DYNAMIC GROUP - INDIA
www.dynamicgroup.in | info@dynamicgroup.in
(91) 9025 66 55 66

FORTINET

The FortiGate Cookbook

Recipes for Success with your FortiGate

FortiOS 5.2

The FortiGate Cookbook 5.2

October 3, 2014

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.

Contents

Change Log

Date	Change Description
October 3, 2014	Added new recipes: • Registering your FortiGate and configuring the system settings • Controlling which applications can access network resources and the Internet • Using a static URL filter to block access to a specific website • Using IPsec VPN to provide communication between offices • Setting up BGP over a dynamic IPsec VPN between Two FortiGates. • Setting up an Internet connection through a FortiGate unit using a 3G/4G modem and a FortiExtender Updated: • Tips for using the FortiGate Cookbook • Using a WAN link interface for redundant Internet connections • Glossary
August 26, 2014	Added new recipes: • Extra help: Switch mode vs Interface mode • Using port forwarding to allow limited access to an internal server • Using a FortiAP in Tunnel mode to add wireless access • Using a FortiAP in Bridge mode to add wireless access • Using MAC access control to allow access to the wireless network • Configuring IPsec VPN between a FortiGate and Microsoft Azure™ • Configuring redundant architecture using two FortiGates and internal switching Updated recipes: • Preventing security certificate warnings when using SSL full inspection • Using a custom certificate for SSL inspection

Introduction

The FortiGate Cookbook provides examples, or recipes, of basic and advanced FortiGate configurations to administrators who are unfamiliar with the unit. All examples require access to the graphical user interface (GUI), also known as the web-based manager.

Each example begins with a description of the desired configuration, followed by step-by-step instructions. Some topics include extra help sections, containing tips for dealing with some common challenges of using a FortiGate unit.

Using the FortiGate Cookbook, you can go from idea to execution in simple steps, configuring a secure network for better productivity with reduced risk.

The Cookbook is divided into the following chapters:

- Getting Started: recipes to help you start using your FortiGate.
- Security Features: recipes about using a FortiGate to protect your network.
- Wireless Networking: recipes about managing a wireless network with your FortiGate.
- Authentication: recipes about authenticating users and devices on your network.
- IPsec VPN: recipes about IPsec virtual private networks (VPNs), including authentication methods.
- SSL VPN: recipes about SSL virtual private networks (VPNs), including authentication methods.

This edition of the FortiGate Cookbook was written using FortiOS 5.2.1

Tips for using the FortiGate Cookbook

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

Understanding the basics

While the FortiGate Cookbook was written with new FortiGate users in mind, some basic steps, such as logging into the FortiGate unit, are not included in most recipes. This information can be found in the QuickStart guide for your FortiGate unit.

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 FortiGate model you are using and the firmware build. For example, the menu **Router > Static > Static Routes** is not available on some models. Also, on different models, the Ethernet interface that would normally connect to the Internet could be named port1, wan1, wan2, or external.

Also, some features are only available through the CLI on certain FortiGate models, generally the desktop models (FortiGate/WiFi-20 to 90 Series).

FortiGate ports

The specific ports being used in the documentation are chosen as examples. When you are configuring your FortiGate 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 unit 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 FortiGate unit, 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.

IPv4 vs IPv6

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 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.

Text elements

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

Icons

Several icons are used throughout the FortiGate Cookbook:

The exclamation icon indicates a warning, which includes information that should be read carefully before continuing with the recipe.

The lightbulb icon indicates a note, which includes information that may be useful but is not strictly necessary for completion of the recipe.

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.

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.

This section contains the following recipes:

- Extra help: Switch mode vs Interface mode
- Connecting a private network to the Internet using NAT/Route mode
- Adding a FortiGate in Transparent mode without changing your existing configuration
- Using a WAN link interface for redundant Internet connections
- Extra help: Troubleshooting your installation
- Registering your FortiGate and configuring the system settings
- Verifying and updating the FortiGate unit's firmware
- Setting up FortiGuard services
- Extra help: FortiGuard
- Logging network traffic to gather information
- Creating and ordering IPv4 security policies to provide network access
- Using SNMP to monitor the FortiGate unit
- Using port forwarding to allow limited access to an internal server

Extra help: Switch mode vs Interface 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
end
```

2. Command to change the FortiGate to interface mode:

```
config system global
   set internal-switch-mode interface
end
```

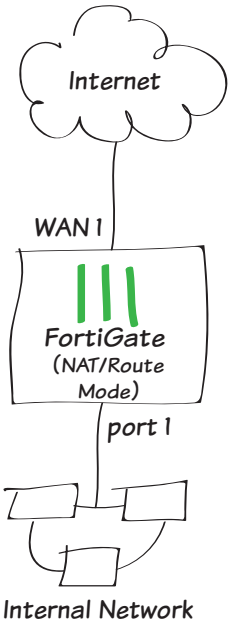
Connecting a private network to the Internet using NAT/Route mode

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 "Extra help: Switch mode vs Interface mode" on page 5.

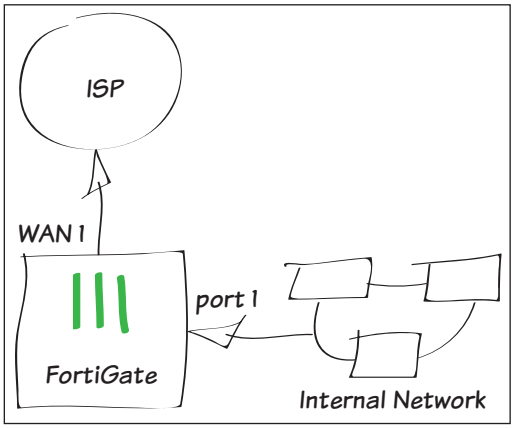
1. Connecting the network devices and logging onto the FortiGate
2. Configuring the FortiGate's interfaces
3. Adding a default route
4. (Optional) Setting the FortiGate's DNS servers
5. Creating a policy to allow traffic from the internal network to the Internet
6. Results



1. Connecting the network devices and logging onto the FortiGate

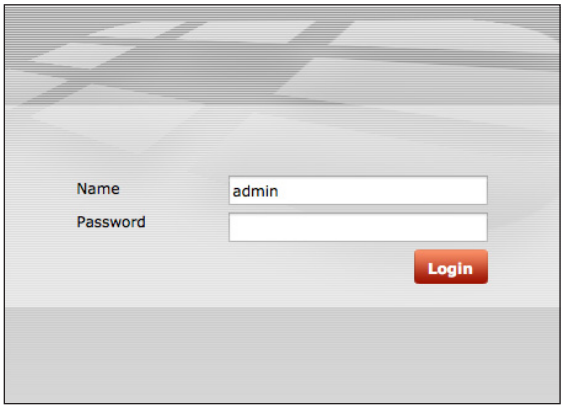
Connect the FortiGate's Internet-facing interface (typically WAN1) to your ISP-supplied equipment and Connect a PC to the FortiGate using an internal port (typically port 1).

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).

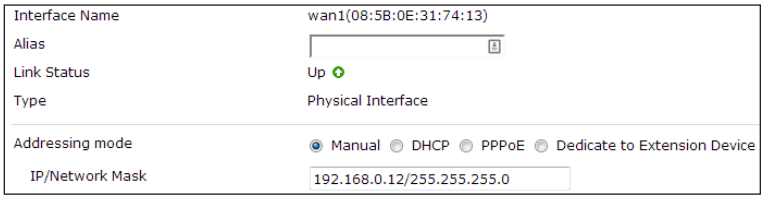
Login using an admin account (the default admin account has the username admin and no password).



2. Configuring the FortiGate's interfaces

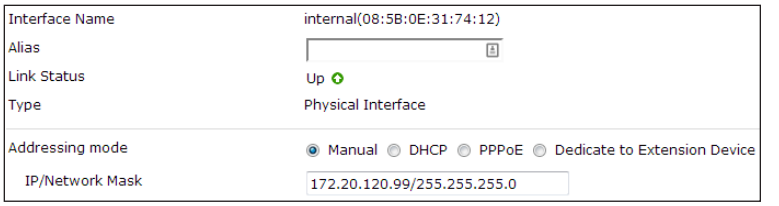
Go to **System > Network > Interfaces** and edit the Internet-facing interface.

Set **Addressing Mode** to **Manual** and the **IP/Netmask** to your public IP address.



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

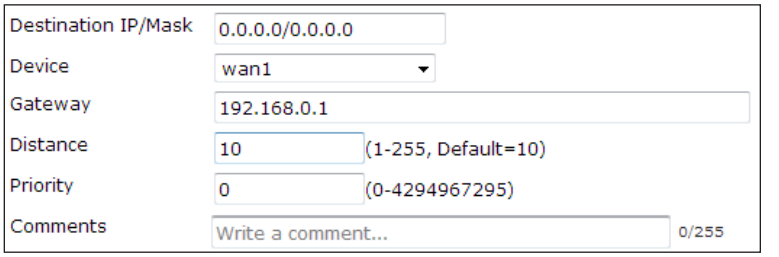
Set **Addressing Mode** to **Manual** and set the **IP/Netmask** to the private IP address you wish to use for the FortiGate.



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.

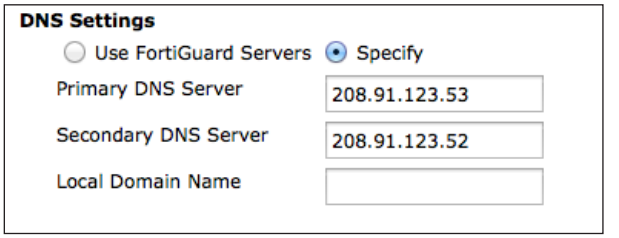
Set the **Destination IP/Mask** to 0.0.0.0/0.0.0.0, the **Device** to the Internet-facing interface, and the **Gateway** to the gateway (or default route) provided by your ISP or to the next hop router, depending on your network requirements.



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.



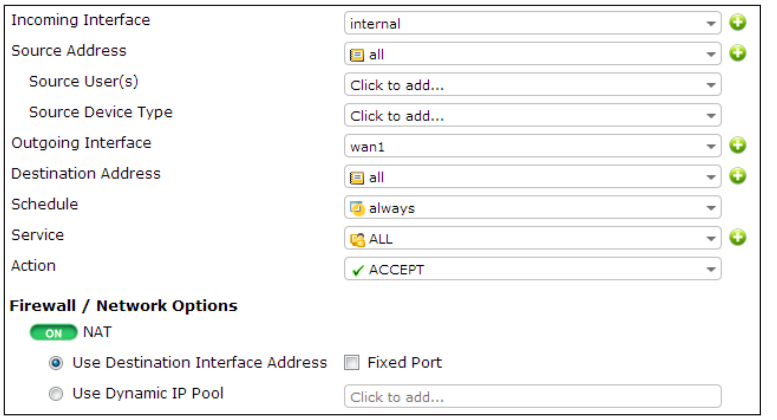
5. Creating a policy to allow traffic from the internal network to the Internet

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.

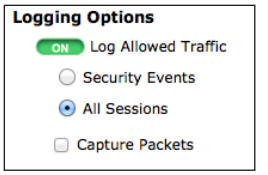
Go to **Policy & Objects > Policy > IPv4** and create a new policy (if your network uses IPv6 addresses, go to **Policy & Objects > Policy > IPv6**).

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.



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**.

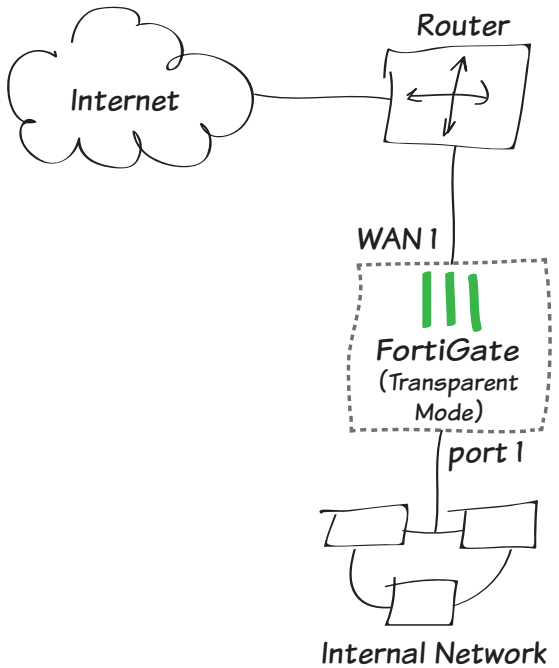
#	Date/Time	Dst Interfa...	Src Interfa...	Destination	Sent / Received
1	13:10:25	wan1	lan	8.247.14.128 (static.licdn.com)	1.10 KB / 640 B
2	13:10:25	wan1	lan	138.108.6.20 (secure-us.imrworldwide.com)	1.05 KB / 4.29 KB
3	13:10:24	wan1	lan	64.94.107.50 (map-pb.quantserve.com.akadns.net)	967 B / 444 B
4	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

Adding a FortiGate in Transparent mode without changing your existing configuration

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).

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**.

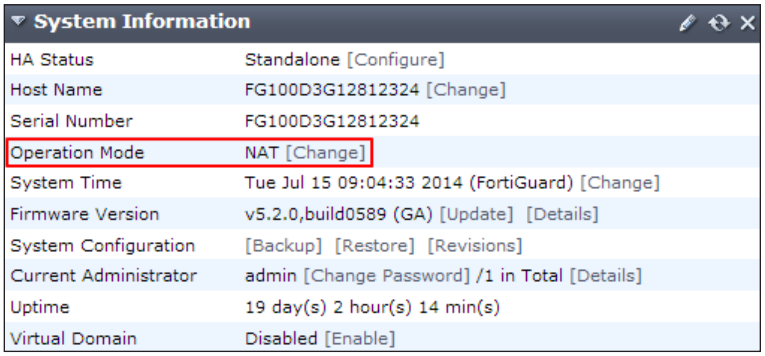
1. Changing the FortiGate's operation mode
2. (Optional) Setting the FortiGate's DNS servers
3. Creating a policy to allow traffic from the internal network to the Internet
4. Connecting the network devices



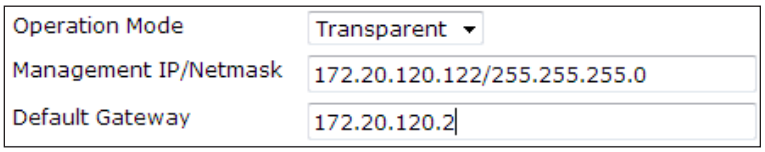
1. Changing the FortiGate's operation mode

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

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



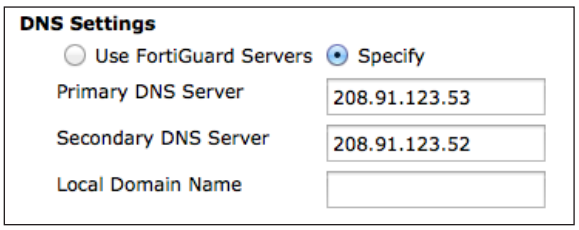
Set the **Operation Mode** to **Transparent**. Set the **Management IP/Netmask** and **Default Gateway** to connect the FortiGate unit to the internal network.



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

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

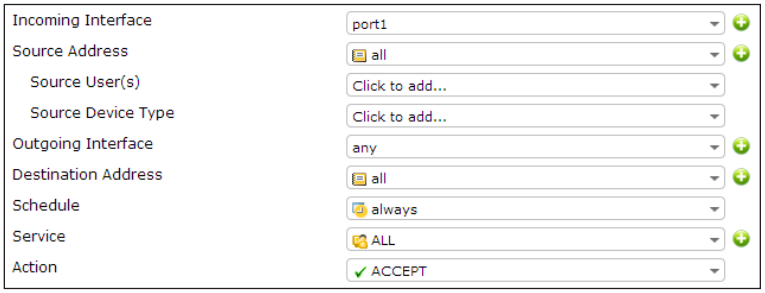
The FortiGate unit's DNS Settings are set to use FortiGuard DNS servers by default, which is sufficient for most networks. However, if you need to change the DNS servers, go to **System > Network > DNS** and add **Primary** and **Secondary** DNS servers.



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

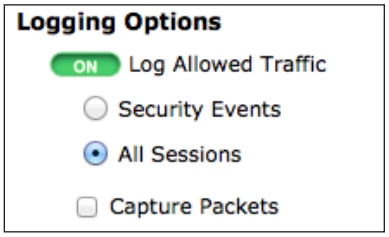
Go to **Policy & Objects > Policy > IPv4** and create a new policy (if your network uses IPv6 addresses, go to **Policy & Objects > Policy > IPv6**).

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



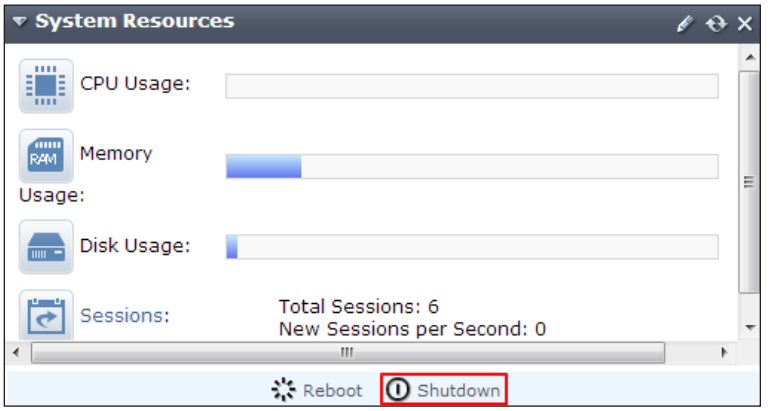
It is recommended to avoid using any security profiles until after you have successfully installed the FortiGate unit. After the installation is verified, you can apply any required security profiles.

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**):

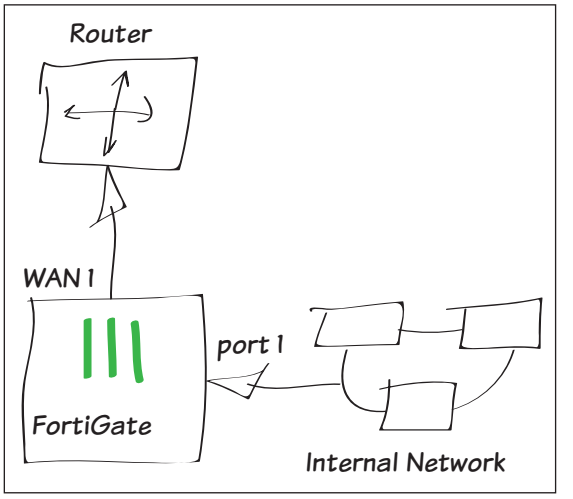
```
execute shutdown
```

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.



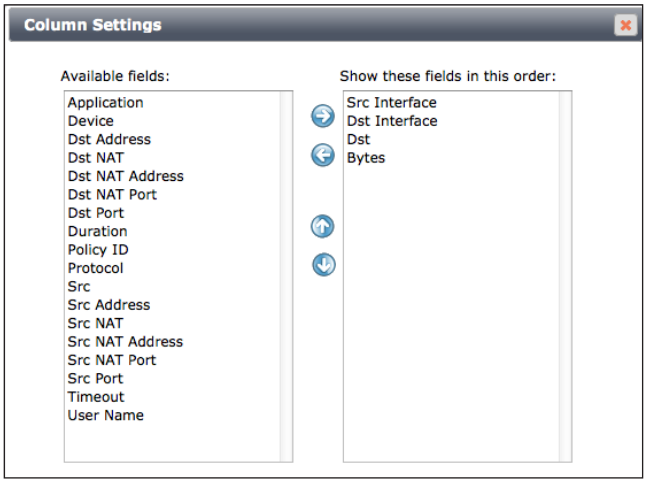
5. Results

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.

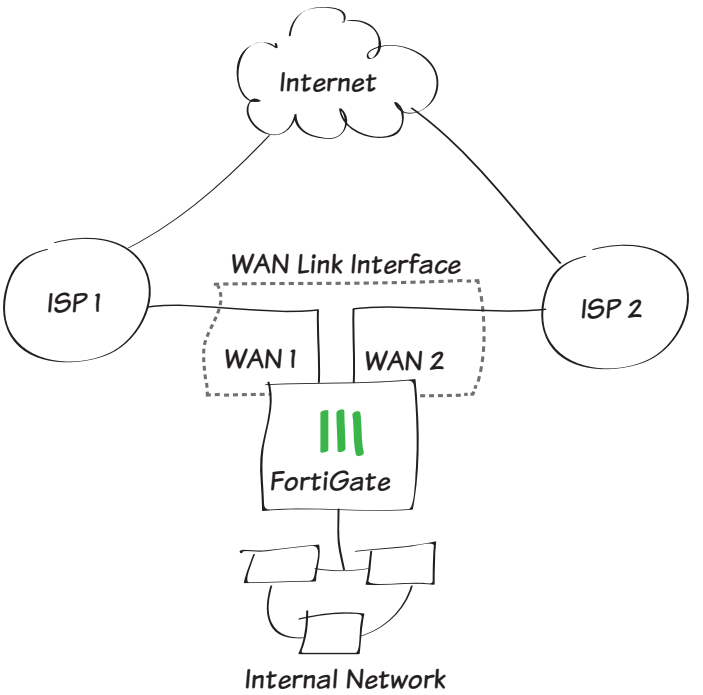


Using a WAN link interface for redundant Internet connections

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.

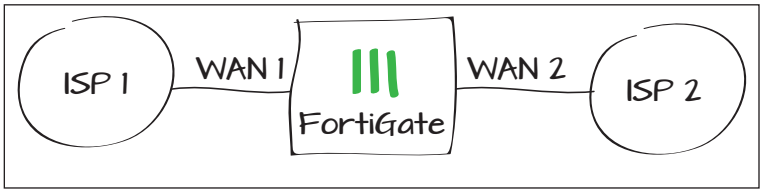
This example includes weighted load balancing so that most of your Internet traffic is handled by one ISP.

1. Connecting your ISPs to the FortiGate
2. Deleting security policies and routes that use WAN1 or WAN2
3. Creating a WAN link interface
4. Creating a default route for the WAN link interface
5. Allowing traffic from the internal network to the WAN link interface
6. Results



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.



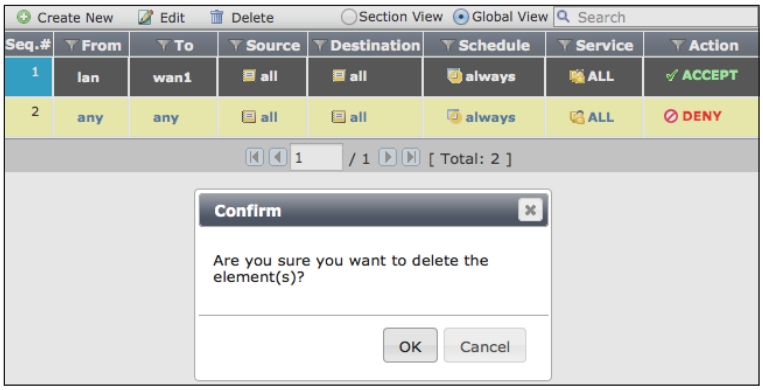
2. Deleting security policies and routes that use WAN1 or WAN2

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.

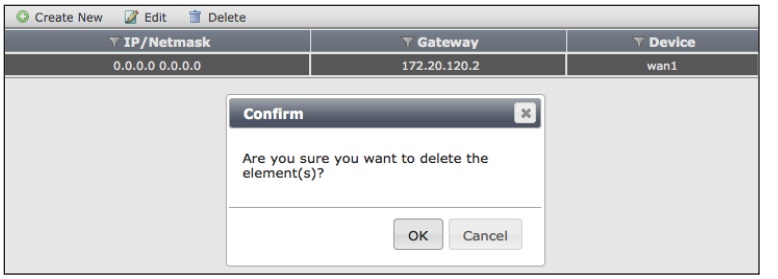
Many FortiGate models include a default Internet access policy that uses WAN1. This policy must also be deleted.

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.



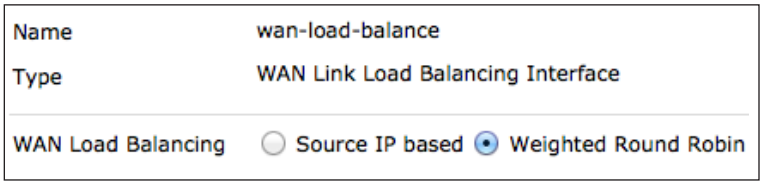
Go to **Router > Static > Static Routes** and delete any routes that use WAN1 or WAN2.



3. Creating a WAN link interface

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

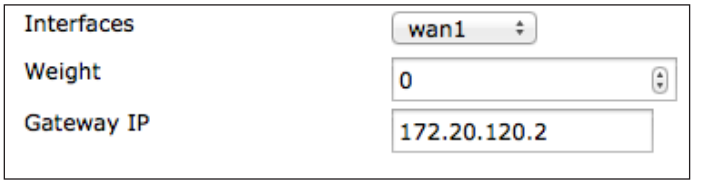
Set **WAN Load Balancing** to **Weighted Round Robin**. This will allow you to prioritize the WAN1 interface so that more traffic uses it.



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

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

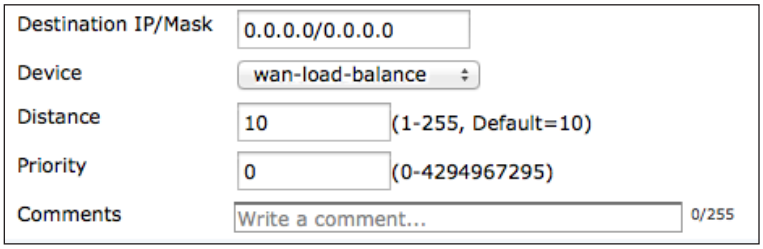
The weight settings will cause 75% of traffic to use WAN1, with the remaining 25% using WAN2.



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.

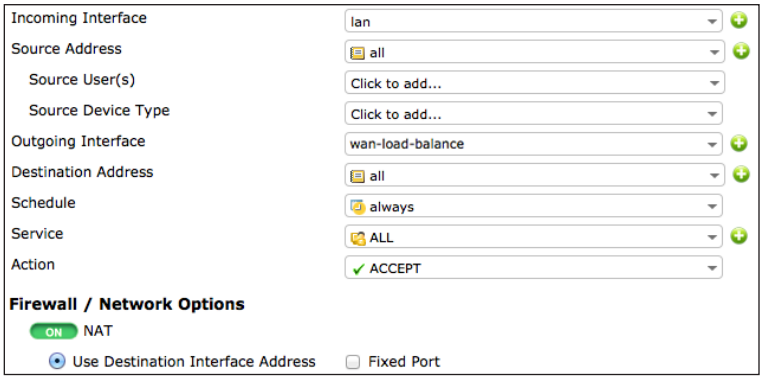


5. Allowing traffic from the internal network to the WAN link interface

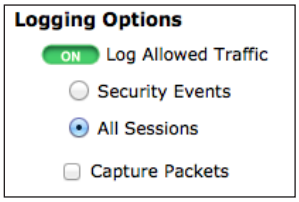
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

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

Extra help: Troubleshooting your 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.

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:

```
config system interface
   edit <interface>
      set macaddr <xx:xx:xx:xx:xx:xx>
   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 wan1 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.

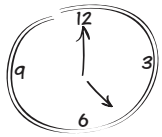
You can also contact the technical assistance center. For contact information, go to support.fortinet.com.

Registering your FortiGate and configuring the system 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
2. Setting the system time
3. (Optional) Restricting administrative access to a trusted host
4. Changing the default admin password
5. Results

Register your FortiGate



Set the system time

Configure the admin account

1. Registering your FortiGate

Registering your FortiGate allows you to receive FortiGuard updates and is required for firmware upgrades and access to support.fortinet.com.

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

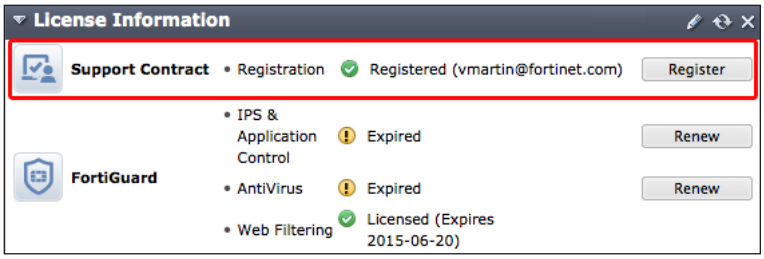
Go to **System > Dashboard > Status** and locate the **License Information** widget.

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.

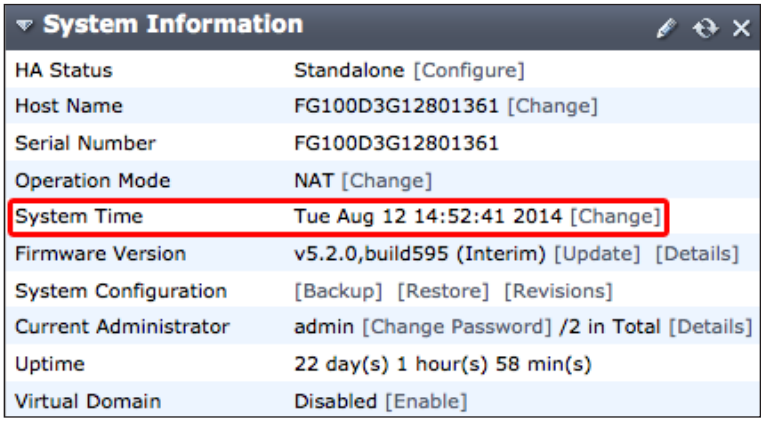
The **License Information** widget now displays the unit as **Registered**.



2. Setting the system time

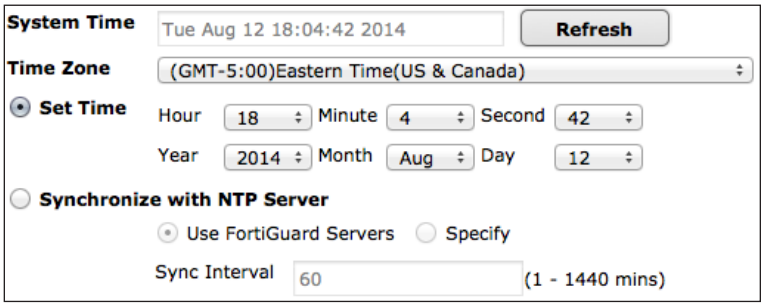
Go to **System > Dashboard > Status** and locate the **System Information** widget.

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

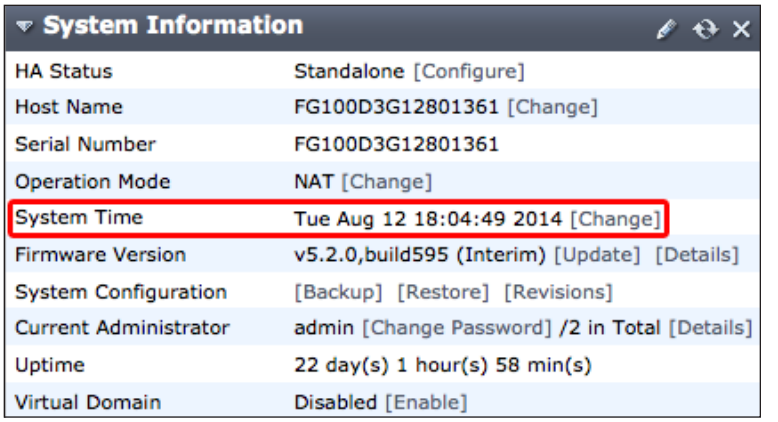


Select your **Time Zone** and either set the time manually or select **Synchronize with NTP Server**.

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.



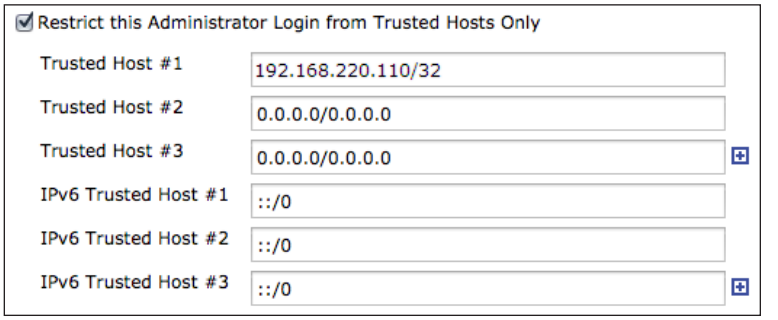
3. (Optional) Restricting administrative access to a trusted host

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.

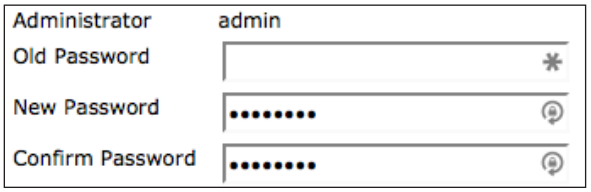


4. Changing the default admin password

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.

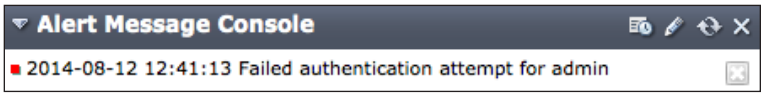


5. Results

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.



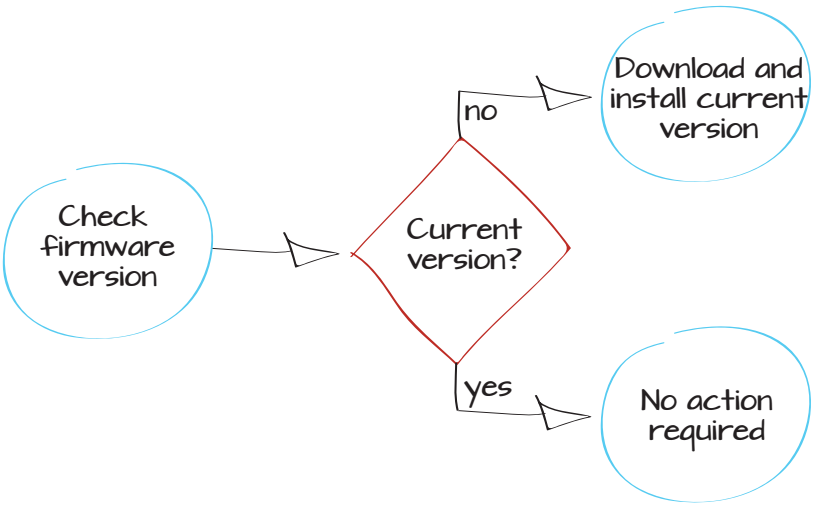
(Optional) If access has been restricted to a trusted host, attempts to connect from a device that is not trusted will be denied.

Verifying and updating the FortiGate unit'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. Updating FortiOS ensures the FortiGate unit makes use of the latest tools and security features available.

Always review the Release Notes and Supported Upgrade Paths documentation before installing a new firmware. These documents can be found at http://docs.fortinet.com.

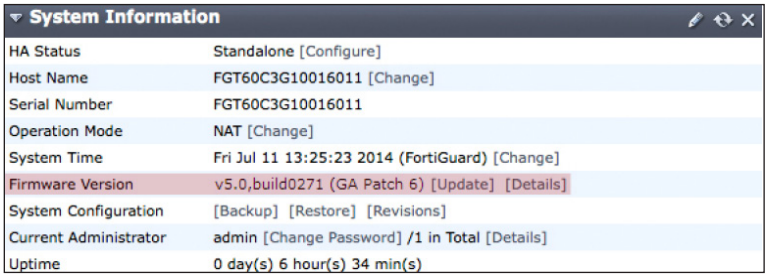
1. Checking the current FortiOS firmware
2. Downloading the latest FortiOS firmware
3. Updating the FortiGate to the latest firmware
4. Results



1. Checking the current FortiOS firmware

Log in to the web-based manager and go to **System > Dashboard > Status** and view the **System Information** dashboard widget to see the **Firmware Version** currently installed on your FortiGate unit.

Go to http://docs.fortinet.com/fortigate/release-information and refer to the Release Information section to determine the most recent version of FortiOS.

