Recipes for success with your FortiGate

the FortiGate Cookbook

FORTIOS 5.4 VERSION

FORTINET

The FortiGate Cookbook 5.4

February-18-16

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

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

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

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

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

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

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

Table of Contents

Change Log

Date	Change description
Feb 18, 2016	Initial publication

Introduction

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

The FortiGate recipes is divided into the following sections:

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

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

This version of the complete FortiGate cookbook was written using FortiOS 5.4.0.

Tips

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

Understanding the basics

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

Screenshots vs. text

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

Model and firmware

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

For example, some FortiGate have a default interface called **lan**, while on other FortiGate models this interface is called **internal**.

Ports

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

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

IP addresses and object names

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

Text elements

Bold text indicates the name of a GUI field or feature. When required, *italic text* indicates information that you must enter. Italics are also used for notes, which contain information you may find useful.

Selecting OK/Apply

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

IPv4 vs IPv6 policies

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

Turning on FortiOS features

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

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

Getting Started

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

Installation

- Installing a FortiGate in NAT/Route mode
- Installing a FortiGate in Transparent mode
- VDOM configuration
- Troubleshooting your FortiGate installation

Setting up your FortiGate

- Creating security policies
- Creating a virtual wire pair

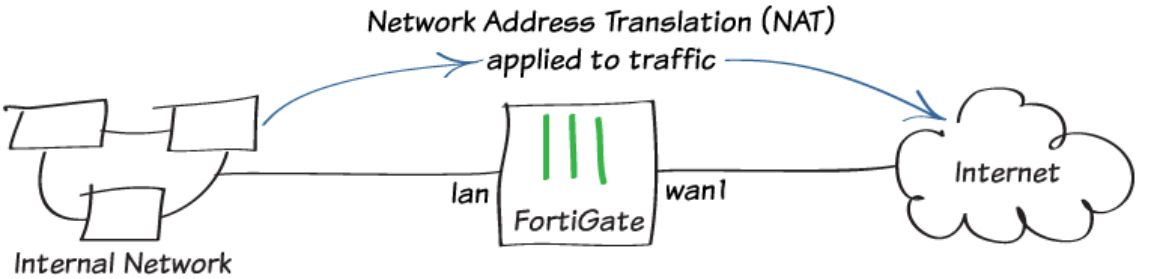
Common configurations

- Limiting bandwidth with traffic shaping

Using a FortiGate with other Fortinet products

- Managing FortiSwitches with a FortiGate

Installing a FortiGate in NAT/Route mode



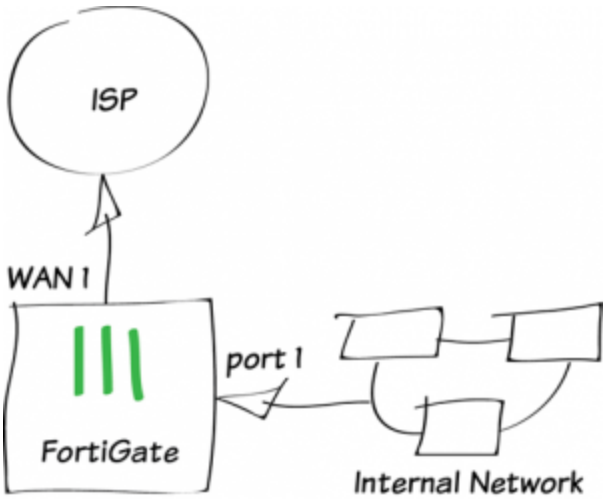
In this example, you will learn how to connect and configure a new FortiGate unit in NAT/Route mode to securely connect a private network to the Internet.

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

1. Connecting the network devices and logging onto the FortiGate

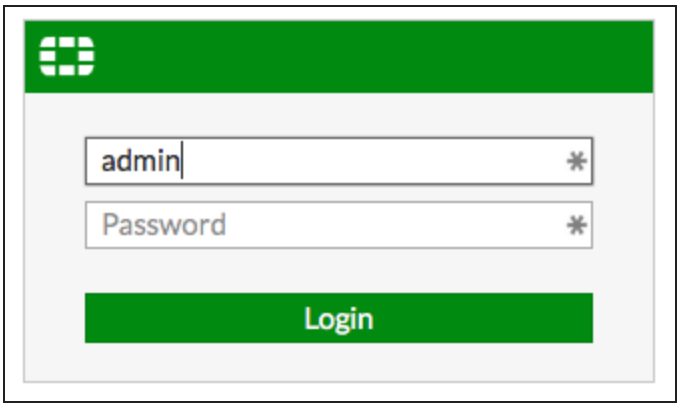
Connect the FortiGate's Internet-facing interface (typically WAN1) to your ISP-supplied equipment and Connect a PC to the FortiGate using an internal port (typically port 1).

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).

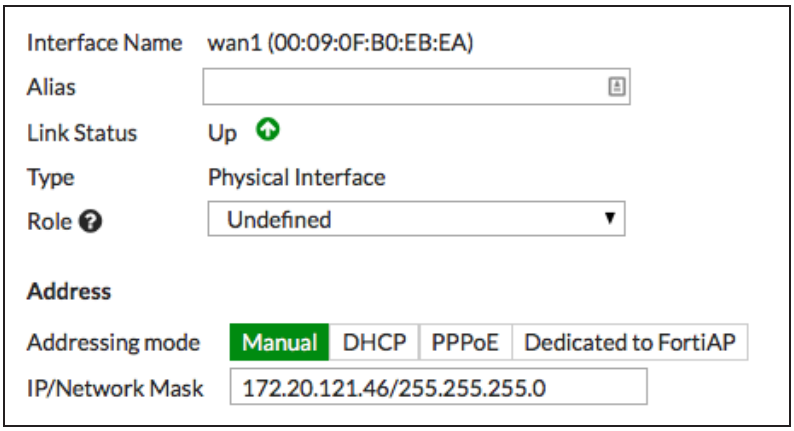
Login using an admin account (the default admin account has the username admin and no password).



2. Configuring the FortiGate's interfaces

Go to **Network > Interfaces** and edit the Internet-facing interface (in the example, *wan1*).

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



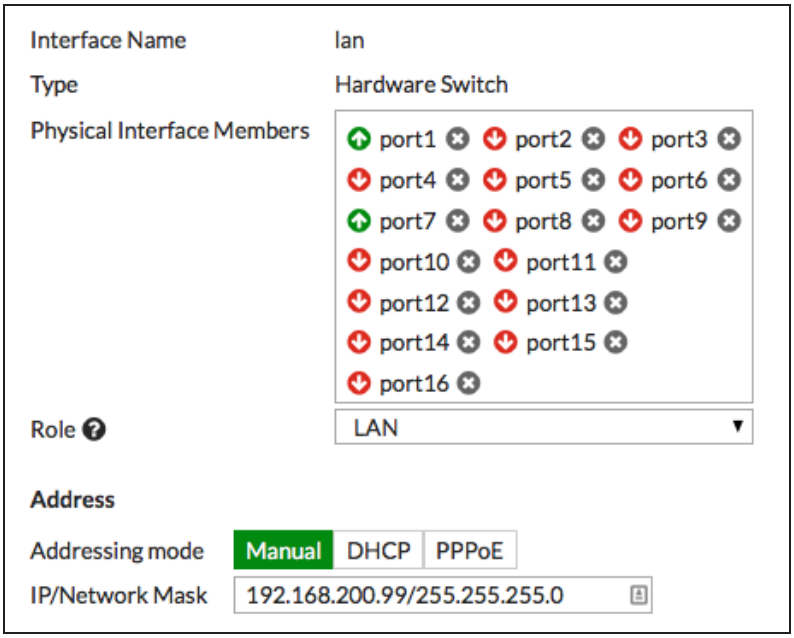
If you have ISP equipment between your FortiGate and the Internet (for example, a router), then the wan1 IP will also use a private IP assigned by the ISP equipment. If this equipment uses DHCP, set **Addressing Mode** to **DHCP** to get an IP assigned to the interface.

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

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

Make sure the interface's **Role** is set to **LAN**.

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

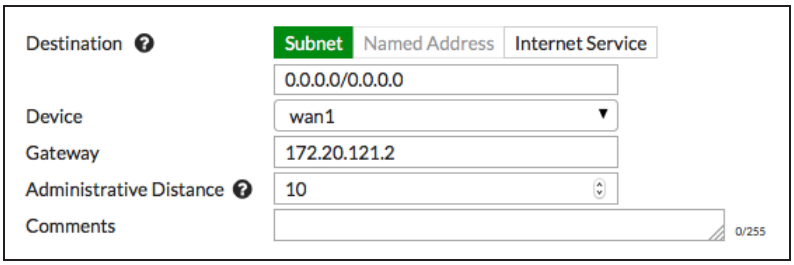


3. Adding a default route

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

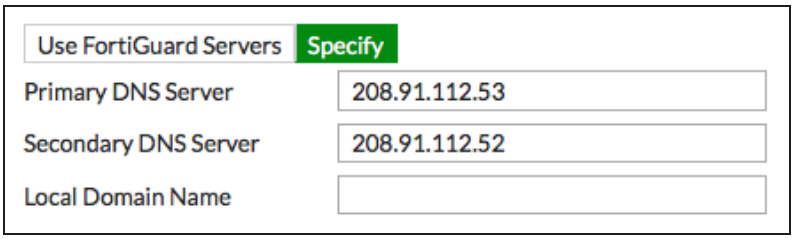
Set **Destination** to **Subnet**, **Destination IP/Mask** to *0.0.0.0/0.0.0.0*, the **Device** to the Internet-facing interface, and the **Gateway** to the gateway (or default route) provided by your ISP or to the next hop router, depending on your network requirements.

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 **Network > DNS**, select **Specify**, and add **Primary** and **Secondary** servers.



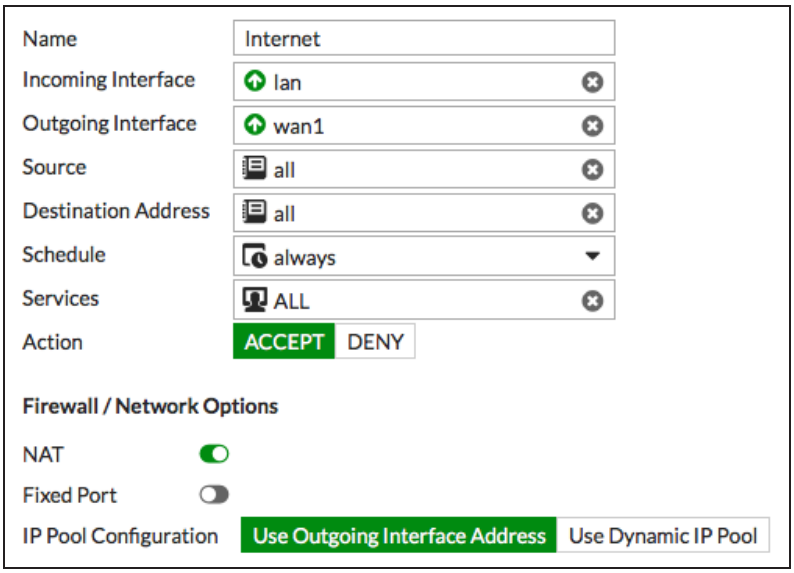
5. Creating a policy to allow traffic from the internal network to the Internet

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.

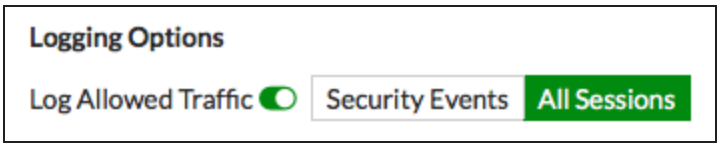
Go to **Policy & Objects > IPv4 Policy** and create a new policy. Give the policy a **Name** that indicates that the policy will be for traffic to the Internet (in the example, *Internet*).

Set the **Incoming Interface** to the **lan** interface and the **Outgoing Interface** to the Internet-facing interface. Set **Source**, **Destination Address**, **Schedule**, and **Services** as required.

Make sure the **Action** is set to **ACCEPT**. Turn on **NAT** and make sure **Use Outgoing 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**.

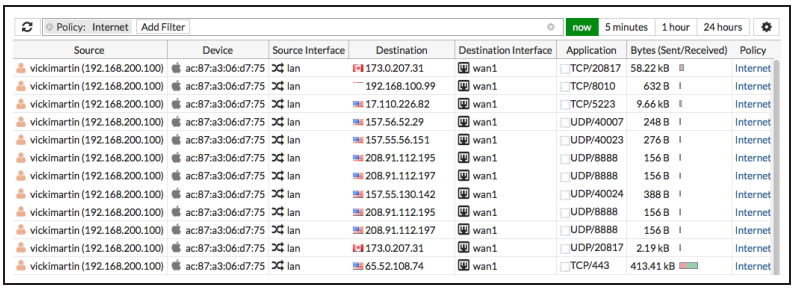


5. Results

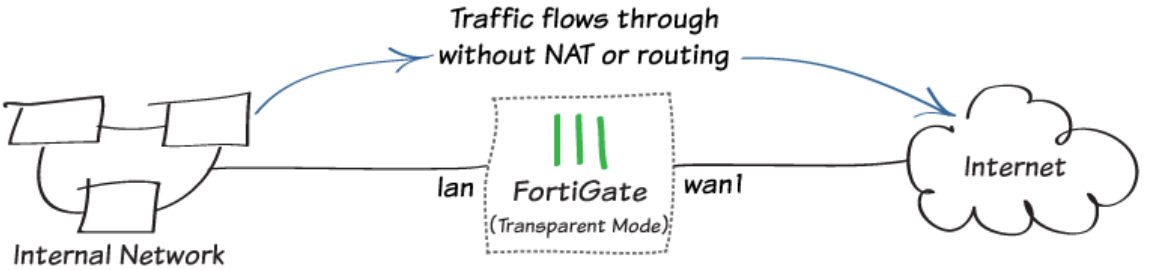
You can now browse the Internet using any computer that connects to the FortiGate's internal interface.

You can view information about the traffic being processed by your FortiGate by going to **FortiView > All Sessions** and selecting the **now** view.

Select **Add Filter** and filter for **Policy**, selecting the name of your new policy. Only traffic flowing through the new policy is displayed.



Installing a FortiGate in Transparent mode



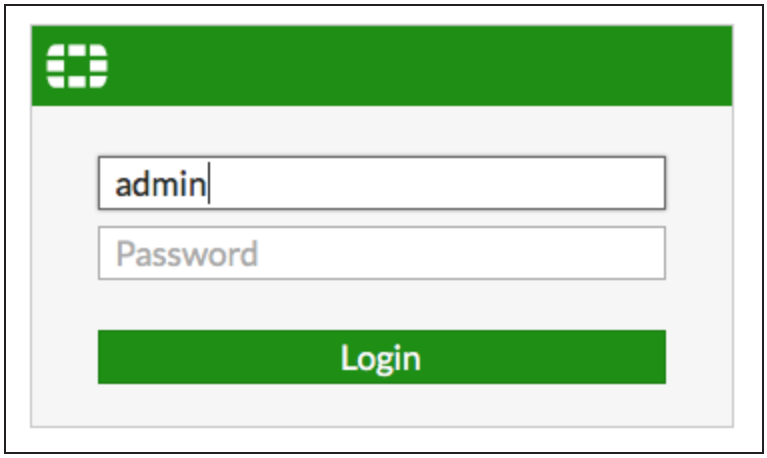
In this example, you will learn how to connect and configure a new FortiGate unit in Transparent mode to securely connect a private network to the Internet.

