortiGates configured and ready for incoming connections, the spoke FortiGates can be configured. Below is the steps for configuring SPOKE1. To configure additional spoke FortiGates change the unit specific information.

Create the IPsec tunnel

```
config vpn ipsec phase1-interface
   edit "HUB-PRIMARY"
   set interface "port1"
   set mode aggressive
   set proposal aes256-sha256
   set localid "SPOKES"
   set xauthtype client
   set authusr "SPOKE1"
   set authpasswd Spoke1SuperSecret
   set mesh-selector-type subnet
   set remote-gw 100.64.10.2
   set psksecret SuperSecretSpokeSecret
   next
   edit "HUB-BACKUP"
   set interface "port1"
   set mode aggressive
   set proposal aes256-sha256
   set localid "SPOKES"
   set xauthtype client
   set authusr "SPOKE1"
   set authpasswd Spoke1SuperSecret
   set mesh-selector-type subnet
   set remote-gw 100.64.11.2
   set psksecret SuperSecretSpokeSecret
   next
end
```

```
config vpn ipsec phase2-interface
   edit "PRIMARY-P2"
   set phase1name "HUB-PRIMARY"
   set proposal aes256-sha256
```

```
   set keepalive enable
   set src-addr-type name
   set dst-addr-type name
   set src-name "VPN_SUBNETS"
   set dst-name "all"
   next
   edit "BACKUP-P2"
   set phase1name "HUB-BACKUP"
   set proposal aes256-sha256
   set keepalive enable
   set src-addr-type name
   set dst-addr-type name
   set src-name "VPN_SUBNETS"
   set dst-name "all"
   next
end
```

Creating addresses for the subnets

```
config firewall address
   edit "NET_192.168.12.0/24"
   set subnet 192.168.12.0 255.255.255.0
   next
   edit "NET_100.64.254.12/32"
   set subnet 100.64.12.254 255.255.255.255
   next
end
```

Creating an address group for the subnets

```
config firewall addrgrp
   edit "VPN_SUBNETS"
   set member "NET_100.64.254.12/32" "NET_192.168.12.0/24"
   next
end
```

Configuring static routes

Use edit 0 to create a route with the next unused number.

```
config router static
   edit 0
   set dst 100.64.11.2 255.255.255.255
   set device "port1"
   next
   edit 0
   set dst 100.64.10.2 255.255.255.255
```

```
    set device "port1"
    next
    edit 0
    set device "HUB-PRIMARY"
    next
    edit 0
    set device "HUB-BACKUP"
    set priority 20
    next
end
```

Configuring the firewall policies

Use edit 0 to create a policy with the next unused number.

```
config firewall policy
    edit 0
    set srcintf "port2" "loop0"
    set dstintf "HUB-PRIMARY"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    next
    edit 0
    set srcintf "HUB-PRIMARY"
    set dstintf "port2" "loop0"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    next
    edit 0
    set srcintf "port2" "loop0"
    set dstintf "HUB-BACKUP"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    next
    edit 0
    set srcintf "HUB-BACKUP"
```

```
    set dstintf "port2" "loop0"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    next
end
```

Each spoke configuration calls for similar Phase1 parameters, but differs for the rest of the configuration in a few keys areas:

- **Aggressive mode**: As the hub is validating the inbound ID, we have configured our peer ID to the matching string "SPOKES".
- **X-Auth**: Our spokes are acting as X-auth clients, and each of our unit is using distinct credentials passed to the hub device during IKE phase1 negotiation.
- **Phase 2 quick mode selectors:** As the title of this recipe suggests, this is where the spoke provisioning routing automation happens. We've defined address objects, added them to a group, and performed the configuration found in Phase2. There is however a peculiarity where if we have more than one subnet behind our spoke unit, the "set mesh-selector-type subnet" command must be configured to ensure multiple Phase2 SAs are negotiated for each subnet listed in our group.
- **Routing**: As previously expressed, we have configured our default routing to flow through the primary hub (**blue** links) and failover routing to the backup hub (**orange** links, using route priority adjustment). Notice that we are explicitly routing each hub's public IP through the public Internet to ensure that traffic will not flow through the VPN tunnel (and result in flapping).