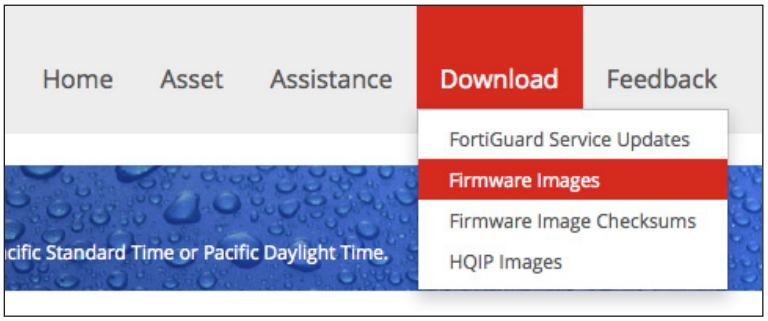


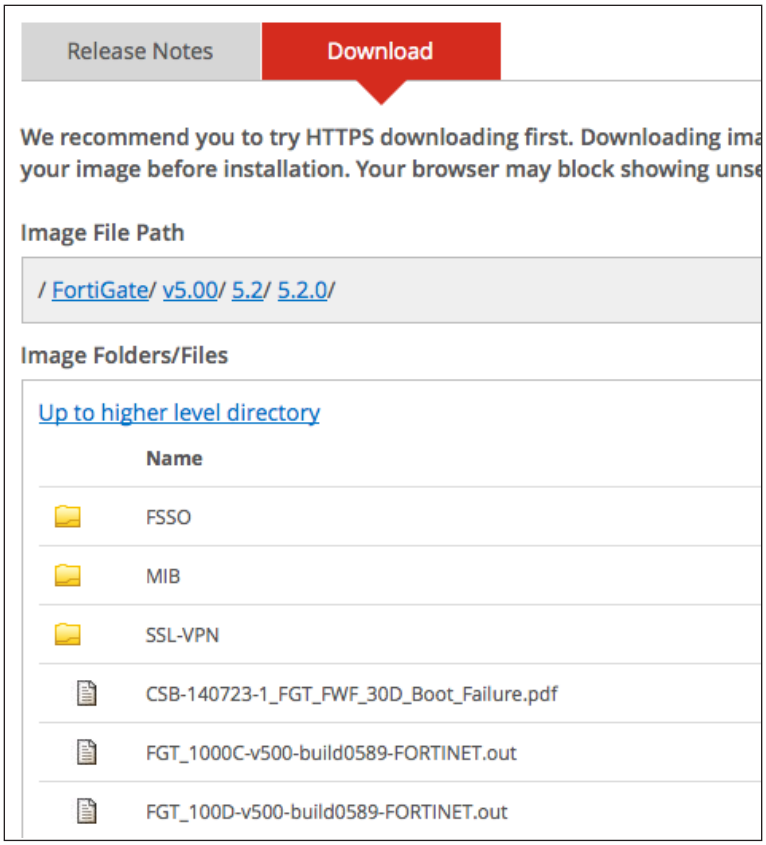
2. Downloading the latest FortiOS firmware

To download a new firmware version, browse to https://support.fortinet.com and log in using your Fortinet account ID/email and password.

Your FortiGate unit must be registered before you can access firmware images from the Support site.

Go to **Download > Firmware Images** from the **Select Product** drop down menu choose **FortiGate**. Locate and download the firmware for your FortiGate model.

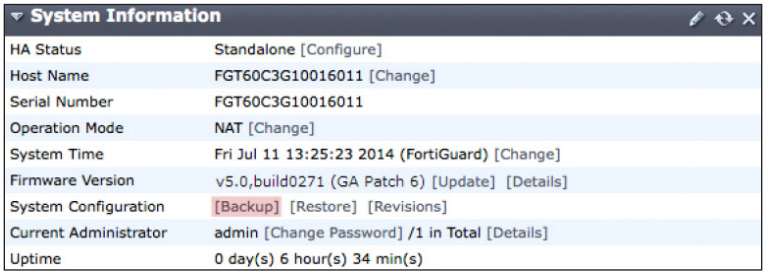




3. Updating the FortiGate to the latest firmware

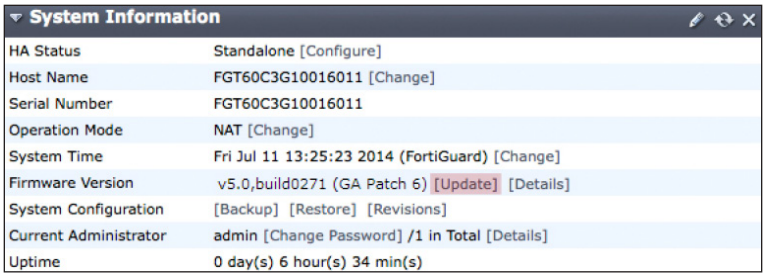
Go to **System > Dashboard > Status**.

Backup your configuration from the **System Information** dashboard widget, next to **System Configuration**. Always remember to back up your configuration before doing any firmware upgrades.



Under **System Information > Firmware Version**, select **Update**.

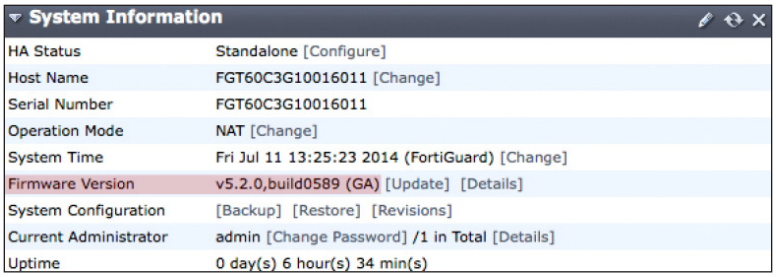
Find the firmware image file that you downloaded and select **OK** to upload and install the firmware build on the FortiGate unit.



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.

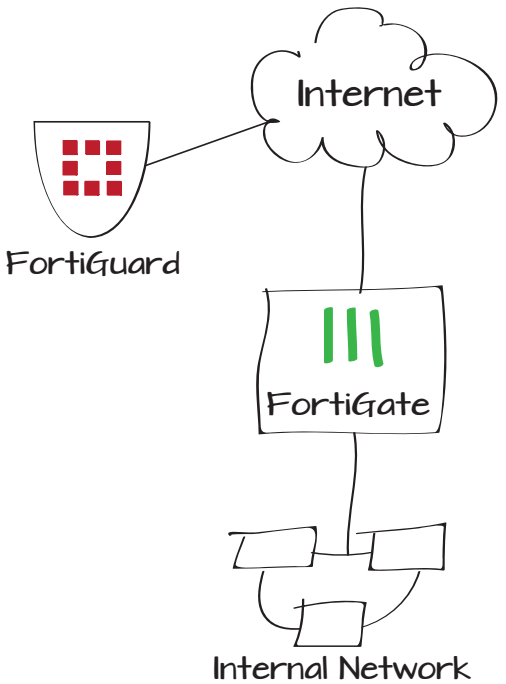
From the FortiGate web-based manager, go to **System > Dashboard > Status**. In the **System Information** dashboard widget, the **Firmware Version** will show the updated version of FortiOS.



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
2. Troubleshooting communication errors
3. Results



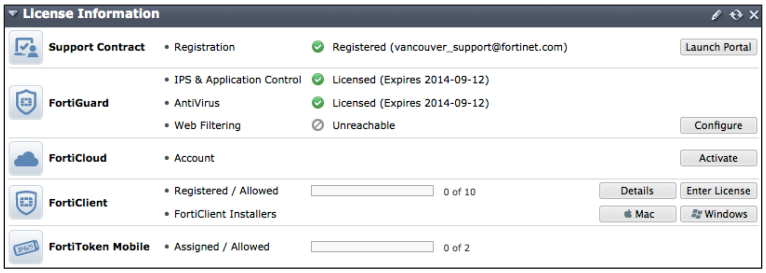
1. Verifying the connection

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

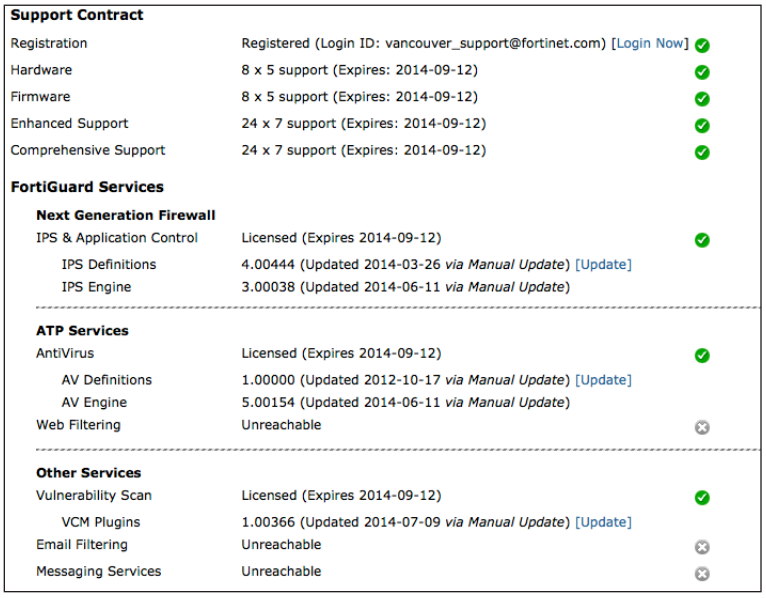
Any subscribed services should have a , indicating that connections are successful.

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

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



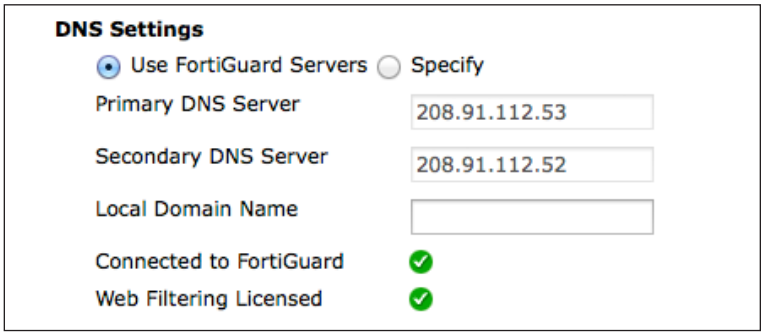
You can also view the FortiGuard connection status by going to **System > Config > FortiGuard**.



2. Troubleshooting communication errors

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

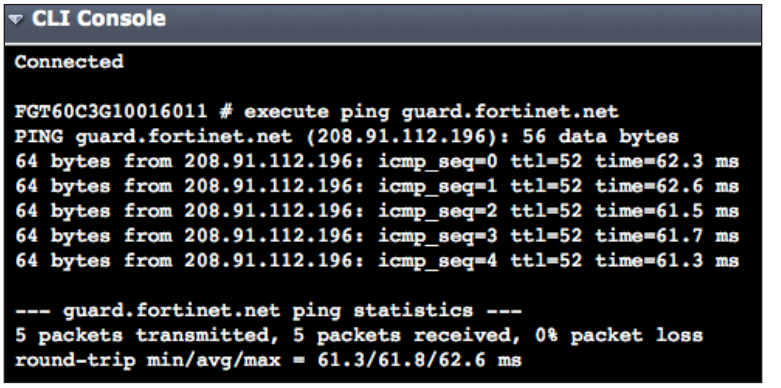
In this screenshot the FortiGate has been successfully tested already.



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**:

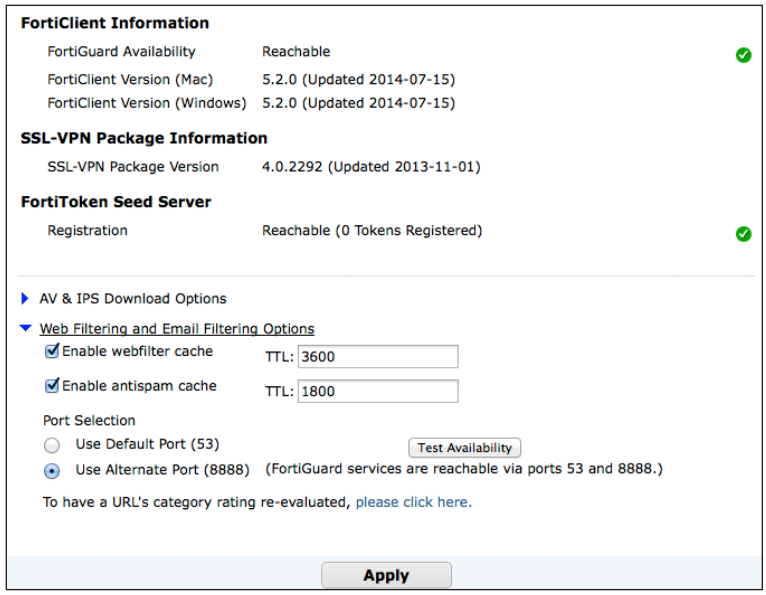
```
execute ping guard.fortinet.net
```

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** click **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)**.

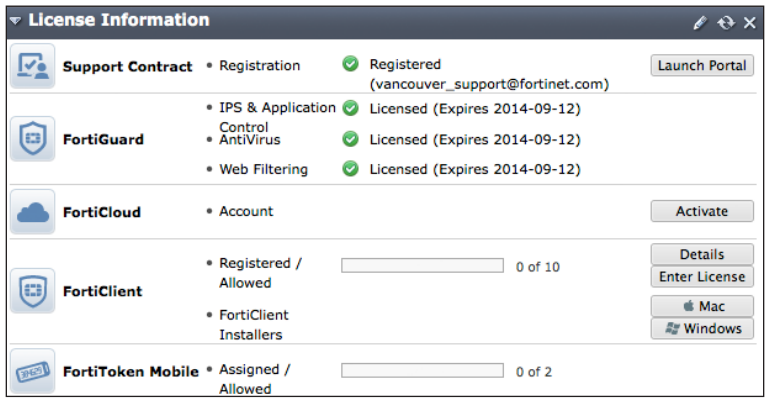


If you are updating using the FortiManager, the FortiGate unit can also use port 80. If further problems occur, you may have to unblock ports using the CLI. See page 480 of the CLI Reference for FortiOS 5.2. for more information.

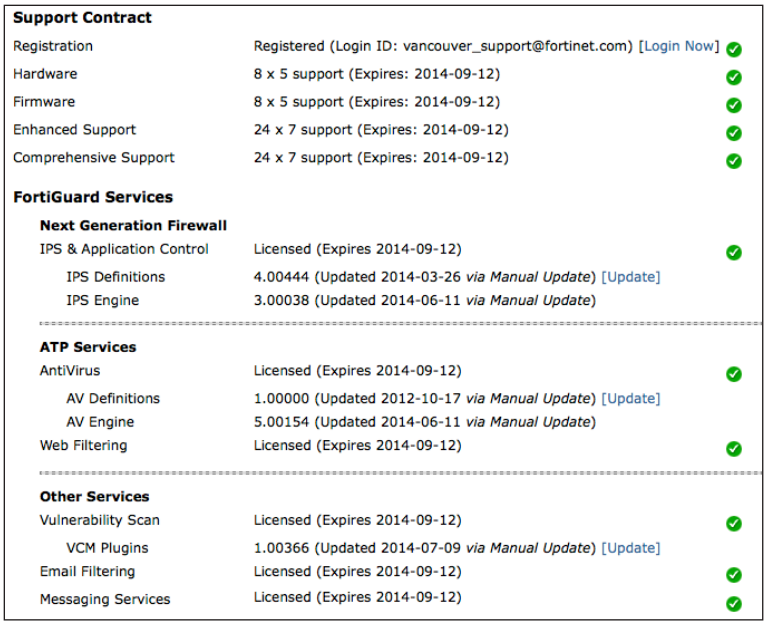
3. Results

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

Any subscribed services should have a ✓, 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 , indicating that connections are successful.



Extra help: FortiGuard

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:

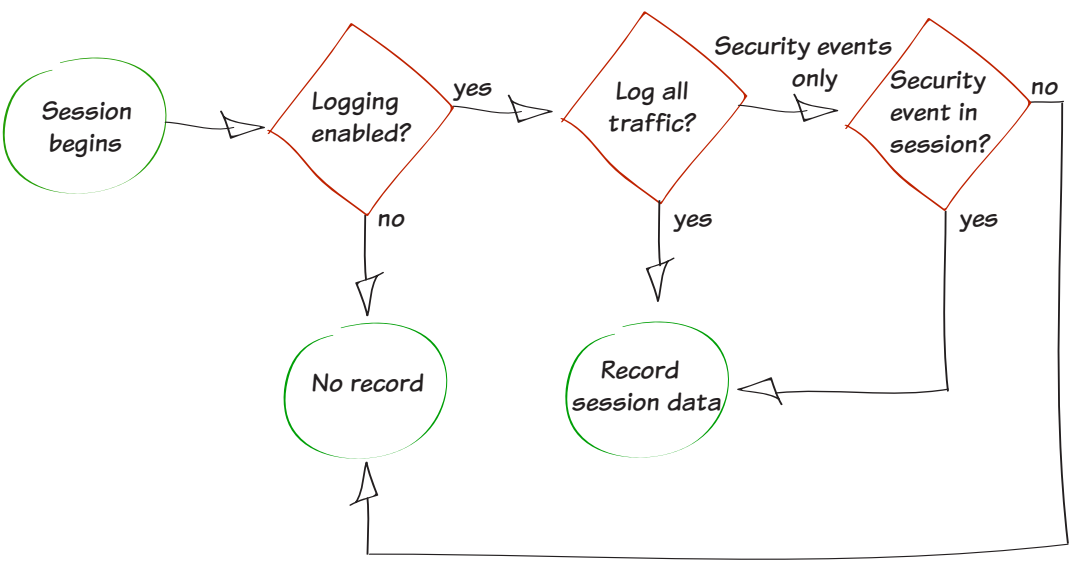
```
config system global
   set ip-src-port-range 2048-20000
end
```

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 network traffic to gather information

This example demonstrates how to 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
2. Enabling logging in the security policies
3. Results



1. Recording log messages and enabling event logging

Go to **Log & Report > Log Config > Log Settings**.

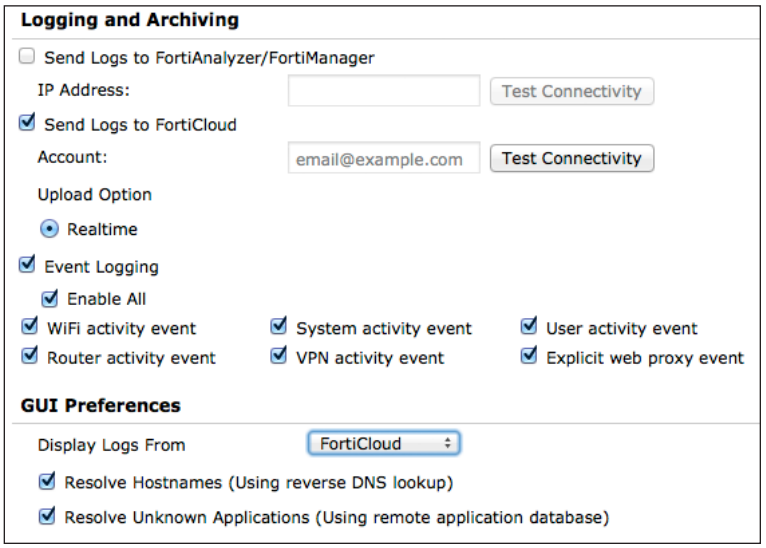
Select where log messages will be recorded. You can save log messages to disk if it is supported by your FortiGate unit, to a FortiAnalyzer or FortiManager unit if you have one, or to FortiCloud if you have a subscription. Each of these options allow you to record and view log messages and to create 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**).

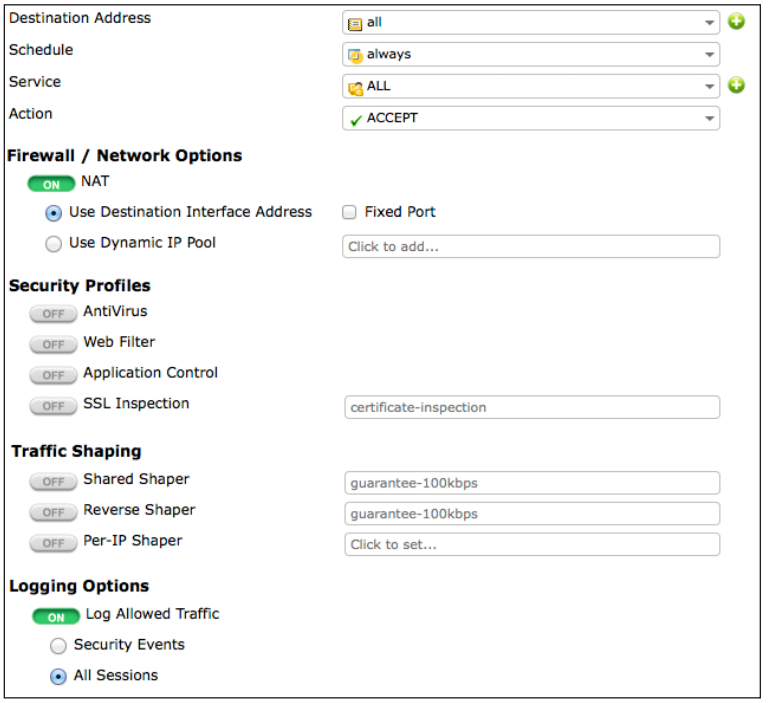


2. Enabling logging in the security policies

Go to **Policy & Objects > Policy > IPV4**. Edit the policies controlling the traffic you wish to log.

Under **Logging Options**, select either **Security Events** or **All Sessions**.

In most cases, you should select Security Events. All Sessions provides detailed traffic analysis but also but requires more system resources and storage space.



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
10:23:02	192.168.1.117	00:0c:29:c2:38:8e	208.91.113.70
10:22:23	192.168.1.117	00:0c:29:c2:38:8e	208.91.112.53
10:22:02	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184
10:20:03	192.168.1.100	00:09:0f:7e:71:fe	208.91.112.53
10:18:58	192.168.1.117	00:0c:29:c2:38:8e	208.91.112.50
10:18:51	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184
10:15:43	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184
10:13:44	192.168.1.100	00:09:0f:7e:71:fe	208.91.112.53
10:12:54	192.168.1.117	00:0c:29:c2:38:8e	208.91.113.70
10:12:32	192.168.1.100	00:09:0f:7e:71:fe	208.91.113.184

Creating and ordering IPv4 security policies to provide network access

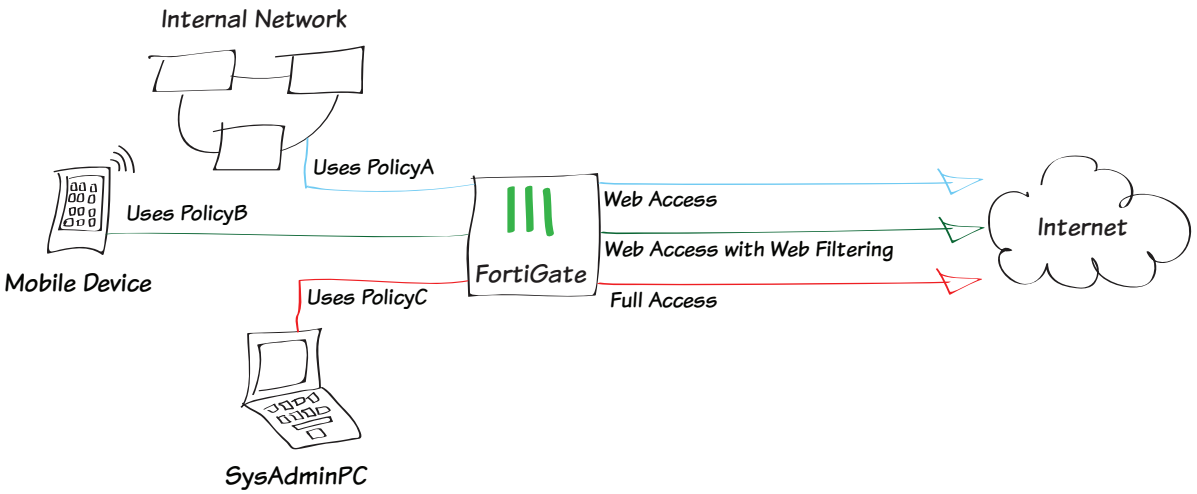
This example shows how to create and order multiple security policies in the policy table, in order to apply the appropriate policy to various types of network traffic.

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.

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

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 "Using a FortiAP in Bridge mode to add wireless access" on page 90.

1. Configuring PolicyA to allow general web access
2. Creating PolicyB to allow access for mobile devices
3. Defining SysAdminPC
4. Creating PolicyC to allow access for SysAdminPC
5. Ordering the policy table
6. Results

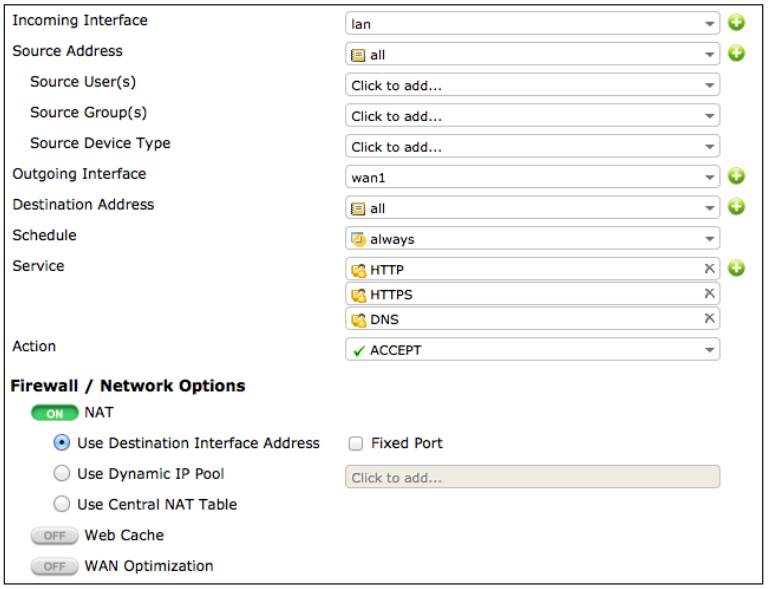


1. Configuring PolicyA to allow general web access

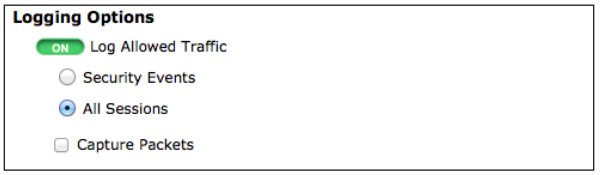
Go to **Policy & Objects > Policy > IPv4** and edit the policy allowing outgoing traffic.

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**.



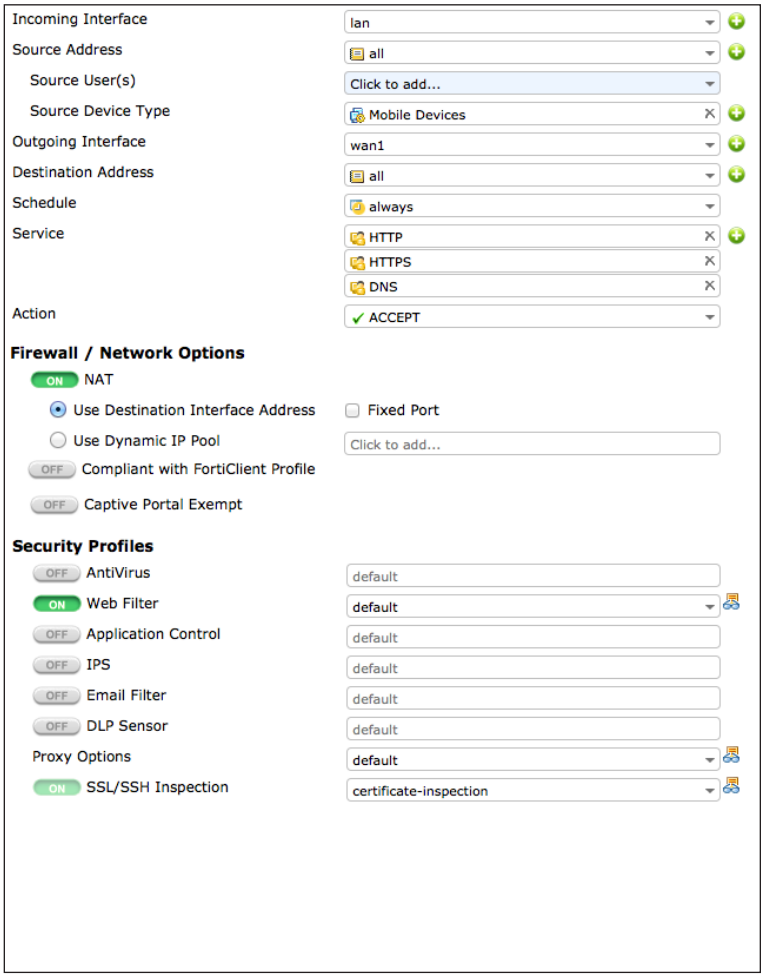
2. Creating PolicyB to allow access for mobile devices

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

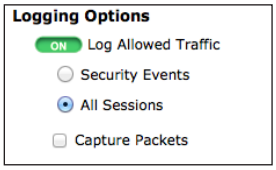
Enable **NAT**.

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.



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

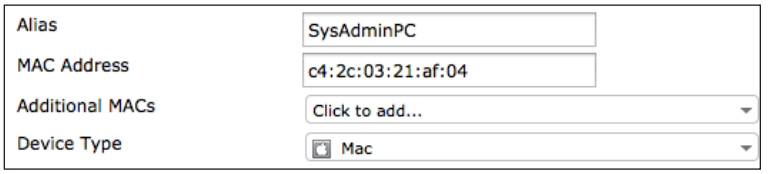
Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.



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**.

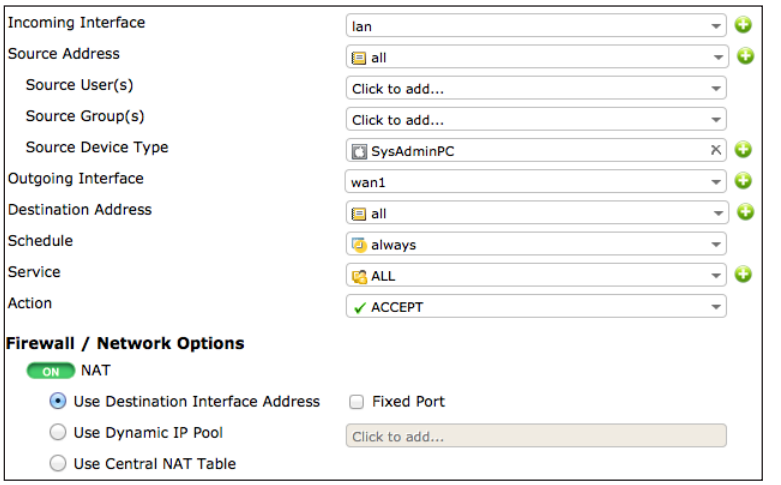


4. Configuring PolicyC to allow access for SysAdminPC

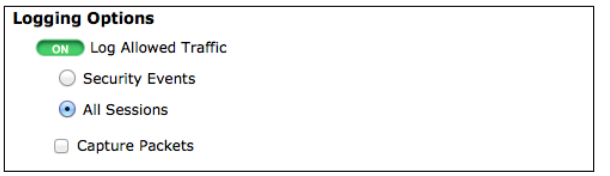
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

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. 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.

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 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 reorder the policies, select any area in the far-left column (in the example, **Seq.#**) for PolicyB and drag the policy to the top of the list. Repeat this for PolicyC, so that the order is now PolicyC, PolicyB, PolicyA, and the default deny policy.

Refresh the page to see the updated **Seq.#** values.

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	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

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.

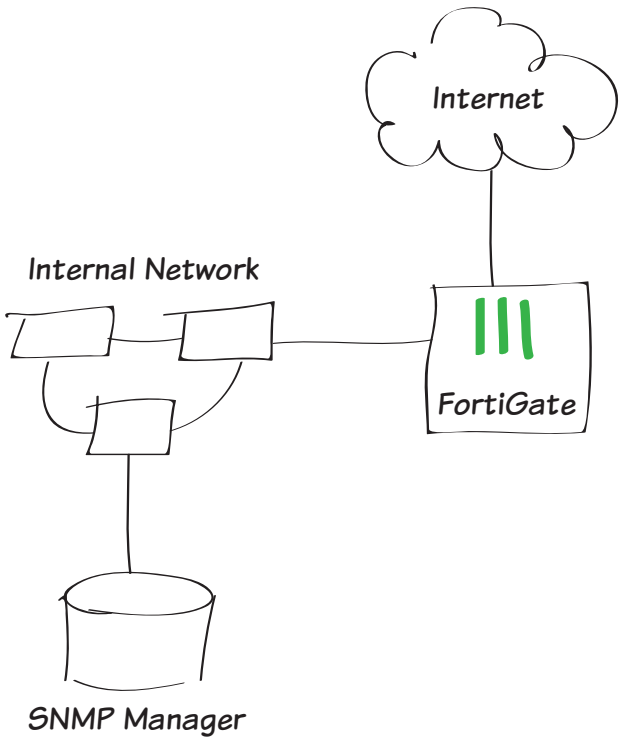
(Optional) Attempt to make an SSL connection to a web server with all three devices. Only the system administrator's PC will be able to connect.

Using SNMP to monitor the FortiGate unit

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

In this example, the FortiGate SNMP agent allows an SNMP manager to receive system information from a FortiGate unit and allows the FortiGate to sent traps to the SNMP manager.

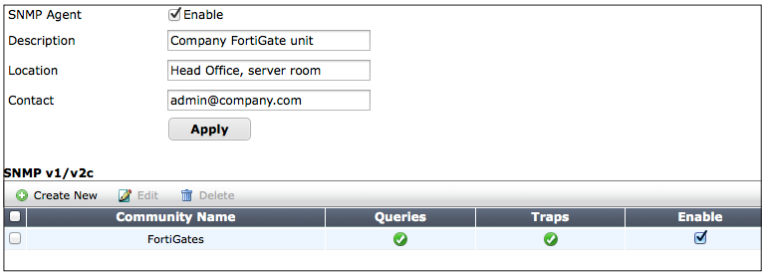
1. Configuring the FortiGate SNMP agent
2. Enabling SNMP on a FortiGate interface
3. Downloading Fortinet MIB files and configuring an example SNMP manager
4. Results



1. Configuring the FortiGate SNMP agent

Go to **System > Config > SNMP**.

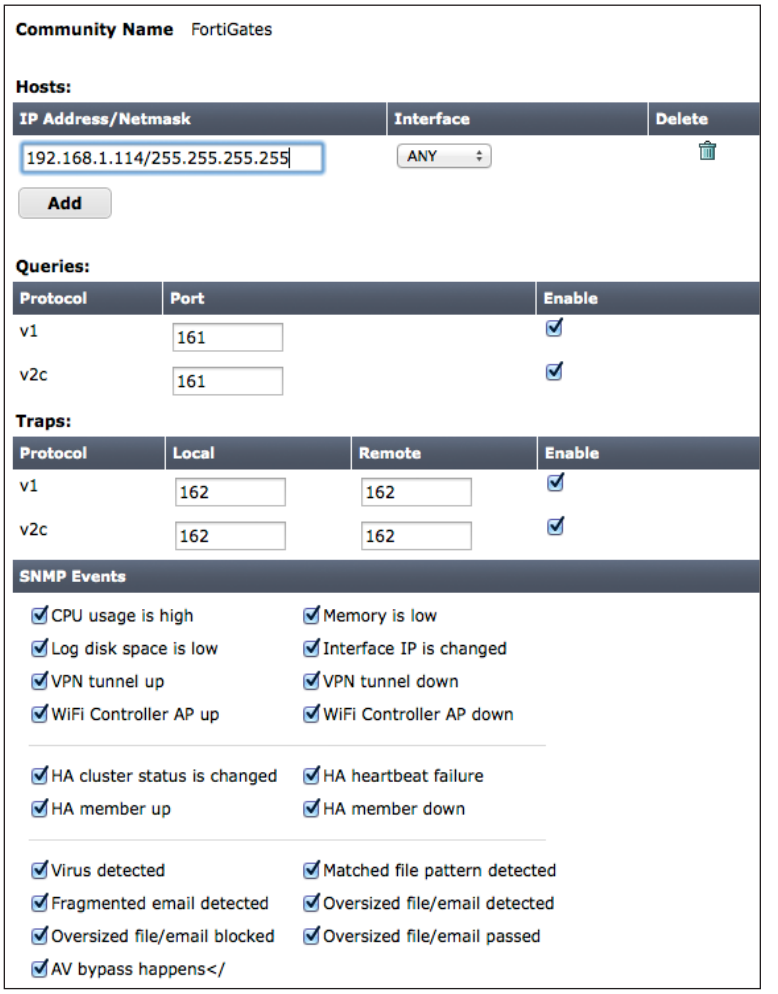
Under **SNMP v1/v2c** click **Create New** to generate a new community.



For the **Hosts**, enter 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.