Transparent mode is used if you want to apply security scanning to traffic without applying routing or network address translation (NAT), such as when a FortiGate is used as an Internal Segmentation Firewall (ISFW).

1. Changing the FortiGate's operation mode

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).

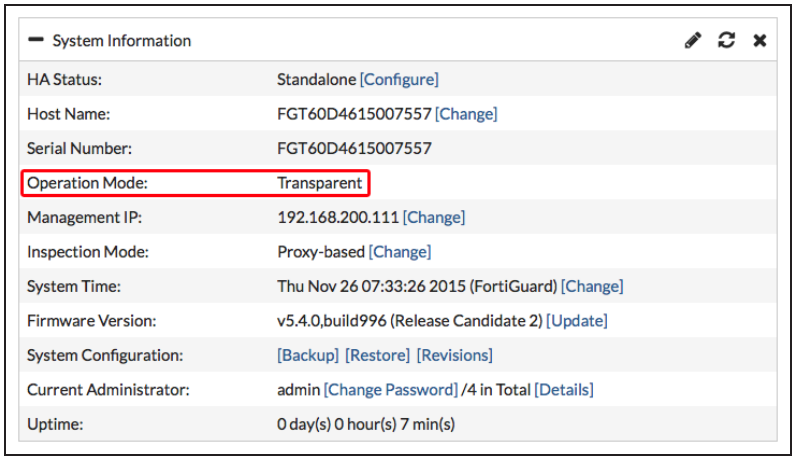


Go to the **Dashboard** and enter the following command into the CLI console widget, substituting your own IP addresses where necessary:

```
config system settings
   set opmode transparent
   set manageip 192.168.200.111 255.255.255.0
   set gateway 192.168.200.99
end
```

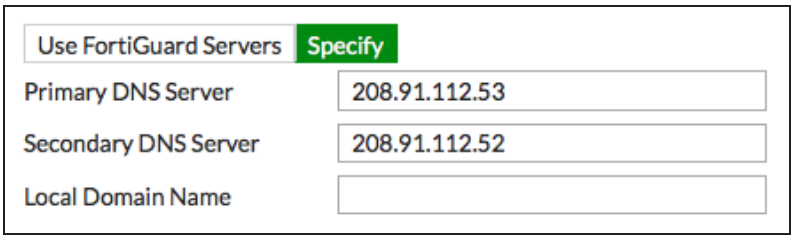
You can now access the FortiGate using the new Management IP address (in the example, *https://192.168.200.111*).

Go to the **Dashboard**. The **System Information widget** shows the **Operation Mode** is **Transparent**.



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 **Network > DNS**, select **Specify**, and add **Primary** and **Secondary** DNS servers.



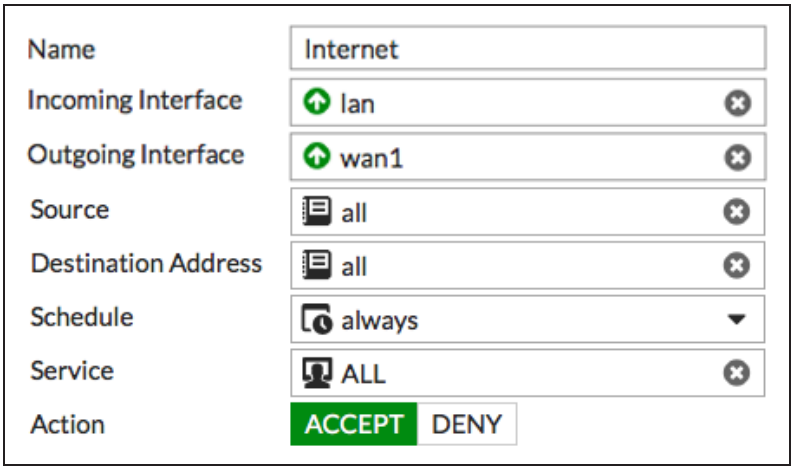
3. Creating a policy to allow traffic from the internal network to the Internet

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.

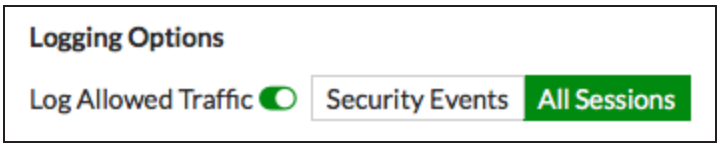
Go to **Policy & Objects > IPv4 Policy** and create a new policy. Give the policy a **Name** that indicates that the policy will be for traffic to the Internet (in the example, *Internet*).

Set the **Incoming Interface** to the **internal** interface (called **internal** on some FortiGate models) and the **Outgoing Interface** to the Internet-facing interface (typically **wan1**). Set **Source**, **Schedule**, and **Services** as required.

Make sure the **Action** is set to **ACCEPT**.