Where the spoke configurations will be different

As explained earlier, the spoke FortiGate configurations will be slightly different on each individual spoke. The settings will be similar on all of the spoke with the following exceptions:

- **X-Auth**: Our spokes are acting as X-auth clients, and each of our unit is using distinct credentials passed to the hub device during IKE phase1 negotiation.

```
    config vpn ipsec phase1-interface
    edit "HUB-PRIMARY"
     set authusr (The account will be the one associated with the specific spoke)
    set authpasswd (The password will be the one associated with the specific spoke)
    next
  edit "HUB-BACKUP"
    set authusr (The account will be the one associated with the specific spoke)
    set authpasswd (The password will be the one associated with the specific spoke)
    next
  end
```

- **Phase 2 quick mode selectors:** This is where the spoke routing automation happens. We've defined address objects, added them to a group, and performed the configuration found in Phase2. There is however a peculiarity where if we have more than one subnet behind our spoke unit, the following setting must be used to ensure multiple Phase2 SAs are negotiated for each subnet listed in our group:

```
config vpn ipsec phase1-interface
edit <name>
set mesh-selector-type subnet
end
end
```

- **Routing**: This wont necessarily be different between the different spoke FortiGates, but as previously mentioned, in this example recipe we have configured our default routing to flow through the primary hub and failover routing to the backup hub. Notice that we are explicitly routing each hub's public IP through the public Internet to ensure that traffic will not flow through the VPN tunnel (and result in flapping).

Results

And this concludes our VPN configuration! But this recipe would not be complete without a very important verification step. Lets look at the routing table on the **hub**:

```
HUB # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
S*      0.0.0.0/0 [10/0] via 192.168.56.2, port1
S       100.64.254.12/32 [15/0] is directly connected, HUB_0S
100.64.254.13/24 [15/0] is directly connected, HUB_1
C       192.168.11.0/24 is directly connected, port2
S       192.168.12.0/24 [15/0] is directly connected, HUB_0S
192.168.13.0/24 [15/0] is directly connected, HUB_1
C       192.168.56.0/24 is directly connected, port1
```

As can be seen above, our spoke subnets have been automatically injected into the hub's routing tables. A closer look at the VPN details of one spoke confirms that the hub received the negotiated subnets during quick mode negotiation and inserted distinct SAs for each SA.

```
FGT1 # get vpn ipsec tunnel details
gateway
name: 'HUB_0'
type: route-based
local-gateway: 192.168.56.11:0 (static)
remote-gateway: 192.168.56.12:0 (dynamic)
mode: ike-v1
interface: 'port1' (2)
rx  packets: 56  bytes: 8736  errors: 0
tx  packets: 41  bytes: 3444  errors: 0
dpd: enabled/negotiated  idle: 5000ms  retry: 3  count: 0
selectors
name: 'HUB-P2'
auto-negotiate: disable
mode: tunnel
```

```
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:192.168.12.0-192.168.12.255:0
--------OUTPUT TRUNCATED--------
selectors
name: 'HUB-P2'
auto-negotiate: disable
mode: tunnel
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:100.64.254.12-100.64.254.12:0
--------OUTPUT TRUNCATED--------
```

If you require communication between the spokes, this can be routed through the hub FortiGates. The only change to the example recipe's configuration is an addition policy on each of the hub FortiGates which defines the both the Incoming Interface and the Outgoing Interface as the VPN Dialup Interface (in this example, SPOKES)

On the Spoke FortiGates, once the poke tunnels have been established, you can see the default route to the primary datacenter and the alternate though less preferred route to the backup datacenter by running the command `get router info routing-table all`

```
FGT-SPOKE-1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
S* 0.0.0.0/0 [10/0] is directly connected, HUB-PRIMARY             [10/0] is
directly connected, HUB-BACKUP, [20/0]
S 100.64.10.2/32 [10/0] is directly connected, port1
S 100.64.11.2/32 [10/0] is directly connected, port1
C 100.64.12.0/24 is directly connected, port1
C 100.64.254.12/32 is directly connected, lo0
C 192.168.12.0/24 is directly connected, port2
```