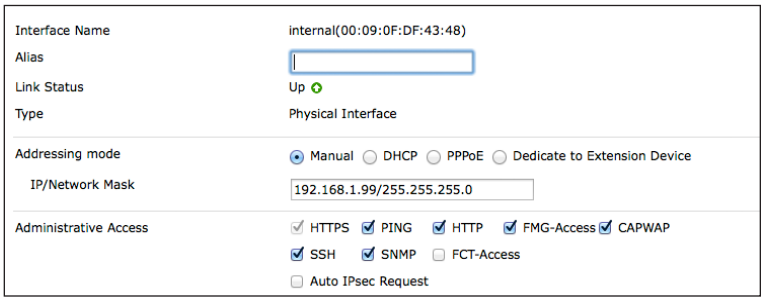
Enable the **SNMP Events** (traps) that you need. In most cases, leave all the options enabled.



2. Enabling SNMP on a FortiGate interface

Go to **System > Network > Interfaces**. Edit an interface that is on the same network as the SNMP manager.

Enable **SNMP Administrative Access** on the interface.



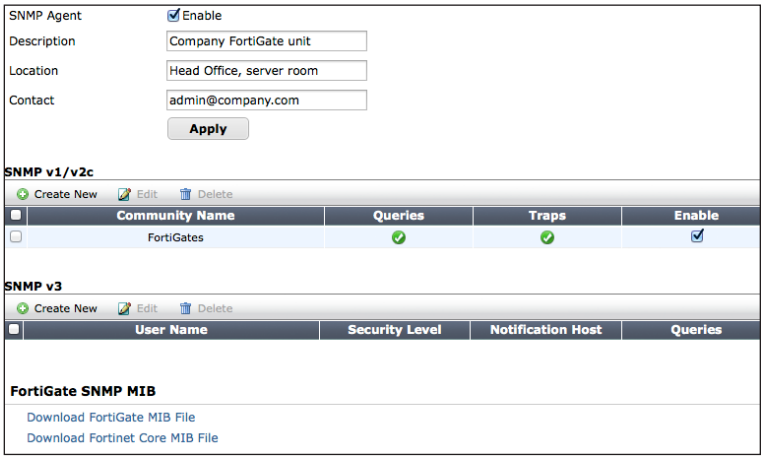
3. Downloading the Fortinet MIB files and configuring an example SNMP manager

Depending on the SNMP manager you are using, you may have to download and install the Fortinet and FortiGate MIB files.

Go to **System > Config > SNMP** to download FortiGate SNMP MIB file and the Fortinet Core MIB file.

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

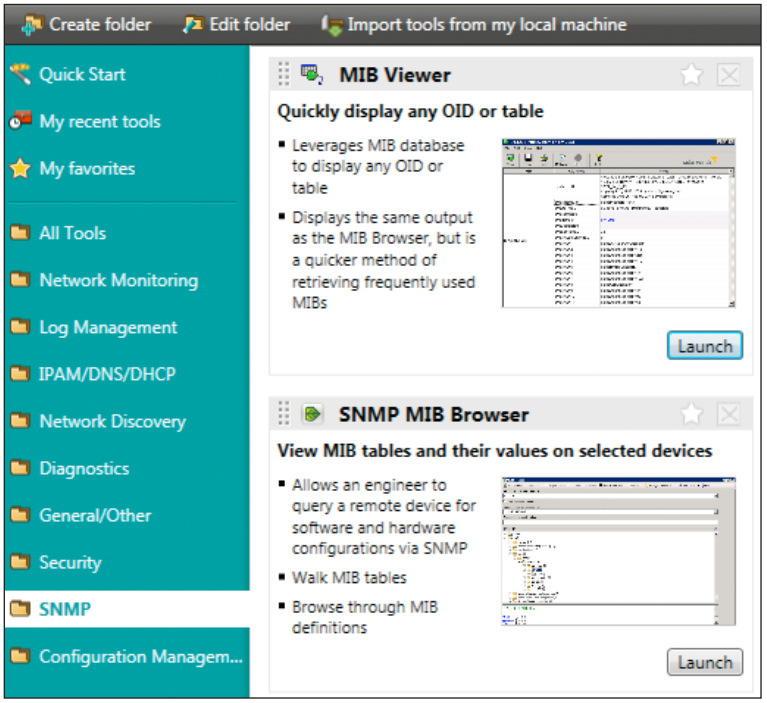
Configure the SNMP manager at 192.168.1.114 to receive traps from the FortiGate unit. Install the FortiGate and Fortinet MIBs if required.



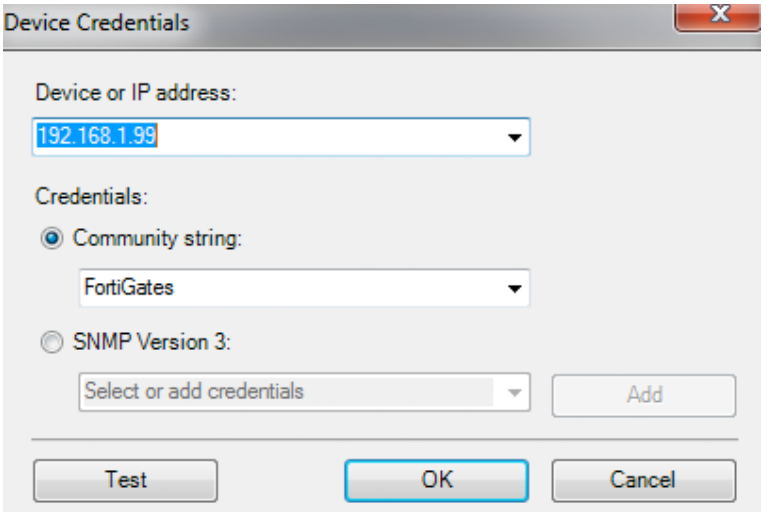
4. Results

This example uses the SolarWinds SNMP trap viewer.

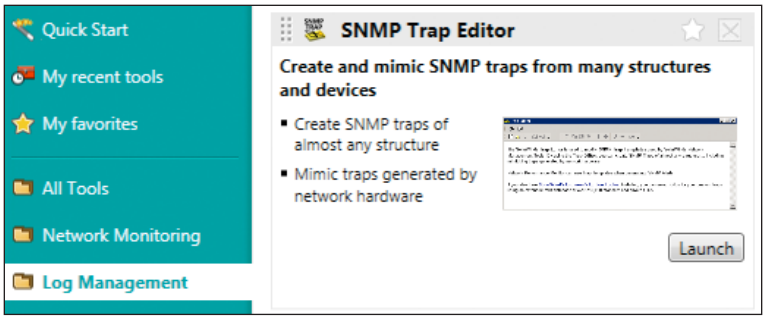
In the SolarWinds Toolset Launch Pad, go to **SNMP > MIB Viewer** and select **Launch**.



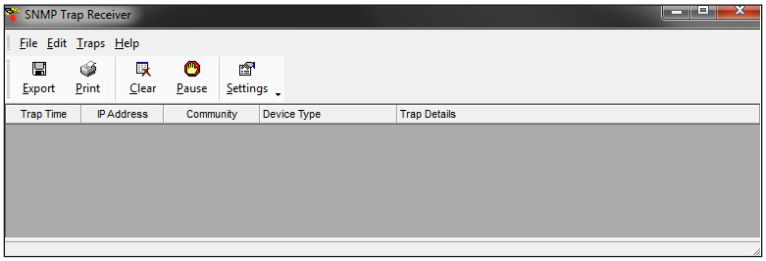
Choose **Select Device**, enter the IP address of the FortiGate unit, and select the appropriate **Community String** credentials.



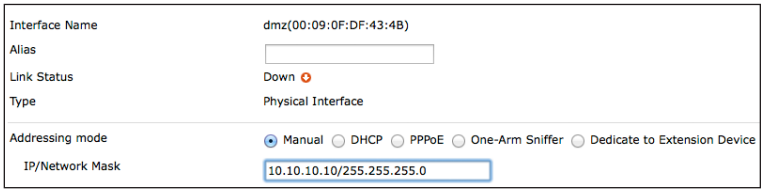
In the SolarWinds Toolset Launch Pad, go to **Log Management > SNMP Trap Receiver** and select **Launch**.



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

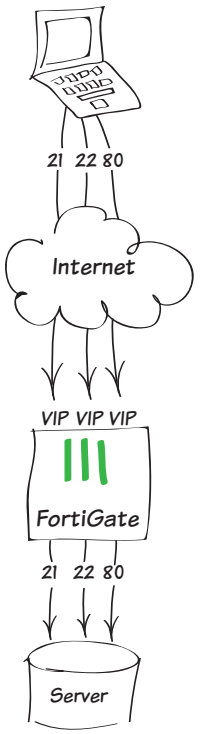
On the FortiGate unit, view log messages showing the trap was sent by going to **Log & Report > Event Log > System**.

cfgpath	system.interface	**Date/Time**	10:49:28 (Fri Mar 8 10:49:28 2013)
Virtual Domain	root	**Level**	information
Timestamp	Fri Mar 8 10:49:28 2013	**cfgtid**	2949201
logid	44547	**Sub Type**	system
User Interface	GUI(172.20.120.21)	**User**	admin
Action	Edit	**cfgobj**	dmz
roll	65409	**cfgattr**	ip[10.10.10.99 255.255.255.0->10.10.10.1 255.255.255.0]
Message	Edit system.interface dmz		

Using port forwarding to allow limited access to an internal server

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.

1. Creating three virtual IPs
2. Adding the virtual IPs to a VIP group
3. Creating a security policy
4. Results

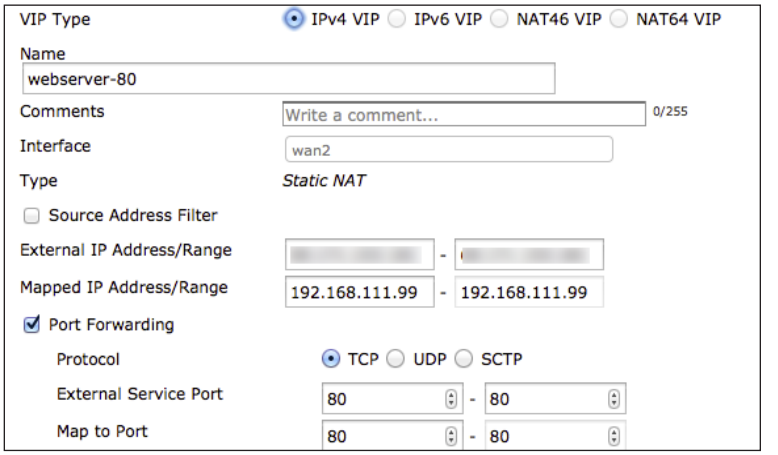


1. Creating three virtual IPs

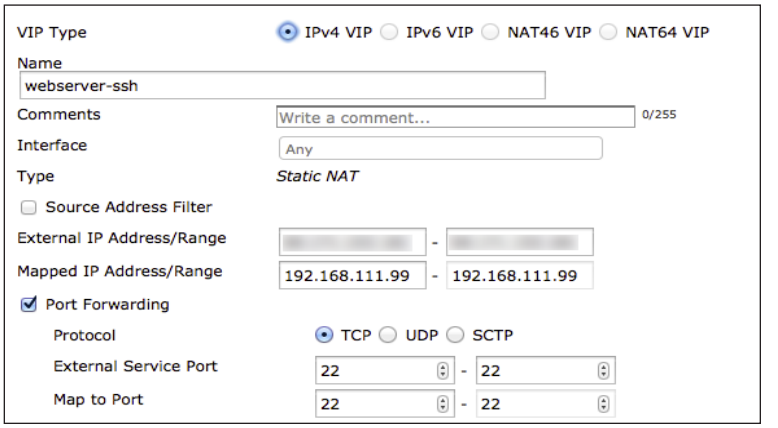
Go to **Policy & Objects > Objects > Virtual IPs > Create New > Virtual IP.**

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

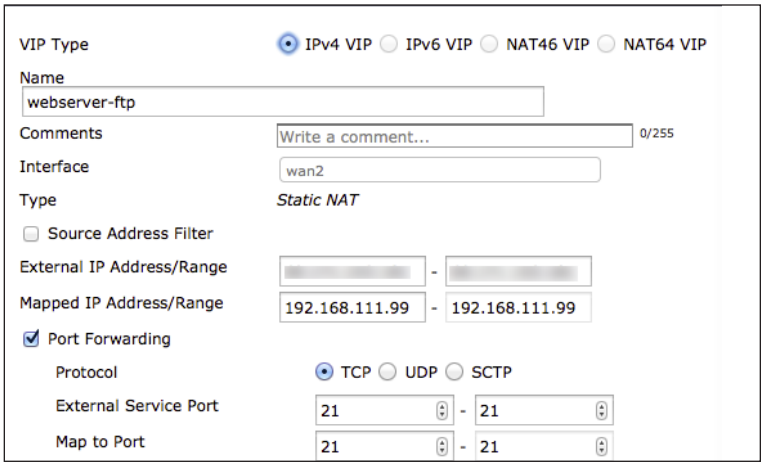
While this example maps port 80 to port 80, any valid External Service port can be mapped to any listening port on the destination computer.



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



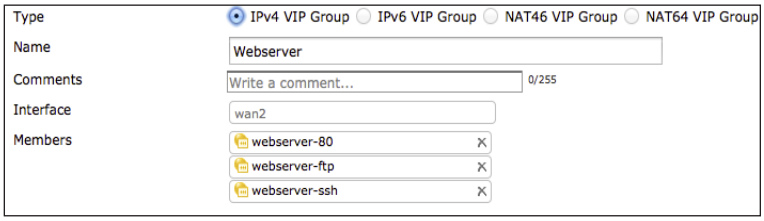
Create a third a virtual IP for TCP port 21. Label this VIP *webserver-ftp*.



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.

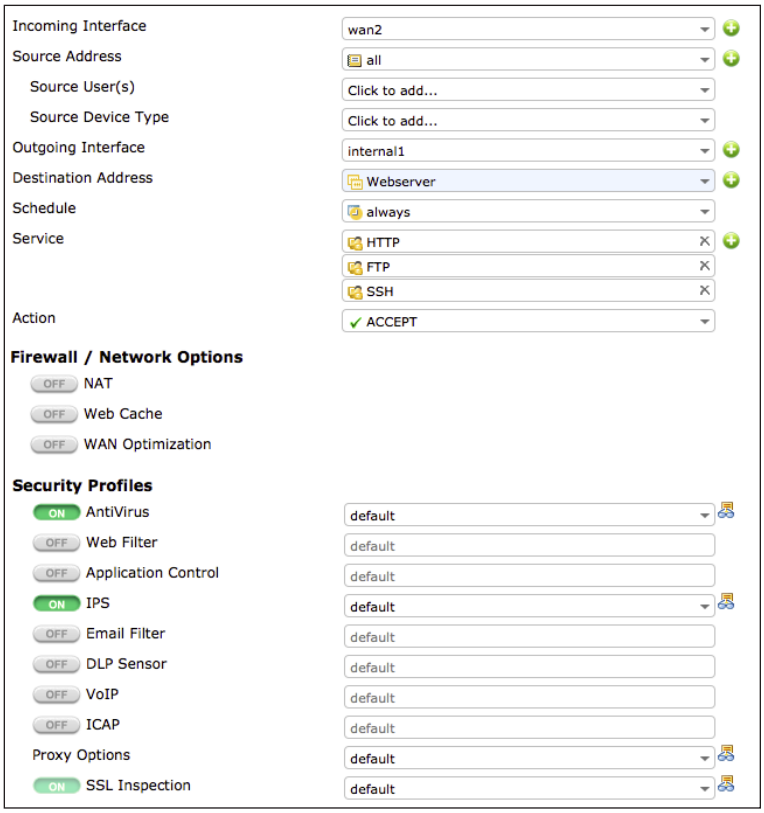


3. Creating a security policy

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

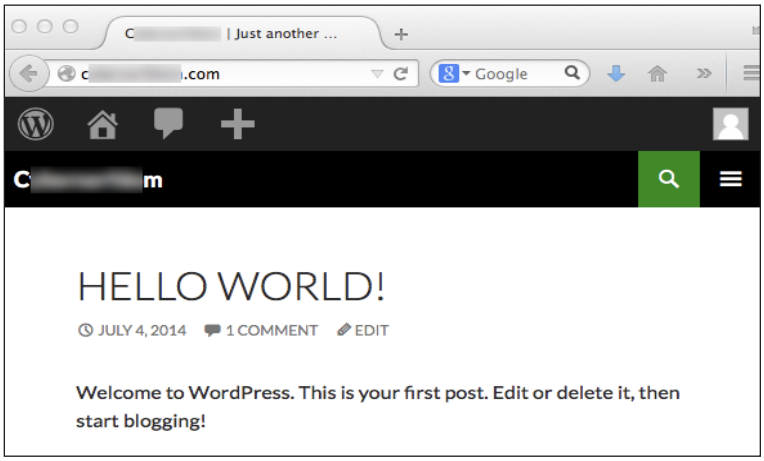
Set **Incoming Interface** to your Internet-facing interface, **Outgoing Interface** to the interface connected to the server, and **Destination** address to the VIP group. Set **Service** to allow **HTTP**, **FTP**, and **SSH** traffic.

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

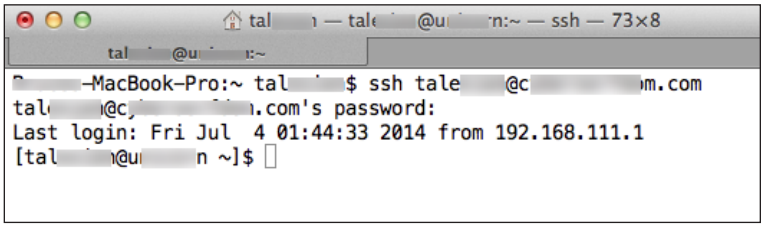


4. Results

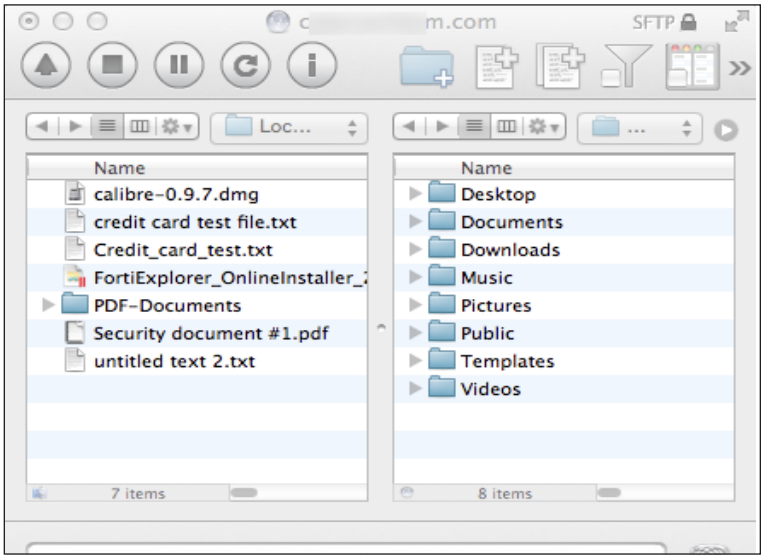
To ensure that TCP port 80 is open, connect to the web server on the other side of the firewall.



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.



Security Features

This section contains information about using a FortiGate's security features, including AntiVirus, Web Filtering, Application Control, Intrusion Protection System (IPS), Email Filtering, and Data Leak Prevention (DLP).

Each security feature has a default profile. You can also create custom profiles to meet the needs of your network. These profiles are then applied to your security policies and used to monitor and, if necessary, block external and internal traffic that is considered risky or dangerous.

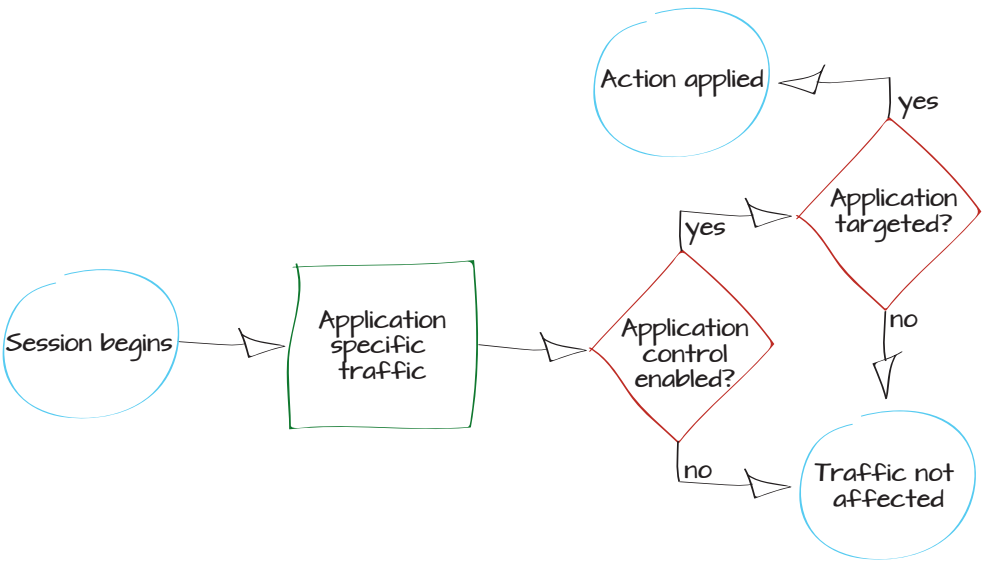
This section contains the following recipes:

- Controlling which applications can access network resources and the Internet
- Using a static URL filter to block access to a specific website
- Preventing security certificate warnings when using SSL full inspection
- Using a custom certificate for SSL inspection

Controlling which applications can access network resources and the Internet

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.

1. Enabling Application Control and multiple security profiles
2. Using the default application profile to monitor network traffic
3. Adding the default profile to a security policy
4. Reviewing the FortiView dashboards
5. Creating an application profile to block applications
6. Adding the blocking sensor to a security policy
7. Results



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.**

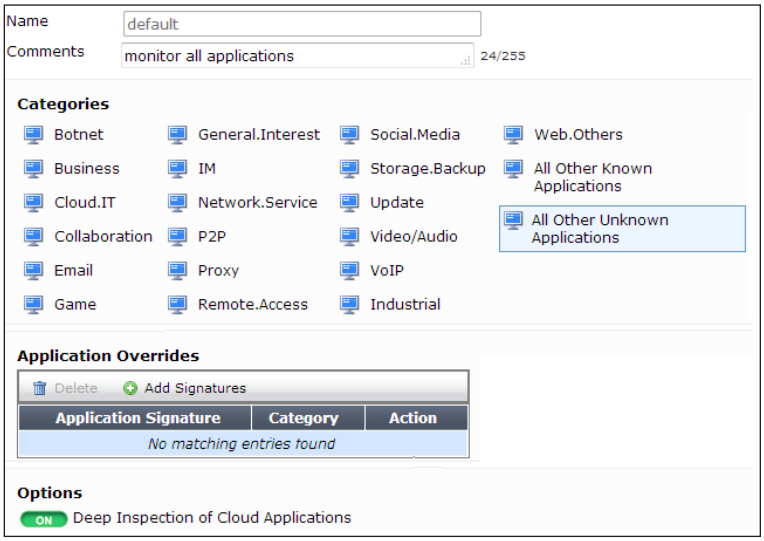
Apply the changes.

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.



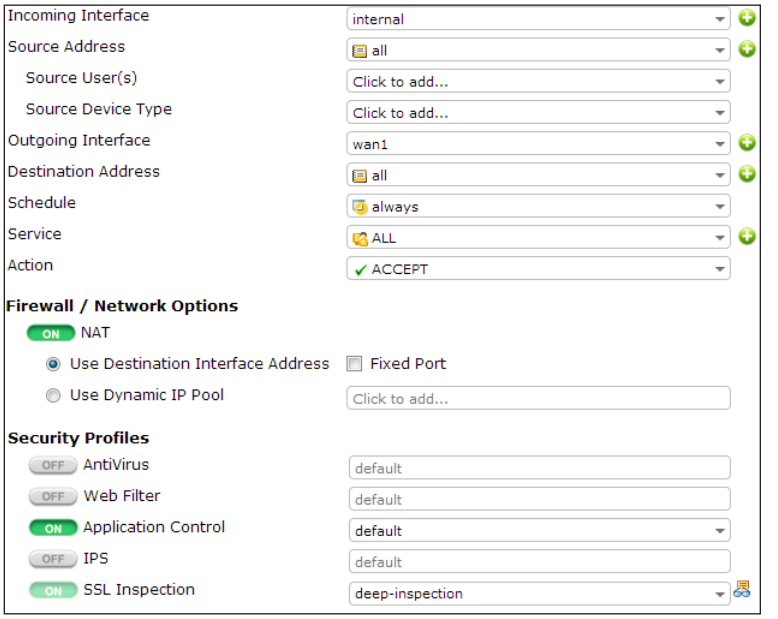
3. Adding the default profile to a security policy

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.

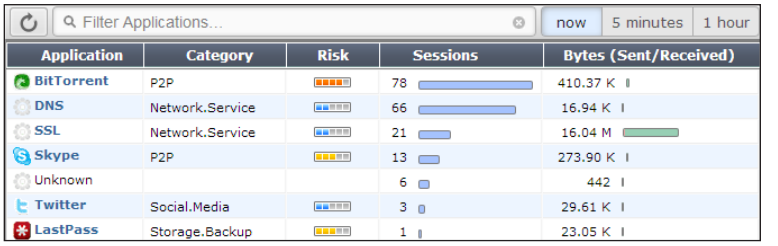
Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see "Preventing security certificate warnings when using SSL full inspection" on page 72.



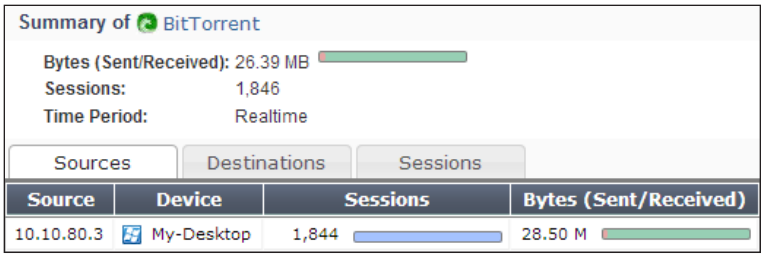
4. Reviewing the FortiView dashboards

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

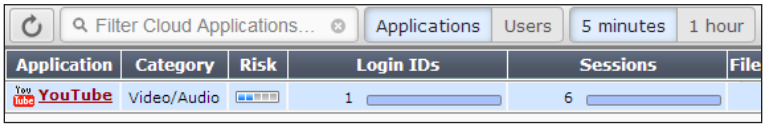
This dashboard shows the traffic that is currently flowing through your FortiGate, arranged by application (excluding Cloud Applications).



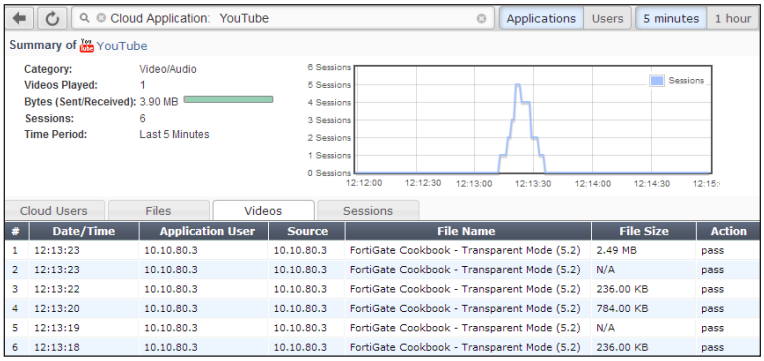
If you wish to know more about an application's traffic, double-click on its entry to view drilldown information, including traffic sources, traffic destinations, and information about individual sessions.



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.



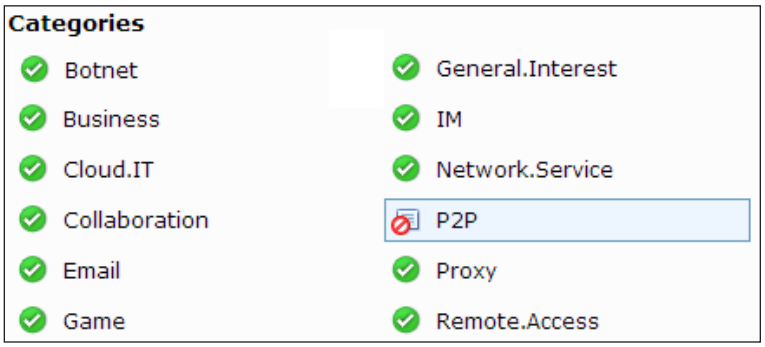
5. Creating an application profile to block applications

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.

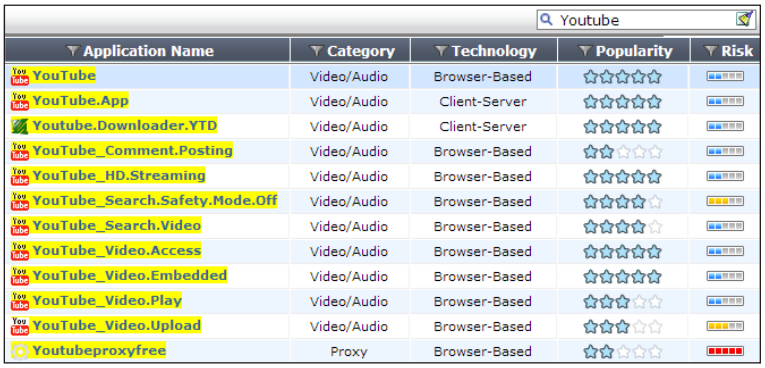
Select the **P2P** category and set it to **Block**.



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

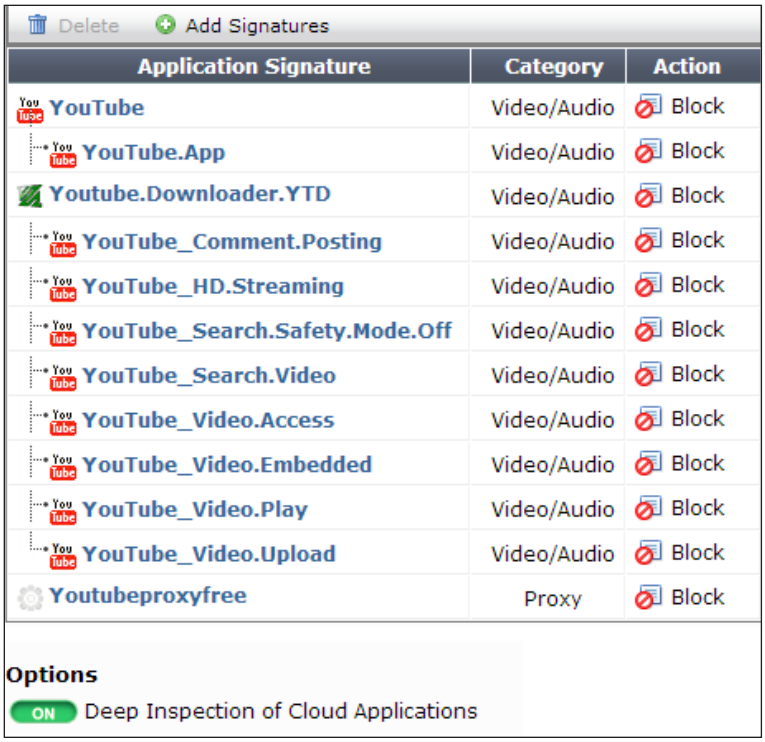
Search for *Youtube* and select all the signatures that are shown.

Select **Use Selected Signatures**.



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

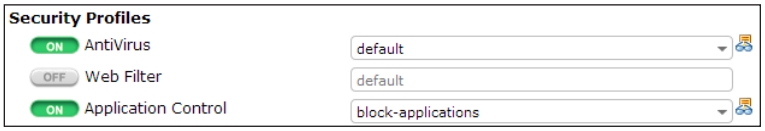
Enable **Deep Inspection of Cloud Applications.**



6. Adding the blocking sensor to a security policy

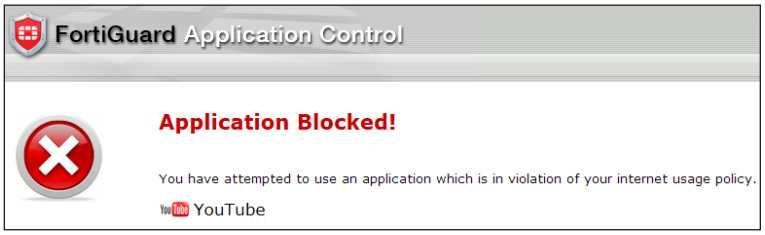
Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet.

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



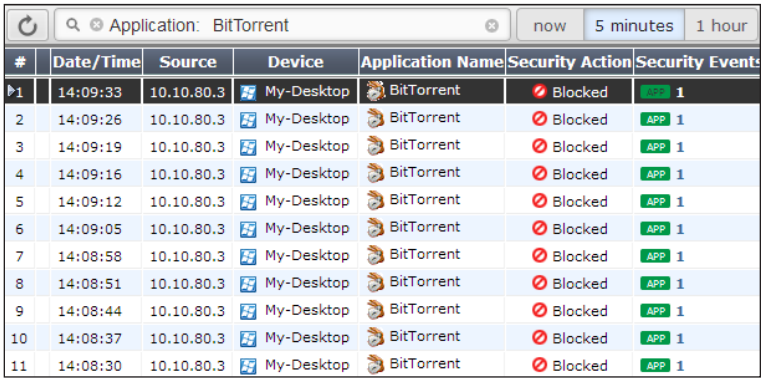
7. Results

Attempt to browse to www.youtube.com. 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.



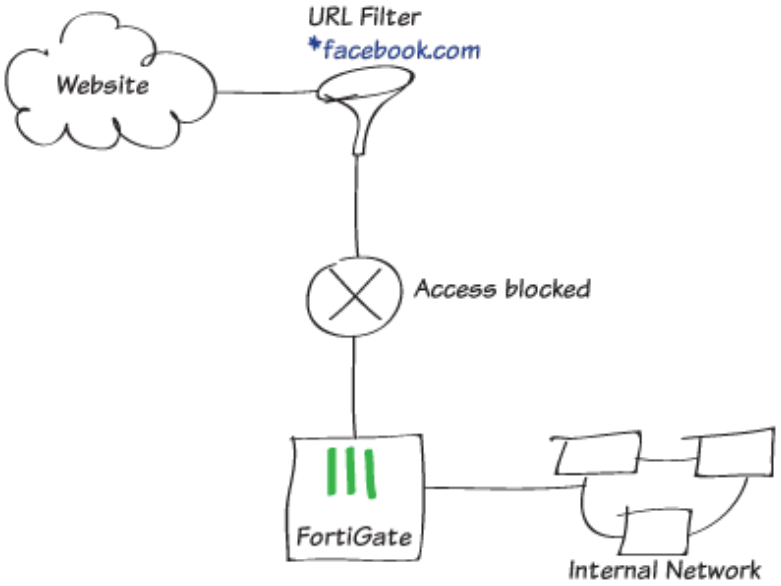
#	Date/Time	Source	Device	Application Name	Security Action	Security Events
1	14:09:33	10.10.80.3	My-Desktop	BitTorrent	Blocked	1
2	14:09:26	10.10.80.3	My-Desktop	BitTorrent	Blocked	1
3	14:09:19	10.10.80.3	My-Desktop	BitTorrent	Blocked	1
4	14:09:16	10.10.80.3	My-Desktop	BitTorrent	Blocked	1
5	14:09:12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

Using a static URL filter to block access to a specific website

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. 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. And by using SSL inspection, you ensure that this website is also blocked when accessed through HTTPS protocol.

This example uses IPv4 security policies, but this method also works with IPv6 policies. Simply substitute any IPv4 configurations with IPv6 configurations.

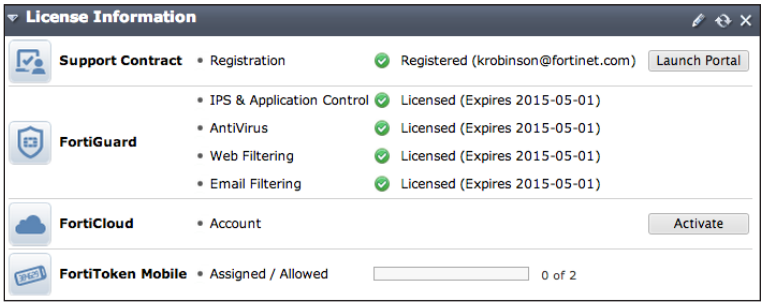
1. Verifying FortiGuard Services subscription
2. Editing the Web FIter profile
3. Verifying the SSL inspection profile
4. Creating a security policy
5. Results



1. Verifying FortiGuard Services subscription

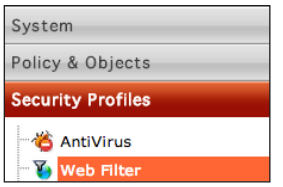
Go to **System** > **Dashboard** > **Status**.

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.