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

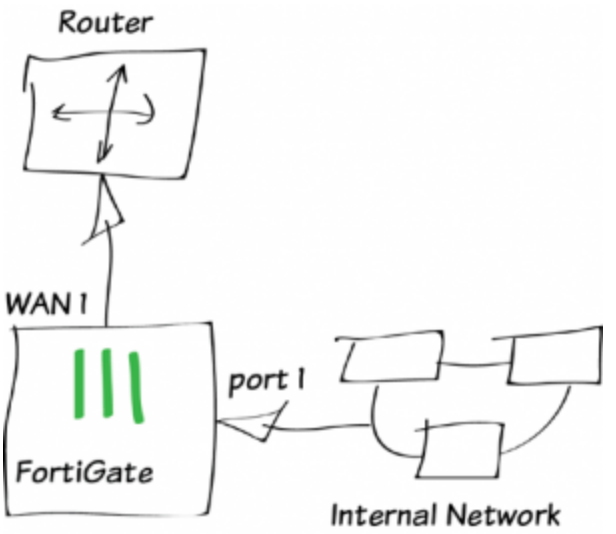
Alternatively, you can enter the following command in the **CLI Console**:

```
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.



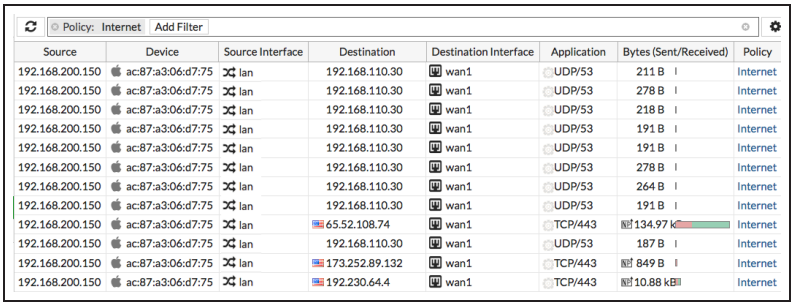
Power on the FortiGate unit.

5. Results

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

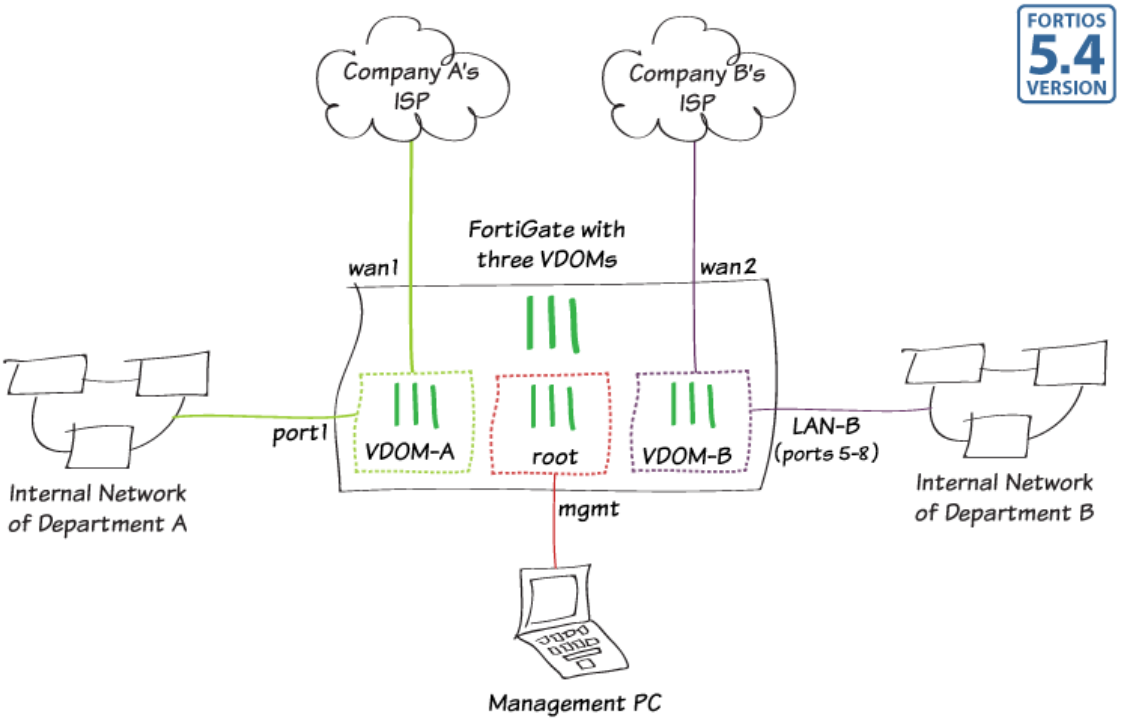
You can view information about the traffic being processed by your FortiGate by going to **FortiView > All Sessions** and selecting the **now** view.

Select **Add Filter** and filter for **Policy**, selecting the name of your new policy. Only traffic flowing through the new policy is displayed.



Source	Device	Source Interface	Destination	Destination Interface	Application	Bytes (Sent/Received)	Policy
192.168.200.150	ac:87:a3:06:d7:75	lan	192.168.110.30	wan1	UDP/53	211 B	Internet
192.168.200.150	ac:87:a3:06:d7:75	lan	192.168.110.30	wan1	UDP/53	278 B	Internet
192.168.200.150	ac:87:a3:06:d7:75	lan	192.168.110.30	wan1	UDP/53	218 B	Internet
192.168.200.150	ac:87:a3:06:d7:75	lan	192.168.110.30	wan1	UDP/53	191 B	Internet
192.168.200.150	ac:87:a3:06:d7:75	lan	192.168.110.30	wan1	UDP/53	191 B	Internet
192.168.200.150	ac:87:a3:06:d7:75	lan	192.168.110.30	wan1	UDP/53	278 B	Internet
192.168.200.150	ac:87:a3:06:d7:75	lan	192.168.110.30	wan1	UDP/53	264 B	Internet
192.168.200.150	ac:87:a3:06:d7:75	lan	192.168.110.30	wan1	UDP/53	191 B	Internet
192.168.200.150	ac:87:a3:06:d7:75	lan	65.52.108.74	wan1	TCP/443	134.97 k	Internet
192.168.200.150	ac:87:a3:06:d7:75	lan	192.168.110.30	wan1	UDP/53	187 B	Internet
192.168.200.150	ac:87:a3:06:d7:75	lan	173.252.89.132	wan1	TCP/443	849 B	Internet
192.168.200.150	ac:87:a3:06:d7:75	lan	192.230.64.4	wan1	TCP/443	10.88 kB	Internet

VDOM configuration



This example illustrates how to use virtual domains (VDOMs) to host multiple FortiOS instances on a single FortiGate.

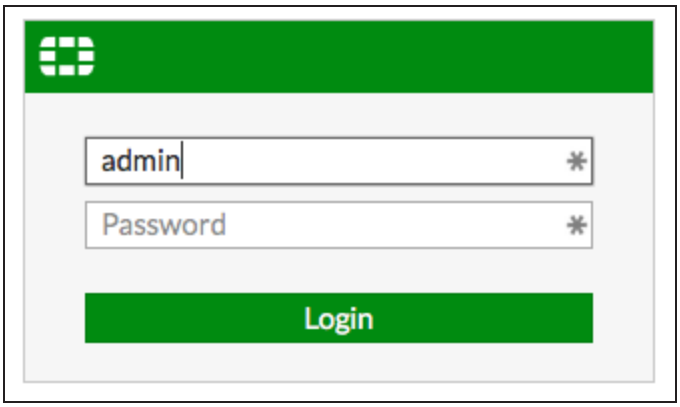
In this example, two companies (called Company A and Company B) use the same FortiGate but have different Internet service providers (ISPs). To provide both departments with network and Internet connectivity, each company has its own VDOM (called VDOM-A and VDOM-B) that are managed independently.

The **root** VDOM will be used to manage the FortiGate's global settings.

1. Switching to VDOM mode and creating two VDOMs

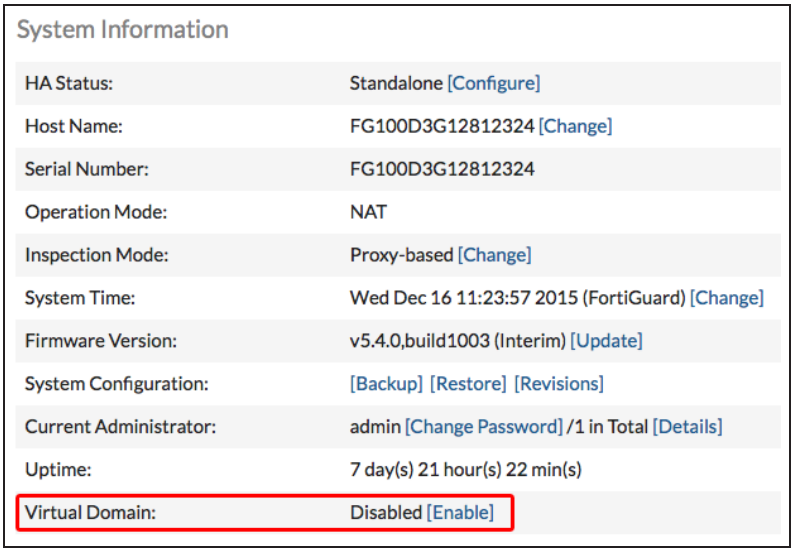
Connect a PC to FortiGate using an Ethernet cable, as described in your model's QuickStart Guide.

Log in using the admin account (the default admin account has the username admin and no password).



Go to the **Dashboard** and locate the **System Information** widget. Find **Virtual Domain** and select **Enable**.

You will be required to re-login after enabling virtual domains because the GUI menu options change.



Certain FortiGate models will not show the above option in the System Information widget. For these models, go to the **Dashboard** and enter the following command in the **CLI Console**:

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

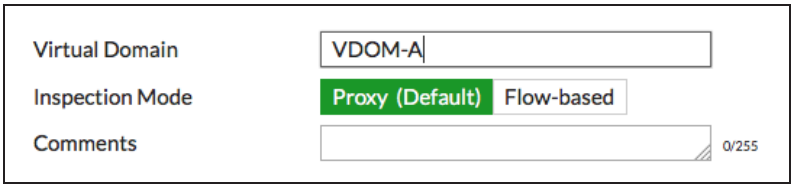
Enter *y* when you are asked if you want to continue.

You will be required to re-login to the GUI after enabling virtual domains because the GUI menu options change.

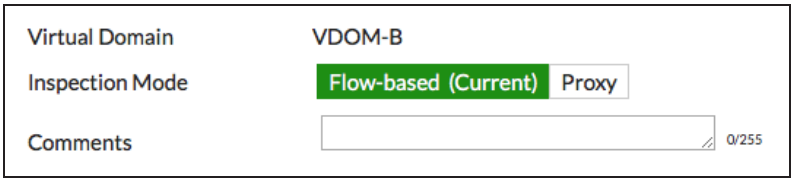
Make sure that **Global** is selected from dropdown menu located in the top-left corner. This allows you to make changes to the global configuration.

Go to **System > VDOM** and create two VDOMs: *VDOM-A* and *VDOM-B*.

In this example, the **Inspection Mode** is set to **Proxy** for VDOM-A. This will allow this VDOM to use both proxy and flow-based security scanning.



The **Inspection Mode** for VDOM-B is set to **Flow-based**, so only flow-based security scanning is available.

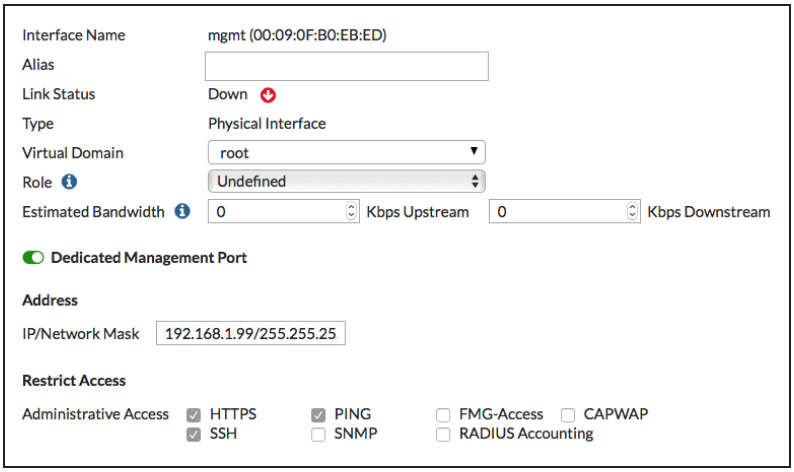


2. Configuring the root VDOM for FortiGate management

Go to **Network > Interfaces**. By default, all interfaces are in the **root** VDOM.

Edit the interface you wish to use to manage the FortiGate (in the example, *mgmt*). If you wish to use this interface exclusively for FortiGate management, you can enable **Dedicated Management Port**.

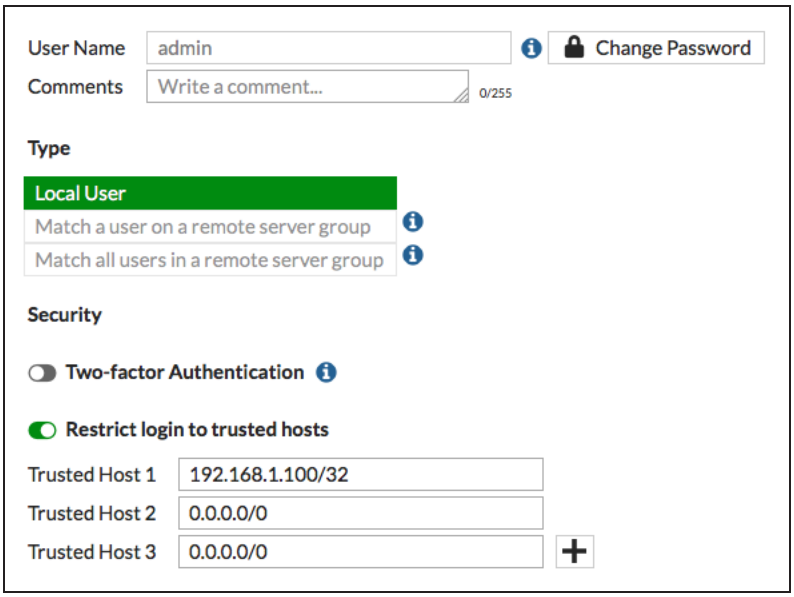
Set **Administrative Access** to **HTTPS**, **PING**, and **SSH**.



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

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

Enable **Restrict login to trusted hosts** and add the IP/Netmask of the admin PC. This ensures that the admin must login using the admin PC to be able to manage the FortiGate.