We can test the failover function by shutting down the port1 interface on the primary hub. This will bring down the VPN between the primary hub and the spokes. Once the DPD detects the fault, traffic switches over to the backup hub as shown here:

```
FGT-SPOKE-1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
S* 0.0.0.0/0 [10/0] is directly connected, HUB-BACKUP, [20/0]
S 100.64.10.2/32 [10/0] is directly connected, port1
S 100.64.11.2/32 [10/0] is directly connected, port1
C 100.64.12.0/24 is directly connected, port1
C 100.64.254.12/32 is directly connected, lo0
C 192.168.12.0/24 is directly connected, port2
```

Final notes

- The technique shown here does not involve dynamic routing so this configuration and its very straight forward template can be easily used to scale up the topology to include thousands of spoke sites.
- To make it even easier, this configuration can be entirely built and automated with FortiManager, which has support for provisioning hub-and-spoke dialup topologies.

Glossary

BGP: Border Gateway Protocol is primarily used to connect the networks of large organizations that have two or more ISP connections, or between other autonomous systems. If used in such a situation, a FortiGate can use BGP for routing.

BYOD: Bring Your Own Device (also called device management) is the practice of allowing network users to access an organization's (usually wireless) network with their own computers, smart phones, tablets and other devices. BYOD has a major impact on networks with large and diverse user bases, such as educational institutions, but also affects large and small business networks.

CA: A certificate authority (CA) is an entity that issues digital certificates, which are used to establish secure connections over a network, typically the Internet. The CA acts as a trusted third-party by verifying the identity of a certificate's owner: for example, the certificate found when you go to https://www.facebook.com is verified as belonging to Facebook.

Certificates: In networking, certificates (including public key certificates, digital certificates, and identity certificates) provide digital signatures for websites or other electronic communication and allow you to verify whether a digital identity is legitimate.. A FortiGate can use certificates for many things, including SSL inspection and user authentication.

CLI: The Command Line Interface is a text-based interface used to configure a FortiGate unit. Most steps in the FortiGate Cookbook use the Graphical User Interface (see GUI), but some configuration options are only available using the CLI.

DHCP: Dynamic Host Configuration Protocol is a networking protocol that allows devices to request network parameters, such as IP addresses, automatically from a DHCP server, reducing the need to assign these settings manually. A FortiGate can function as a DHCP server for your network and can also receive its own network parameters from an external DHCP server.

Dial-up/dynamic VPN: A dial-up VPN, also called a dynamic VPN, is a type of IPsec VPN where one of the endpoints has a dynamic IP address.

DMZ: A Demilitarized Zone is an interface on a FortiGate unit that provides external users with secure access to a protected subnet on the internal network without giving them access to other parts of the network. This is most commonly done for subnets containing web servers, which must be accessible from the Internet. The DMZ interface will only allow traffic that has been explicitly allowed in the FortiGate's configuration. FortiGate models that do not have a DMZ interface can use other interfaces for this purpose.

DNS: Domain Name System is used by devices connecting to the Internet to locate websites by mapping a domain name to a website's IP address. For example, a DNS server maps the domain name www.fortinet.com to the IP address 66.171.121.34. Your FortiGate unit controls which DNS servers the network uses. A FortiGate can also function as a DNS server.

DSR: In a typical load balancing scenario, server responses to client requests are routed through a load balancer on their way back to the client. The load balancer examines the headers of each response and can insert a cookie before sending the server response on to the client. In a Direct Server Return (DSR) configuration, the server receiving a client request responds directly to the client IP, bypassing the load balancer. Because the load balancer only processes incoming requests, load balancing performance is dramatically improved when using

DSR in high bandwidth applications. In such applications, it is not necessary for the load balancer to receive and examine the server's responses. So the client makes a request and the server simply streams a large amount of data to the client.