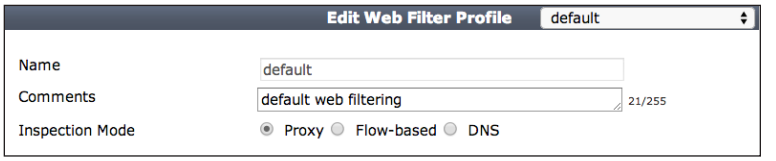


2. Editing the Web Filter profile

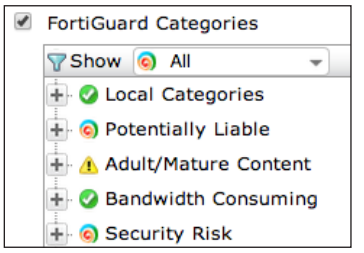
Go to **Security Profiles** > **Web Filter** and edit the default Web Filter profile.



Set **Inspection Mode** to **Proxy**.

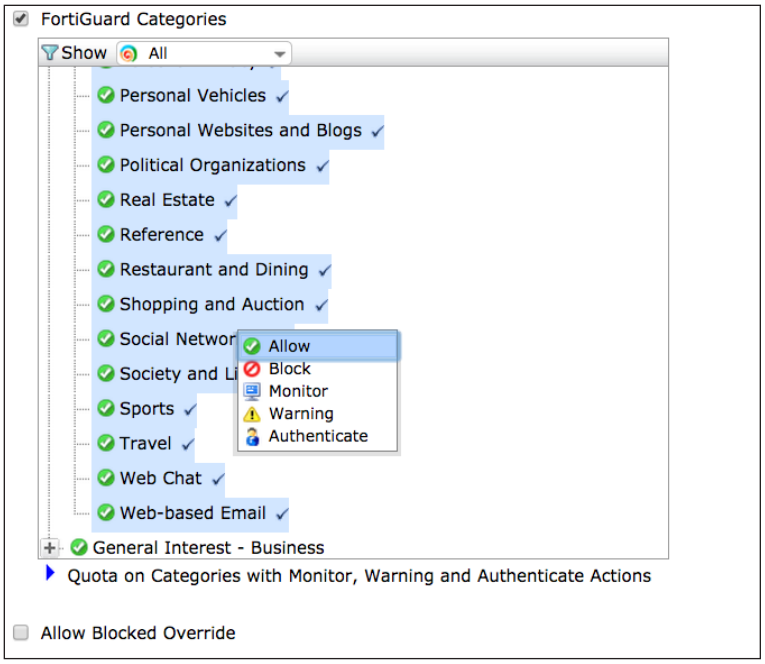


Enable the **FortiGuard Categories** that allow, block, monitor, warn, or authenticate depending on the type of content.

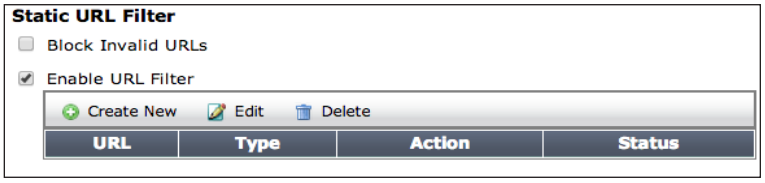


Learn more about FortiGuard Categories at the FortiGuard Center web filtering rating page: www.fortiguard.com/static/webfiltering.html

Under FortiGuard Categories, go to **General Interest - Personal**. Right-click on the **Social Networking** subcategory and ensure it is set to **Allow**.

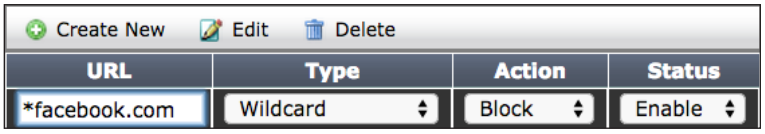


To prohibit visiting one particular social networking site in that category, go to **Static URL Filter**, select **Enable URL Filter**, and then click **Create New**.



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
```



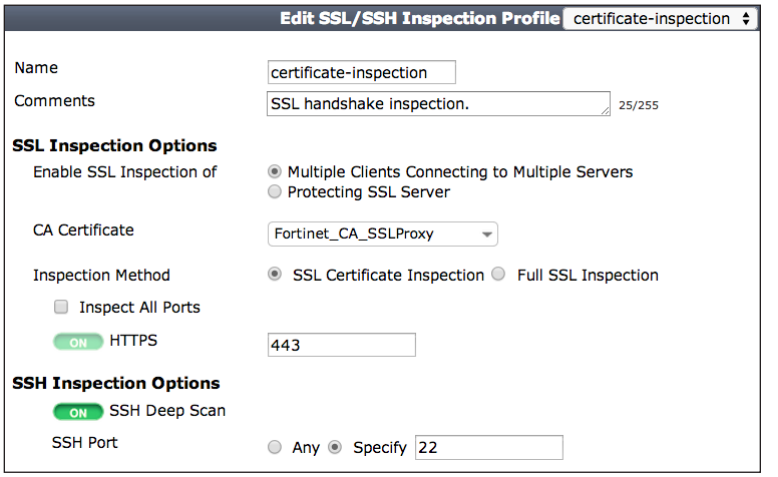
Set **Type** to **Wildcard**, set **Action** to **Block**, and set **Status** to **Enable**.

3. Verifying the SSL inspection profile

Go to **Policy & Objects > Policy > SSL Inspection** and edit the **certificate-inspection** profile.

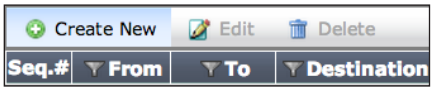
Ensure that **CA Certificate** is set to the default **Fortinet_CA_SSLProxy**.

Ensure **Inspection Method** is set to **SSL Certificate Inspection** and **SSH Deep Scan** is set to **ON**.



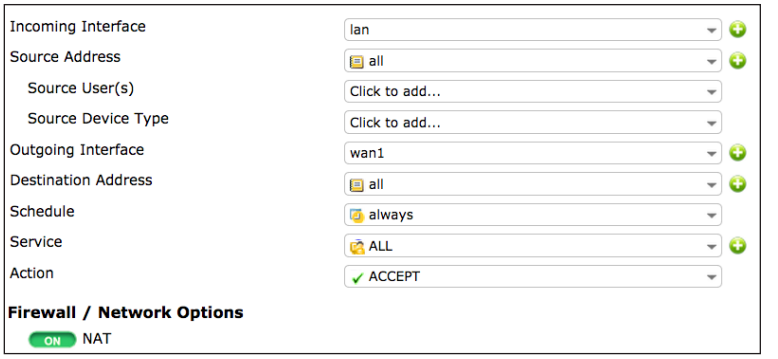
4. Creating a security policy

Go to **Policy & Objects > Policy > IPv4**, and click **Create New**.

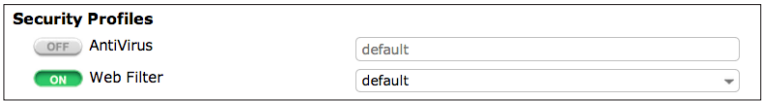


Set the **Incoming Interface** to allow packets from your internal network and set the **Outgoing Interface** to proceed to the Internet-facing interface (typically **wan1**).

Enable **NAT**.

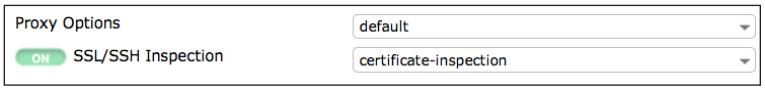


Under **Security Profiles,** enable **Web Filter** and select the **default** web filter.

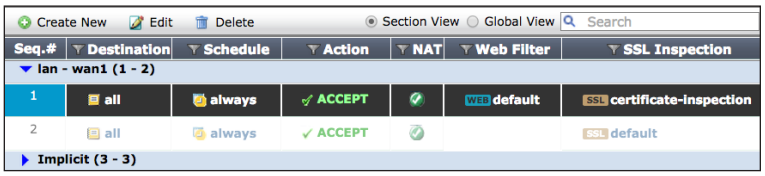


This automatically enables **SSL/SSH Inspection**.

Select **certificate-inspection** from the dropdown menu.



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.



5. Results

Visit the following sites to verify that your web filter is blocking websites ending in facebook.com:

- facebook.com
- attachments.facebook.com
- upload.facebook.com
- camdencc.facebook.com
- mariancollege.facebook.com

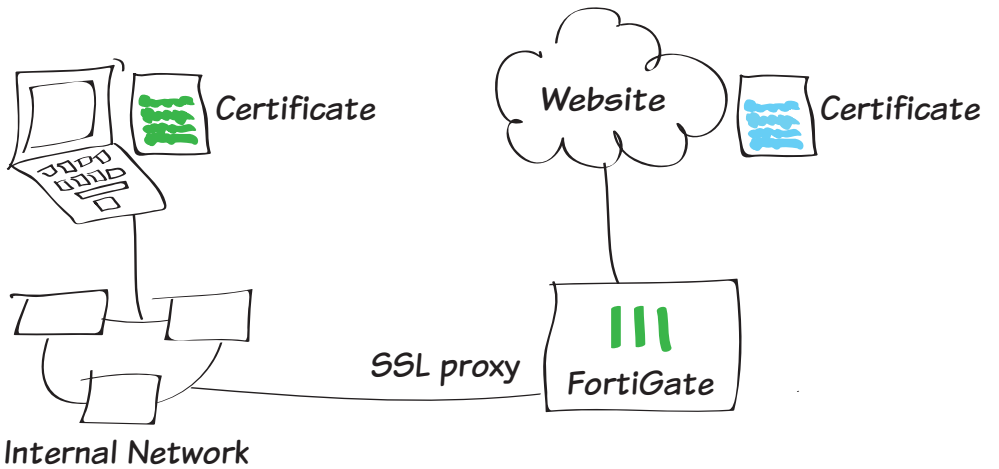
A FortiGuard **Web Page Blocked!** page should appear.

Visit https://www.facebook.com to verify that HTTPS protocol is blocked. A **Web Page Blocked!** page should appear.

Preventing security certificate warnings when using SSL full inspection

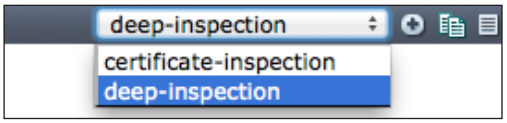
This example illustrates how to prevent your users from getting a security certificate warning when you have enabled full SSL inspection (also called deep inspection). Instead of having users select **Continue** when they receive an error, a bad habit to encourage, you will provide them with the FortiGate SSL CA certificate to install on their browsers. The certificate error only occurs when SSL inspection uses the deep-inspection profile.

1. Viewing the deep-inspection SSL profile
2. Enabling certificate configuration in the web-based manager
3. Downloading the Fortinet_CA_SSLProxy certificate
4. Importing the CA certificate into the web browser
5. Results



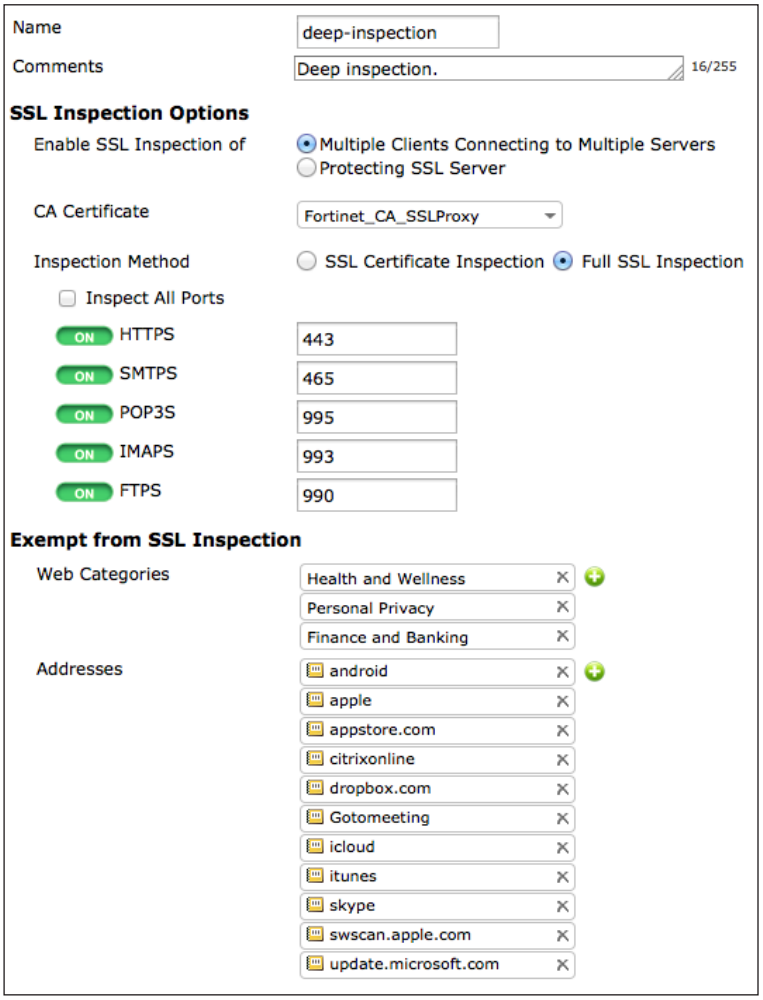
1. Viewing the deep-inspection SSL profile

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.



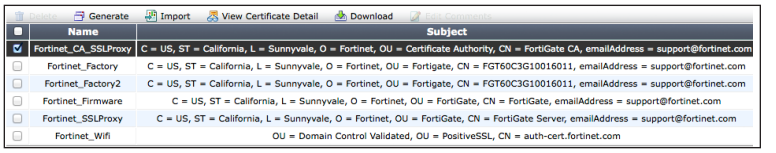
2. Enabling certificate configuration in the web-based manager

Go to **System > Config > Features**. Click **Show More**, enable **Certificates**, and **Apply**.

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.

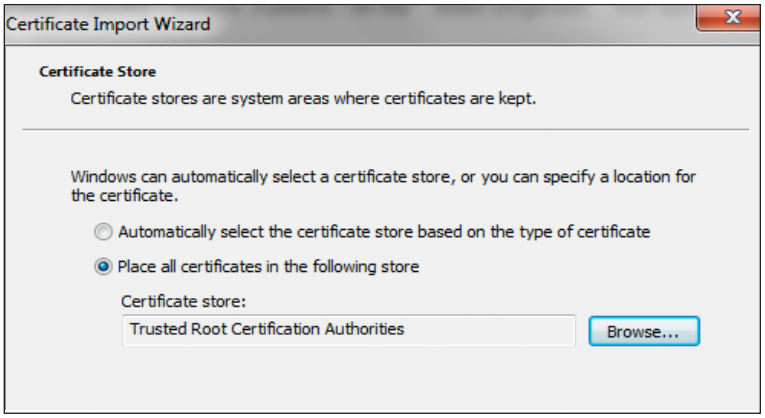


4. Importing the CA certificate into the web browser

For Internet Explorer:

Go to **Tools > Internet Options**. On the **Content** tab, select **Certificates** and find the **Trusted Root Certification Authorities**.

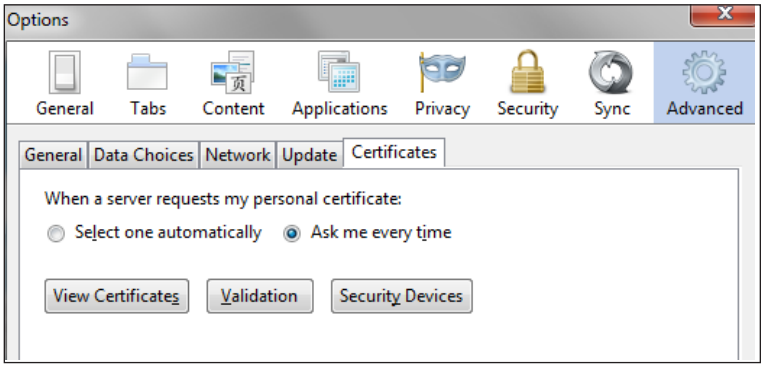
Import the certificate using the Import Wizard. Make sure that the certificate is imported into Trusted Root Certification Authorities.



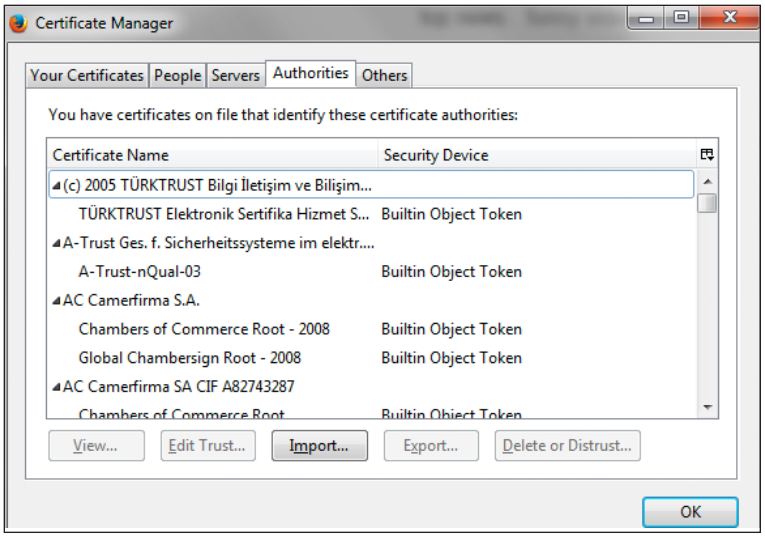
You will see a warning because the FortiGate unit's certificate is self-signed. It is safe to select **Yes** to install the certificate.

For Firefox:

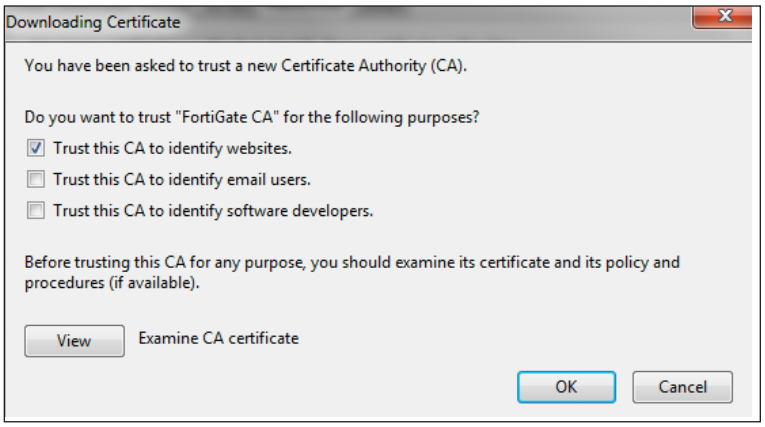
Depending on the platform, go to **Menu > Options or Preferences > Advanced** and find the **Certificates** tab.



Click **View Certificates**, specifically the **Authorities** certificate list

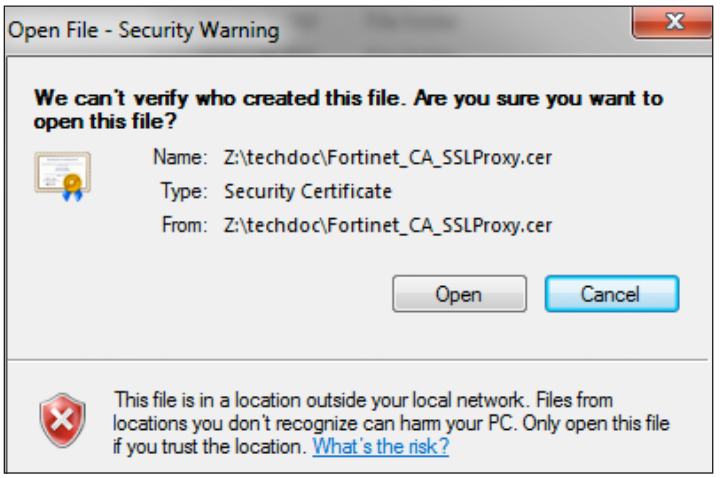


Click **Import** and select the Fortinet_ CA_SSLProxy certificate file.



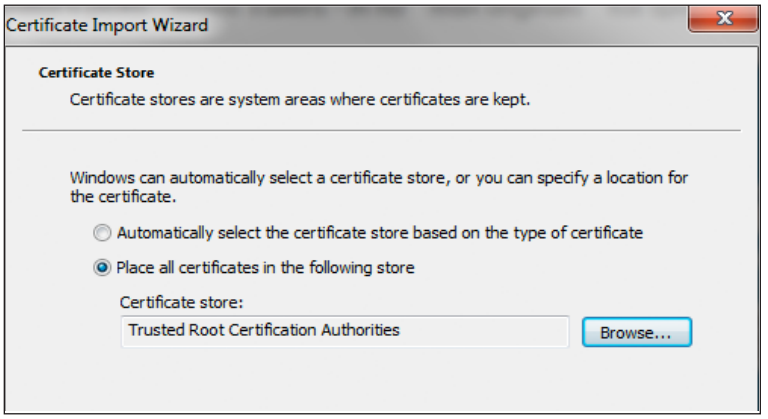
For Google Chrome and Safari:

Locate and open the downloaded Fortinet_CA_SSLProxy certificate file. Choose **Open** and click **Install Certificate**. The Import Wizard appears.



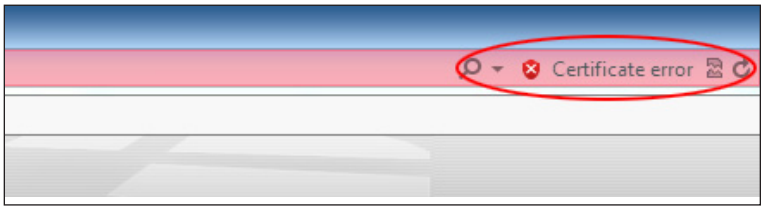
Import the certificate using the Import Wizard. Make sure that the certificate is imported into **Trusted Root Certification Authorities**.

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.

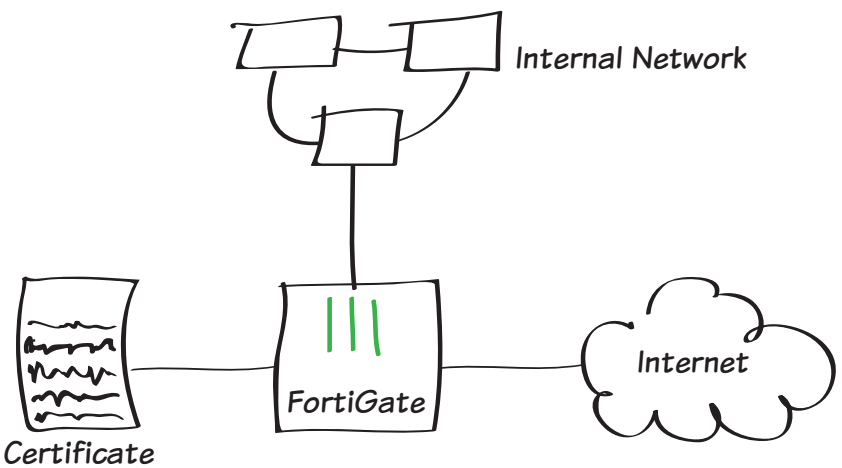
iTunes will now be able to run without a certificate error.

Using a custom certificate for SSL inspection

This recipe shows how use a FortiGate unit to generate a custom certificate signing request and to get this certificate signed by an enterprise root Certificate Authority (CA). This recipe also shows how to import the CA-signed certificate back into your FortiGate and how to add the certificate to an SSL inspection profile.

A certificate with *CA=TRUE* and/or *KeyUsage=CertSign* present in the metadata is necessary to perform deep inspection. By importing a custom certificate from a recognized third-party CA, you create a chain of trust that does not exist when the FortiGate's default certificate is used. This allows network users to trust the FortiGate as a CA in its own right.

1. Generating a certificate signing request (CSR)
2. Importing a signed server certificate from an enterprise root CA
3. Creating an SSL inspection profile
4. Configuring a firewall policy
5. Results



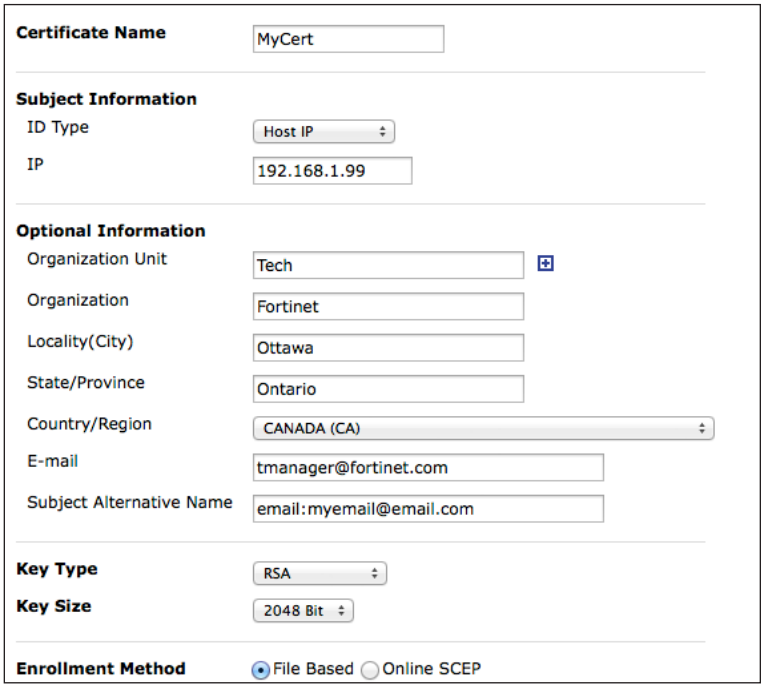
1. Generating a certificate signing request (CSR)

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 **Organization Units**.

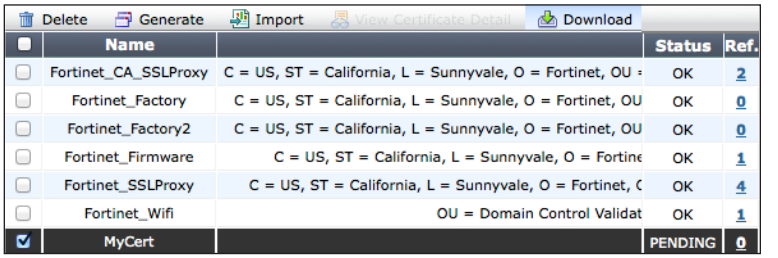
You may enter **Subject Alternative Names** for which the certificate is valid. Separate the names using commas.

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**.

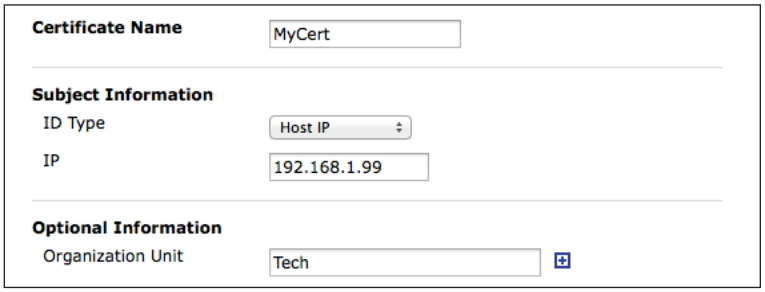
This CSR will need to be submitted and signed by an enterprise root CA before it can be used. When submitting the file, ensure that the template for a **Subordinate Certification Authority** is used.



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.

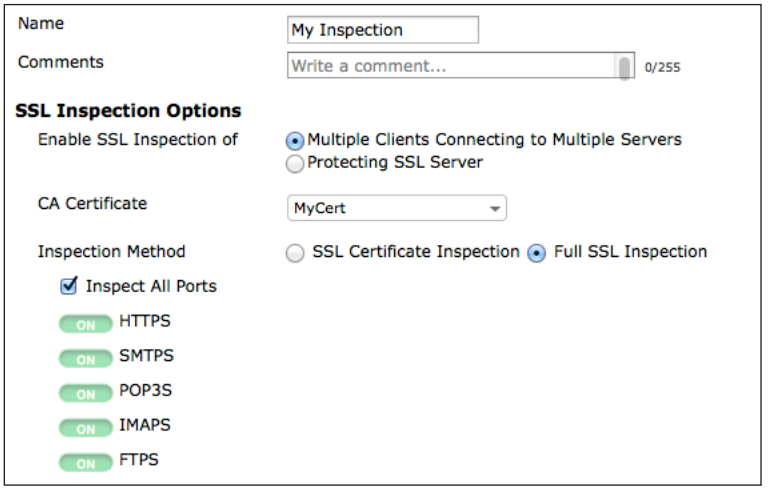
You can also use the FortiGate unit's default certificate. For information about using the default certificate, see "Preventing security certificate warnings when using SSL full inspection" on page 72.

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. 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, see “Preventing security certificate warnings when using SSL full inspection” on page 72.

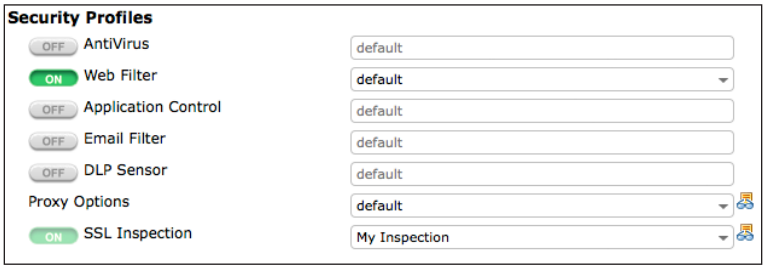


If the certificate does not appear in the list, verify that the template used to sign the certificate was for a CA and not simply for user or server identification.

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.

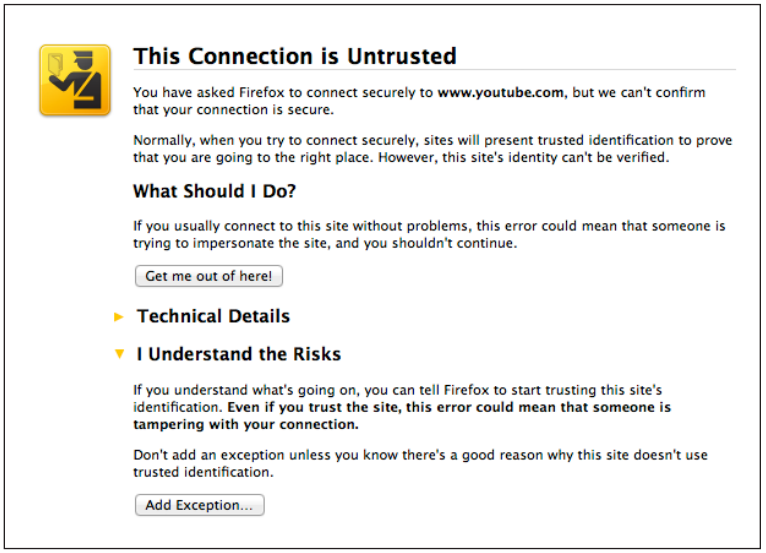
Under **Security Profiles**, ensure that **SSL Inspection** and **Web Filter** are **On**. From the **SSL Inspection** dropdown menu, select your new profile. The **Web Filter** can remain as **default**.



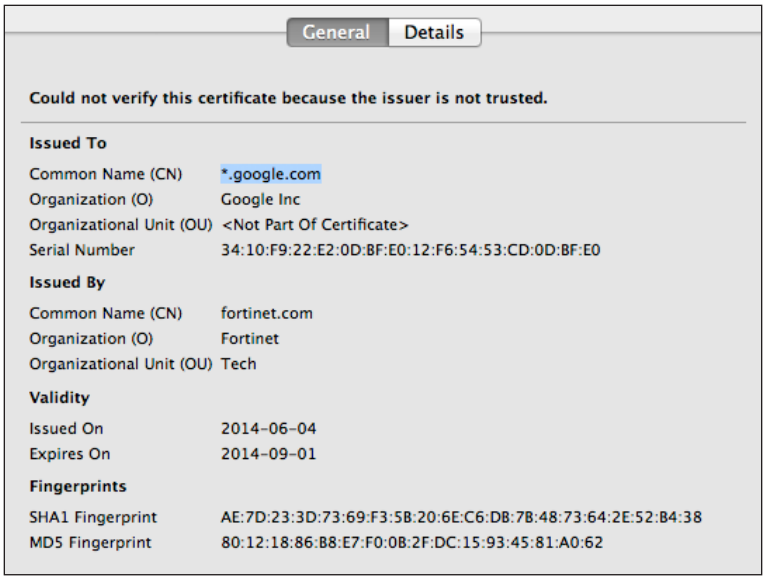
5. Results

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 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.

Wireless Networking

This section contains information about adding wireless to your network.

FortiOS WiFi networking provides a wide range of capabilities for integrating wireless networks into your organization's network architecture. Each WiFi network, or SSID, is represented by a virtual network interface to which you can apply firewall policies, security profiles, and other features in the same way you would for physical wired networks.

This section contains the following recipes:

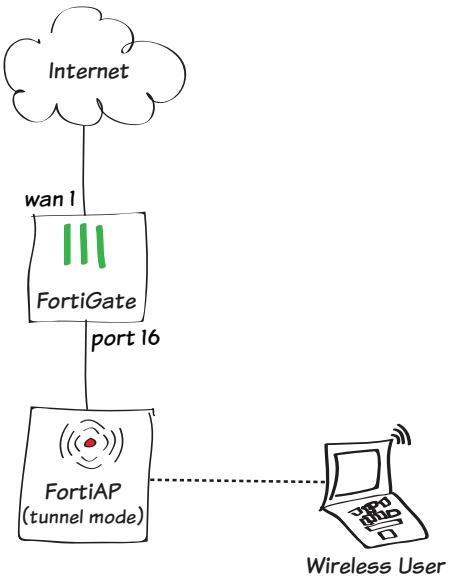
- Using a FortiAP in Tunnel mode to add wireless access
- Using a FortiAP in Bridge mode to add wireless access
- Using MAC access control to allow access to the wireless network

Using a FortiAP in Tunnel mode to add wireless access

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.

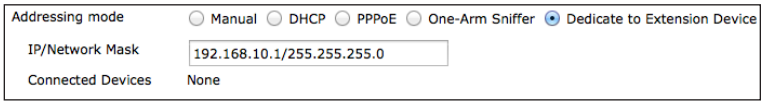
In this example, a FortiAP unit is connected to and managed by a FortiGate unit, allowing wireless access to the network. For information about using a FortiAP in Bridge mode, see "Using a FortiAP in Bridge mode to add wireless access" on page 90.

1. Connecting and authorizing the FortiAP unit
2. Creating an SSID
3. Creating a custom FortiAP profile
4. Allowing wireless access to the Internet
5. Results



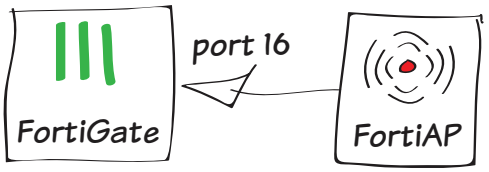
1. Connecting and authorizing the FortiAP unit

Go to **System > Network > Interfaces** and edit the interface that will connect to the FortiAP (in the example, port 16).



Set **Addressing Mode** to **Dedicate to Extension Device** and set an **IP/Network Mask**.

Connect the FortiAP unit to the interface.



Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. The FortiAP is listed, with a  beside it because the device is not authorized.

Mesh	Access Point	State	Connected Via
▫	FAP11C3X13000412	?	192.168.10.2

The FortiAP may not appear until a few minutes have passed.

Highlight the FortiAP unit on the list and select **Authorize**. A is now shown beside the FortiAP, showing that it is authorized but not yet online.

Mesh	Access Point	State	Connected Via
▫	FAP11C3X13000412	✓	192.168.10.2

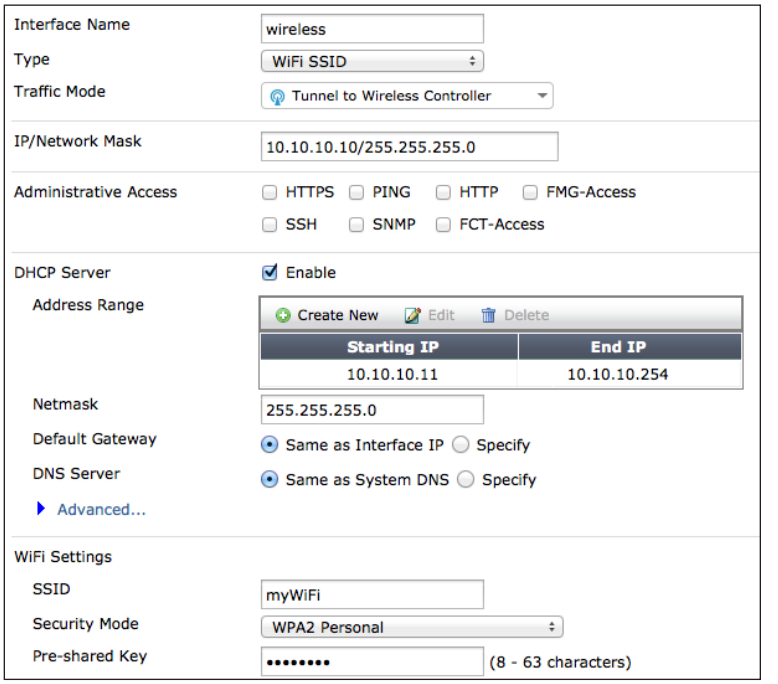
2. Creating an SSID

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**.

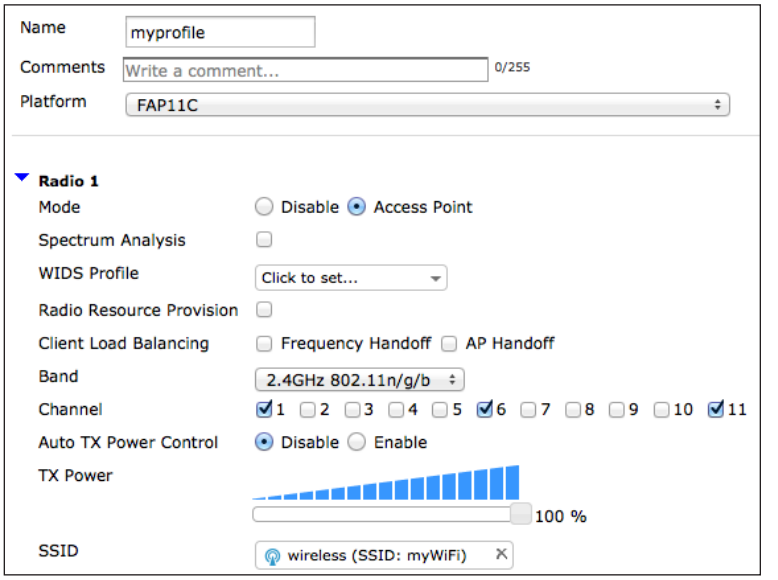


3. Creating a custom FortiAP profile

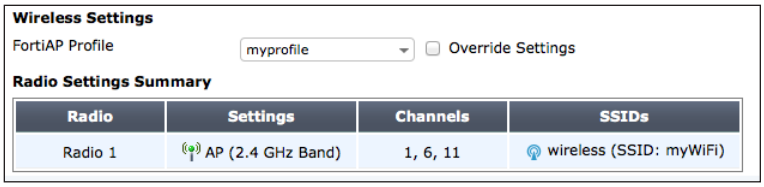
Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and create a new profile.

Set **Platform** to the correct FortiAP model you are using (in the example, FAP11C).

Set **SSID** to use the new SSID.



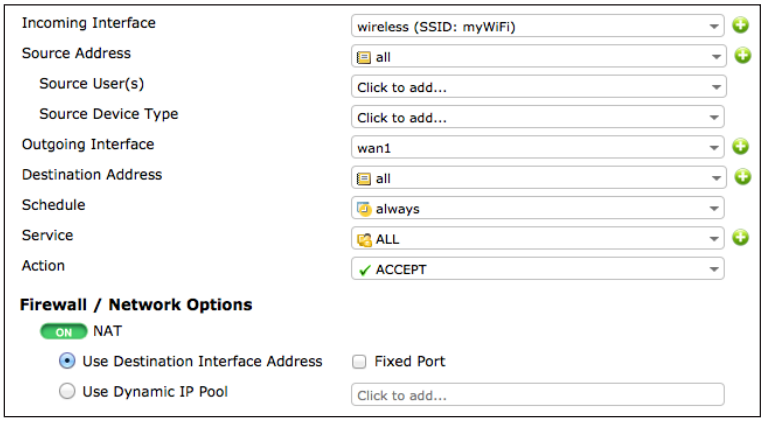
Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. Edit the FortiAP and set **FortiAP Profile** to use the new profile.



4. Allowing wireless access to the Internet

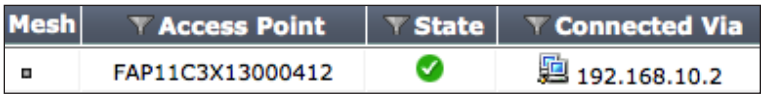
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

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 ✓ now appears beside the FortiAP, showing that the unit is authorized and online.



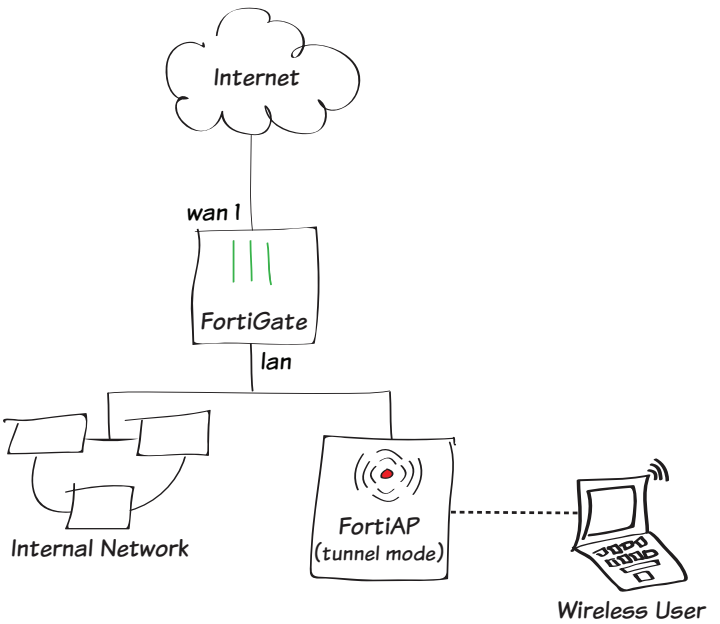
Connect to the SSID with a wireless device. After a connection is established, you are able to browse the Internet.

Using a FortiAP in Bridge mode to add wireless access

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.

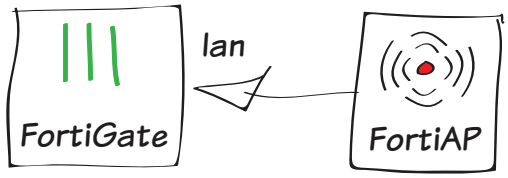
In this example, a FortiAP unit is connected to and managed by a FortiGate unit in Bridge mode. For information about using a FortiAP in Tunnel mode, see "Using a FortiAP in Tunnel mode to add wireless access" on page 86.

1. Connecting and authorizing the FortiAP unit
2. Creating an SSID
3. Creating a custom FortiAP profile
4. Results



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 beside it because the device is not authorized.

Mesh	Access Point	State	Connected Via
	FAP11C3X13000412		192.168.10.2

The FortiAP may not appear until a few minutes have passed.

Highlight the FortiAP unit on the list and select **Authorize**. A is now shown beside the FortiAP, showing that it is authorized but not yet online.

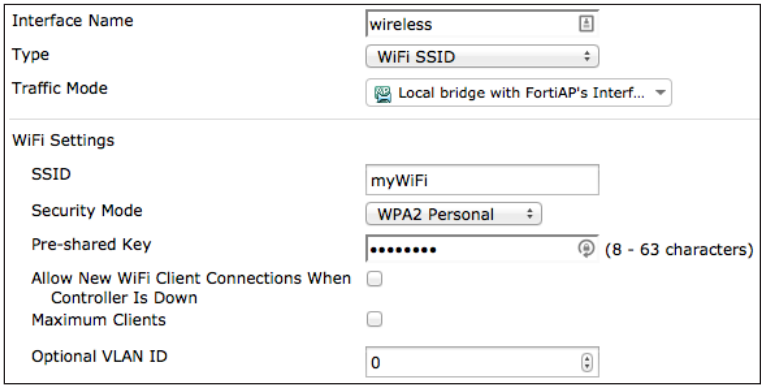
Mesh	Access Point	State	Connected Via
	FAP11C3X13000412		192.168.10.2

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**.

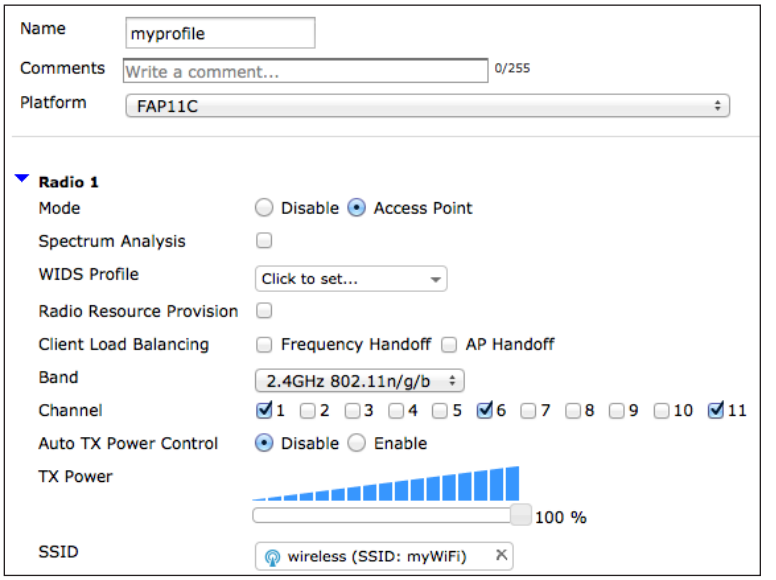


3. Creating a custom FortiAP profile

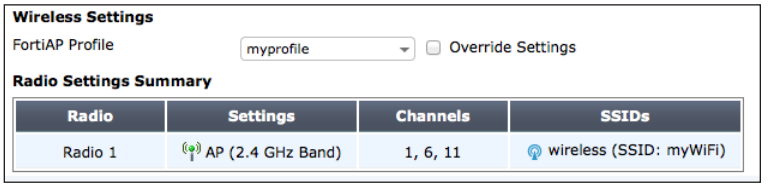
Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and create a new profile.

Set **Platform** to the correct FortiAP model you are using (FAP11C in the example).

Set **SSID** to use the new SSID.

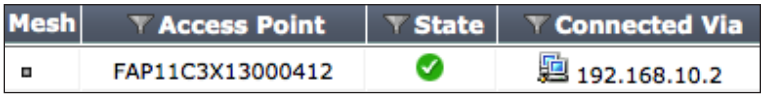


Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and edit the FortiAP. Set **FortiAP Profile** to use the new profile.



5. Results

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. A ✓ 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.

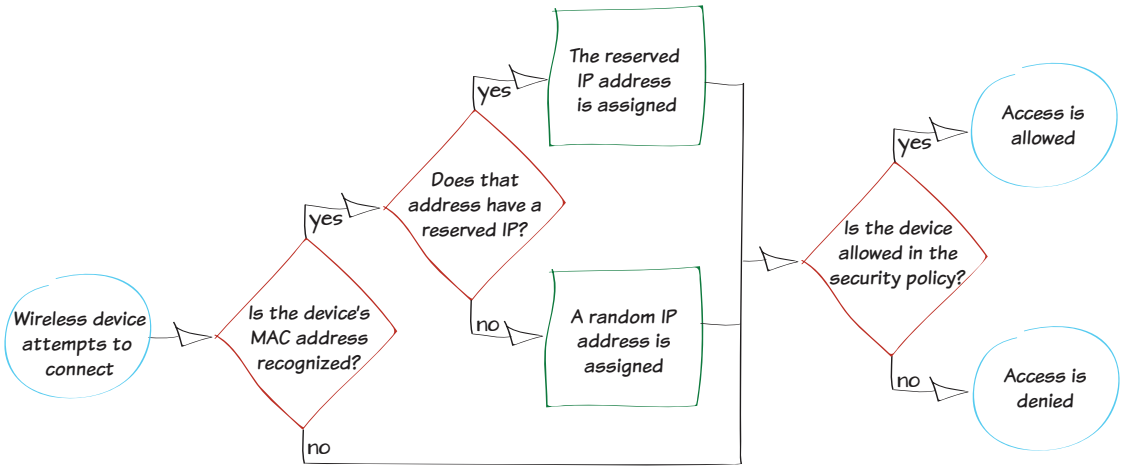
Using MAC access control to allow access to the wireless network

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.

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
2. Defining a device using its MAC address
3. Creating a device group
4. Reserving an IP address for the device
5. Creating a security policy for wireless traffic
6. Results



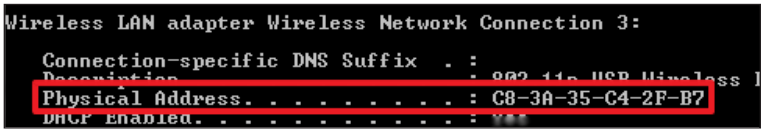
1. Finding the MAC address of a device

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`.

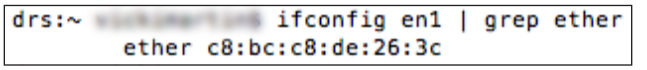
This output displays configuration information for all of your network connections. Look for the information about the wireless adapter and take note of the **Physical Address**.



For Mac OS X devices:

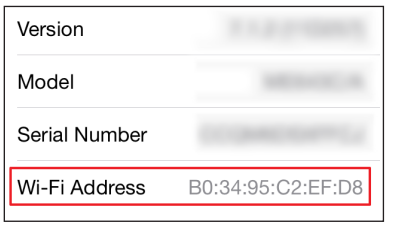
Open **Terminal** and type `ifconfig en1 | grep ether`.

Take note of the displayed MAC address.



For iOS devices:

Open **Settings > General** and take note of the **Wi-Fi Address**.



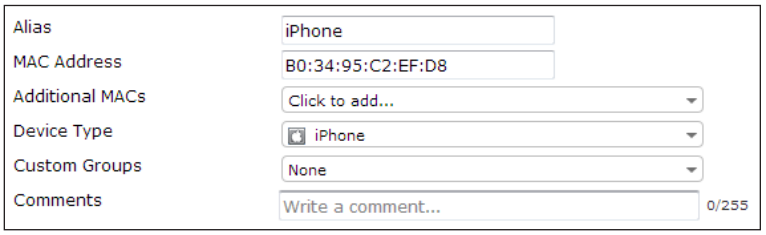
For Android devices:

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.

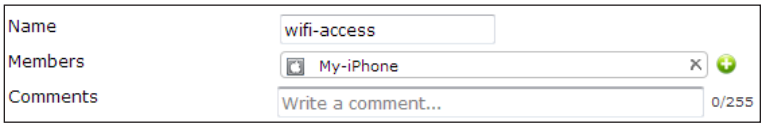
Status	Device	OS	IP Address
Online	My-Desktop	Windows	10.10.80.3
Offline	My-Android	Android / 2.2.2	10.10.80.4
Offline	My-iPhone	iPod / iOS	10.10.80.7
Offline	My-Netbook	Windows	10.10.80.5
Offline	My-Printer	Linux	10.10.80.6

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.

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.

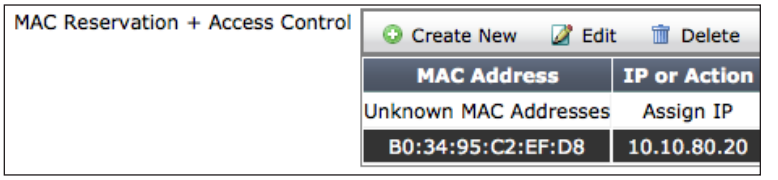


4. Reserving an IP address for the device

Go to **System > Network > Interfaces** and edit the wireless interface.

Under **DCHP Server**, expand **Advanced**. Create a new entry in the **MAC Reservation + Access Control** list that reserves an IP address within the DCHP range for the device's MAC address.

If the FortiAP is in bridge mode, you will need to edit the internal interface.

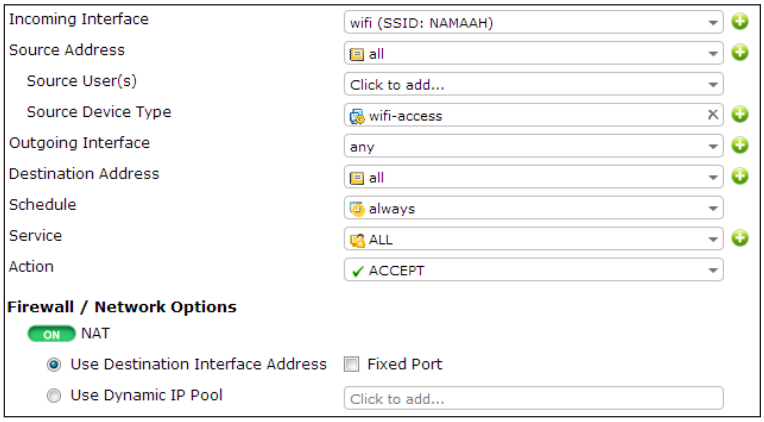


5. Creating a security policy for wireless traffic

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.

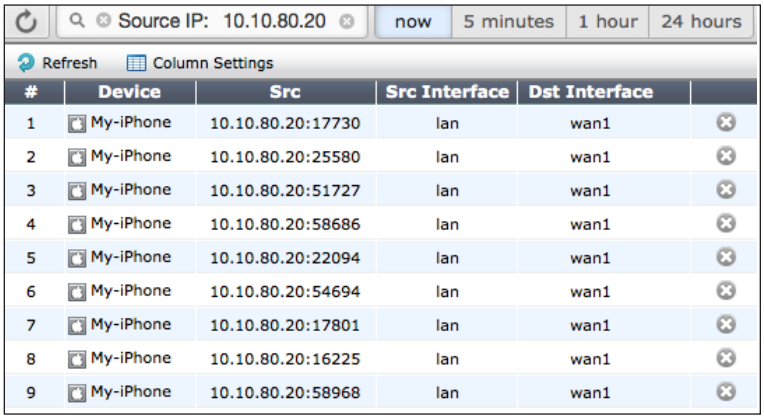


6. Results

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

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.

This section contains the following recipes:

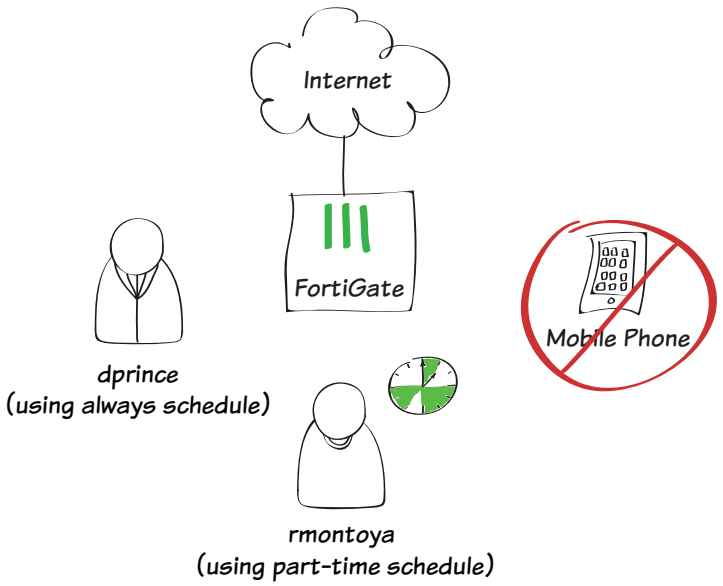
- Allowing network access based on schedule and device type

Allowing network access based on schedule and device type

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.

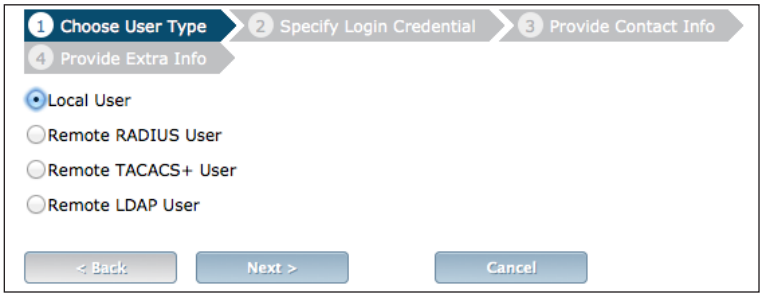
1. Defining two users and two user groups
2. Creating a schedule for part-time staff
3. Defining a device group for mobile phones
4. Creating a policy for full-time staff
5. Creating a policy for part-time staff that enforces the schedule
6. Creating a policy that denies mobile traffic
7. Results

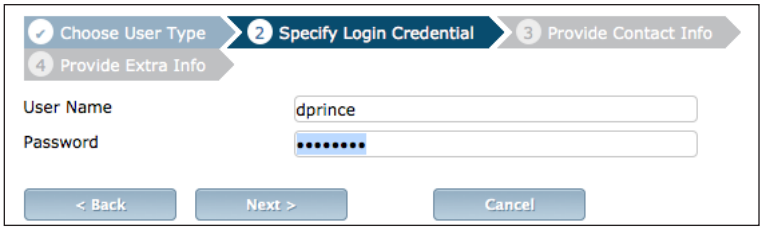


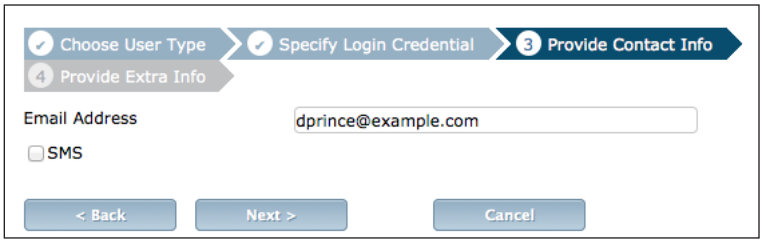
1. Defining two users and two user groups

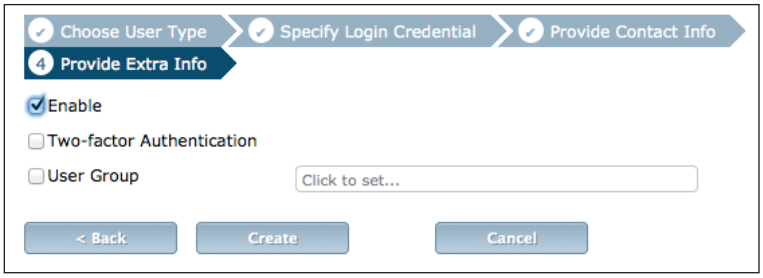
Go to **User & Device > User > User Definitions**.

Create two new users (in the example, *dprince* and *rmontoya*).







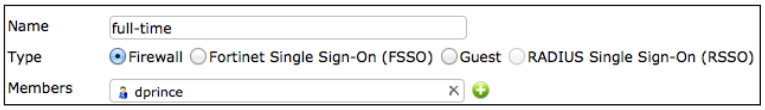


Both user definitions now appear in the user list.

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.*

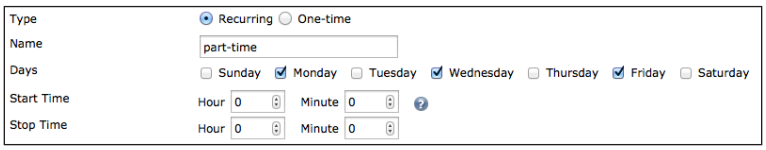


Create a second user group, *part-time*, and add user *rmontoya*.

2. Creating a schedule for part-time staff

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

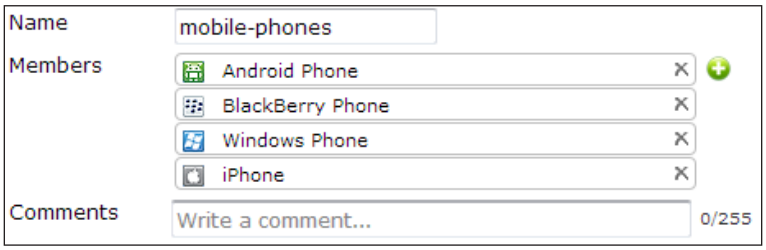
Set an appropriate schedule. In order to get results later, do not select the current day of the week.



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**.

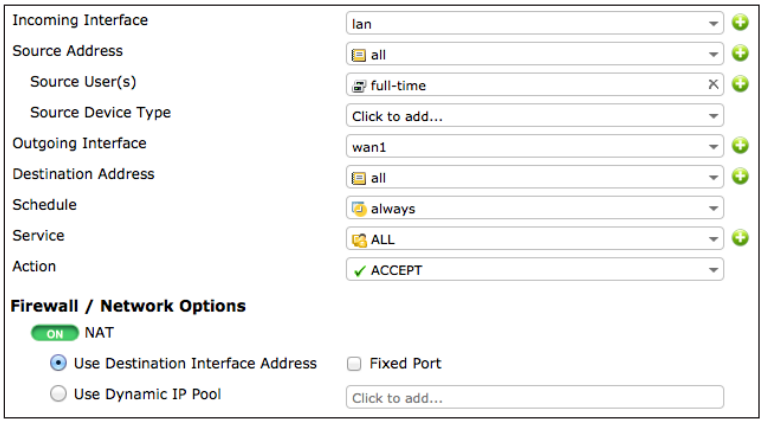


4. Creating a policy for full-time staff

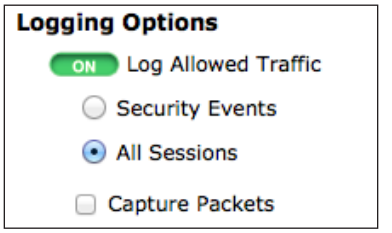
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

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**.

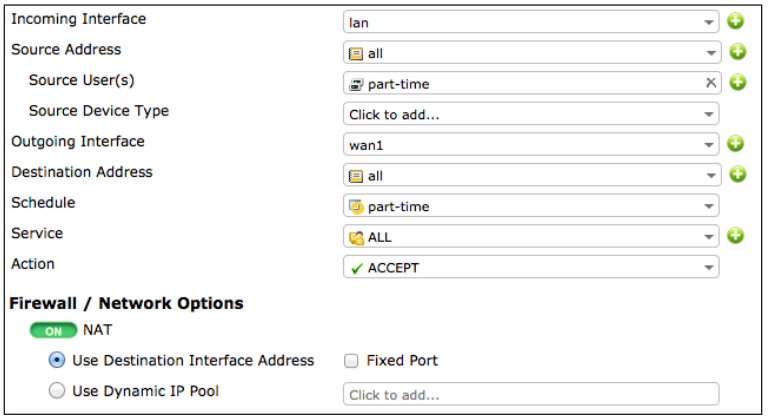


5. Creating a policy for part-time staff that enforces the schedule

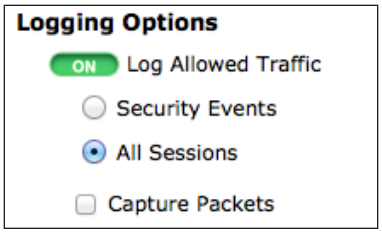
Go to **Policy & Objects > Policy > IPv4** and create a new policy.

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
```