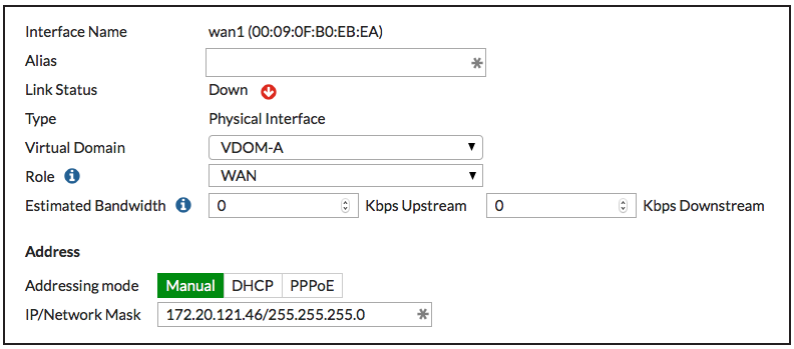
3. Adding interfaces to VDOM-A

In this example, two interfaces will be added to VDOM-A: one for Internet access and one for use by the local network.

If an interface is used in an existing FortiGate configuration, its VDOM assignment cannot be changed. Because some FortiGate models have a default configuration, you may need to delete existing policies and routes in order to add a particular interface.

Go to **Network > Interfaces** and edit the interface that VDOM-A will use for Internet access (in the example, **wan1**). [tippy title="*" class="myclass" showheader="false" width="auto" height="auto"]In the example, the interface's **Link Status** is **Down** because nothing is currently connected to the interface.[/tippy]

Set **Virtual Domain** to **VDOM-A** and **Role** to **WAN**.



If your FortiGate is directly connecting to your ISP, set **Addressing Mode** to **Manual** and set the **IP/Netmask** to the public IP address your ISP has provided you with (in the example, *172.20.121.46/255.255.255.0*).

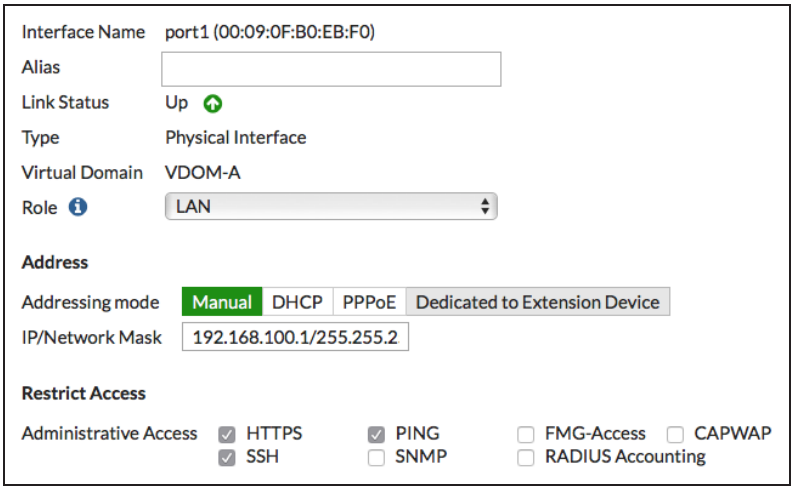
If you have some ISP equipment between your FortiGate and the Internet (for example, a router), then the wan1 IP will also use a private IP assigned by the ISP equipment. If this equipment uses DHCP, set **Addressing Mode** to **DHCP** to get an IP assigned to the interface.

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

Go to **Network > Interfaces** and edit the interface that will be connected to VDOM-A's internal network (in the example, **port1**).

Set **Virtual Domain** to **VDOM-A** and **Role** to **LAN**.

Set **Addressing Mode** to **Manual**, assign an **IP/Network Mask** to the interface (in the example, *192.168.100.1/255.255.255.0*), set **Administrative Access** to **HTTPS**, **PING**, and **SSH**.

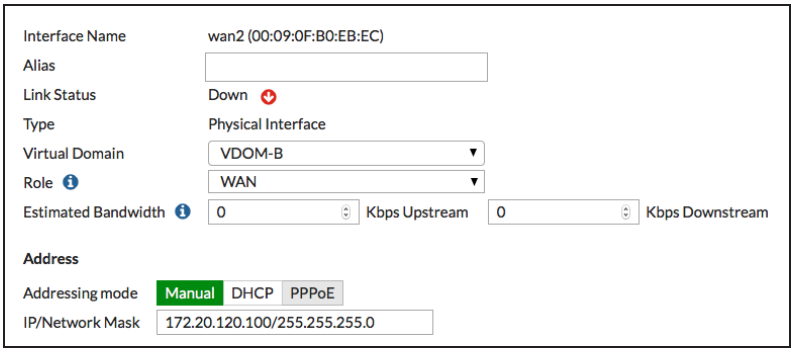


4. Adding interfaces to VDOM-B

In this example, multiple interfaces will be added to VDOM-B: one for Internet access and four additional interfaces for use by the internal network. These four interfaces will be combined into a hardware switch interface called LAN-B, which the FortiGate treats as a single interface. This example also adds a DHCP server to LAN-B to provide IP addresses for the VDOM-B's internal network.

Go to **Network > Interfaces** and edit the interface that VDOM-B will use for Internet access (in the example, **wan2**).

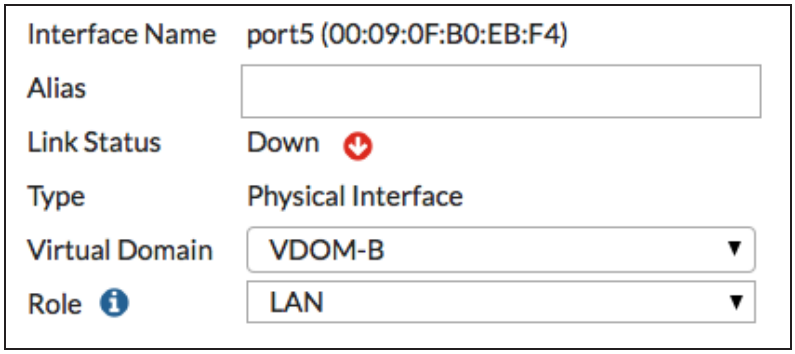
Set **Virtual Domain** to **VDOM-B** and **Role** to **WAN**. Set an appropriate **Addressing Mode** and **IP/Netmask** (in the example, *172.20.120.100/255.255.255.0*).



Go to **Network > Interfaces** and edit a physical interface that will be used by VDOM-B's internal network (in the example, **port5**).

Set **Virtual Domain** to **VDOM-B** and **Role** to **LAN**.

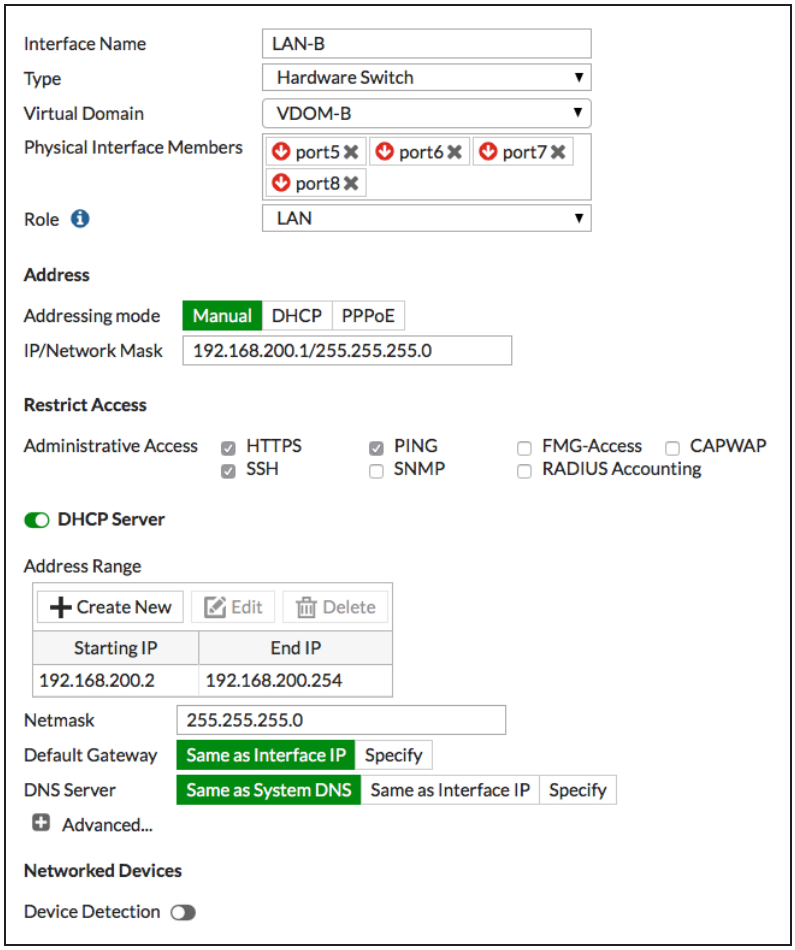
Repeat this process for any other physical interfaces that will be used by VDOM-B (in the example, **port6**, **port7**, and **port8**).



Go to **Network > Interfaces** and create a new interface to be used by VDOM-B's internal network, called *LAN-B*.

Set **Type** to **Hardware Switch** and **Virtual Domain** to **VDOM-B**. Add VDOM-B's physical interfaces as **Physical Interface Members**. Set **Role** to **LAN**.

Set **Addressing Mode** to **Manual**, assign an **IP/Network Mask** to the interface (in the example, *192.168.200.1/255.255.255.0*), set **Administrative Access** to **HTTPS**, **PING**, and **SSH** and enable **DHCP Server**.

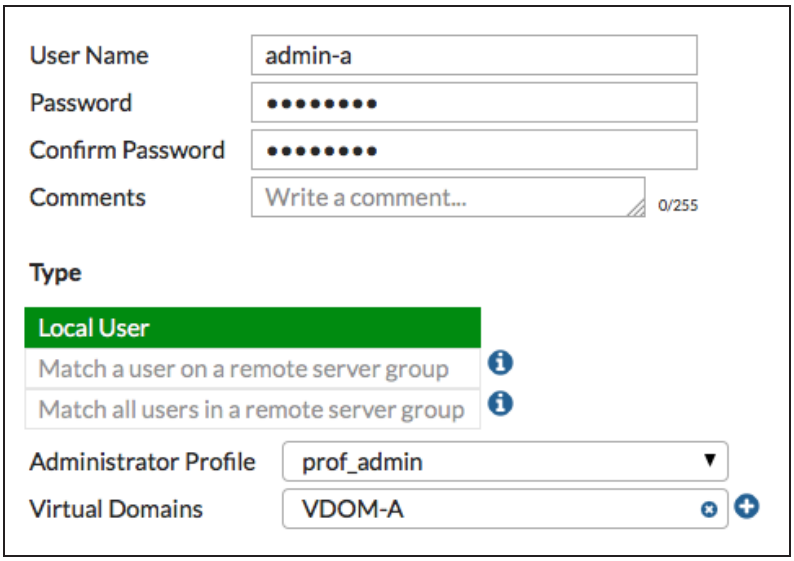


5. Adding administrators to each VDOM

Go to **System > Administrators**. Create an administrator for VDOM-A, called *admin-a*.

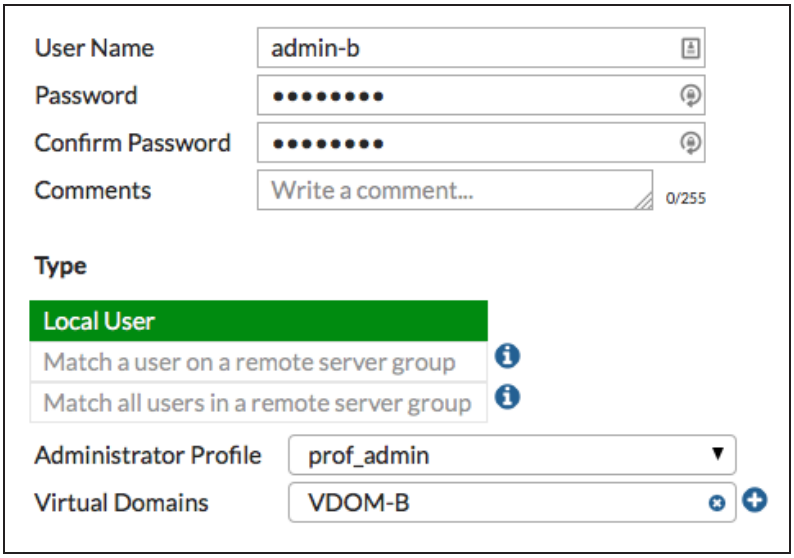
This administrator will be able to access and configure VDOM-A, without accessing either the root VDOM or VDOM-B. The account will also not be able to affect global settings.

Enter and confirm a **Password**. Set **Type** to **Local User** and **Administrator Profile** to **prof_admin**. Remove the **root** VDOM from the **Virtual Domains** list, then add **VDOM-A**.



Create an administrator that can access VDOM-B, called *admin-b*.

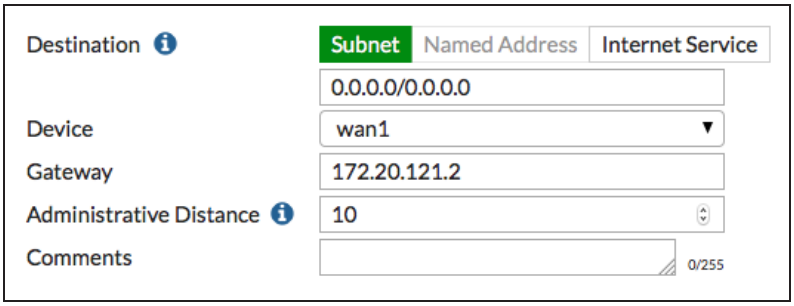
Enter and confirm a **Password**. Set **Type** to **Local User** and **Administrator Profile** to **prof_admin**. Remove the **root** VDOM from the **Virtual Domains** list, then add **VDOM-B**.



6. Configuring VDOM-A

Access **VDOM-A**'s configuration using the dropdown menu and go to **Network > Static Routes** to add a default route.

Set **Destination** to **Subnet**, **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.