Dynamic IP address: A dynamic IP address is one that can change without the device's user having to do anything. Dynamic IP addresses allow networks to control the IP addresses of devices that connect to them. This allows you to connect portable devices to different networks without needing to manually change their IP addresses.

Dynamic IP addresses are set by network protocols, most often DHCP.

ECMP: Equal Cost Multipath Routing allows next-hop packet forwarding to a single destination to occur over multiple best paths that have the same value in routing metric calculations. ECMP is used by a FortiGate for a variety of purposes, including load balancing.

Explicit Proxy: Explicit proxy is a type of configuration where all clients are configured to allow requests to go through a proxy server, which is a server used as an intermediary for requests from clients seeking resources from other servers. When a FortiGate uses explicit proxy, the clients sending traffic are given the IP address and port number of the proxy server.

FortiAP: A FortiAP unit is a wireless Access Point that can be managed by a FortiGate. Most FortiAP functions can also been accomplished using a FortiWiFi unit.

FortiClient: The FortiClient software provides a variety of features, including antivirus, web filtering, firewall, and parental controls, to individual computers and mobile devices. It can also be used to connect to a FortiGate using either an SSL or IPsec VPN.

FortiClient is available for Windows, Mac OSX, iOS, and Android, and can be set up quickly. After being installed, it automatically updates its virus definition files, does a full system scan once per week, and much more.

FortiClient can be downloaded at www.forticlient.com.

FortiOS: FortiOS is the operating system used by FortiGate and FortiWiFi units. It is also referred to as firmware.

FTP: File Transfer Protocol is a standard protocol used to transfer computer files from one host to another host over a computer network, usually the Internet, using FTP client and server applications.

Gateway: A gateway is the IP address that traffic is sent to if it needs to reach resources that are not located on the local subnet. In most FortiGate configurations, a default route using a gateway provided by an Internet service provider must be set to allow Internet traffic.

GUI: The Graphical User Interface, also known as the web-based manager, is a graphics-based interface used to configure a FortiGate unit and is an alternative to using the Command Line Interface (see CLI). You can connect to the GUI using either a web browser or FortiExplorer. Most steps in the FortiGate Cookbook use the GUI.

HTTP: Hypertext Transfer Protocol is a protocol used for unencrypted communication over computer networks, including the Internet, where it is used to access websites. FortiGate units handle more HTTP traffic than any other protocol.

HTTPS: Hypertext Transfer Protocol Secure is a protocol that secures HTTP communications using the Secure Sockets Layer (SSL) protocol. HTTPS is the most commonly used secure communication protocol on the Internet.

Interfaces: Interfaces are the points at which communication between two different environments takes place. These points can be physical, like the Ethernet ports on a FortiGate, or logical, like a VPN portal.

IP address: An Internet Protocol address is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication. FortiGate units can use IP addresses to filter traffic and determine whether to allow or deny traffic. Both IP version 4 and IP version 6 (see IPv4 and IPv6) are supported by your FortiGate.

IPsec: Internet Protocol Security is used to for securing IP communications by authenticating and encrypting each packet of a session. A FortiGate primarily uses this protocol to secure virtual private networks (see VPN).

IPv4: Internet Protocol version 4 is the fourth version of the Internet Protocol (IP), the main protocol used for communication over the Internet. IPv4 addresses are 32-bit and can be represented in notation by 4 octets of decimal digits, separated by a period: for example, 172.16.254.1.

IPv6: Internet Protocol version 6 is the sixth version of the Internet Protocol (IP), the main protocol used for communication over the Internet (IPv5 never became an official protocol). IPv6 was created in response to the depletion of available IPv4 addresses. IPv6 addresses are 128-bit and can be represented in notation by 8 octets of hexadecimal digits, separated by a colon: for example, 2001:db8:0000:0000:0000:0000:0000:0000. IPv6 addresses can be shortened if all the octets are 0000; for example, the previous address can also be written as 2001:db8::

LAN/internal: The LAN/internal interface is an interface that some FortiGate models have by default. This interface contains a number of physical ports that are all treated as a single interface by the FortiGate unit. This allows you to configure access for the entire Local Area Network at the same time, rather than configuring each port individually.