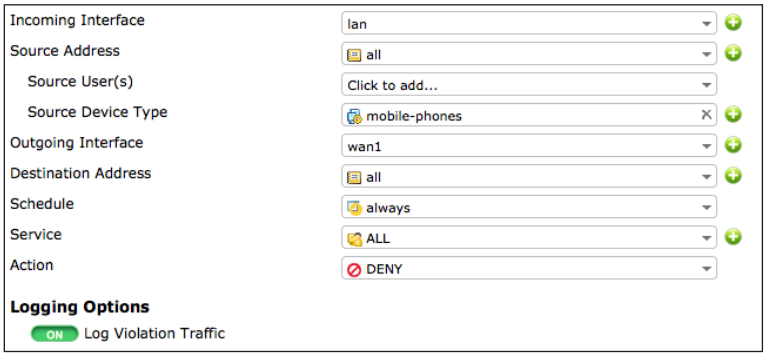
This will ensure that part-time users will have their access revoked during days they are not scheduled, even if their current session began when access was allowed.

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**.

Leave **Log Violation Traffic** turned on.



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

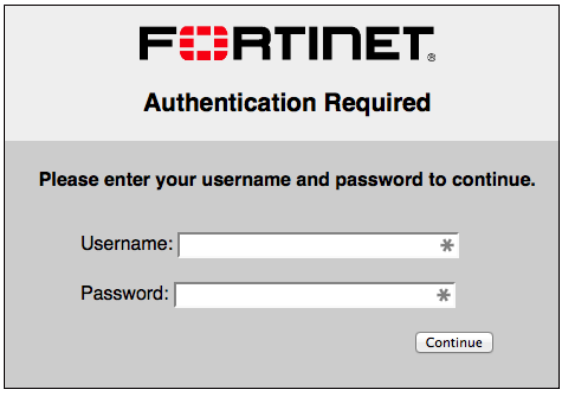
In order for this policy to be used, it must be located at the top of the policy list. Select any area in the far-left column of the policy and drag it to the top of the list.

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

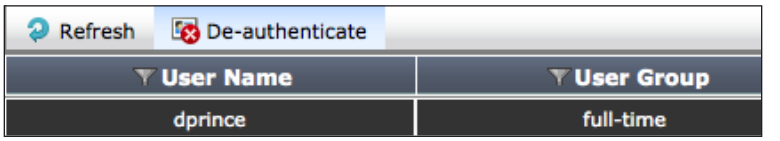
Browse the Internet using a computer. You will be prompted to enter authentication credentials.

Log in using the *dprince* account. You will be able to access the Internet at any time.

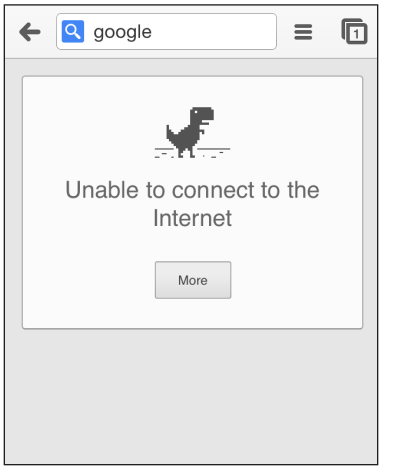


Go to **User & Device > Monitor > Firewall**. Highlight **dprince** and select **De-authenticate**.

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

IPsec VPN

This section contains information about configuring a variety of different IPsec VPNs, as well as different methods of authenticating IPsec VPN users.

IPsec VPNs use Internet Protocol Security (IPsec) to create a Virtual Private Network (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.

This section contains the following recipes:

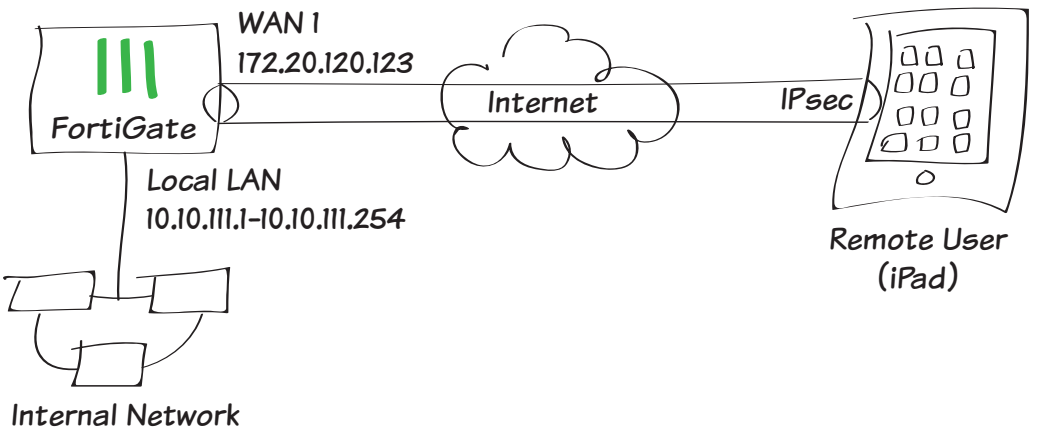
- Configuring an IPsec VPN for iOS devices
- Extra help: IPsec VPN
- Using IPsec VPN to provide communication between two offices
- Configuring IPsec VPN between a FortiGate and Microsoft Azure™
- Setting up BGP over a dynamic IPsec VPN between two FortiGates

Configuring an 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.

1. Creating a user group for iOS users
2. Adding a firewall address for the local network
3. Configuring IPsec VPN using the IPsec VPN Wizard
4. Creating a security policy for access to the Internet
5. Configuring VPN on the iOS device
6. Results

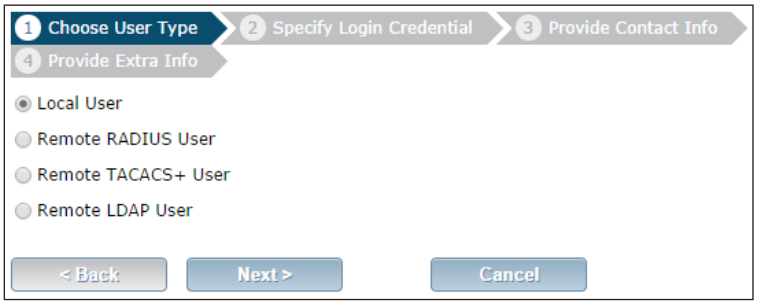


1. Creating a user group for iOS users

Go to **User & Device > User > User Definition**.

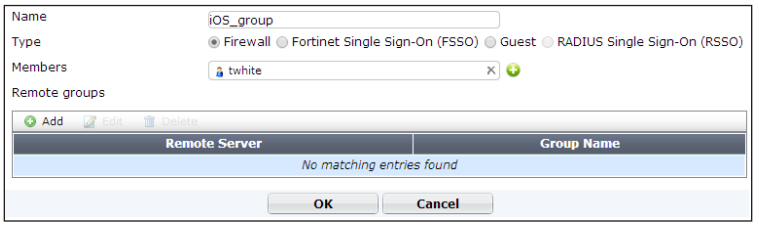
Create a new **Local User** with the User Creation Wizard.

Proceed through each step of the wizard, carefully entering the appropriate information.



Go to **User & Device > User > User Groups**.

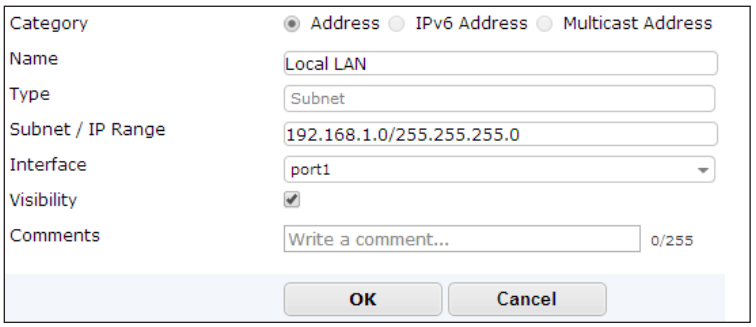
Create a user group for iOS users and add the user you created.



2. Adding a firewall address for the local network

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

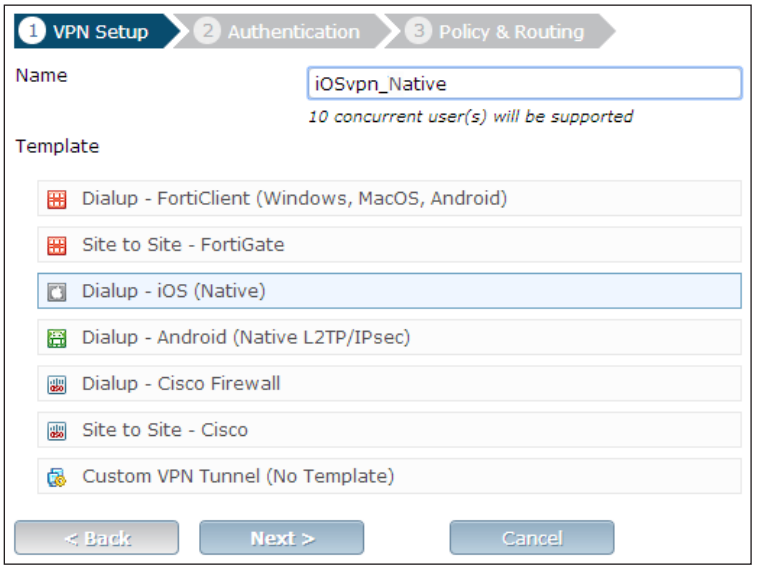
Add a firewall address for the Local LAN, including the subnet and local interface.



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**.

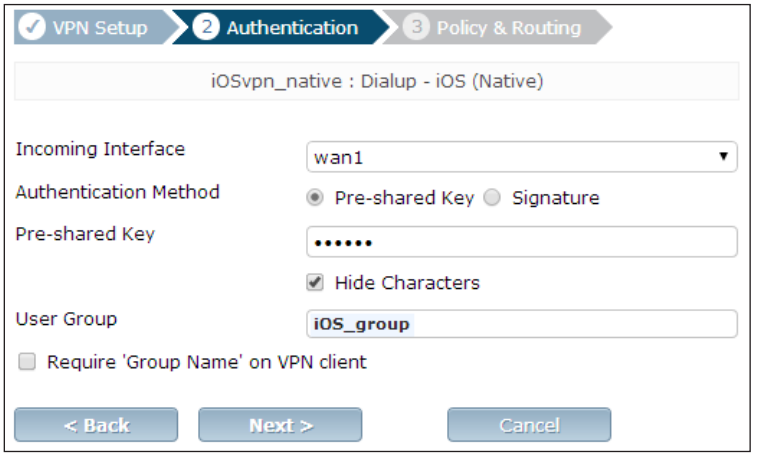


Set the **Incoming Interface** to the internet-facing interface.