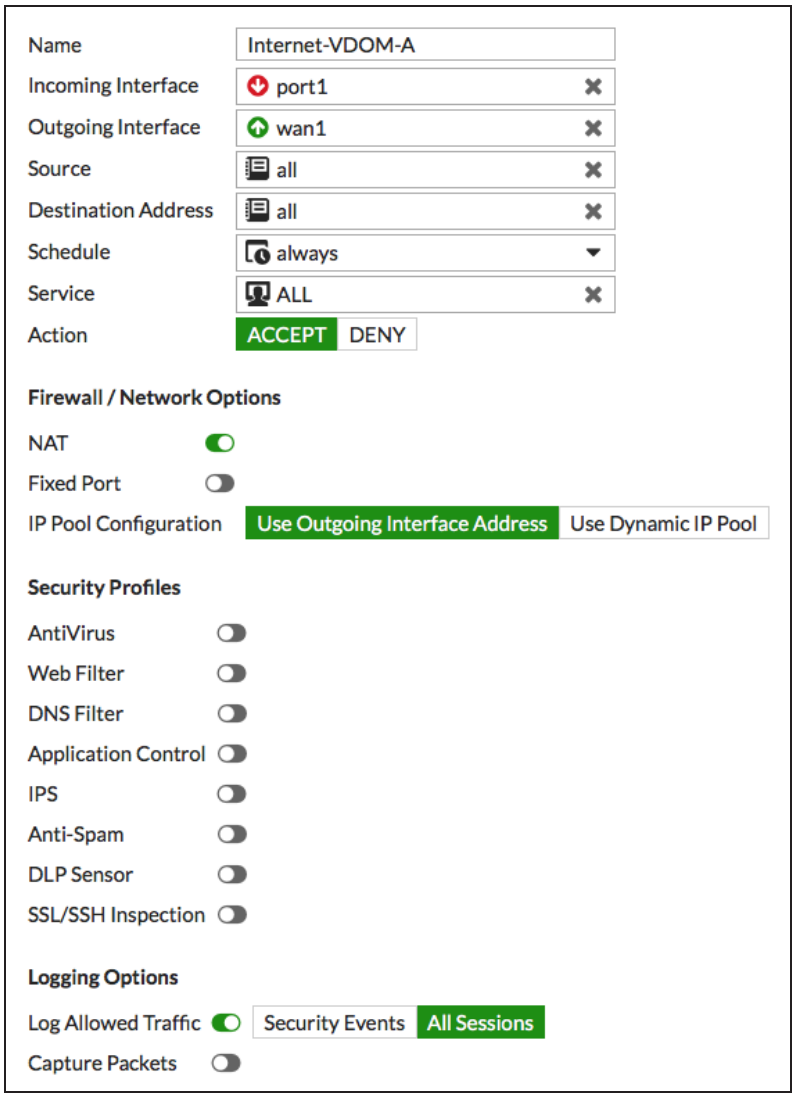


Go to **Policy & Objects > IPv4 Policies** and create a new policy to allow Internet access for VDOM-A. Give the policy a **Name** that indicates that the policy will be for traffic to the Internet (in the example, *Internet-VDOM-A*).

Set **Incoming Interface** to **port1**, **Outgoing Interface** to **wan1**, **Source** to **all**, **Destination Address** to **all**, and **Service** to **ALL**. Make sure **NAT** is enabled.

Because this VDOM uses proxy inspection, you can enable a variety of security profiles that use either proxy or flow-based inspection.

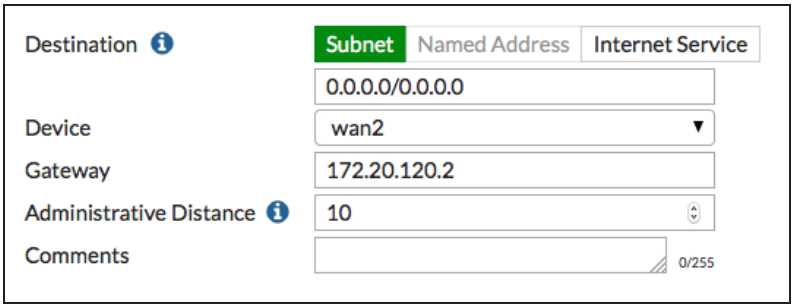
For testing purposes, under **Logging Options**, enable **Log Allowed Traffic** and select **All Sessions**.



7. Configuring VDOM-B

Access **VDOM-B**'s configuration using the dropdown menu and go to **Network > Static Routes** to add default route.

Set **Destination** to **Subnet**, **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.

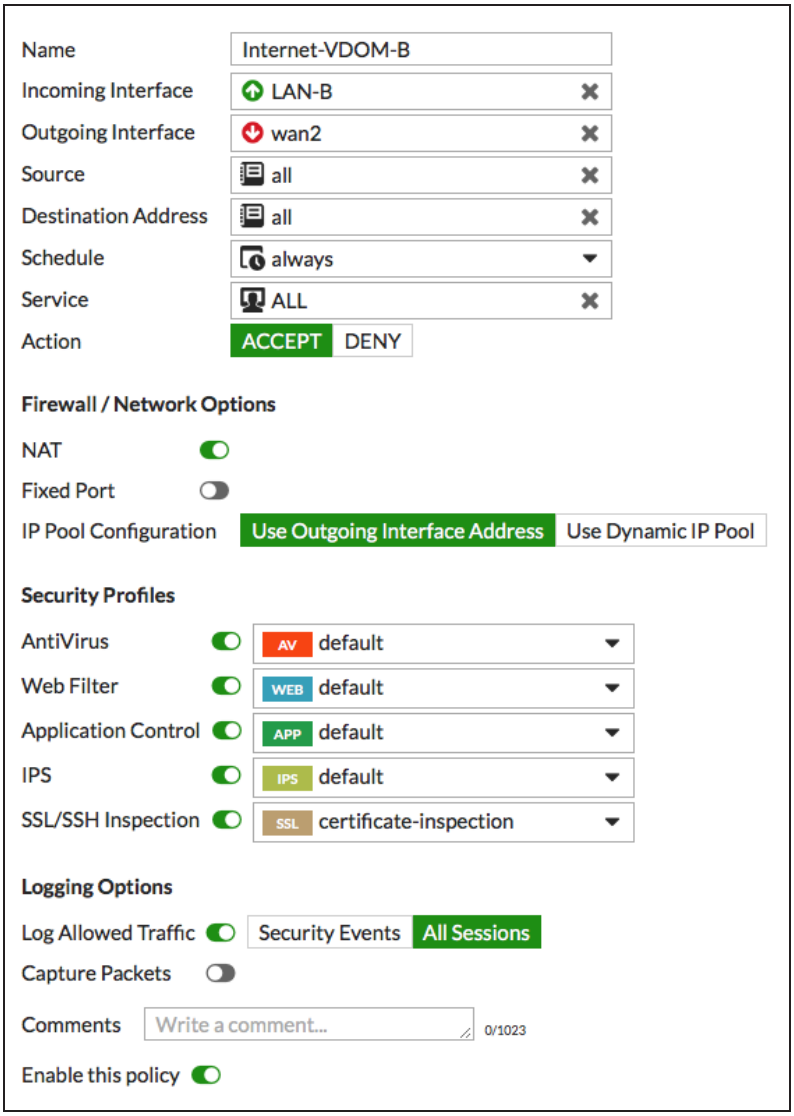


Go to **Policy & Objects > IPv4 Policies** and create a new policy to allow Internet access for VDOM-B. Give the policy a **Name** that indicates that the policy will be for traffic to the Internet (in the example, *Internet-VDOM-B*).

Set **Incoming Interface** to **LAN-B**, **Outgoing Interface** to **wan2**, **Source** to **all**, **Destination Address** to **all**, and **Service** to **ALL**. Make sure **NAT** is enabled.

Because this VDOM uses flow-based inspection, you can only enable security profiles that use flow-based inspection.

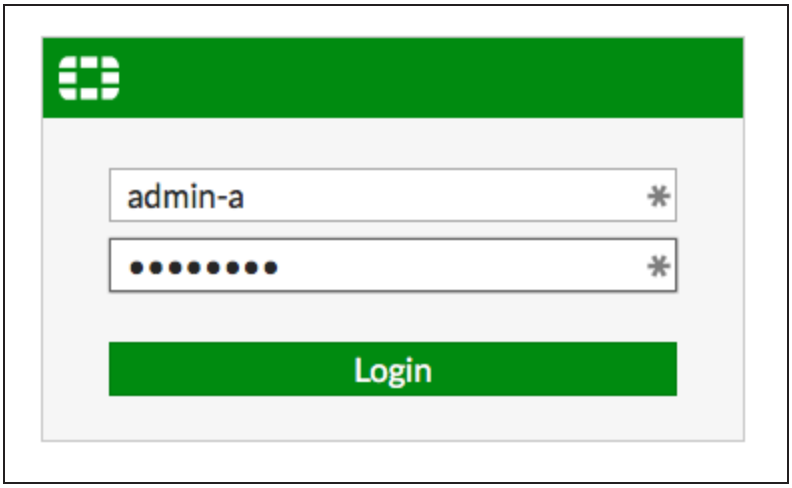
For testing purposes, under **Logging Options**, enable **Log Allowed Traffic** and select **All Sessions**.



8. Results

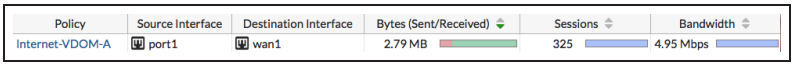
Using a PC located on VDOM-A's internal network, browse to the IP of the LAN-A interface (in the example, *https://192.168.100.1*).

Login to the VDOM using **admin-a**'s credentials. When the GUI loads, only the options for configuration VDOM-A appear.



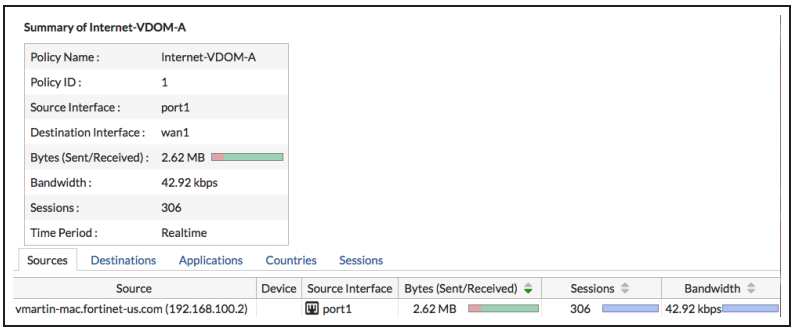
Generate Internet traffic for VDOM-A.

Go to **FortiView > Policies** and select the **now** view. You can see traffic flowing through the **Internet-VDOM-A** policy.



Policy	Source Interface	Destination Interface	Bytes (Sent/Received)	Sessions	Bandwidth
Internet-VDOM-A	port1	wan1	2.79 MB	325	4.95 Mbps

Right-click on the policy, then select **Drill Down to Details**. You can see more information about the traffic.



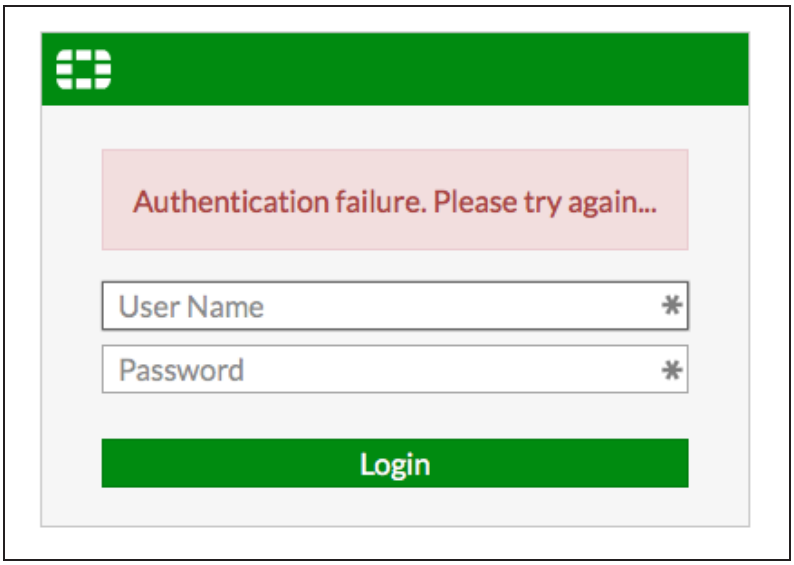
Summary of Internet-VDOM-A

Policy Name :	Internet-VDOM-A
Policy ID :	1
Source Interface :	port1
Destination Interface :	wan1
Bytes (Sent/Received) :	2.62 MB
Bandwidth :	42.92 kbps
Sessions :	306
Time Period :	Realtime

Sources | Destinations | Applications | Countries | Sessions

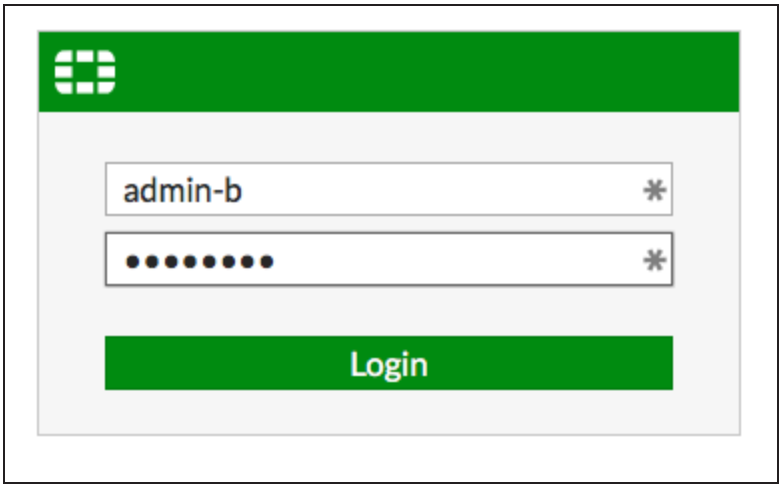
Source	Device	Source Interface	Bytes (Sent/Received)	Sessions	Bandwidth
vmartin-mac.fortinet-us.com (192.168.100.2)		port1	2.62 MB	306	42.92 kbps

Logout of the VDOM, then attempt to login using the global **admin**'s credentials. You will not be able to log in. You can also not log in using **admin-b**'s credentials.



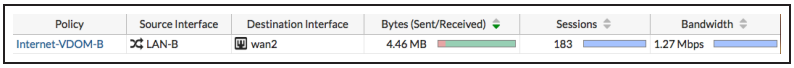
Using a PC located on VDOM-B's internet network, browse to the IP of the LAN-B interface (in the example, *https://192.168.200.1*).

Login to the VDOM using **admin-b**'s credentials. When the GUI loads, only the options for configuration VDOM-B appear.



Generate Internet traffic for VDOM-B.

Go to **FortiView > Policies** and select the **now** view. You can see traffic flowing through the **Internet-VDOM-B** policy.



Policy	Source Interface	Destination Interface	Bytes (Sent/Received)	Sessions	Bandwidth
Internet-VDOM-B	LAN-B	wan2	4.46 MB	183	1.27 Mbps

Troubleshooting your FortiGate installation

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

Most methods can be used for 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. Make sure that each cable connects to the correct device and the correct Ethernet port on that device. Also, check the Unit Operation widget in the Dashboard 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.

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 the Internet-facing interface.

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

Verify that the default route is correct. View the **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 your **FortiGuard** settings and expand **Web Filtering and Email Filtering Options**. 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
 set macaddr
 end
 end
```