LDAP: Lightweight Directory Access Protocol is a protocol used for accessing and maintaining distributed directory information services over a network. LDAP servers are commonly used with a FortiGate for user authentication.

MAC address: A Media Access Control address is a unique identifier assigned to a network interface used for network communication. A MAC address is assigned to a device by the manufacturer and so this address, unlike an IP address, is not normally changed. MAC addresses are represented in notation by six groups of two hexadecimal digits, separated by hyphens or colons: for example, 01:23:45:67:89:ab. Your FortiGate can identify network devices using MAC addresses.

Multicast: Multicast is a method of group communication where information is addressed to a group of destinations simultaneously. A FortiGate can use multicast traffic to allow communication between network devices.

NAT: Network Address Translation is a process used to modify, or translate, either the source or destination IP address or port in a packet header. The primary use for NAT is to allow multiple network devices on a private network to be represented by a single public IP address when they browse the internet. FortiGate also supports many other uses for NAT.

Packet: A packet is a unit of data that is transmitted between communicating devices. A packet contains both the message being sent and control information, such as the source address (the IP address of the device that sent the packet) and the destination address (the IP address of the device the packet is being sent to).

Ping: Ping is a utility used to test whether devices are connected over a IP network and to measure how long it takes for a reply to be received after the message is sent, using a protocol called Internet Control Message Protocol (ICMP). If ICMP is enabled on the destination interface, you can ping the IP address of a FortiGate interface to

test connectivity between your computer and the FortiGate. You can also use the CLI command `execute ping` to test connectivity between your FortiGate and both internal and external devices.

Ports: See Interfaces and Port Numbers.

Port numbers: Port numbers are communication endpoints used to allow network communication. Different ports are used for different application-specific or process-specific purposes; for example, HTTP protocol commonly uses port 80.

Pre-shared key: In cryptography, a pre-shared key is a character string (like a password) known by two parties, and used by those parties to identify each other. Pre-shared keys are commonly used for granting access to IPsec VPNs and WiFi networks.

Pre-shared keys are different from regular passwords because they are not normally associated with a specific individual's credentials.

RADIUS: Remote Authentication Dial In User Service is a protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service. RADIUS servers are commonly used with a FortiGate for user authentication, including single-sign on.

RTSP: The Real Time Streaming Protocol is a media control protocol that is used for controlling streaming audio and video streams. RTSP has a wide range of uses and is often leveraged by other media-related services such as SIP. It most commonly uses TCP and UDP port 554 but additional ports are used by the actual media controlled by RTSP.

FortiOS includes an RSTP session helper that opens the ports used by individual RTSP-controlled streams. FortiRecorder and FortiCamera use RTSP for video streaming.

SCTP: The Stream Control Transmission Protocol is a transport layer protocol (protocol number 132) used most often for sending telephone signalling messages over carrier IP networks.

Session: A session is the dialogue between two or more communicating devices that include all messages that pass between the devices; for example, a session is created when a user browses to a specific website on the Internet for all communication between the user's computer and the web server that hosts the site. Sessions are tracked by a FortiGate unit in order to create logs about the network traffic.

SIP: Session Initiation Protocol is used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol networks. FortiGate units use this protocol for voice over IP (see VoIP).

Site-to-site VPN: A site-to-site VPN allows two networks that are each behind a VPN gateway (for example, a FortiGate unit), to establish secure connections with each other over a public network, typically the Internet.

Site-to-site VPNs most often use IPsec and can be established between two FortiGates, or between a FortiGate and any other IPsec VPN gateway, such as a Cisco ASA or Microsoft Azure.