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.

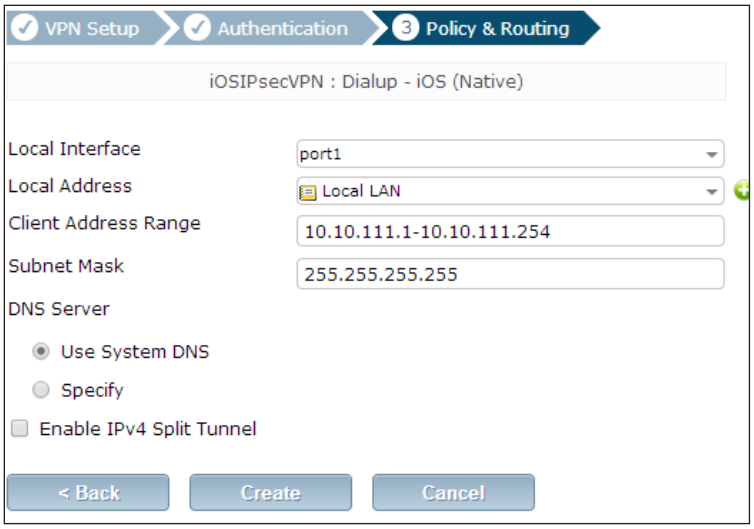


Set **Local Interface** to an internal interface (in the example, port 1) and set **Local Address** to the local LAN address.

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, **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

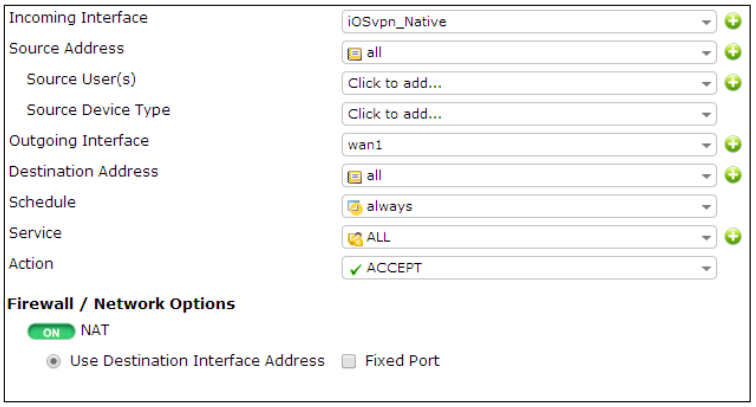
Go to **Policy & Objects > Policy > IPv4**.

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**.

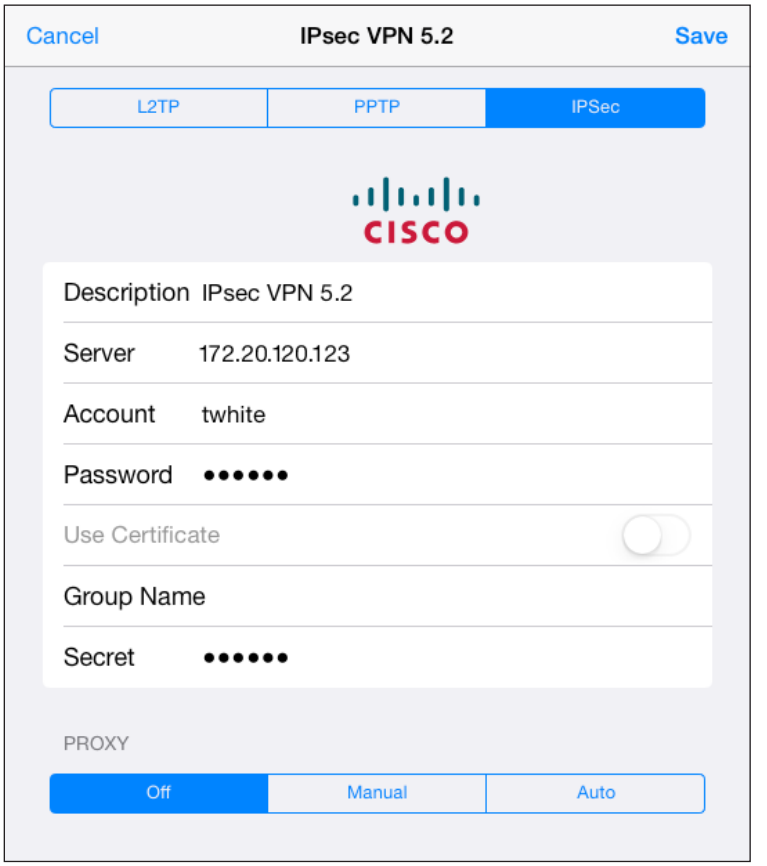
Set **Service** to **all** and ensure that you enable **NAT**.



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.



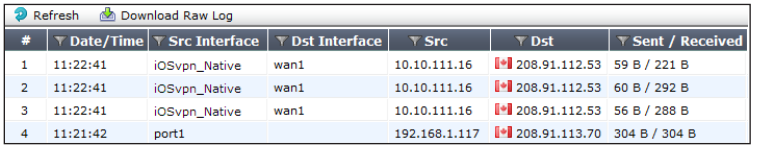
6. Results

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.
iOSvpn_Native_0	Dialup	172.20.120.16		Up	9.22 K

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

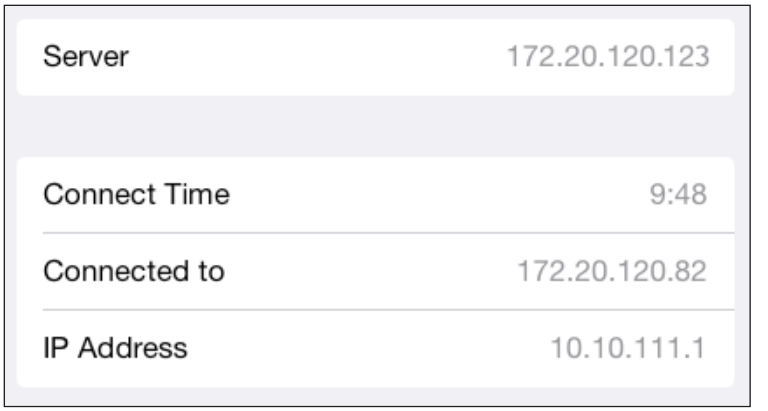
#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received
1	11:28:43	ios_P1	wan1	10.10.111.16	74.121.50.17	1023 B / 579 B
2	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	59 B / 221 B
3	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	60 B / 292 B
4	11:22:41	iOSvpn_Native	wan1	10.10.111.16	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.

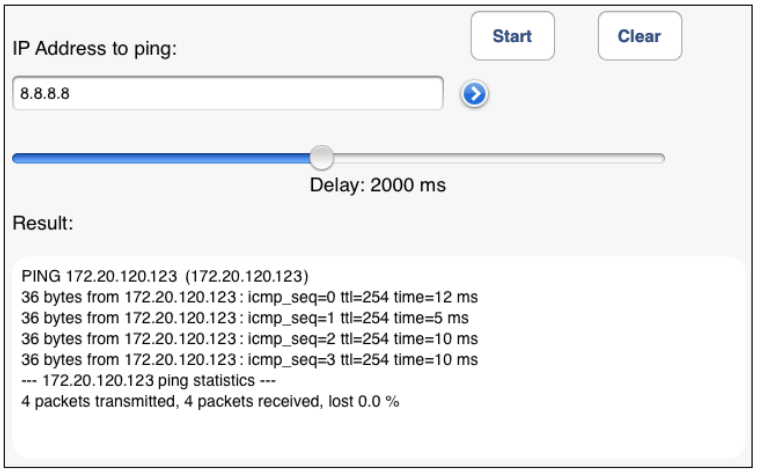
Dst	74.121.50.17	**Virtual Domain**	root
Received	579	**Source Country**	Reserved
Src NAT IP	172.20.120.123	**Sent / Received**	1023 B / 579 B
Duration	2	**Sent**	1023
Src NAT Port	50189	**Application Details**	
Service	HTTP	**Protocol**	6
Destination Country	United States	**Dst Port**	80
roll	65428	**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.



Extra help: IPsec VPN

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.

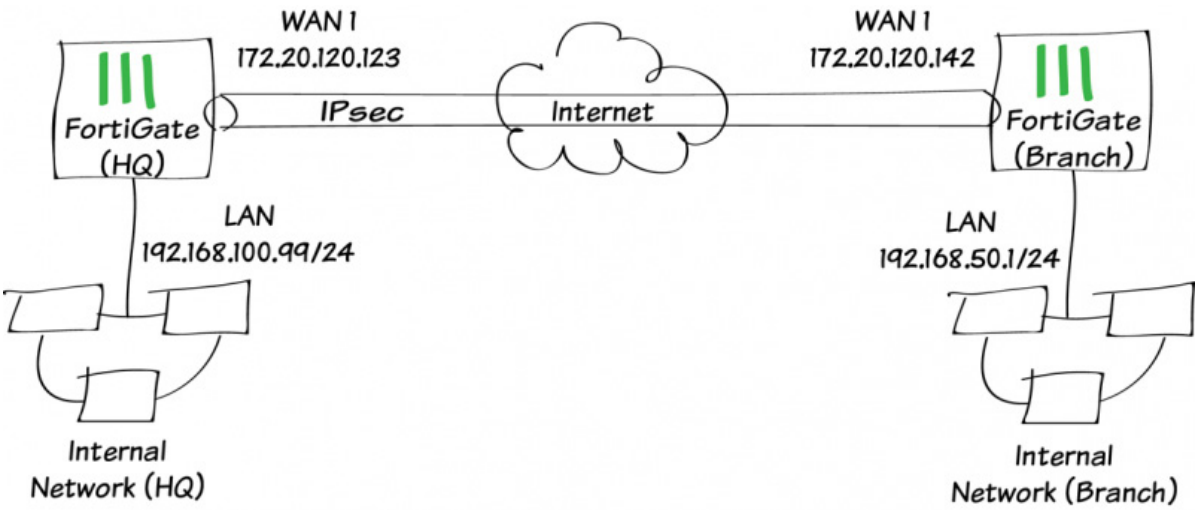
If your VPN tunnel goes down often, check the Phase 2 settings and either increase the **Keylife** value or enable **Autokey Keep Alive**.

Using IPsec VPN to provide communication between two offices

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.

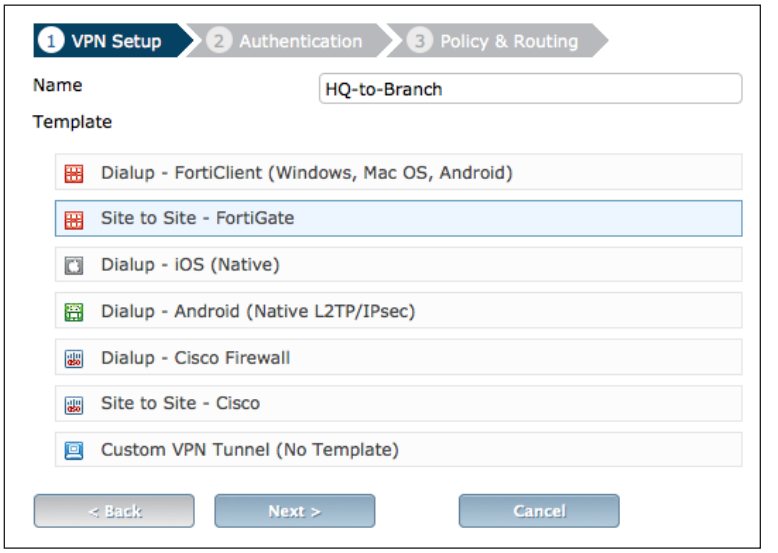
In this example, one office will be referred to as HQ and the other will be referred to as Branch.

1. Configuring the HQ IPsec VPN
2. Configuring the Branch IPsec VPN



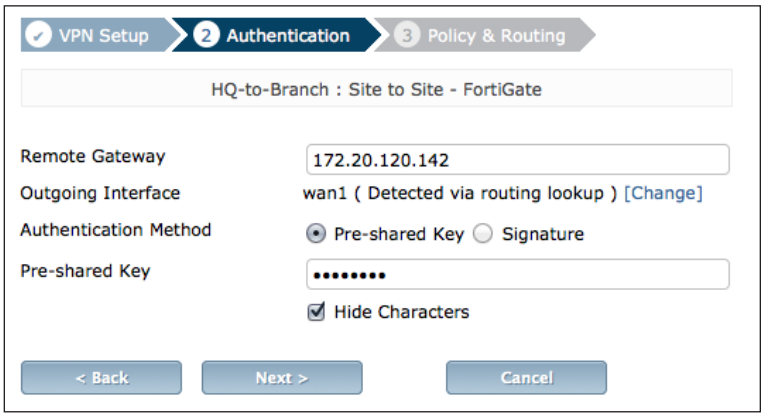
1. Configuring the HQ IPsec VPN

On the HQ FortiGate, go to **VPN > IPsec > Wizard** and select **Site to Site – FortiGate**.

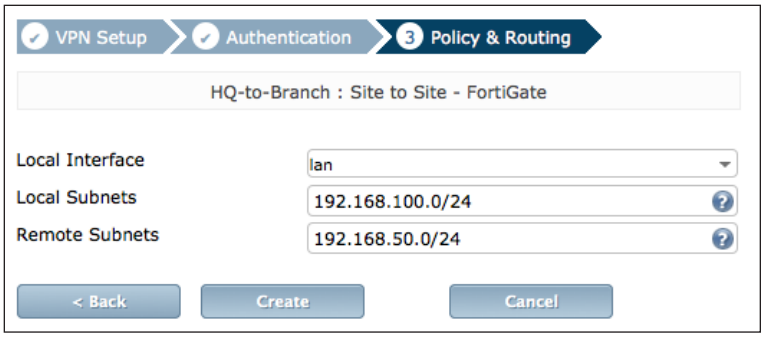


In the **Authentication** step, set the Branch FortiGate's IP as the **Remote Gateway** (in the example, *172.20.120.142*). After you enter the gateway, an available interface will be assigned as the **Outgoing Interface**. If you wish to use a different interface, select **Change**.

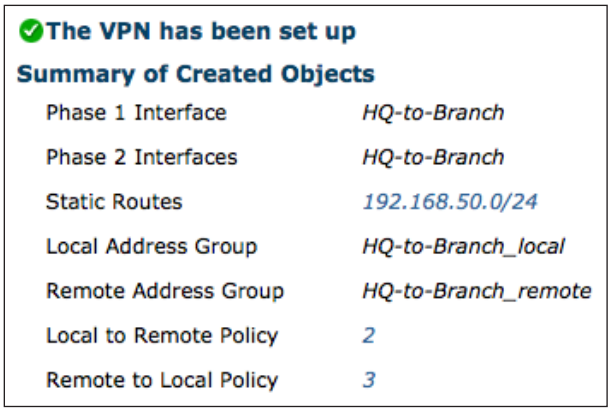
Set a secure **Pre-shared Key**.



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*).

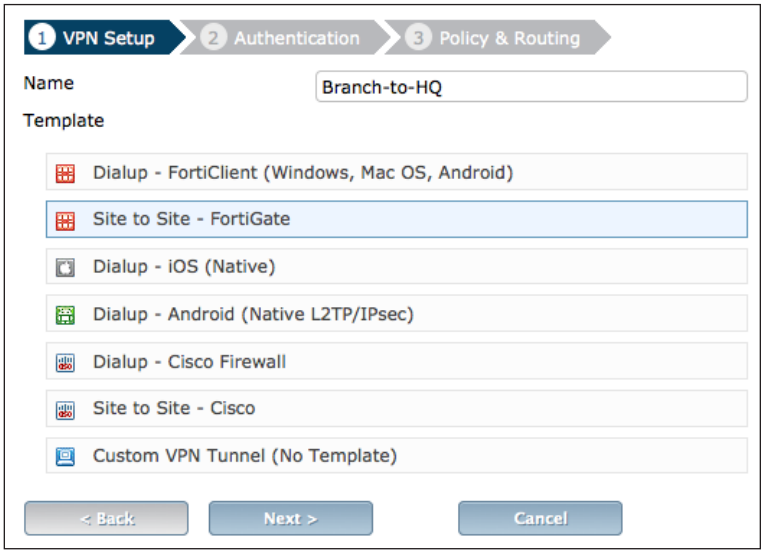


A summary page shows the configuration created by the wizard, including firewall addresses, firewall address groups, a static route, and security policies.



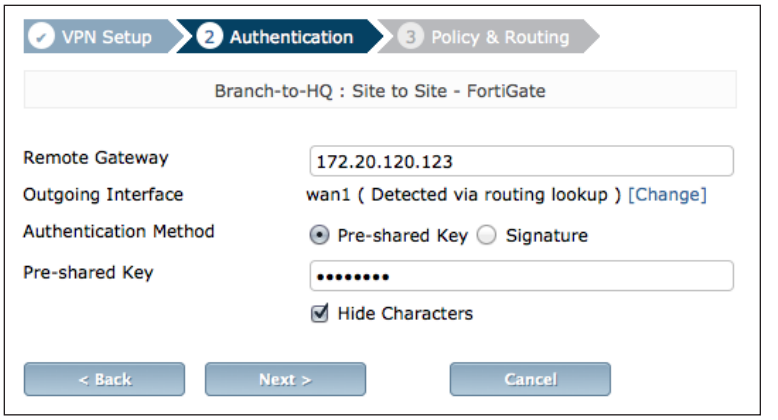
2. Configuring the Branch IPsec VPN

On the HQ FortiGate, go to **VPN > IPsec > Wizard** and select **Site to Site – FortiGate**.

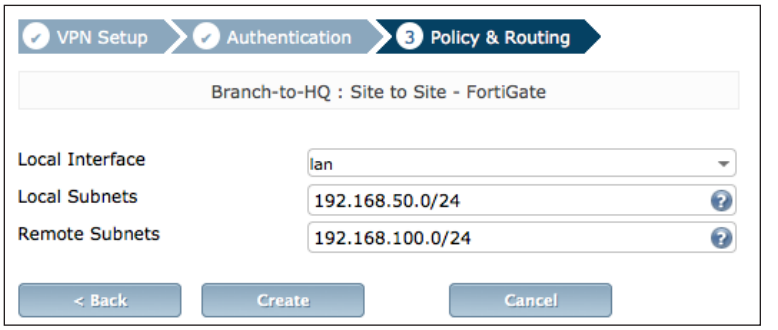


In the **Authentication** step, set the HQ FortiGate's IP as the **Remote Gateway** (in the example, *172.20.120.123*). After you enter the gateway, an available interface will be assigned as the **Outgoing Interface**. If you wish to use a different interface, select **Change**.

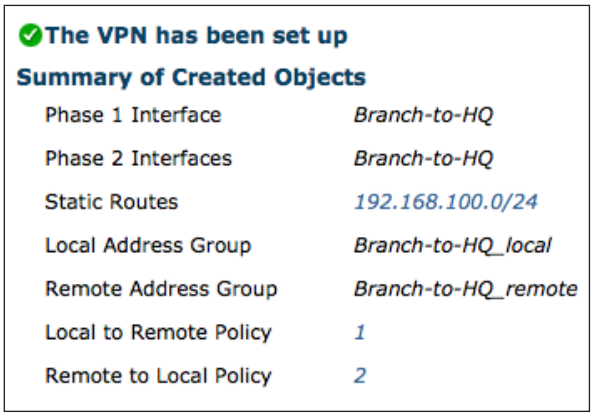
Set the same **Pre-shared Key** that was used for HQ's VPN.



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

Go to **VPN > Monitor > IPsec Monitor** to verify the status of the VPN tunnel. Ensure that its **Status** is **Up**.

Name	Type	Remote Gateway	Status
Branch-to-HQ	Static IP or Dynamic DNS	172.20.120.123	Up

A user on either of the office networks should be able to connect to any address on the other office network transparently.

Refresh the IPsec Monitor to verify that traffic is flowing.

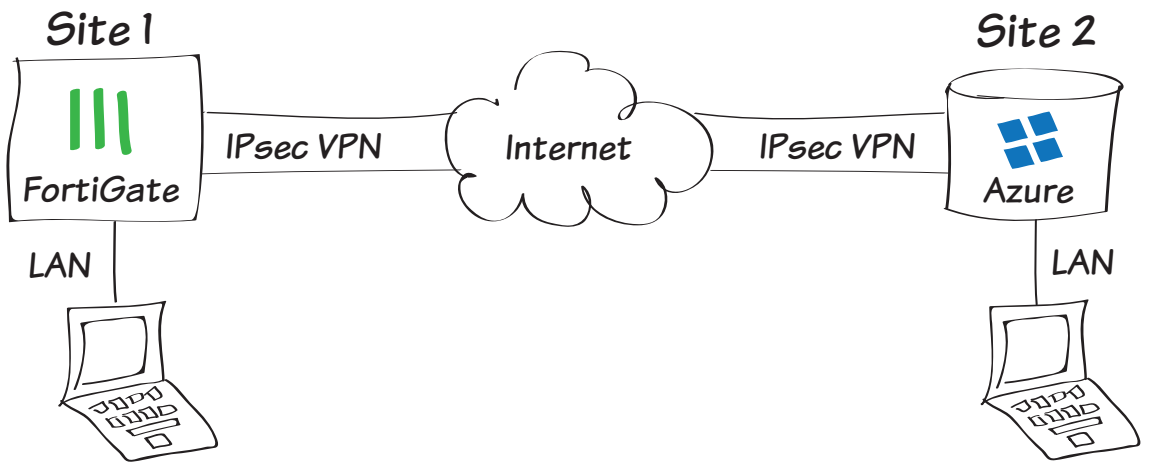
Incoming Data	Outgoing Data
8.16 KB	4.92 KB

Configuring IPsec VPN between a FortiGate and 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.

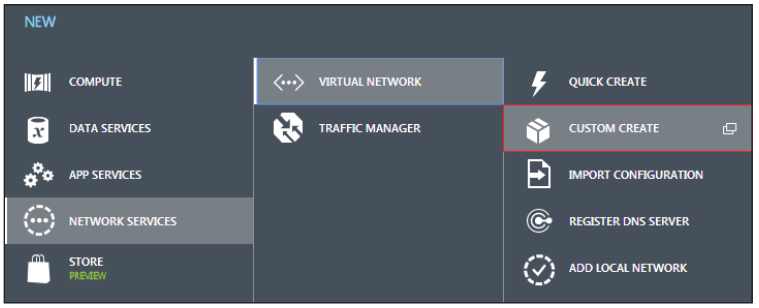
1. Configuring the Microsoft Azure™ virtual network
2. Creating the Microsoft Azure™ virtual network gateway
3. Configuring the FortiGate tunnel
4. Creating the FortiGate firewall addresses
5. Creating the FortiGate firewall policies
6. Results



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.

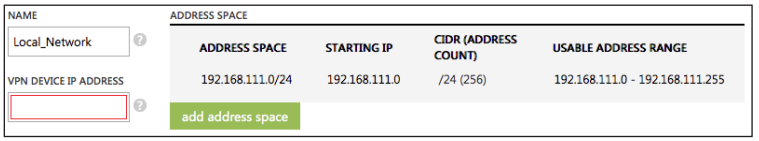
Under 'DNS Servers and VPN Connectivity', enable the **Configure a site-to-site VPN** checkbox and enter DNS server information if required.

Click the **Next** arrow.

Under 'Site-to-Site Connectivity', enter a **Name** and **IP Address** for the FortiGate device.

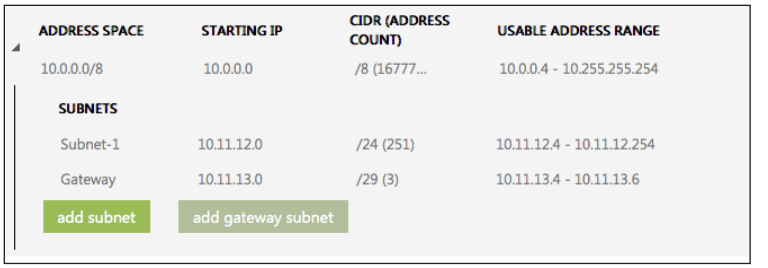
Under Address Space, include a **Starting IP** and **CIDR (Address Count)** for the tunnel, avoiding overlapping subnets.

Click the **Next** arrow.

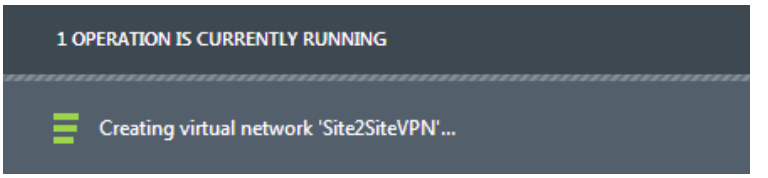


Under ‘Virtual Network Address Spaces’, configure the desired address space or accept the default settings.

Select **add gateway subnet** to configure a gateway IP and click the **Checkmark** in the lower-right corner to accept the configuration.

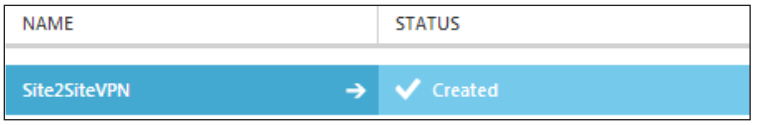


After accepting the configuration, you will have to wait a short period of time for the virtual network to be created, but it shouldn’t be long.

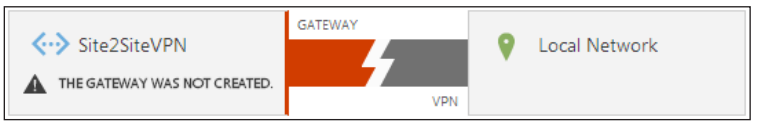


2. Creating the Microsoft Azure™ virtual network gateway

On the ‘networks’ home screen, click the name of the virtual network you just created.

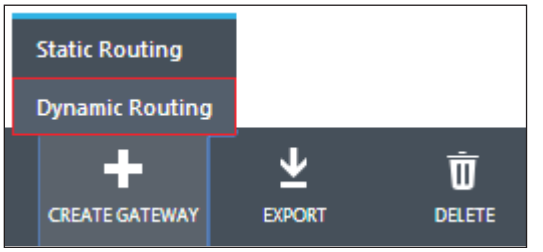


Under this virtual network, go to the **Dashboard**. You will notice that the gateway has not yet been created. You will create the gateway in this step.

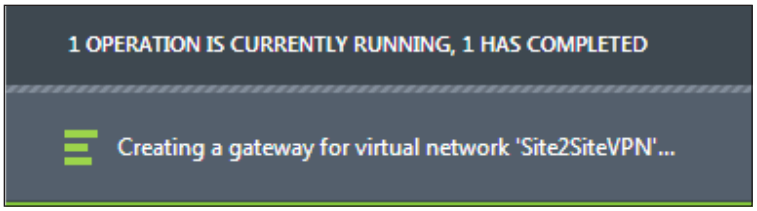


At the bottom of the screen, select **Create Gateway** > **Dynamic Routing**.

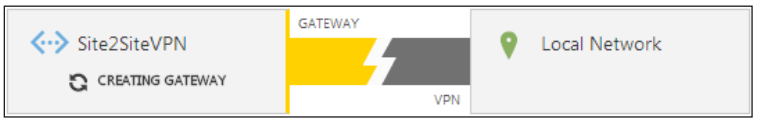
When prompted, select **Yes**.



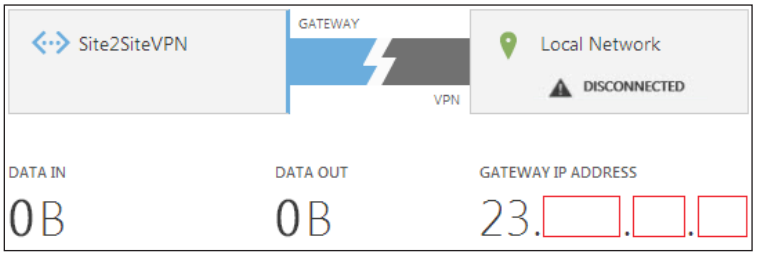
The operation to create the virtual network gateway will run. The process takes a short amount of time.



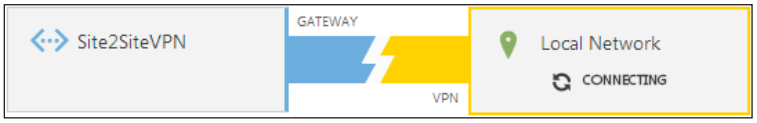
Azure will indicate to you that the gateway is being created. You may wish to leave this running for a few minutes as wait periods in excess of 10 minutes are common.



When the operation is complete, the status changes and you are given a **Gateway IP Address**.



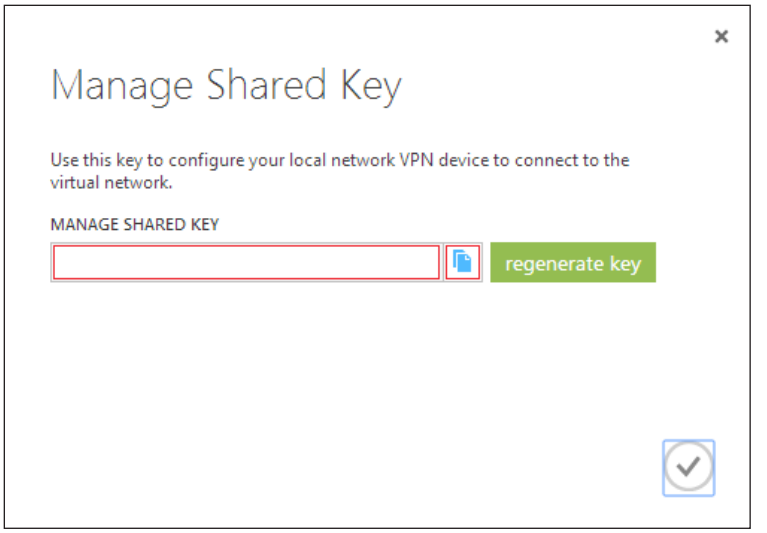
The gateway will then attempt to connect to the Local Network.



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.

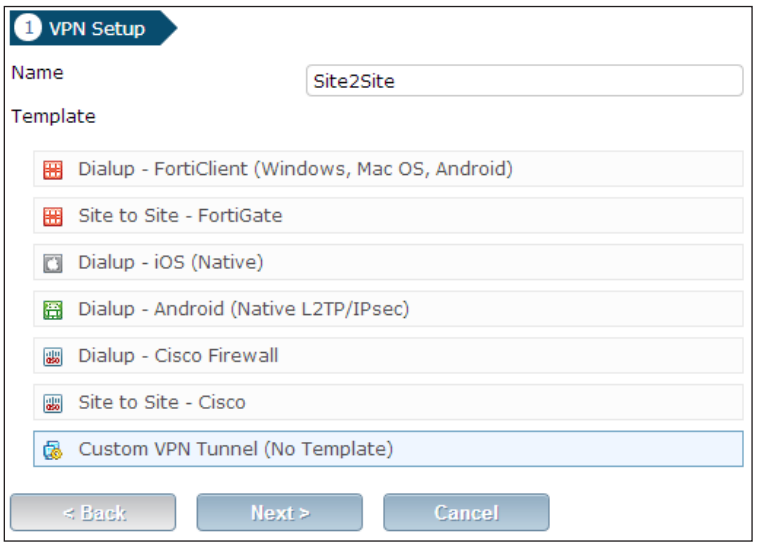


You are now ready to configure the FortiGate endpoint of the tunnel.

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**.

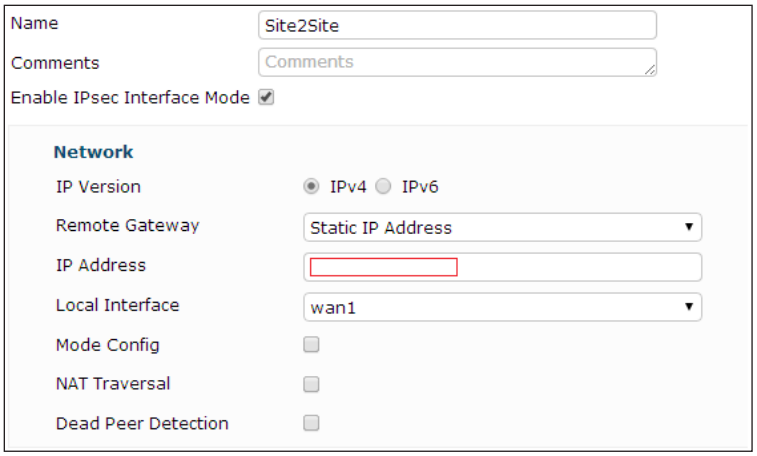


Enter the desired parameters. Set the **Remote Gateway** to **Static IP Address**, and include the gateway **IP Address** provided by Microsoft Azure.

Set the **Local Interface** to **wan1**.

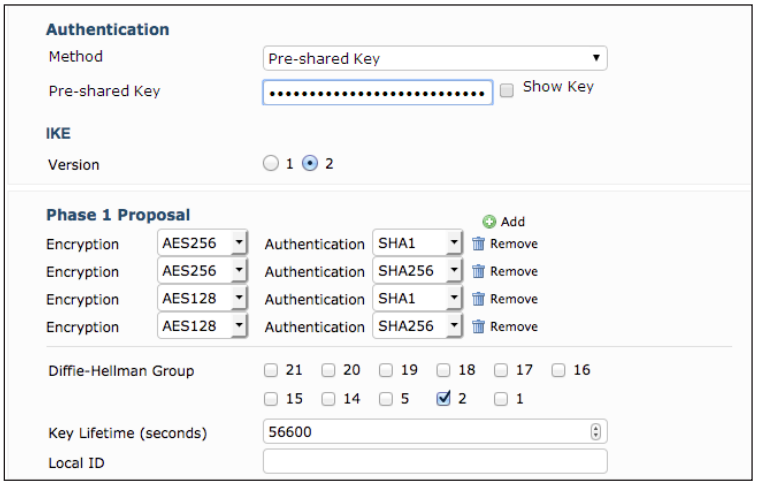
Under **Authentication**, enter the **Pre-shared Key** provided by Microsoft Azure.

Disable **NAT Traversal** and **Dead Peer Detection**.



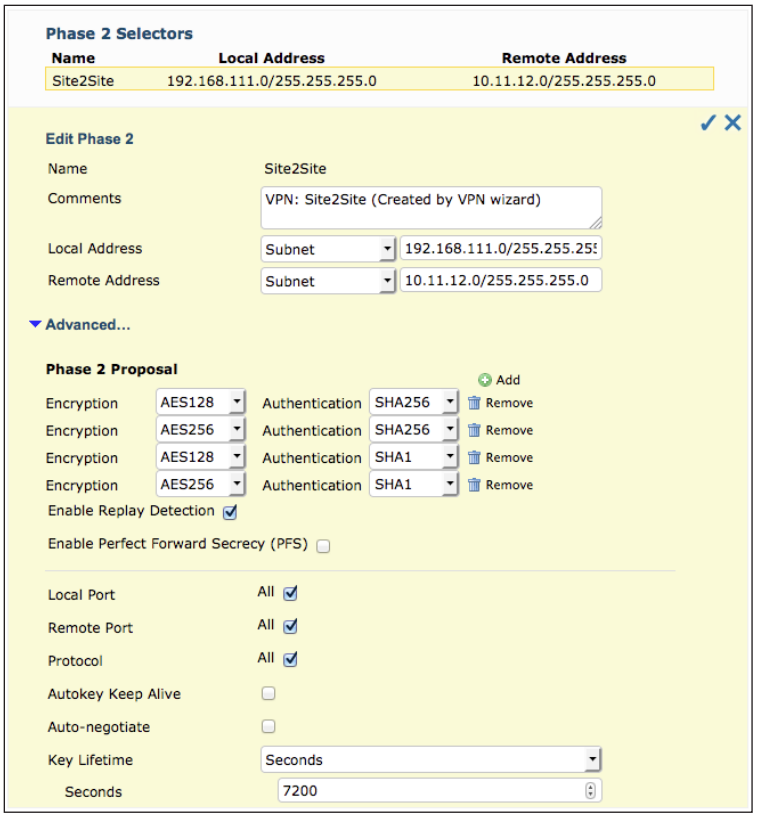
Under **Authentication**, ensure that you enable **IKEv2** and set **DH Group** to **2**.