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

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

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

```
 diagnose netlink brctl name host root.b
 show bridge control interface root.b host.
 fdb: size=2048, used=25, num=25, depth=1
 Bridge root.b host table
 port no device devname mac addr ttl attributes
```

```
3 4 [glossary_exclude]wan1[/glossary_exclude] 00:09:0f:cb:c2:77 88
3 4 [glossary_exclude]wan1[/glossary_exclude] 00:26:2d:24:b7:d3 0
3 4 [glossary_exclude]wan1[/glossary_exclude] 00:13:72:38:72:21 98
4 3 internal 00:1a:a0:2f:bc:c6 6
1 6 [glossary_exclude]dmz[/glossary_exclude] 00:09:0f:dc:90:69 0 Local Static
3 4 [glossary_exclude]wan1[/glossary_exclude] c4:2c:03:0d:3a:38 81
3 4 [glossary_exclude]wan1[/glossary_exclude] 00:09:0f:15:05:46 89
3 4 [glossary_exclude]wan1[/glossary_exclude] c4:2c:03:1d:1b:10 0
2 5 [glossary_exclude]wan2[/glossary_exclude] 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.

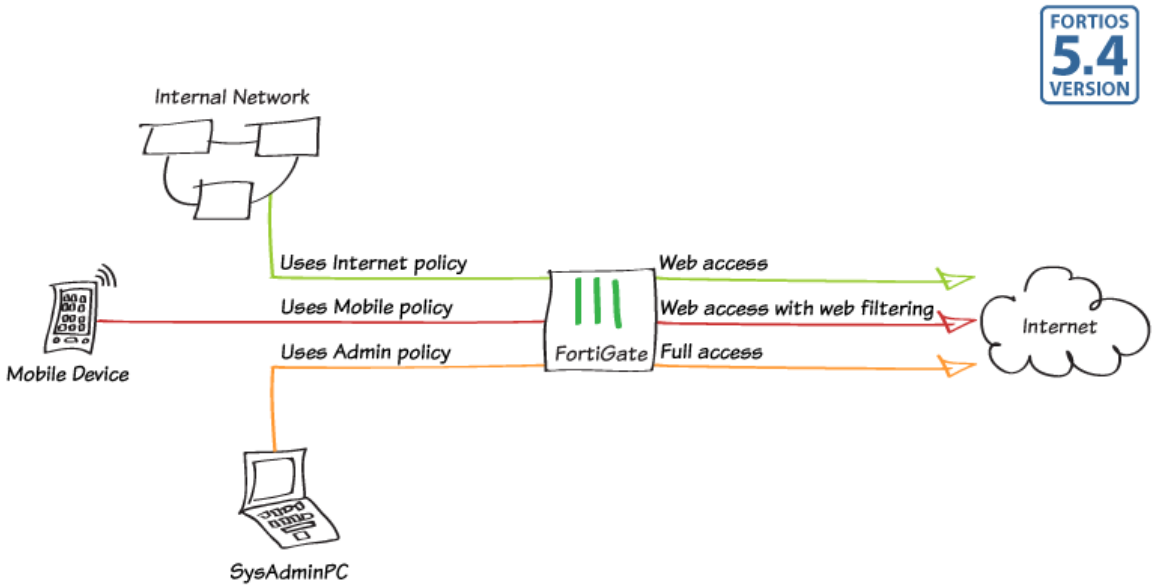
16. Either reset the FortiGate unit to factory defaults or contact the technical assistance center.

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.

Creating security policies



In this recipe, you will create and order multiple security policies in the policy table, to apply the appropriate policy to various types of network traffic.

In the example, three IPv4 policies will be configured:

- *Internet*: a policy allowing general Internet access to the LAN
- *Mobile*: a policy allowing Internet access while applying web filtering for mobile devices[tippy title="*" class-s="myclass" showheader="false" width="auto" height="auto"]In this example, a wireless network has already been configured that is in the same subnet as the wired LAN.[/tippy]
- *Admin*: a policy allowing the system administrator's PC (named SysAdminPC) to have full access

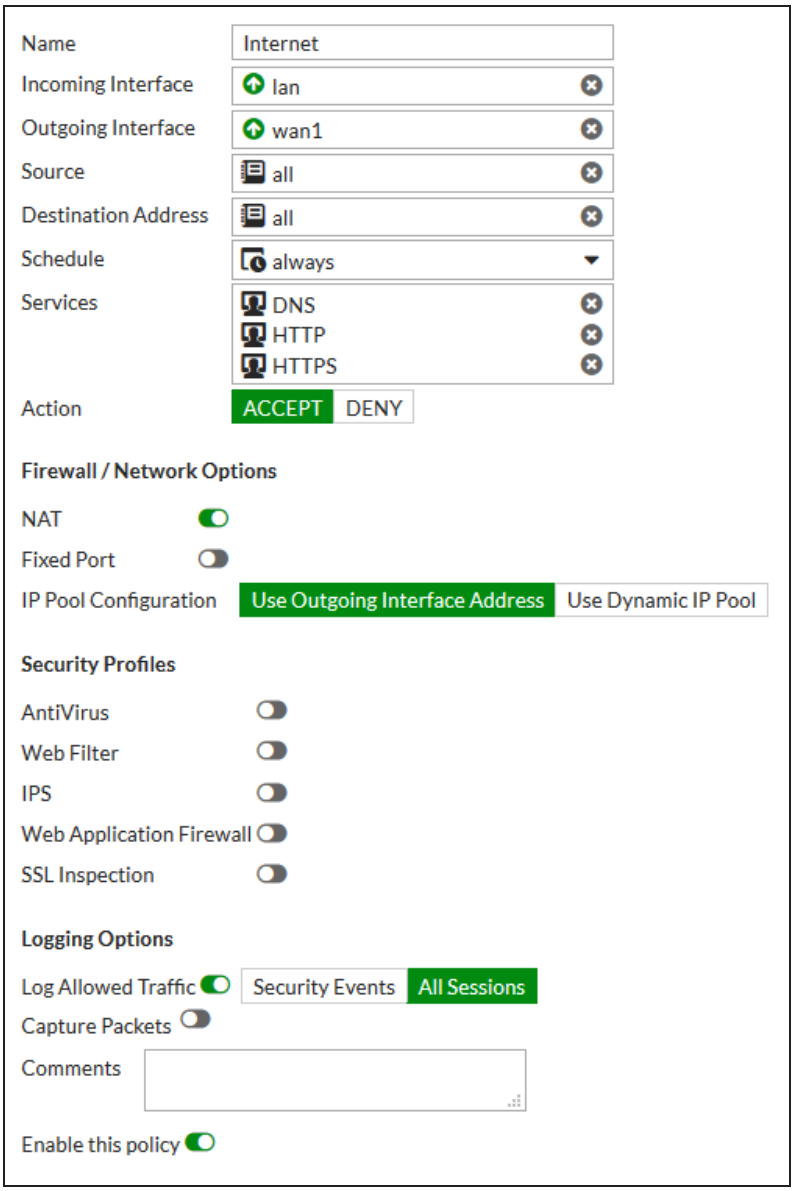
A fourth policy, the default *Implicit Deny* policy, will also be used.

1. Configuring the Internet policy

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

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

Ensure that you have enabled **NAT**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.



2. Creating the Mobile policy

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

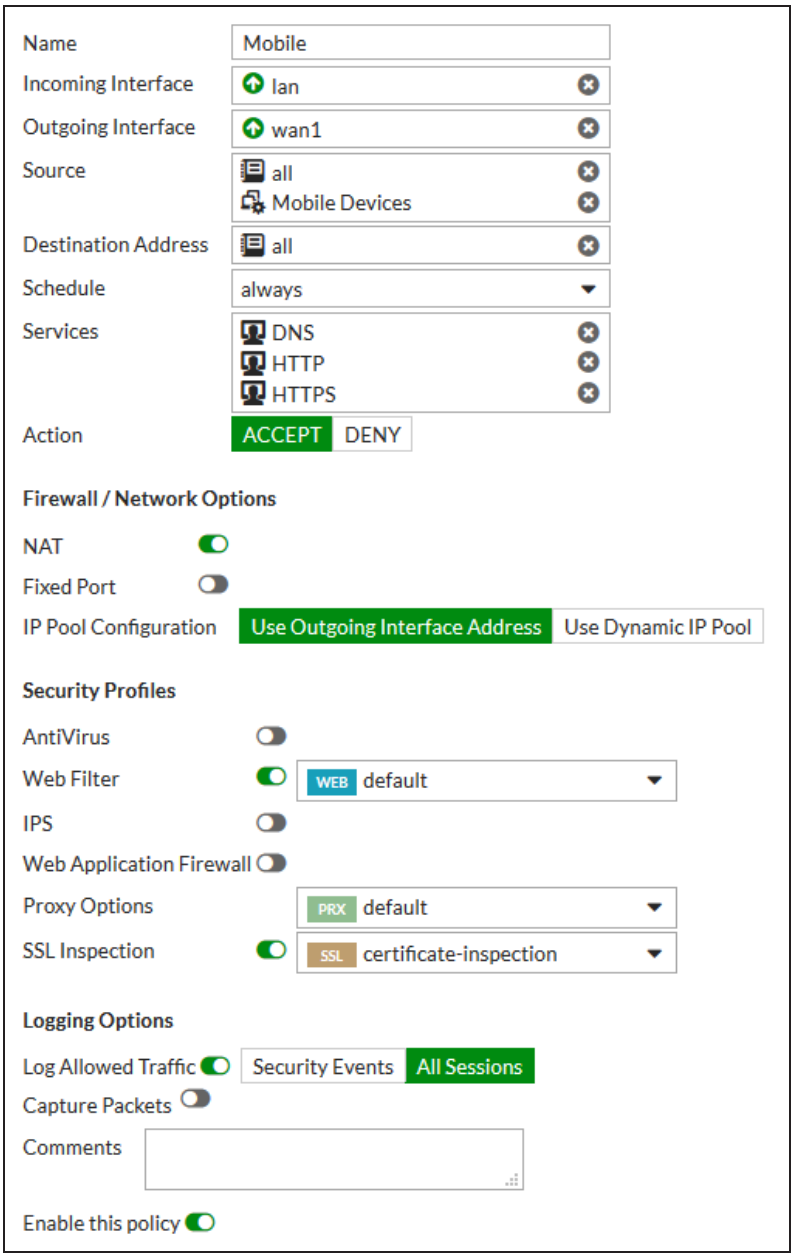
Set **Incoming Interface** to **lan**, **Source Device Type** to **Mobile Devices** (a custom device group that includes tablets and mobile phones), **Outgoing Interface** to your Internet-facing interface, and **Service** to **HTTP**, **HTTPS**, and **DNS**.

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

Enable **NAT**.

Under **Security Profiles**, enable **Web Filter** and set it to use the **default** profile. Enable **SSL Inspection** and and set it to **certificate-inspection** to allow HTTPS traffic to be inspected. Doing this will enable **Proxy Options**; set that to use the **default** profile.

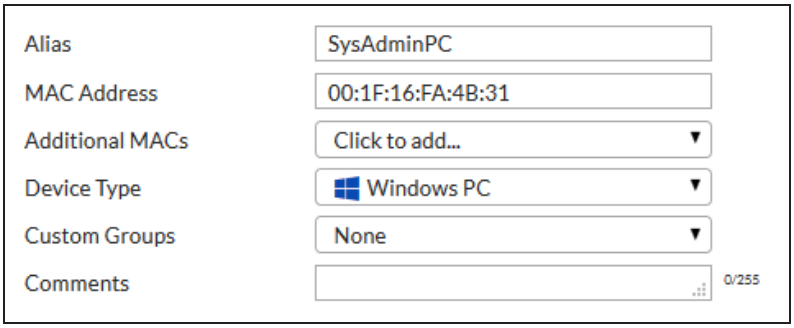
Enable **Log Allowed Traffic** and select **All Sessions**.



3. Defining SysAdminPC

Go to **User & Device > Custom Devices & Groups** and create a new device. This will identify the system administrator's PC.

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

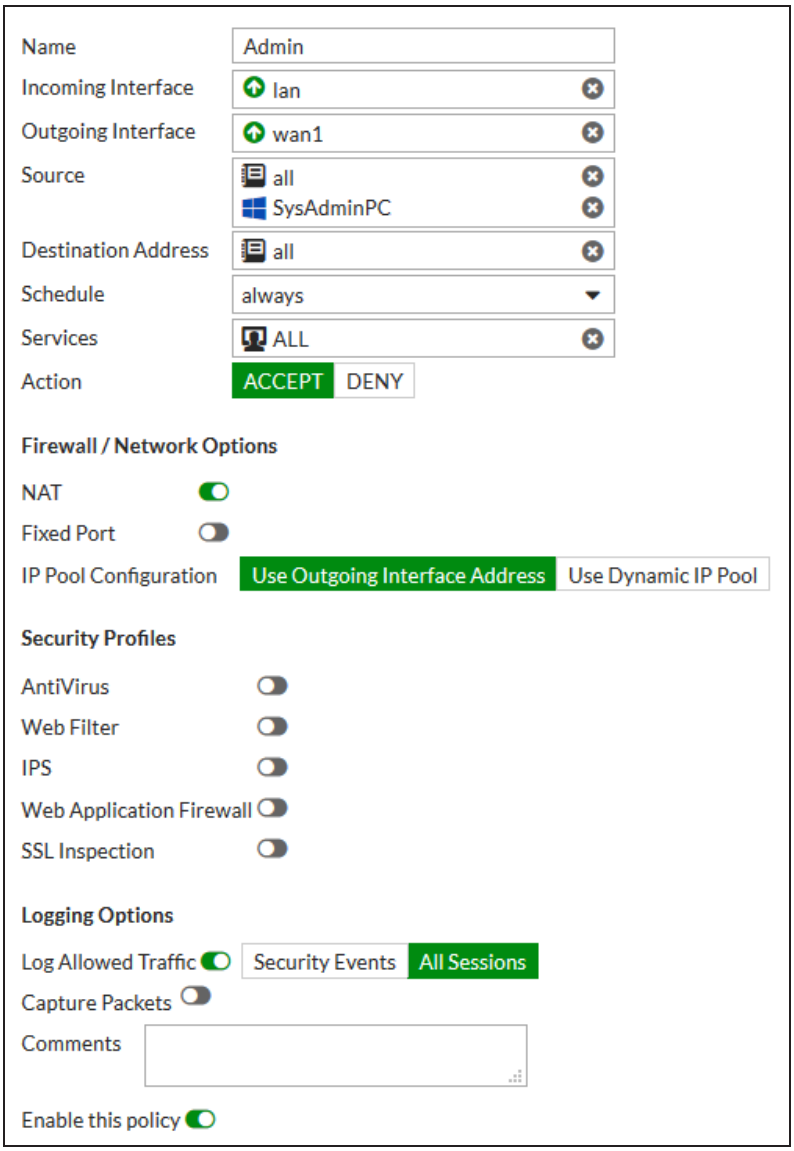


4. Creating the Admin policy

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

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

Enable **NAT**. Enable **Log Allowed Traffic** and select **All Sessions**.



5. Ordering the policy table

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

Currently, the policies are arranged in the order they were created.

Seq.#	Name	From	To	Source	Destination	Service	Action	NAT	Security Profiles	Log
1	Internet	lan	wan1	all	all	DNS HTTP HTTPS	Accept	Enabled		All
2	Mobile	lan	wan1	all Mobile Devices	all	DNS HTTP HTTPS	Accept	Enabled	WEB PRX SSL	All
3	Admin	lan	wan1	all SysAdminPC	all	ALL	Accept	Enabled		All
4	Implicit Deny	any	any	all	all	ALL	Deny			Disabled

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.

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

Seq.#	Name	From	To	Source	Destination	Service	Action	NAT	Security Profiles	Log
1	Admin	lan	wan1	all SysAdminPC	all	ALL	Accept	Enabled		All
2	Mobile	lan	wan1	all Mobile Devices	all	DNS HTTP HTTPS	Accept	Enabled	WEB PRX SSL	All
3	Internet	lan	wan1	all	all	DNS HTTP HTTPS	Accept	Enabled		All
4	Implicit Deny	any	any	all	all	ALL	Deny			Disabled

6. Results

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

Go to **FortiView > Policies** and select the **now** view. You can see traffic flowing through all three security policies.

Policy	Source Interface	Destination Interface	Bytes (Sent/Received)	Sessions	Bandwidth
Admin	lan	wan1	2.16 MB	45	21.31 kbps
Internet	lan	wan1	86.09 kB	17	688 bps
Mobile	lan	wan1	36.86 kB	10	1.29 kbps

Right-click on the *Admin* policy and select **Drill Down to Details**.

View the **Sources** tab to confirm that this policy is being used exclusively by *SysAdminPC*.

Summary of Admin

Policy Name :	Admin
Policy ID :	3
Source Interface :	lan
Destination Interface :	wan1
Bytes (Sent/Received) :	503.50 kB
Bandwidth :	2.24 kbps
Sessions :	32
Time Period :	Realtime

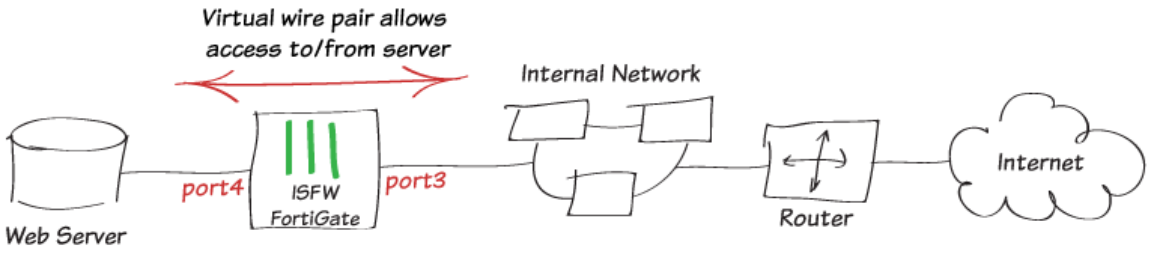
Applications | Sources | Destinations | Countries | Sessions

Source	Device	Source Interface	Bytes (Sent/Received)	Sessions	Bandwidth
172.20.121.47	SysAdminPC	lan	490.24 kB	32	2.24 kbps

(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.

Creating a virtual wire pair



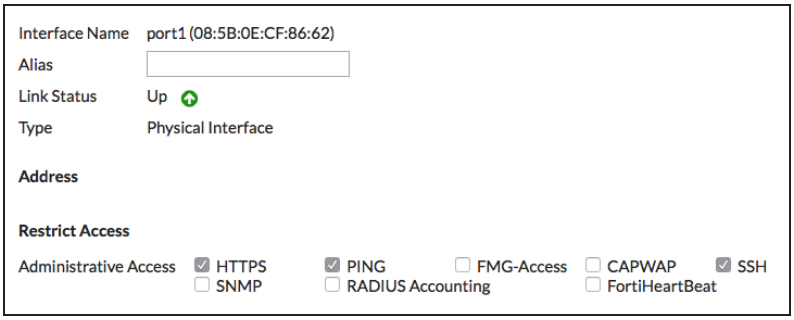
In this example, you will create a virtual wire pair (consisting of port3 and port4) to make it easier to protect a web server that is behind a FortiGate operating as an Internal Segmentation Firewall (ISFW). Users on the internal network will access the web server through the ISFW over the virtual wire pair.

A virtual wire pair consists of two interfaces that have no IP addresses and all traffic received by one interface in the pair can only be forwarded out the other; as controlled by firewall policies. Since the interfaces do not have IP addresses, you can insert a virtual wire pair into a network without having to make any changes to the network.

In FortiOS 5.4, virtual wire pair replaces the feature port pairing from earlier firmware versions. Unlike port pairing, virtual wire pair can be used for a FortiGate in NAT/Route mode, as well as Transparent mode.

1. Adding a virtual wire pair