SLAAC: Stateless Address Autoconfiguration is a feature of IPv6 that allows devices on an IPv6 network to automatically get IPv6 addresses. SLAAC is similar to DHCP except that DHCP requires you to run and configure a DHCP server. SLAAC is built into IPv6 and requires only minor additional configuration. SLAAC is defined by RFC 2462.

SNMP: Simple Network Management Protocol is a protocol that monitors hardware on your network. A FortiGate can use SNMP to monitor events such as high CPU usage, VPN tunnels going down, or hardware becoming

disconnected.

SSH: Secure Shell is a protocol used for secure network services between two devices, including remote command-line access. SSH can be used to access a FortiGate's command line interface (CLI).

SSID: A Service Set Identifier is the name that a wireless access point broadcasts to wireless users. Wireless users select this name to join a wireless network.

SSL: Secure Sockets Layer is a protocol for encrypting information that is transmitted over a network, including the Internet. SSL can be used for secure communications to a FortiGate, as well as for encrypting Internet traffic (see HTTPS) and for allowing remote users to access a network using SSL virtual private network (see VPN).

SSL inspection: Secure Sockets Layer inspection is used by your FortiGate to scan traffic or communication sessions that use SSL for encryption, including HTTPS protocol.

SSO: Single Sign-On is a feature that allows a user to login just once and remembers the credentials to re-use them automatically if additional authentication is required. A FortiGate supports both Fortinet single sign-on (FSSO) and single sign-on using a RADIUS server (RSSO).

Static IP address: Static IP addresses require user intervention to change. Normally a device that always has a wired connection to an Ethernet network has a static IP address.

Static route: A static route is a manually-configured routing entry that is fixed and does not change if the network is changed or reconfigured.

Subnet: A subnetwork, or subnet, is a segment of the network that is separated physically by routing network devices and/or logically by the difference in addressing of the nodes of the subnet from other subnets. Dividing the network into subnets helps performance by isolating traffic from segments of the network where it doesn't need to go, and it aids in security by isolating access. The addressing scope of a subnet is defined by its IP address and subnet mask and its connection to other networks is achieve by the use of gateways.

Subnet Mask: A subnet mask is the part of an IP address that is used to determine if two addresses are on the same subnet by allowing any network enabled device, such as a FortiGate, to separate the network address and the host address. This lets the device determine if the traffic needs to be sent through a gateway to an external network or if it is being sent to host on the local network.

URL: A Uniform Resource Locator is a text string that refers to a network resource. The most common use for URLs is on the Internet, where they are also known as web addresses.

URLs are used by a FortiGate to locate websites on the Internet and can also be used in web filtering to block specific sites from being accessed.

VDOM: Virtual Domains are used to divide a single FortiGate unit into two or more virtual instances of FortiOS that function separately and can be managed independently.

VLAN: Virtual Local Area Networks are used to logically divide a single local area network (LAN) into different parts that function independently. A FortiGate uses VLANs to provide different levels of access to users connecting to the same LAN.

VoIP: Voice over Internet Protocol is a protocol that is used to allow voice communications and multimedia sessions

over Internet Protocol sessions, including the Internet. VoIP protocol is used by a FortiGate when traffic needs to reach a connected VoIP phone or FortiVoice unit.

VPN: A Virtual Private Network is a private network that acts as a virtual tunnel across a public network, typically the Internet, and allows remote users to access resources on a private network. There are two main types of VPNs that can be configured using a FortiGate unit: IPsec VPN (see IPsec) and SSL VPN (see SSL).

WAN/WAN 1: The WAN or WAN1 port on your FortiGate unit is the interface that is most commonly used to connect the FortiGate to a Wide Area Network, typically the Internet. Some FortiGate models have a WAN2 port, which is commonly used for redundant Internet connections.

The FortiGate Cookbook contains a variety of step-by-step examples of how to integrate a FortiGate unit into your network and apply features such as security profiles, wireless networking, and VPN.

Using the FortiGate Cookbook, you can go from idea to execution in simple steps, configuring a secure network for better productivity with reduced risk.

Written for FortiOS 5.2