Enable the encryption types shown and set the **Keylife** to **56600** seconds.



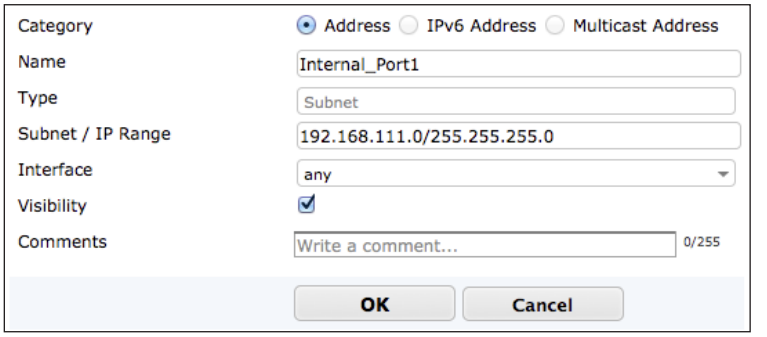
Scroll down to **Phase 2 Selectors** and set **Local Address** to the local subnet and **Remote Address** to the VPN tunnel endpoint subnet (found under 'Virtual Network Address Spaces' in Microsoft Azure).

Enable the encryption types to match Phase 1 and set the **Keylife** to **7200** seconds.

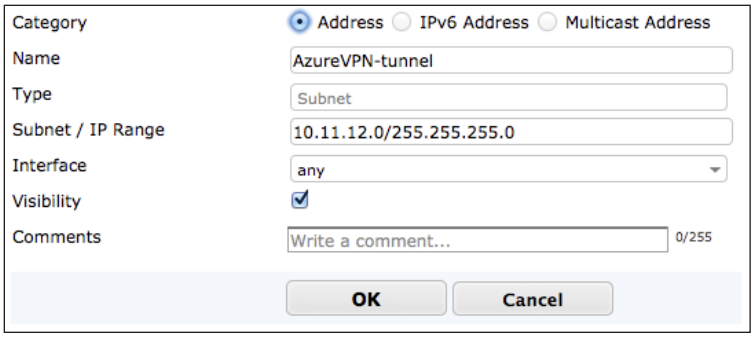


4. Creating the FortiGate firewall addresses

Go to **Policy & Objects** > **Objects** > **Addresses** and configure a firewall address for the local network.



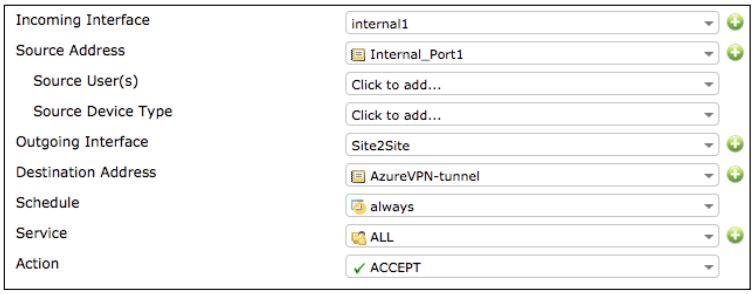
Create another firewall object for the Azure VPN tunnel subnet.



5. Creating the FortiGate firewall policies

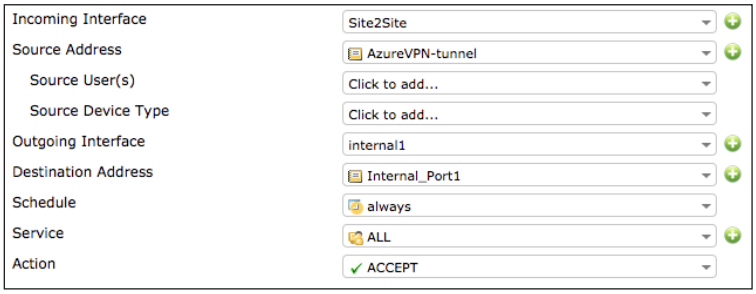
Go to **Policy & Objects** > **Policy** > **IPv4** and create a new policy for the site-to-site connection that allows outgoing traffic.

Set the **Source Address** and **Destination Address** using the firewall objects you just created.



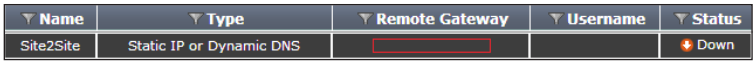
When you are done, create another policy for the same connection to allow incoming traffic.

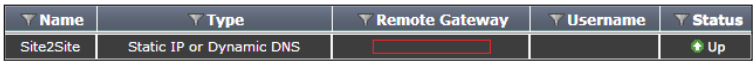
This time, invert the **Source Address** and **Destination Address**.



6. Results

Go to **VPN** > **Monitor** > **IPsec Monitor**. Right-click the tunnel you created and select **Bring Up** to activate the tunnel.





Go to **Log & Report** > **Event Log** > **VPN**.

Select an entry to view more information and verify the connection.

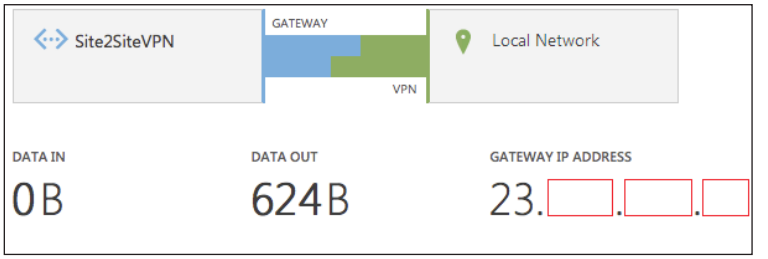
#	Date/Time	Level	Action	Status	Message	VPN Tunnel
12	15:23:04		phase2-up		IPsec phase 2 status change	Site2Site
13	15:23:04		install_sa		install IPsec SA	Site2Site
14	15:23:04		negotiate	success	negotiate IPsec phase 2	Site2Site
15	15:23:04		negotiate	success	progress IPsec phase 1	Site2Site
16	15:23:04		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		

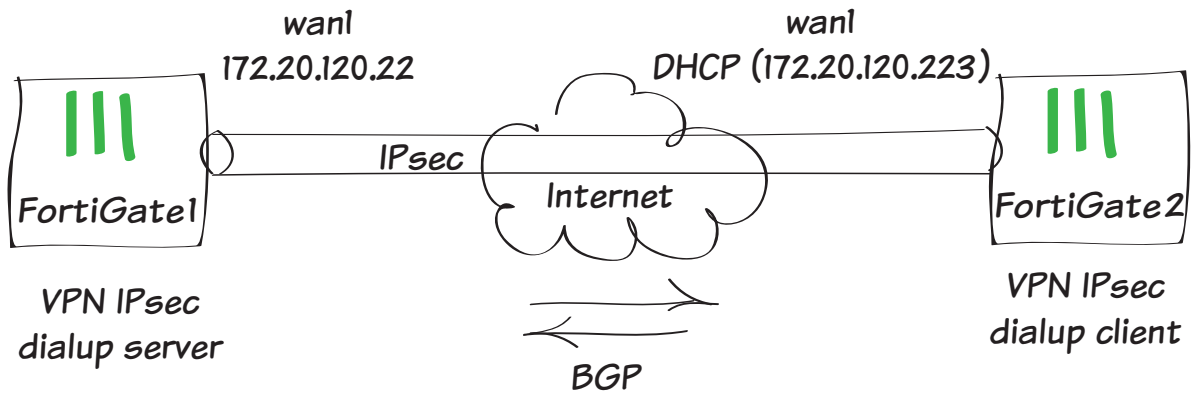
Return to the Microsoft Azure virtual network **Dashboard**. The status of the tunnel will show as **Connected**.

Data In and **Data Out** will indicate that traffic is flowing.



Setting up BGP over a dynamic IPsec VPN between two FortiGates

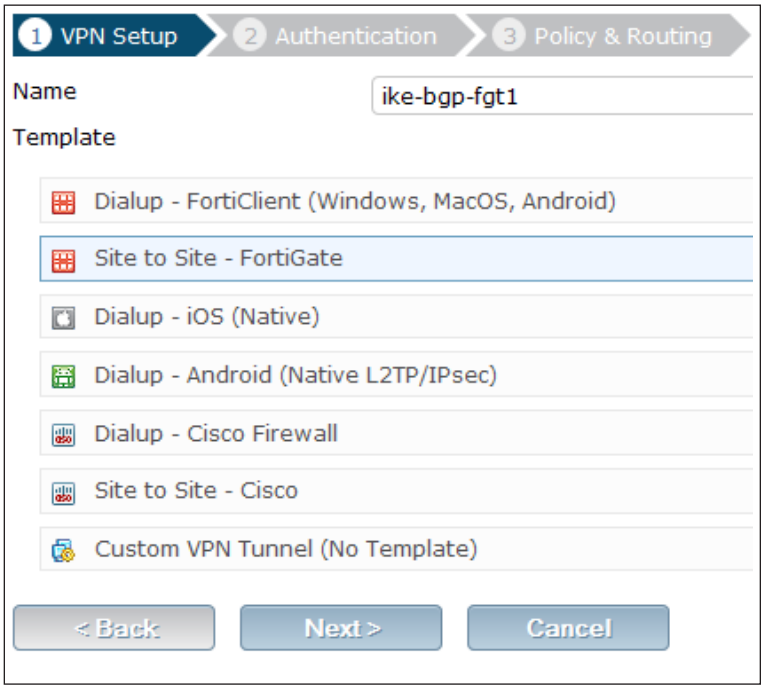
This example shows how to create a dynamic IPsec VPN tunnel and allowing BGP to establish through it.



1. Configuring IPsec in FortiGate 1

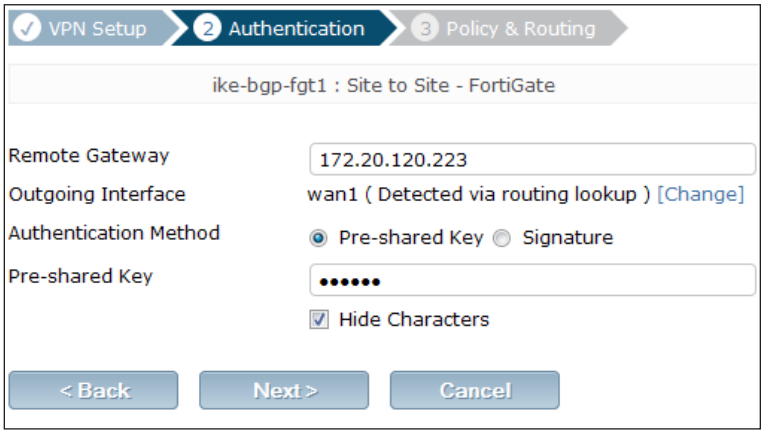
Go to **VPN > IPsec > Wizard** and select **Site to Site - FortiGate**.

Click **Next.**



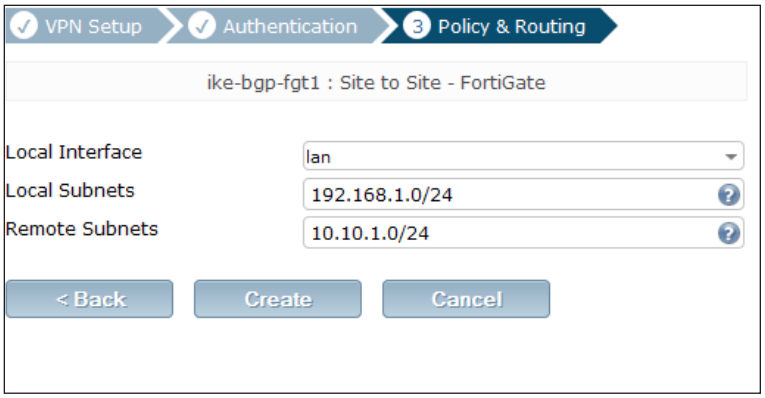
Set **Remote Gateway, Outgoing Interface** and **Pre-shared Key**.

Click **Next.**



Set **Local Interface, Local** and **Remote Subnets.**

Click **Create.**

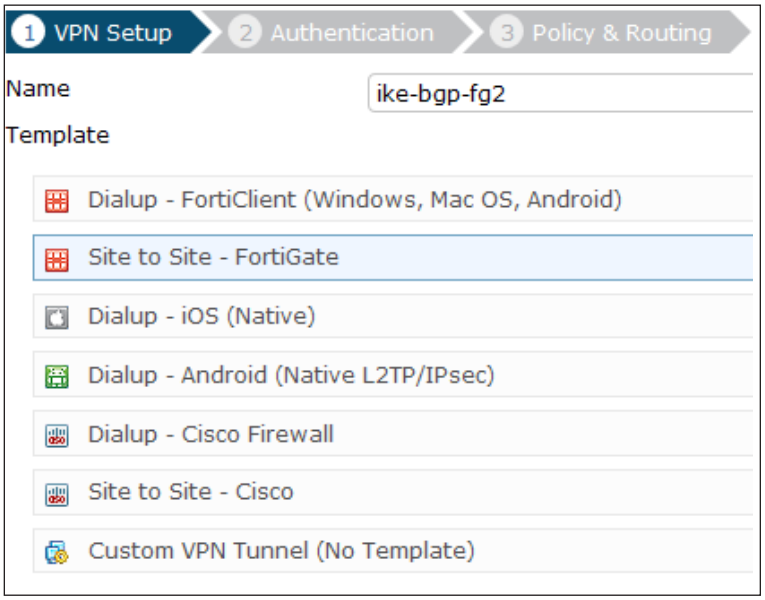


FortiGate then will create phase 1, phase 2, static route, local and remote address group, local to remote and remote to local security policies.

2. Configuring IPsec in FortiGate 2

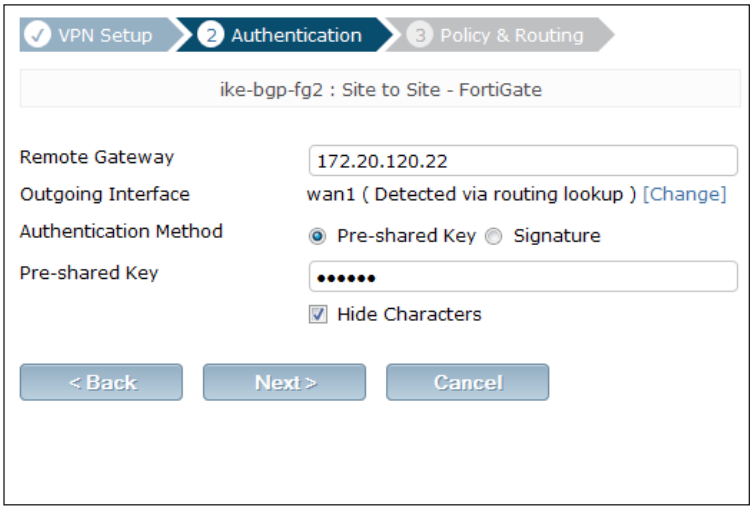
Go to **VPN > IPsec > Wizard** and select **Site to Site - FortiGate**.

Click **Next.**



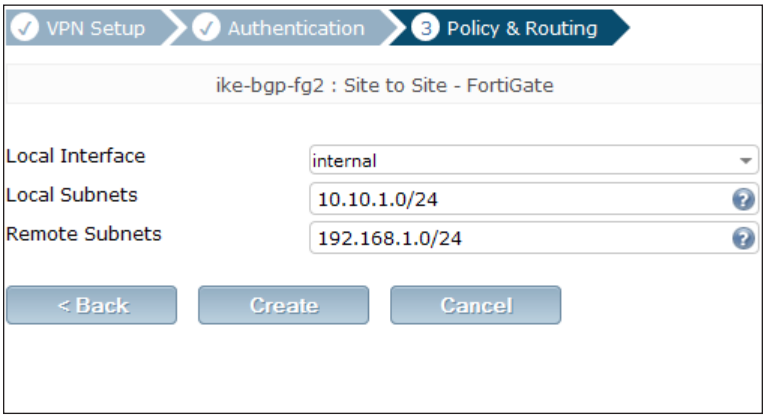
Set **Remote Gateway, Outgoing Interface** and **Pre-shared Key**.

Click **Next.**



Set **Local Interface, Local** and **Remote Subnets.**

Click **Create.**



FortiGate then will create phase 1, phase 2, static route, local and remote address group, local to remote and remote to local security policies.

3. Verifying tunnel is UP

Go to **VPN > Monitor > IPsec Monitor** to verify that the tunnel is **UP**.

4. Configuring BGP in FortiGate 1

Go to **System > Status** to look for **CLI Console** widget and type the following:

```
config router bgp
    set as 1
    set router-id 172.20.120.22
        config neighbor
            edit "172.20.120.223"
                set remote-as 2
            next
        end
        config redistribute "connected"
            set status enable
        end
        config redistribute "static"
            set status enable
        end
end
```

5. Configuring BGP in FortiGate 2

Go to **System > Status** to look for **CLI Console** widget and type the following:

```
config router bgp
    set as 2
    set router-id 172.20.120.223
        config neighbor
            edit "172.20.120.22"
                set remote-as 1
            next
        end
        config redistribute "connected"
            set status enable
        end
        config redistribute "static"
            set status enable
        end
end
```

6. 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	Up Time
Static	0.0.0.0/0	0.0.0.0	fext-wan1	
Static	0.0.0.0/0	25.52.81.253	fext-wan1	
Static	10.10.1.0/24	0.0.0.0	ike-bgp-fgt1	
BGP	10.10.80.0/24	172.20.120.223	wan1	0 00:31:21
Connected	25.52.81.0/24	0.0.0.0	fext-wan1	
Connected	169.254.1.1/32	0.0.0.0	ssl.root	
Connected	169.254.1.1/32	0.0.0.0	ssl.root	
Connected	172.20.120.0/24	0.0.0.0	wan1	
Connected	192.168.1.0/24	0.0.0.0	lan	
Connected	::1/128	::	root	

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	Up Time
Static	0.0.0.0/0	172.20.120.2	wan1	
Connected	10.10.1.0/24	0.0.0.0	internal	
Connected	10.10.80.0/24	0.0.0.0	wifi	
BGP	25.52.81.0/24	172.20.120.22	wan1	0 00:52:04
BGP	169.254.1.1/32	172.20.120.22	wan1	0 00:52:04
Connected	172.20.120.0/24	0.0.0.0	wan1	
Static	192.168.1.0/24	0.0.0.0	ike-bgp-fg2	
Connected	::1/128	::	root	

SSL VPN

This section contains information about configuring a variety of different SSL VPNs, as well as different methods of authenticating SSL VPN users.

SSL VPNs use Secure Sockets Layer (SSL) to create a Virtual Private Network (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.

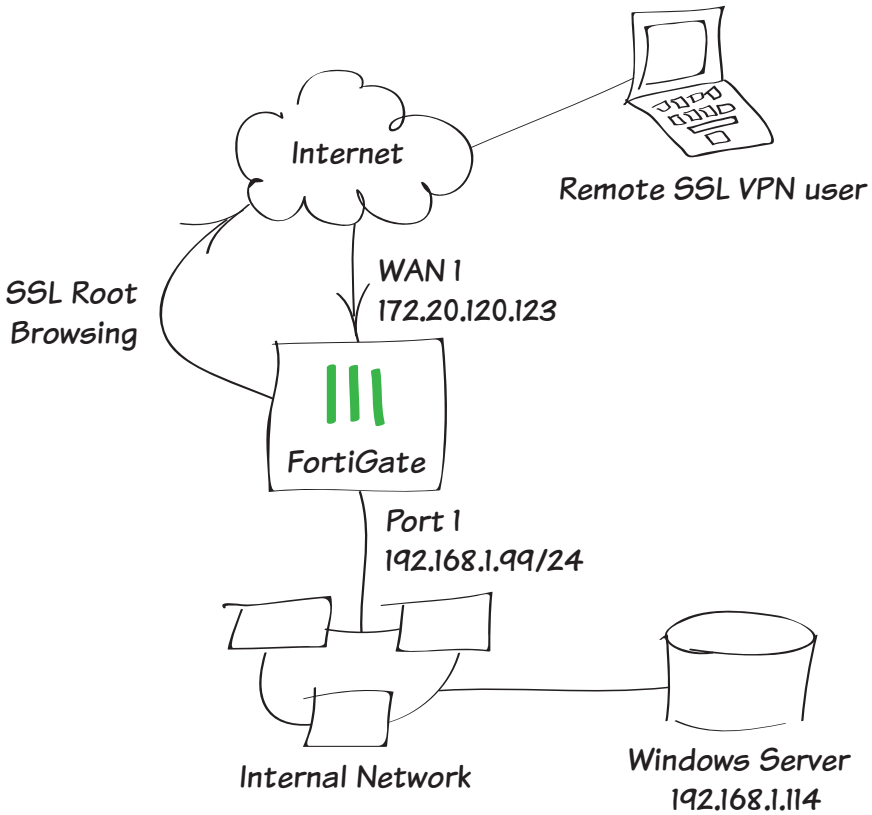
This section contains the following recipes:

- Providing remote users with access using SSL VPN

Providing remote users with access using SSL VPN

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.

1. Creating an SSL VPN portal for remote users
2. Creating a user and a user group
3. Adding an address for the local network
4. Configuring the SSL VPN tunnel
5. Adding security policies for access to the Internet and internal network
6. Setting the FortiGate unit to verify users have current AntiVirus software
7. Results



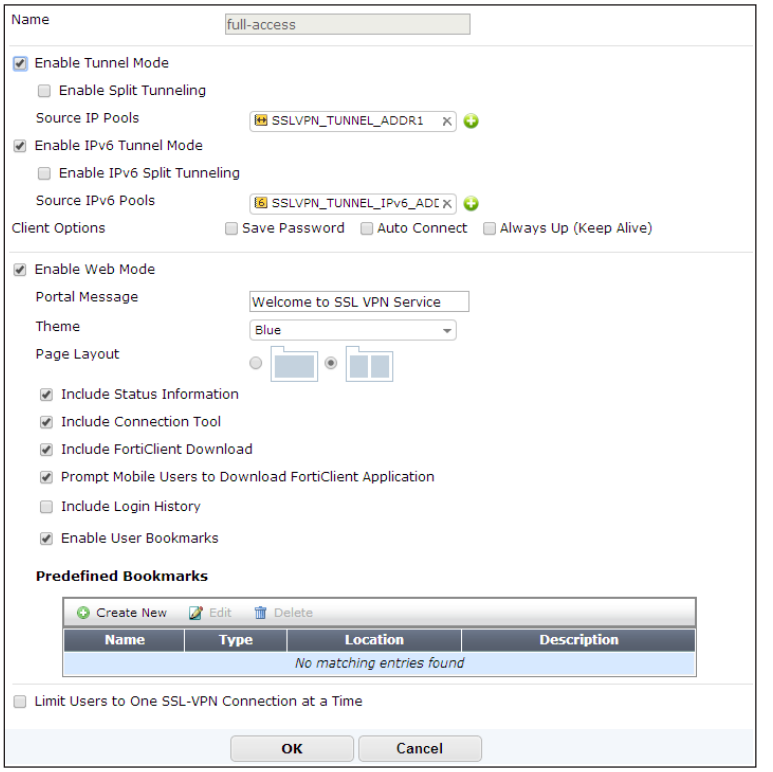
1. Creating an SSL VPN portal for remote users

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.

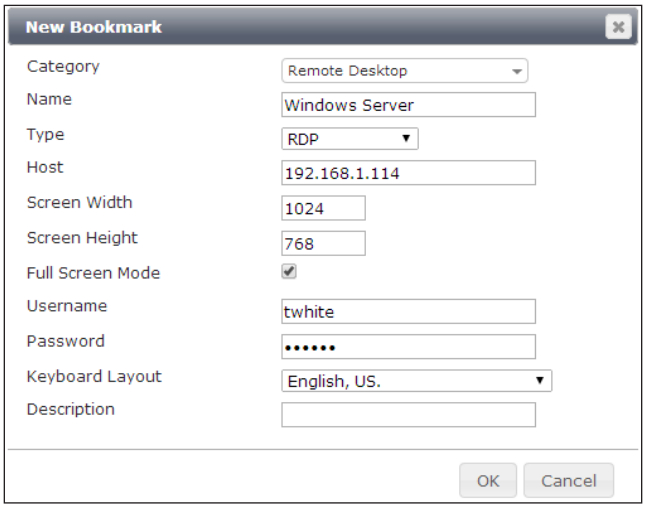
Enable Split Tunneling is *not* enabled so that all Internet traffic will go through the FortiGate unit and be subject to the corporate security profiles.



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.

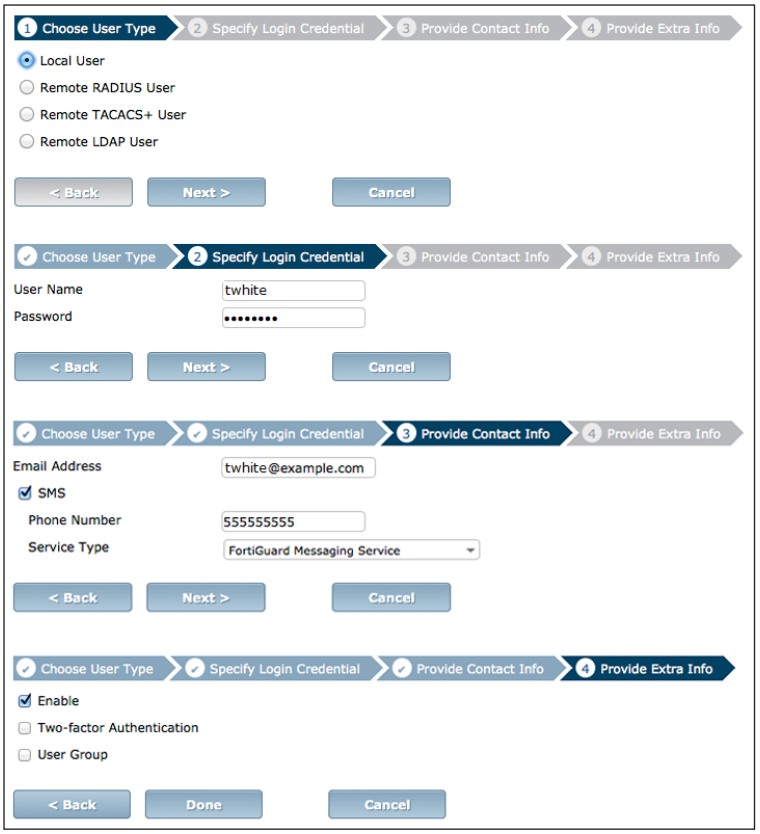
You must include a username and password. You will create this user in the next step, so be sure to use the same credentials.



2. Creating a user and a user group

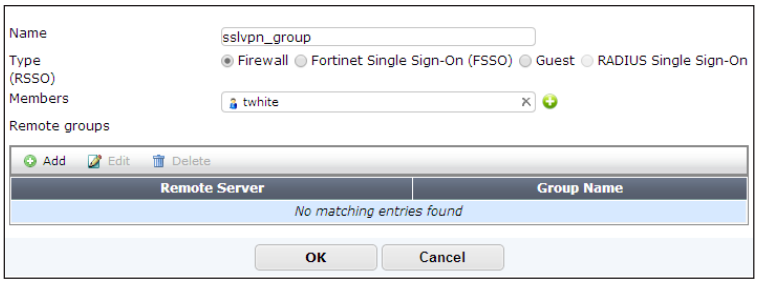
Go to **User & Device > User > User Definition**.

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**.

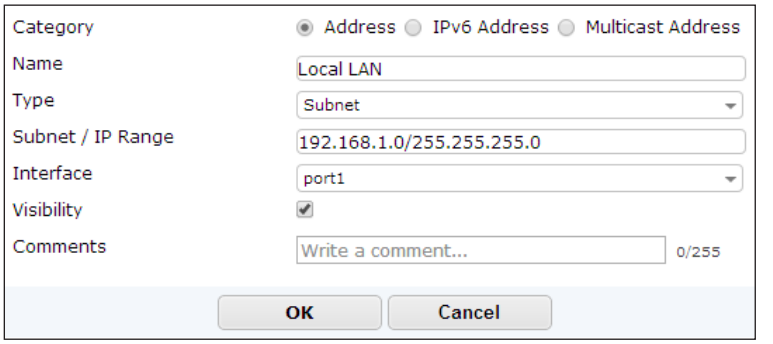
Add the user ‘twhite’ to a user group for SSL VPN connections.



3. Adding an address for the local network

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

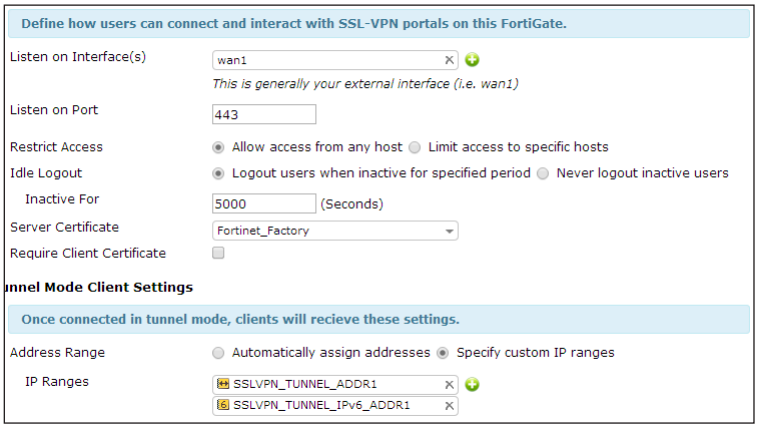
Add the address for the local network. Set **Subnet / IP Range** to the local subnet and set **Interface** to an internal port.



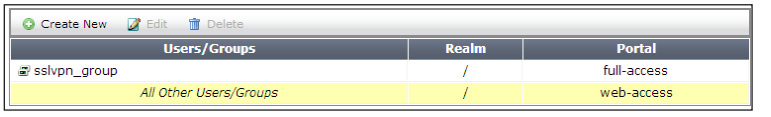
4. Configuring the SSL VPN tunnel

Go to **VPN > SSL > Settings** and set **Listen on Interface(s)** to **wan1**.

Set **Listen on Port** to **443** and **Specify custom IP ranges**.



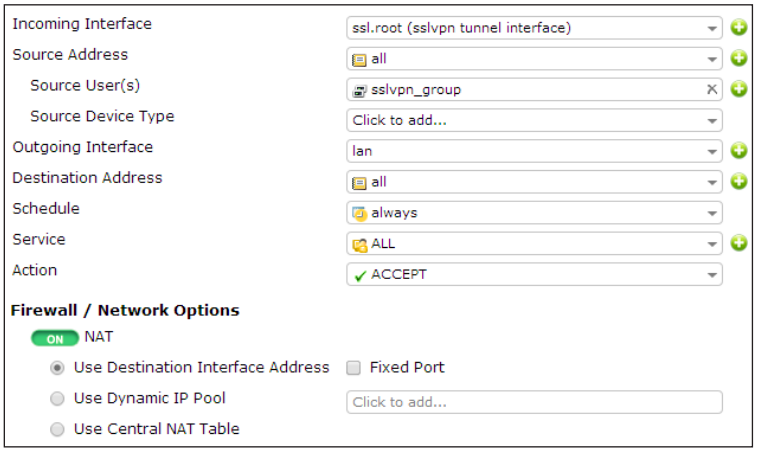
Under **Authentication/Portal Mapping**, add the SSL VPN user group.



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.



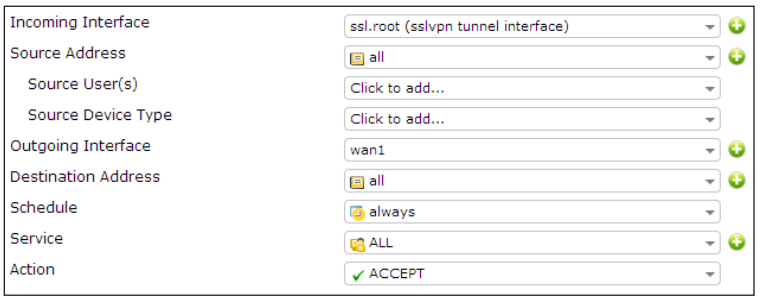
Set **Incoming Interface** to **ssl.root**.

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

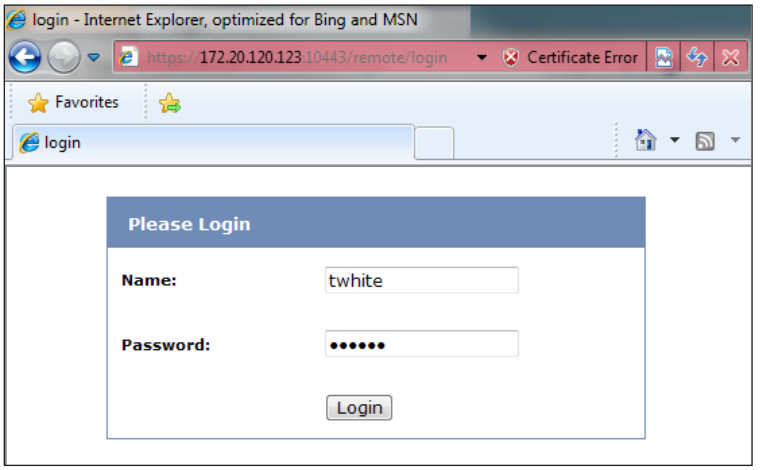
Go to **System > Status > Dashboard**.

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.

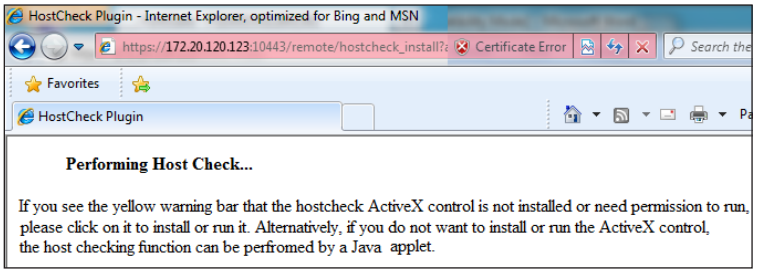
```
# config vpn ssl web portal
(portal) # edit full-access
(full-access) # set host-check av
(full-access) # end
```

7. Results

Log into the portal using the credentials you created in step 2.

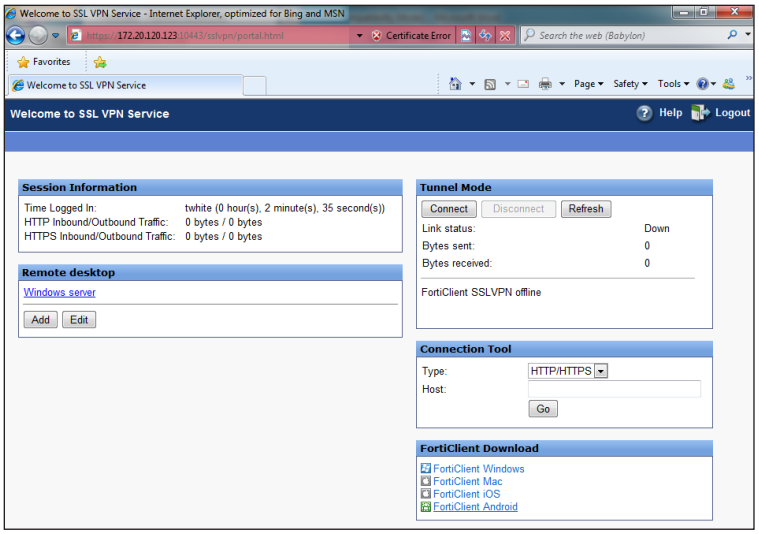


The FortiGate unit performs the host check.

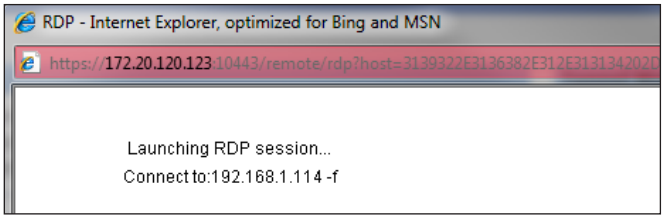


After the check is complete, the portal appears.

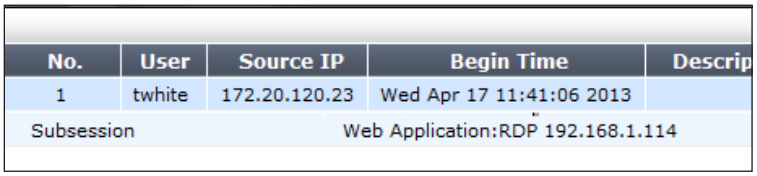
You may need to install the FortiClient application using the available download link.



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.