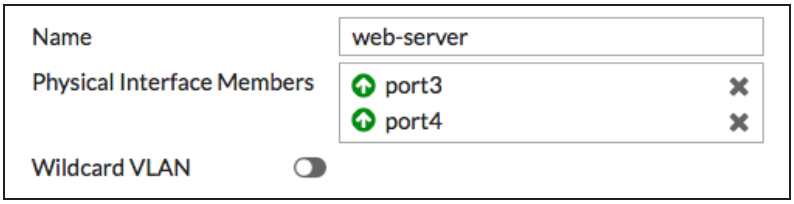
Interfaces used in a virtual wire pair cannot be used to access the ISFW FortiGate. Before creating a virtual wire pair, make sure you have a different port (in the example, *port1*) configured to allow admin access using your preferred protocol.



Go to **Network > Interfaces** and select **Create New > Virtual Wire Pair**.

Add port3 and port4 add to the virtual wire pair.

*]If the interfaces you wish to use are part of a switch, such as the default **lan/internal** interface, you will need to remove them before they can be added to the virtual wire pair.*

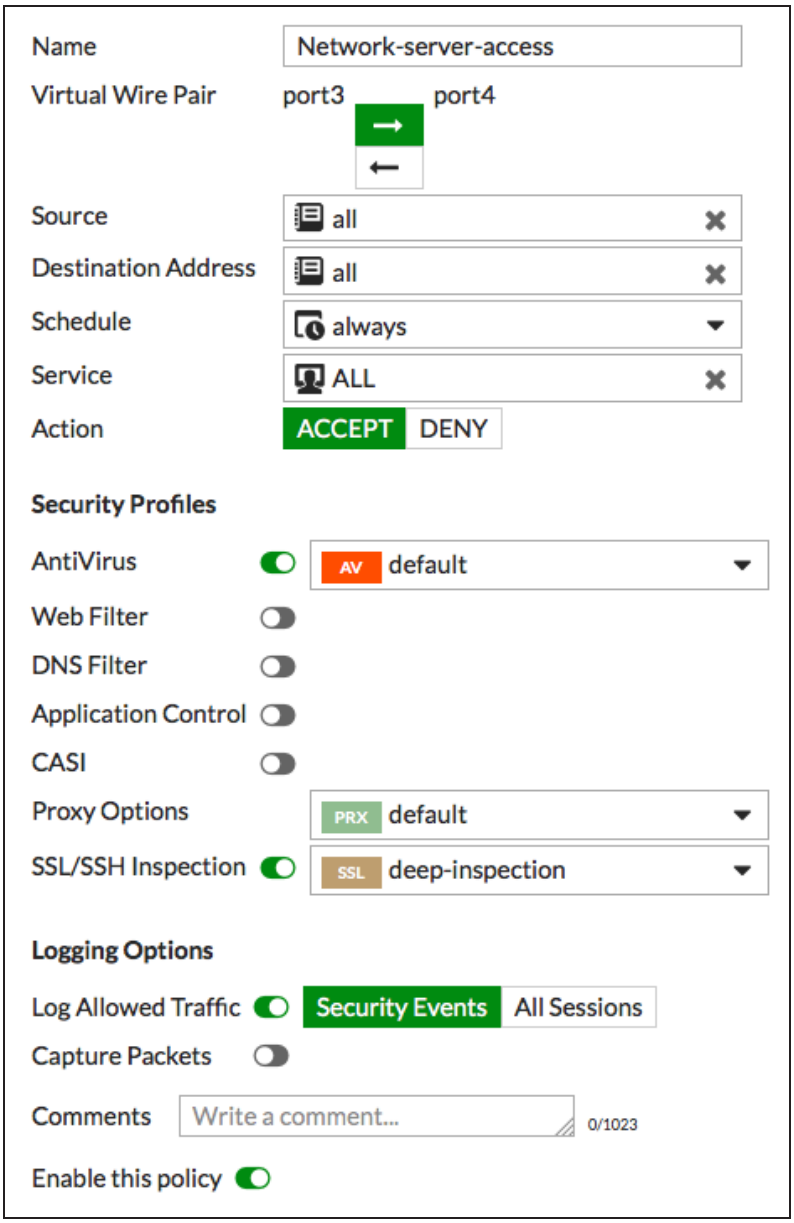


2. Adding virtual wire pair firewall policies

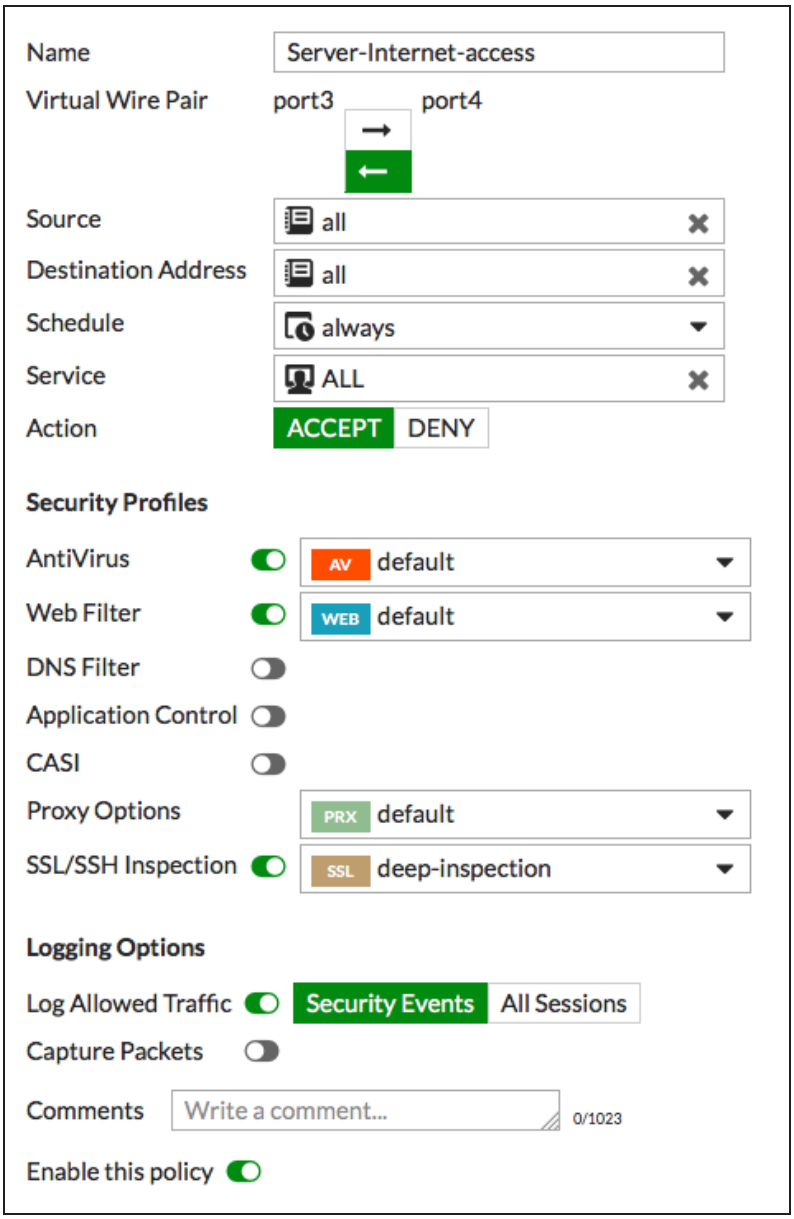
Go to **Policy & Objects > IPv4 Virtual Wire Pair Policy** and create a policy will allow users on the internal network to connect to the server. Give the policy an appropriate name (in the example, *Network-server-access*).

Select the direction that traffic is allowed to flow (from port3 to port4).

Configure the other firewall options as needed. In the example, AntiVirus is enabled to protect the server.



Create a second virtual wire pair policy allowing traffic from port4 to exit out of port3. This policy allows the server to connect to the Internet, in order to download updates.



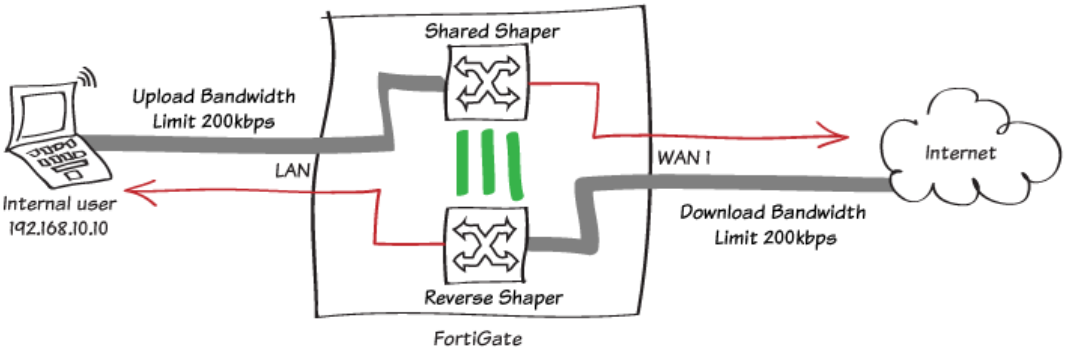
3. Results

To test both virtual wire pair policies, connect to the web server from a PC on the internal network, and also connect to the Internet from the web server.

Go to **FortiView > Policies** to see traffic flowing through both policies.

Policy	Source Interface	Destination Interface	Bytes (Sent/Received)	Sessions	Bandwidth
Server-Internet-access	port4	port3	325.21 kB	21	3.98 kbps
Network-server-access	port3	port4	1.06 kB	6	0 bps

Limiting bandwidth with traffic shaping



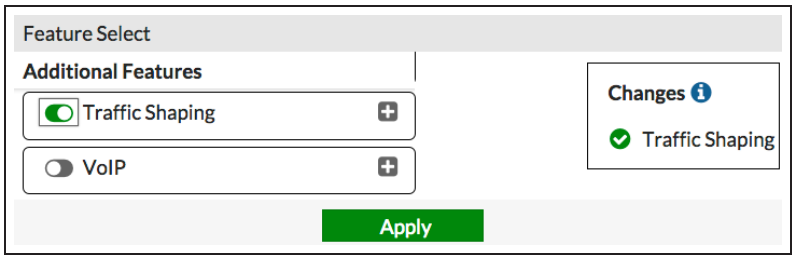
When a particular IP address uses too many resources, you can prevent that IP from consuming your bandwidth indiscriminately. In this recipe, you learn how to use Traffic Shaping on your FortiGate to limit the bandwidth for a specific IP address.

This recipe also explains how to configure traffic shaping to set a maximum bandwidth limit for uploads and/or downloads to 200 kb/s.

1. Enabling Traffic Shaping

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

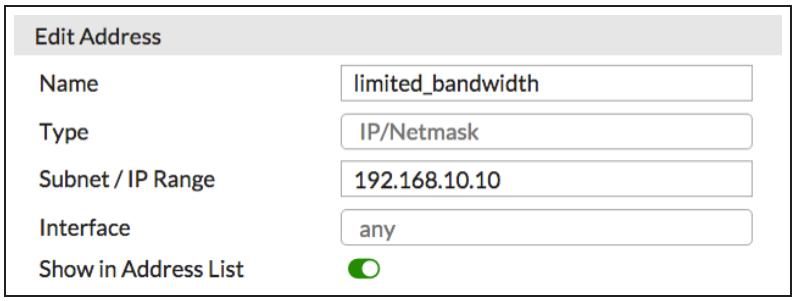
*Two new traffic shaping menus, **Traffic Shapers** and **Traffic Shaping Policy**, will appear under Policy & Objects.*



2. Creating a firewall address

Go to **Policy & Objects > Addresses** to define the address you would like to limit. Select **Create New** and select **Address** from the drop down menu.

Enter a name: **limited_bandwidth**. Set **Type** to **IP/Netmask**. Set the **Subnet/IP Range** to the internal IP address you wish to limit (in this example, *192.168.10.10/32*. Set **Interface** to **Any.**

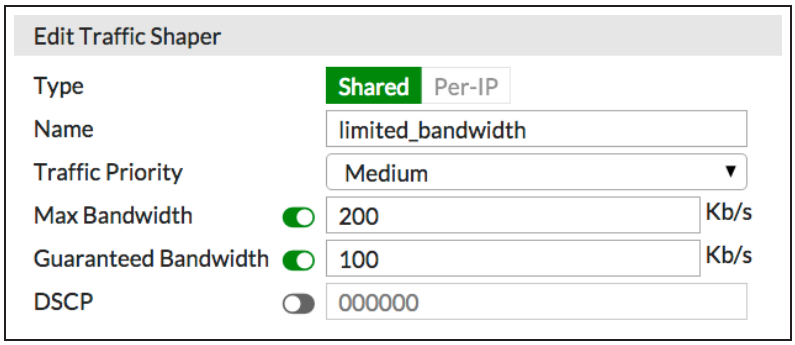


3. Configuring a traffic shaper to limit bandwidth

Go to **Policy & Objects > Traffic Shapers** and select **Create New** to define a new shared Traffic Shaper profile.

Set **Type** to **Shared**.

***Shared shapers** affect upload speeds, **Reverse shapers** affect download speeds, and **Per IP shapers** affect both upload and download speeds simultaneously.*

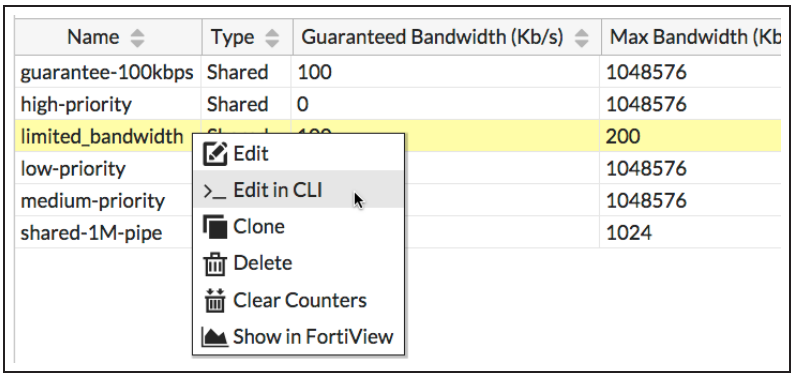


Enter the name **limited_bandwidth** for your shaper and set the **Traffic Priority** to **Medium**.

*Setting a **Traffic Priority** will only have an impact if you have enabled Traffic Shaping in ALL your other Internet access policies using the same two interfaces. There must also be some variation, for example you will not see any differences while all policies are set to the default setting (**High**).*

Select **Max Bandwidth** and enter `200` kb/s (0.2 Mbps). If you would like to set a **Guaranteed Bandwidth** make sure the rate is lower than the Max Bandwidth. Apply your changes.

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

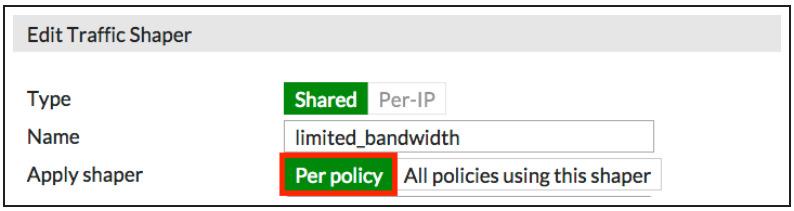


Enter the following CLI commands:

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

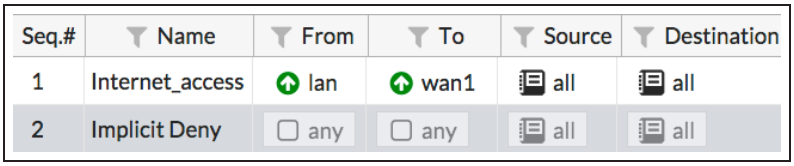
Now that **Per Policy** shaping is enabled, edit your **limited_bandwidth** shaper and set **Apply Shaper** to **Per Policy**.

Now, each security policy using this shaper will have the same distribution of bandwidth, regardless of the number of policies using the shaper. In this example, 200 kb/s (0.2 Mbps) each.



4. Verifying your Internet access security policy

Go to **Policy & Objects > IPv4 Policy** and look at your general Internet access policy. Take a note of the Incoming interface, Outgoing interface, Source and Destination.



If necessary, edit your policy and ensure that **Logging Options** is set to **All**

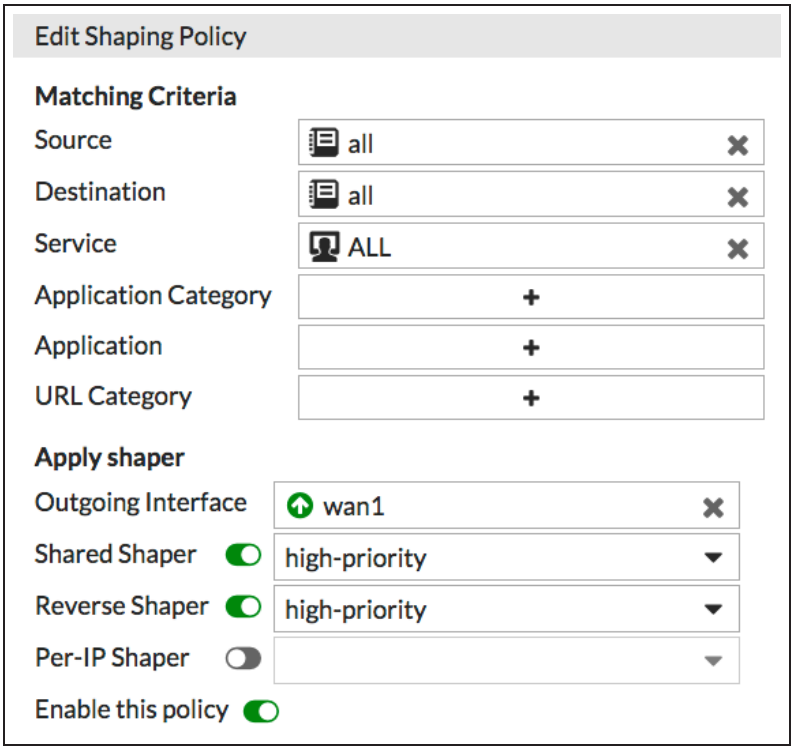
Sessions for testing purposes.

4. Create two Traffic Shaping Policies

Go to **Policy & Objects > Traffic Shaping Policy** and select **Create New** to create a shaping policy that will set regular traffic to high priority.

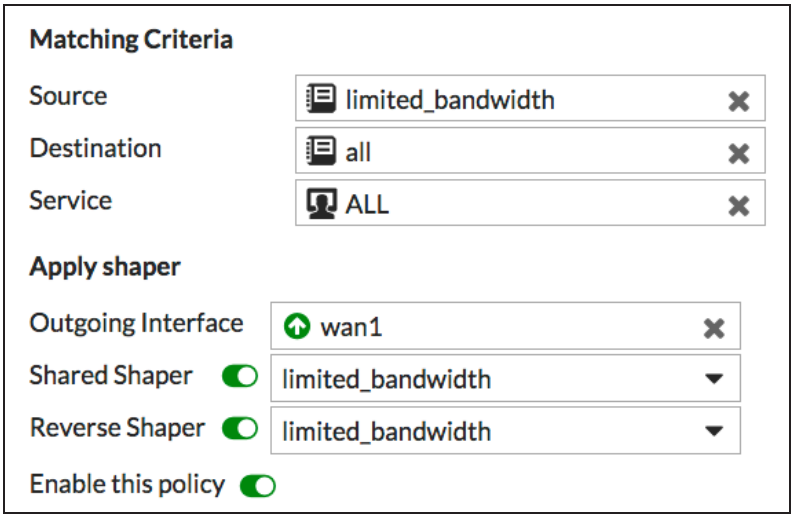
Under **Matching Criteria**, set **Source**, **Destination**, **Service** to match your Internet Access policy.

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



Select **Create New** to create a second traffic shaping policy that will affect the IP address you wish to limit.

Under **Matching Criteria**, set **Source** to **limited_bandwidth**. Set **Destination** and **Service** to **ALL**. Apply the shaper to the same **Outgoing Interface.** Enable **Shared Shaper** and **Reverse Shaper** and set both shapers to **limited_bandwidth**.



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

Click on the far left column of the policy and move it up or down to change the sequence order.

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

5. Results

When a computer with the IP you have specified, 192.168.10.10, browses the Internet from your internal network, its bandwidth will be restricted by the amount you set in your shaper.

Source: 192.168.10.10 Add Filter | now | 5 minutes | 1 hour | 24 hours

Source	Bytes (Sent/Received)	Sessions	Bandwidth	Device
192.168.10.10	5.90 MB	34	199.31 kbps	

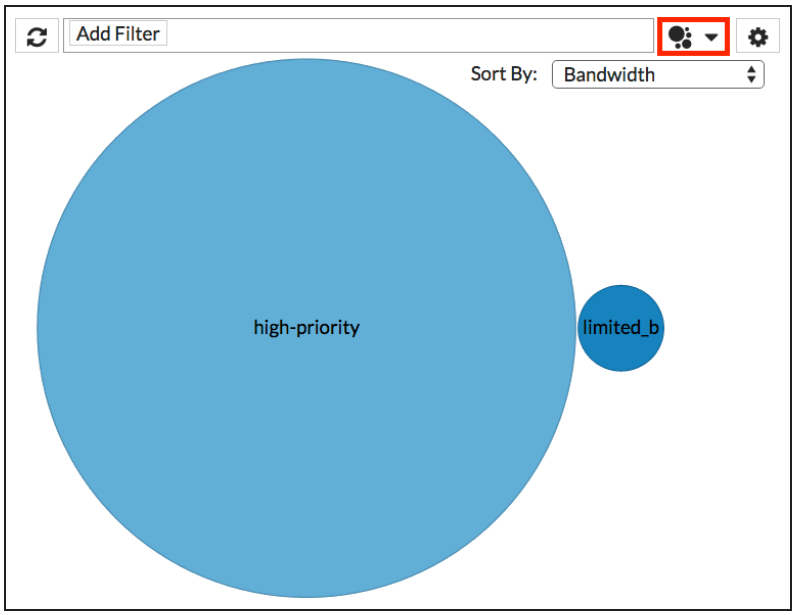
Go to **FortiView > Sources** to view traffic, and use the search field to filter your results by the **Source IP** (192.168.10.10).

Go to **FortiView > Traffic Shaping** to view the current bandwidth usage for any active shapers. Users on the local network will have **high-priority** traffic.