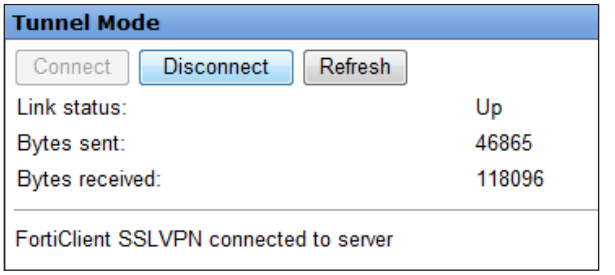


No.	User	Source IP	Begin Time	Descrip
1	twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
Subsession			Web Application:RDP 192.168.1.114	

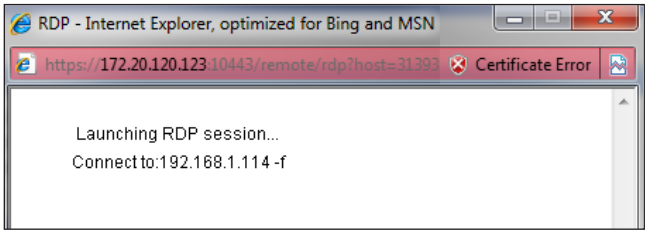
Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.

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.

No.	User	Source IP	Begin Time	D
1	twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
	Subsession		Tunnel IP:10.212.134	

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

#	Date/Time	Src Interface	Dst Interface	Src	Dst
1	14:26:05	ssl.root	wan1	10.212.134.200	74.125.133.95
2	14:26:04	ssl.root	wan1	10.212.134.200	173.194.77.94
3	14:26:04	ssl.root	wan1	10.212.134.200	173.194.43.79
4	14:26:03	ssl.root	wan1	10.212.134.200	66.171.121.34 (fortinet.co
5	14:25:57	ssl.root	wan1	10.212.134.200	74.121.50.17 (www.pages
6	14:25:44	ssl.root	wan1	10.212.134.200	208.91.113.212
7	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
8	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
9	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
10	14:24:39	ssl.root	wan1	10.212.134.200	213.199.179.159
11	14:24:37	ssl.root	wan1	10.212.134.200	213.199.179.159
12	14:24:37	ssl.root	wan1	10.212.134.200	132.246.2.6 (www.msftncs

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

Fortinet Product Integration

This section contains information 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.

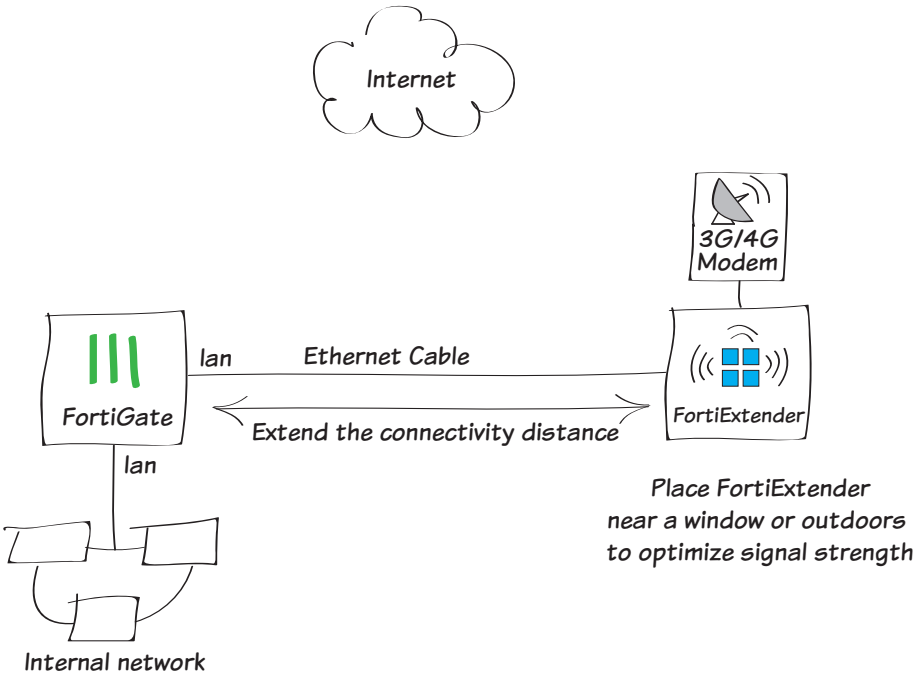
This section contains the following recipes:

- Setting up an Internet connection through a FortiGate unit using a 3G/4G modem and a FortiExtender

Setting up an Internet connection through a FortiGate unit using a 3G/4G modem and a FortiExtender

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.

1. Installing the 3G/4G modem in the FortiExtender
2. Connecting the FortiExtender
3. Configuring the FortiExtender
4. Modem settings
5. Configuring the FortiGate
6. Results



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

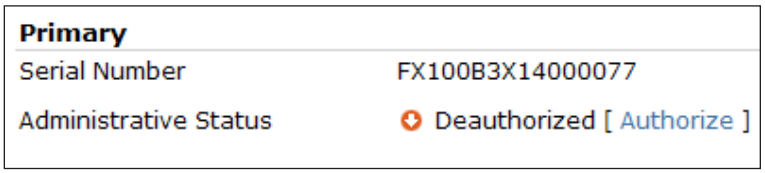
```
config system global
    set fortiextender enable
    set wireless-controller enable
end

config system interface
    edit lan
    set allowaccess capwap
end
```

CAPWAP service must be enabled on the port to which FortiExtender is connected, **lan** interface in this example.

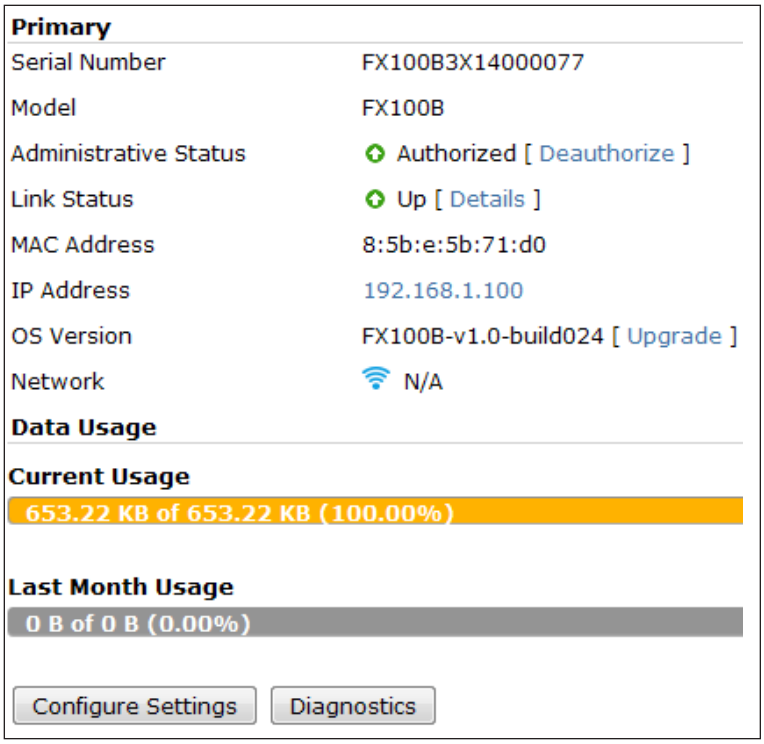
Once enabled, it appears as a virtual WAN interface in the FortiGate, such as **fext-wan1**. Go to **System > Network > Interface** to verify **fext-wan1** interface.

3. Configuring the FortiExtender

Go to **System > Network > FortiExtender** and authorize the FortiExtender.



Once authorized, you can see the status of the FortiExtender.

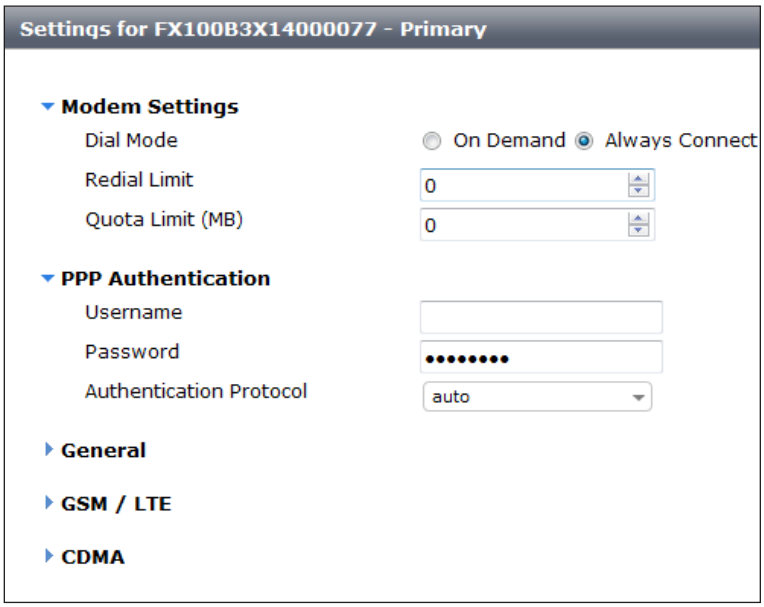


4. Modem settings

The FortiExtender unit allows for two modes of operation for the modem; On Demand and Always Connect.

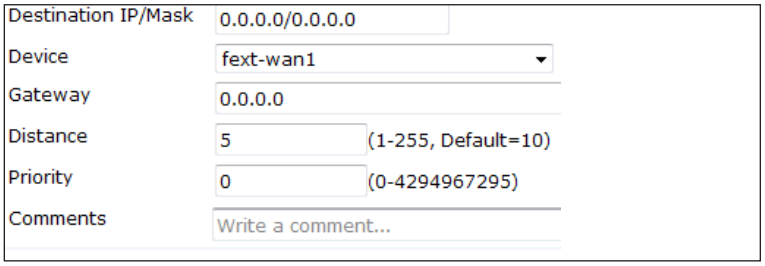
Go to **System > Network > FortiExtender** and click on **Configuring Settings**.

Select **Always Connect** for **Dial Mode** and keep other settings to default.

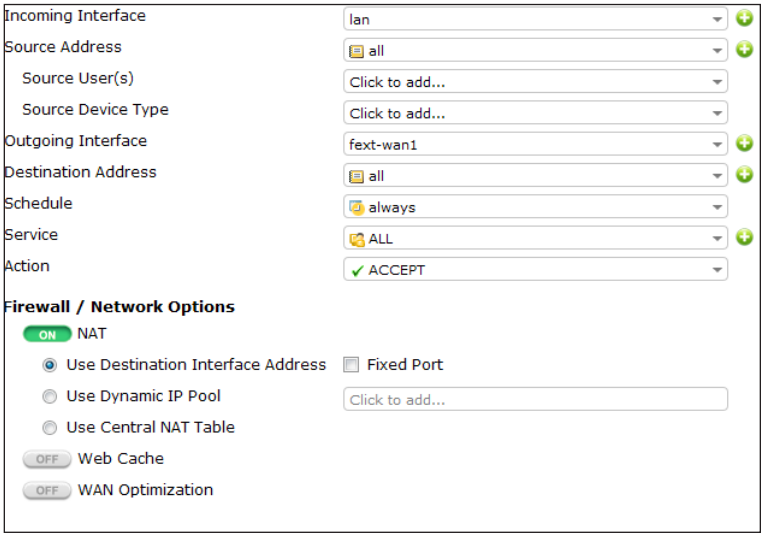


5. Configuring the FortiGate

Go to **Router > Static > Static Routes** and add new route through **fext-wan1** interface.

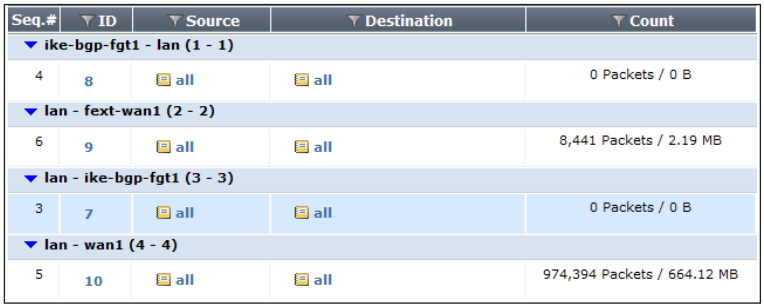


Go to **Policy & Objects > Policy > IPv4** and create a new security policy allowing traffic from **lan** interface to **fext-wan1** interface.



6. Results

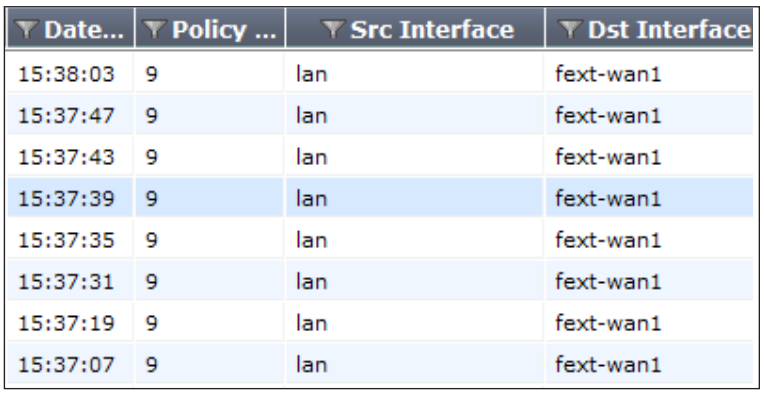
Browse the Internet and go to **Policy & Objects > Policy > IPv4** to verify the **Count**.



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

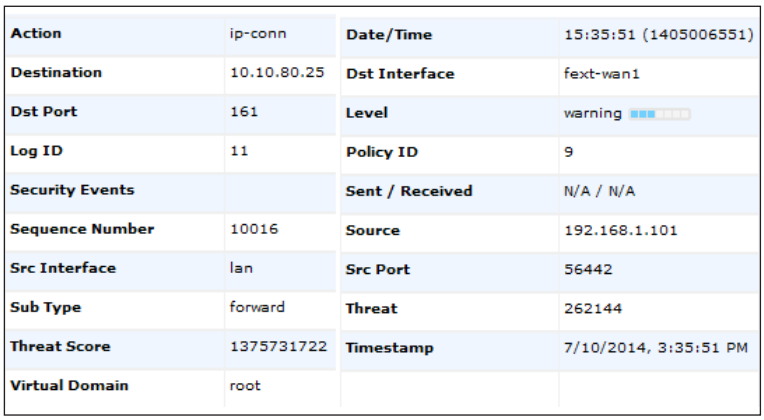
Go to **Log & Report > Traffic Log > Forward Traffic**.

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

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		

Advanced Configurations

FortiGate units can be deployed in many ways to meet a wide range of advanced requirements. This chapter contains some of these advanced configurations.

This section contains the following recipes:

- Configuring redundant architecture using two FortiGates and internal switching

Configuring redundant architecture using two FortiGates and internal switching

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. The Scenario

This section section explains the problems that this new network topology solves, including the cases in which the topology should be used.

2. The Topology

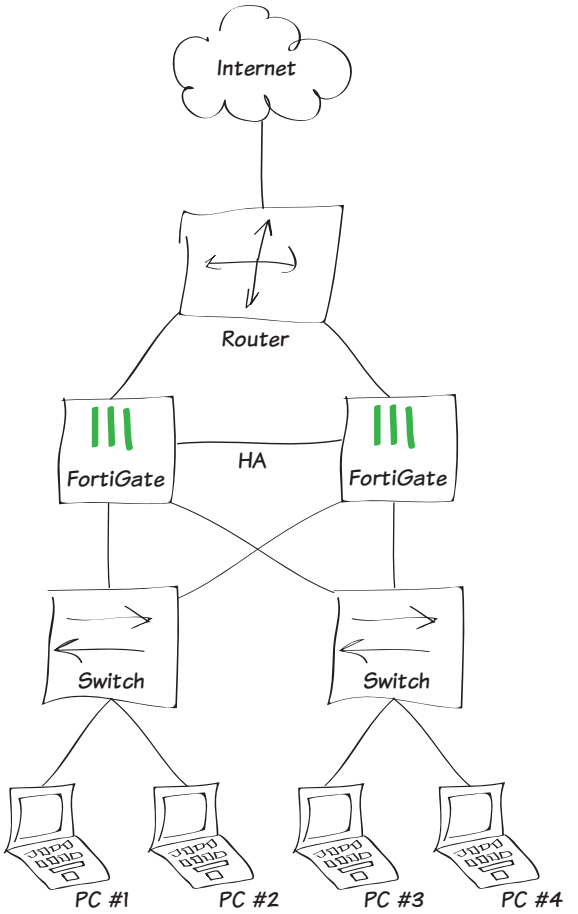
This section includes diagrams of the new topology. It also lists key advantages to this kind of architecture and explains why it solves the problems previously identified in The Scenario.

3. Configuration

This section provides step-by-step instructions for configuring the FortiGates within the new topology.

1. The Scenario

In the standard scenario, we assume the following topology as the starting point:



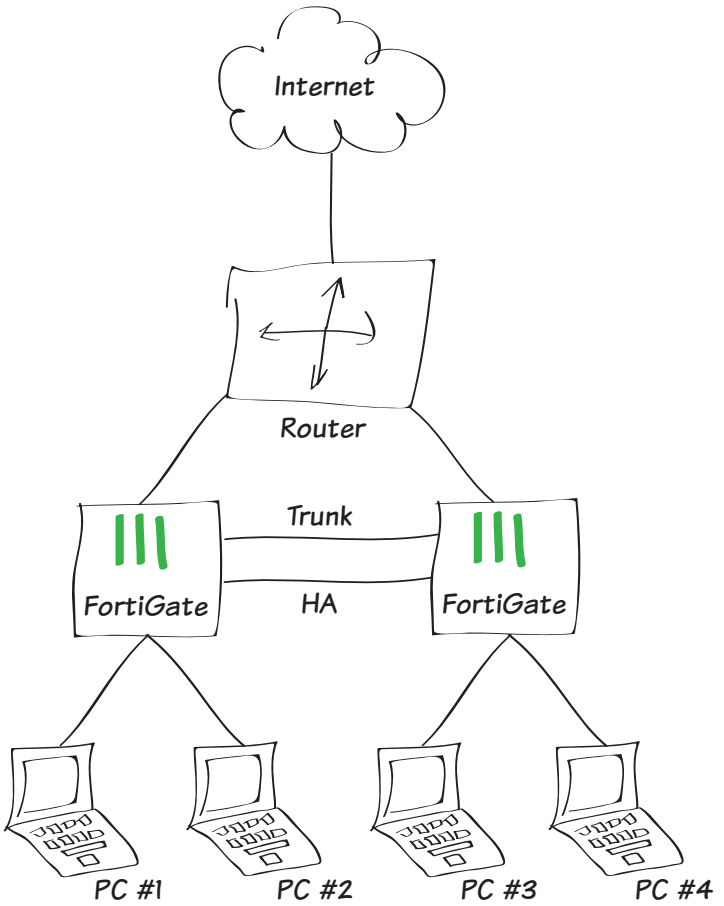
Multi-site customers that want to avoid any “Single Point of Failure” in their remote networks often use this kind of topology. These customers require two FortiGates in Active/Passive mode and therefore two switches on the LAN side to transfer Ethernet payloads to the active FortiGate. There are a few 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.

2. The 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



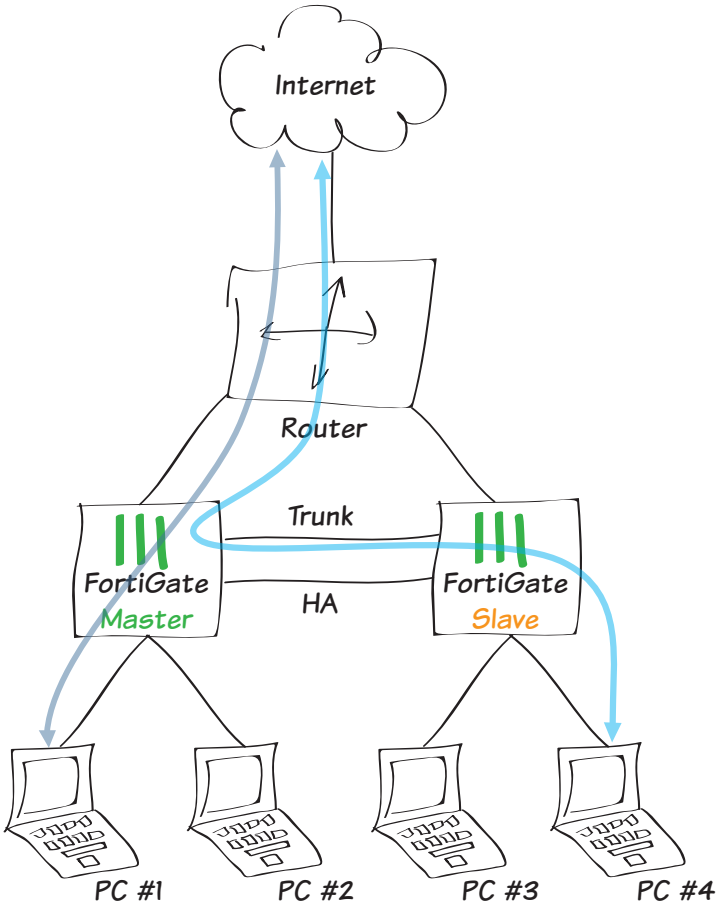
In this new topology, we won't be using additional switches. Instead, we will be using the FortiGate's Integrated Switch Fabric (ISF) solution on both master and slave firewalls.

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:

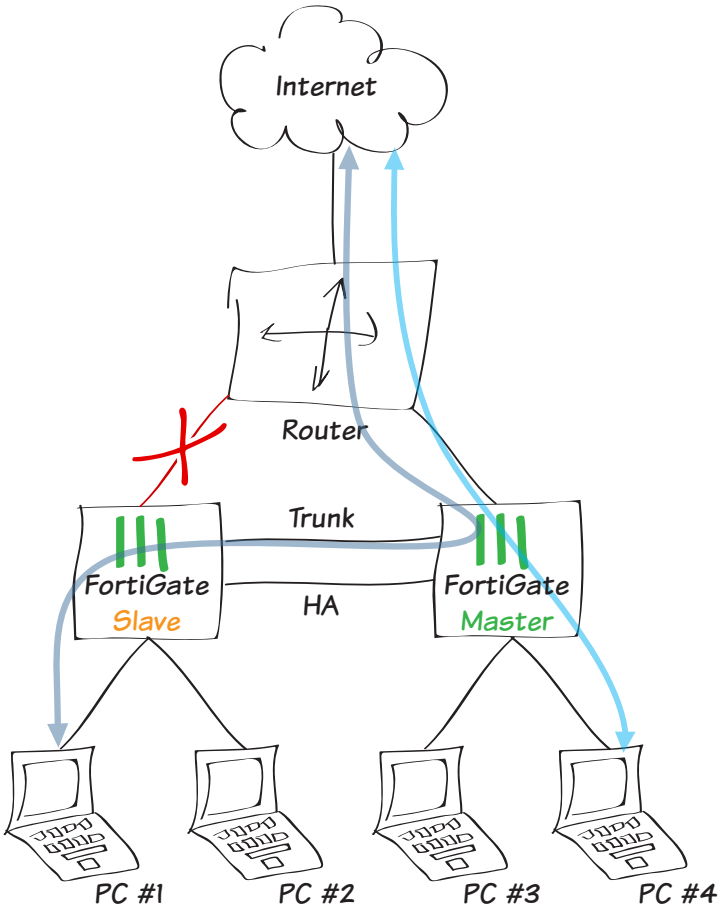


2.2 FortiGate Failover

Case 1: Link failure

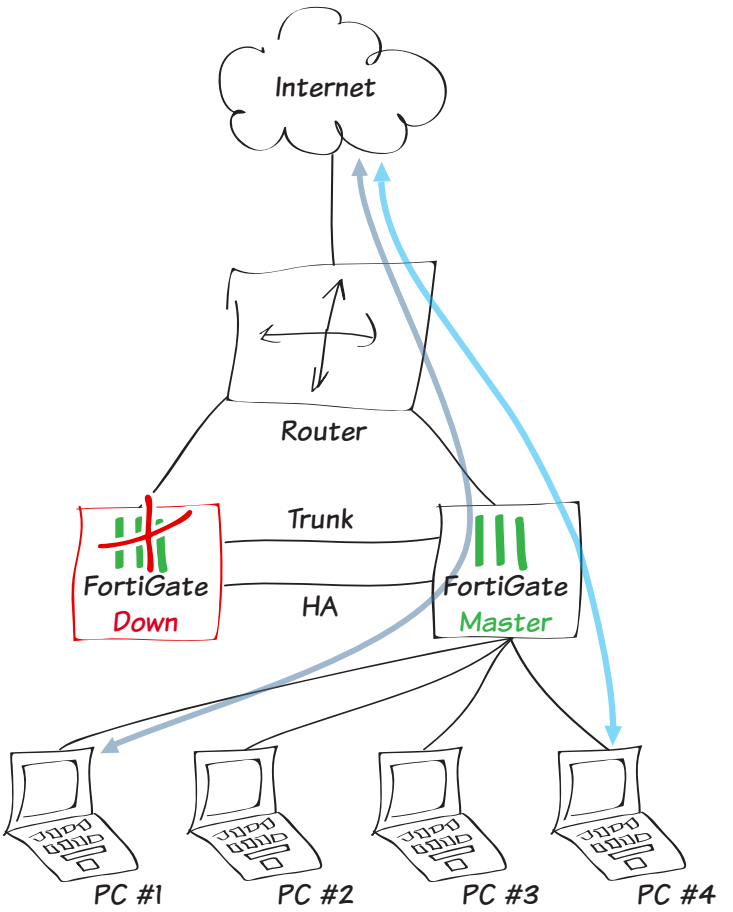
The diagram below represents traffic flow in the event of a failover in the following cases:

- 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 LAN segments into the remaining firewall, just as if one switch were to fail in our standard topology.



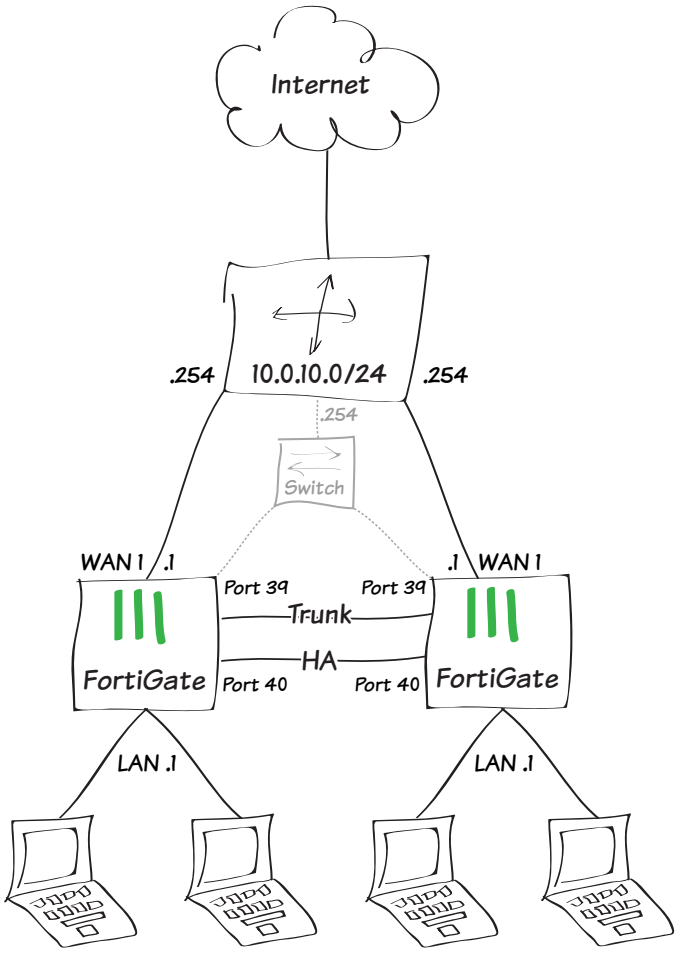
2.3 Key Advantages

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.

3. 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.

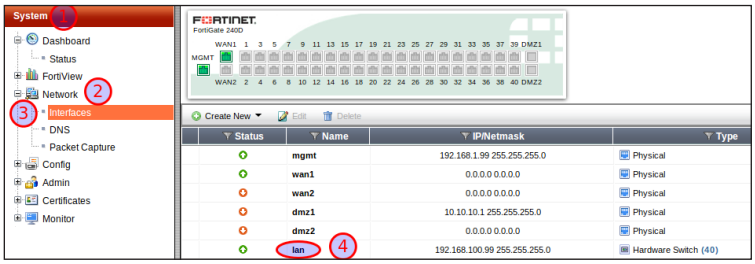
Step 1: Configure the hardware switch

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.

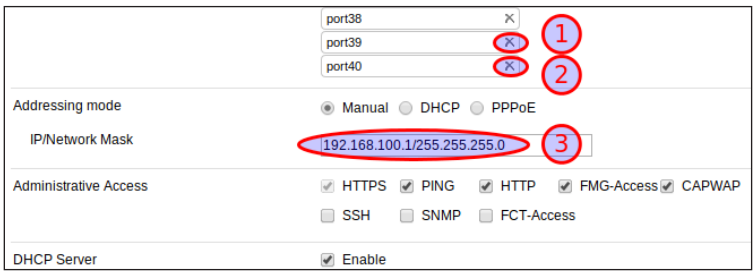
Go to **System** > **Network** > **Interfaces** and double-click **lan** in the interface list.



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.

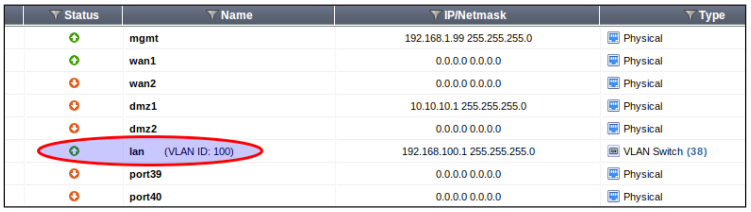
First we need to enable this feature globally. Use the commands shown here:

```
FGT1 # config system global
FGT1 (global) # set virtual-switch-vlan
                enable
FGT1 (global) # end
FGT1 # show system global
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.



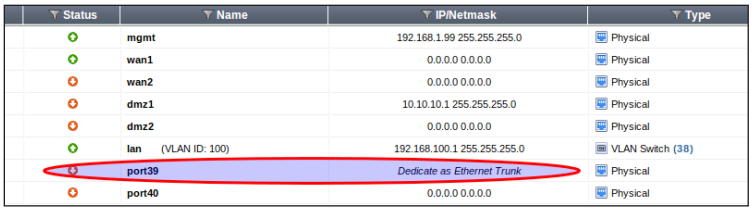
Step 2: Configure the trunk port

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 vdom "root"
        set type physical
        set trunk enable
        set snmp-index 10
    next
end
```

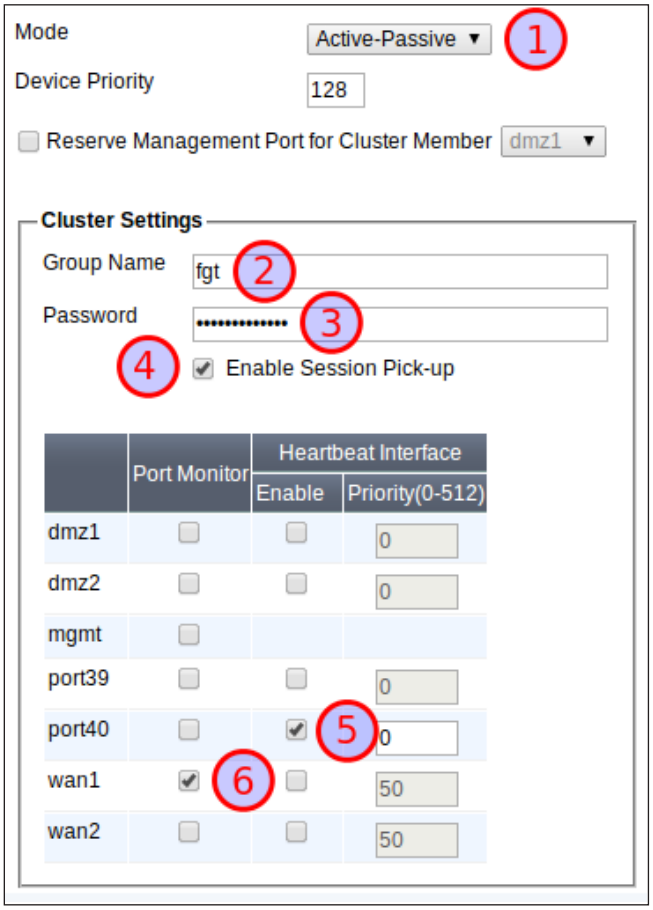
You should now be able to see the trunk port in the interface list.



Step 3: Configure HA

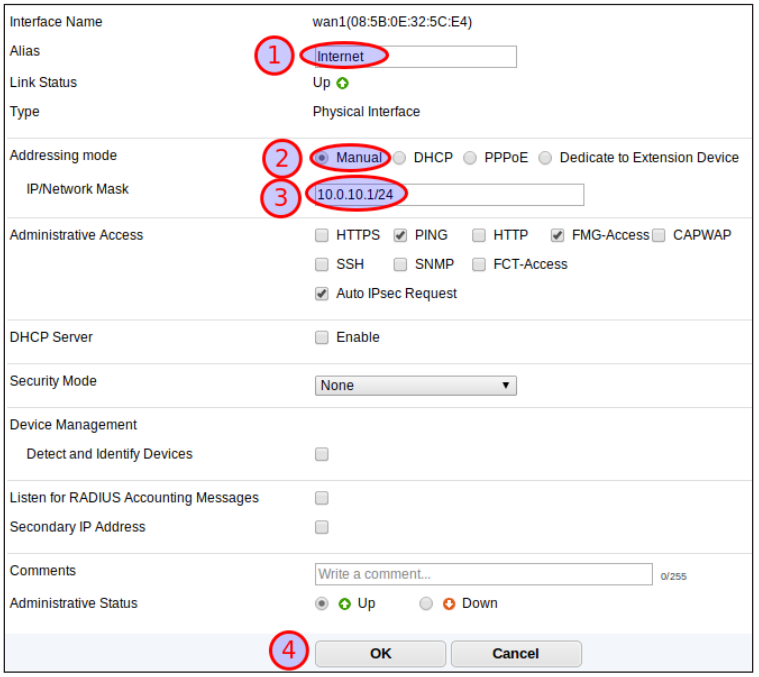
We will now configure High Availability. Port 40 will be used for HeartBeat/Sync communications between cluster members. Port Wan1 will be monitored.

Go to **System** > **Config** > **HA** and configure High Availability as shown:

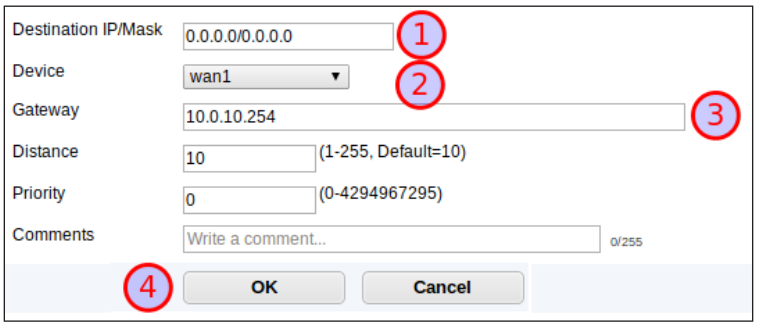


Step 4: Configure WAN1 IP routing

Go to **System** > **Network** > **Interfaces** and edit **wan1** as shown.



Go to **Router** > **Static** > **Static Routes** and create a new route as shown:

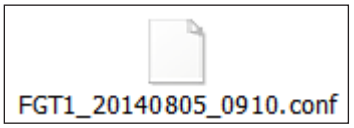


Step 5: Configure your firewall policies

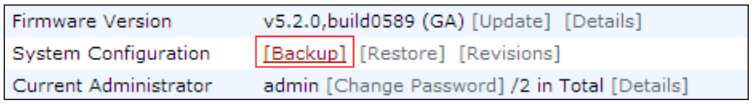
Go to **Policy & Objects** > **Policy** > **IPv4** and configure firewall policies as desired.

Step 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.



Go to **System** > **Dashboard** > **Status** and select **Backup** next to **System Configuration** in the 'System Information' panel.



You can change the hostname and HA priority lines directly in the configuration file prior to restoring it on the second FortiGate.

However, do not use a text editor like Notepad or Word to do the editing. Instead, use a code editor like Notepad++ or TextWrangler that won't add unintended content to the file.

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.

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.

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.

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.

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.

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.

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).

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 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.

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.

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.

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).

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 your FortiGate to locate websites on the Internet and can also be used in web filtering to block specific sites from being accessed.

WAN/WAN1: 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.