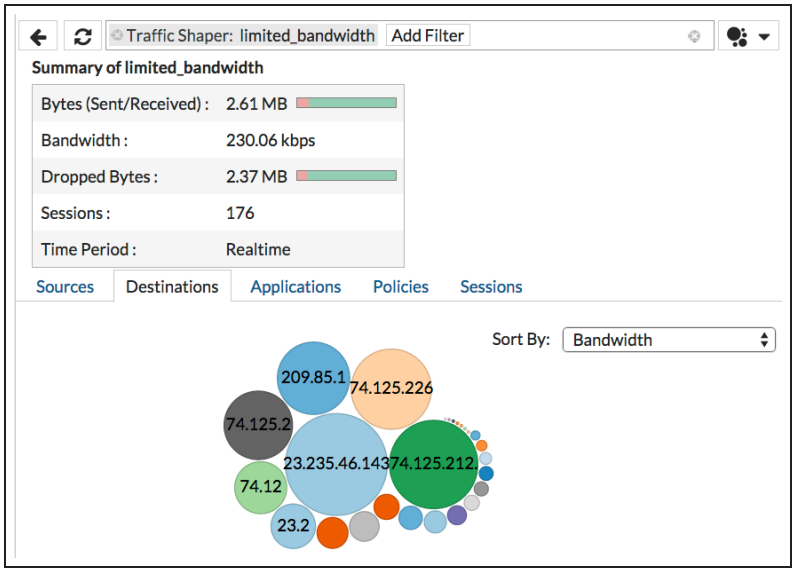
Shaper	Bytes (Sent/Received)	Sessions	Bandwidth	Dropped Bytes
high-priority	175.34 MB	96	5.54 Mbps	0 B
limited_bandwidth	149.87 MB	21	192.37 kbps	3.94 MB

The IP address you have specified will receive **limited-bandwidth** treatment and may experience dropped bytes. Your **limited-bandwidth** shaper should not exceed 200kbps. Note that the results show the **Bytes (Sent/Received)** in Megabytes (MB) and the **Bandwidth** in kilobits per second (kbps).

You can also view these results in a bubble graph by changing the graph type in the drop down menu. Sort by **Bandwidth** to verify that your regular traffic is using more bandwidth.



You can also double-click on either shaper to see more granular information. Select the **Destinations** tab to see which websites are using up the most bandwidth.



Managing FortiSwitches with a FortiGate

Manage up to 16 FortiSwitches from the FortiGate web-based manager or CLI. You can create and assign VLANs and configure port information. The connection between the FortiSwitch and the FortiGate is called a FortiLink.

Prerequisites

A. Connect a cable from any FortiSwitch port to an unused internal port on the FortiGate.
   1. If necessary, enable the port for FortiLink auto-discovery (using the **FortiSwitch** CLI).
      -> In general, the last four copper ports on the FortiSwitch are enabled for auto-detect by default. Refer to the documents below for specific details.

B. You may need to enable the Switch Controller using the **FortiGate** web-based manager.
   1. Go to **System > Config > Features**.
   2. Turn on the **WiFi & Switch Controller feature**.
   3. Select **Apply**.

C. This recipe is applicable to FortiSwitchOS 3.3.0 and above.

Procedure

From the FortiGate web-based manager:

1. Go to **System > Network > Interfaces** and edit the new FortiLink port.
2. Set **Addressing mode** to **Dedicate to Extension Device**.
3. Select **OK**.
4. Go to **WiFi & Switch Controller > Managed Devices > Managed FortiSwitch**.
   -> This page displays the faceplate for each managed FortiSwitch. The FortiLink for the new managed switch will display as a dashed line (FortiLink connection not established).
   -> After a short delay (while FortiGate sets up the connection), the FortiLink displays as a solid line (FortiLink established). For smaller FortiSwitch models, such as FS-108D-POE, the delay may be up to 3 minutes.

Notes

1. In FortiOS 5.4, new FortiLink features include:
   a. POE configuration from the FortiGate.
   b. Link Aggregation Group (LAG) support for Fortilink.

c. Auto-detect the switch FortiLink ports

d. Improved user interface for Managed FortiSwitches, switch ports and VLANs.

2. Refer to the document below to see the FortiSwitch and FortiGate models that support FortiLink.

For additional information, see Managing FortiSwitch with a FortiGate (FortiOS 5.4), which is also available in the FortiOS 5.4 Handbook.

Security

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

AntiVirus

- Sandboxing with FortiSandbox and FortiClient

DNS Filtering

- Protection from Botnet C&C attacks

Endpoint Control

- Enforcing network security using a FortiClient Profile

SSL Inspection

- Why you should use SSL inspection
- Preventing certificate warnings

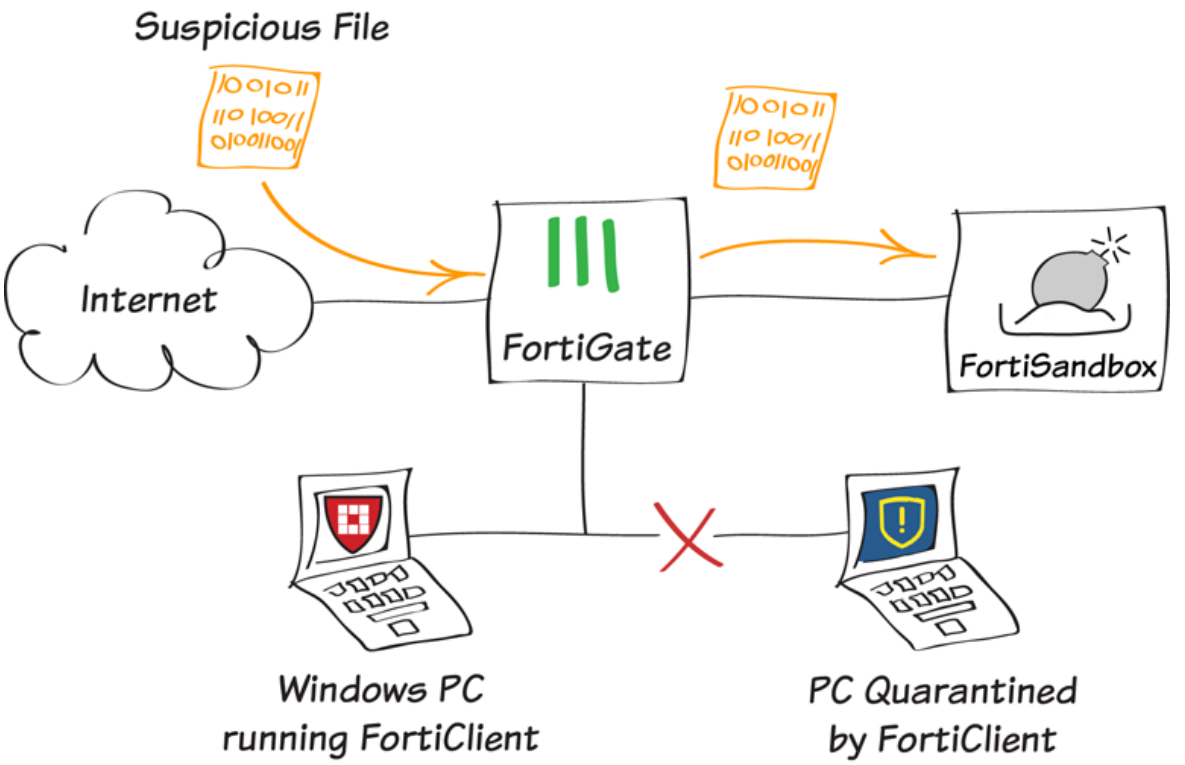
Web Application Firewall

- Protecting web applications

Web Filtering

- Sandboxing with FortiSandbox and FortiClient
- Troubleshooting web filtering

Sandboxing with FortiSandbox and FortiClient



In this recipe, you will set up sandboxing to send suspicious files to a FortiSandbox Appliance for further inspection. The FortiSandbox tests the files for threats that can get past other detection methods using a variety of virtual machines (VMs).

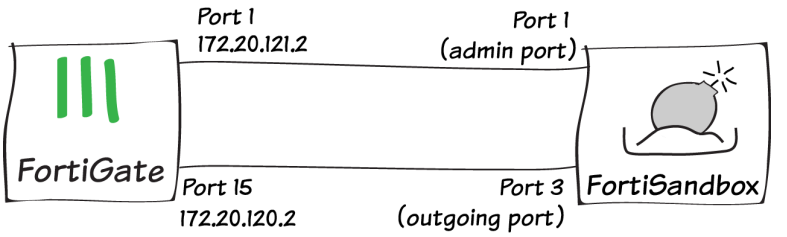
You will also configure your FortiGate to automatically receive signature updates from FortiSandbox and add the originating URL of any malicious file to a blocked URL list. Finally, you will configure FortiClient to use extended scanning that includes FortiSandbox.

This feature is currently only available in FortiClient 5.4 for Windows.

This recipe was tested using FortiOS 5.4 Beta 4, FortiSandbox 2.1.0, and FortiClient for Windows 5.4 Beta 2.

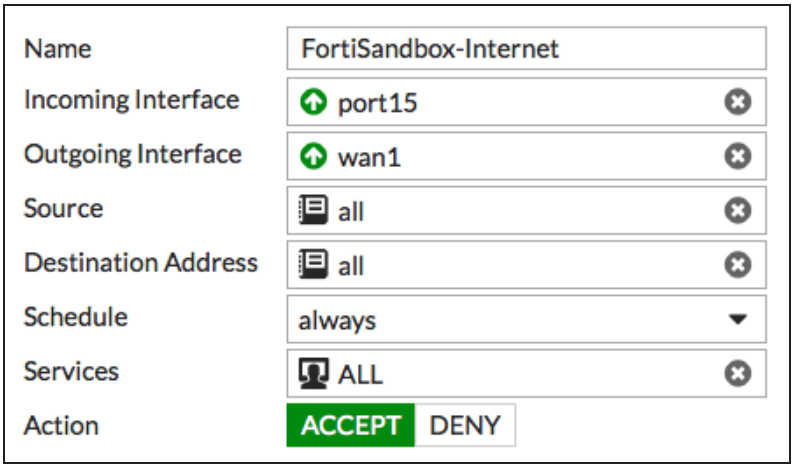
1. Connecting the FortiSandbox

Connect the FortiSandbox to your FortiGate as shown in the diagram, so that port 1 and port 3 on the FortiSandbox are on different subnets.

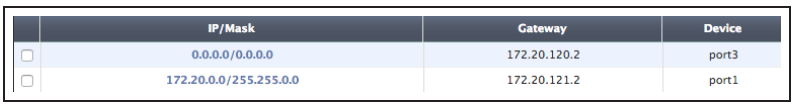


FortiSandbox port 3 is used for outgoing communication triggered by the execution of the files under analysis. It is recommended to connect this port to a dedicated interface on your FortiGate (in the example, port 15), to protect the rest of the network from threats currently being investigated by the FortiSandbox.

FortiSandbox port 3 must be able to connect to the Internet. On the FortiGate, go to **Policy & Objects > IPv4 Policy** and create a policy allowing connections from the FortiSandbox to the Internet (using the isolated interface on the FortiGate mentioned above).



On the FortiSandbox, go to **System > Network > Static Routing** and add static routes for both port 1 and port 3.

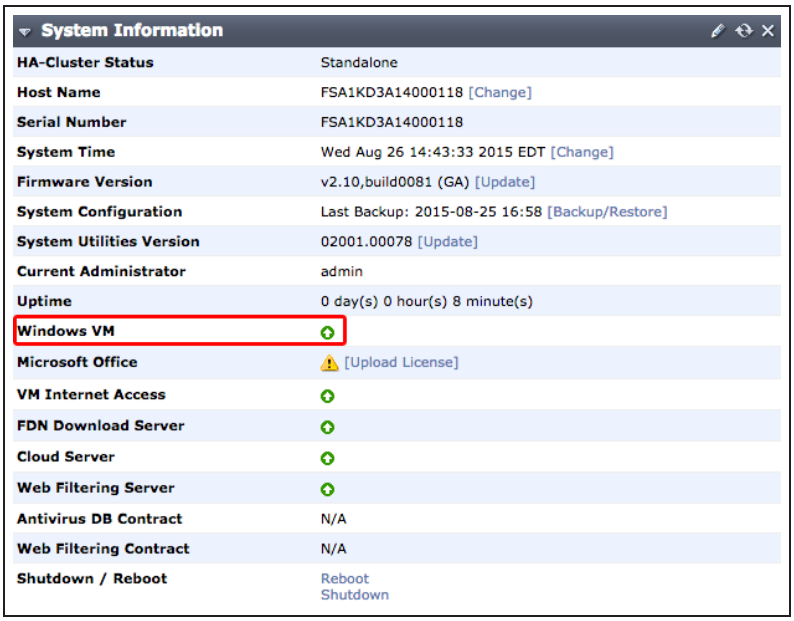


IP/Mask	Gateway	Device
0.0.0.0/0.0.0.0	172.20.120.2	port3
172.20.0.0/255.255.0.0	172.20.121.2	port1

The static route for port 3 must have the **Destination/IP Mask** *0.0.0.0/0.0.0.0*, while port 1 is assigned the **Destination/IP Mask** for traffic in the local network.

Once the FortiSandbox has access to the Internet through port 3, it will begin to activate its VM licenses.

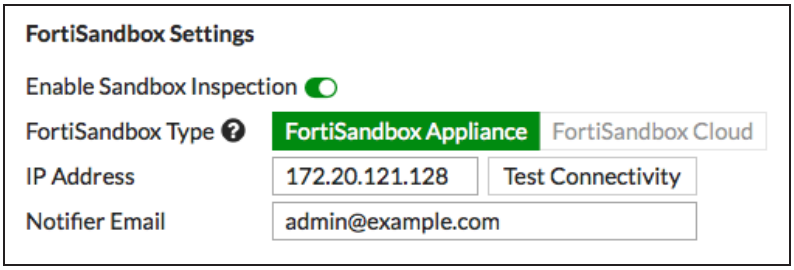
Before continuing with this recipe, wait until a green arrow shows up beside **Windows VM** in the FortiSandbox's **System Information** widget, found at **System > Status**. This indicates that the VM activation process is complete.



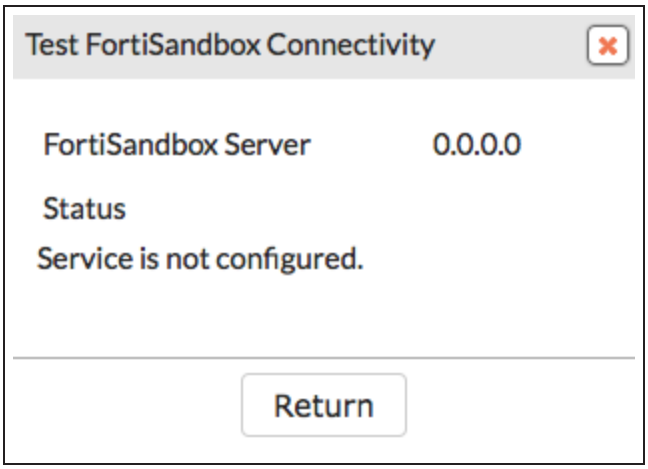
2. Enabling Sandbox Inspection

On the FortiGate, go to **System > Config > FortiSandbox**. Select **Enable Sandbox Inspection** and select **FortiSandbox Appliance**.

Set the **IP Address** (in the example, *172.20.121.128*) and enter a **Notifier Email**, where notifications and reports will be sent.

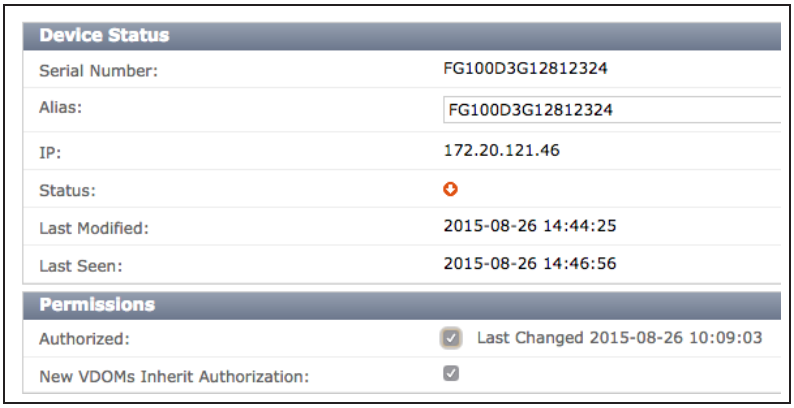


If you select **Test Connectivity**, the **Status** shows as **Service is not configured** because the FortiGate has not been authorized to connect to the FortiSandbox.

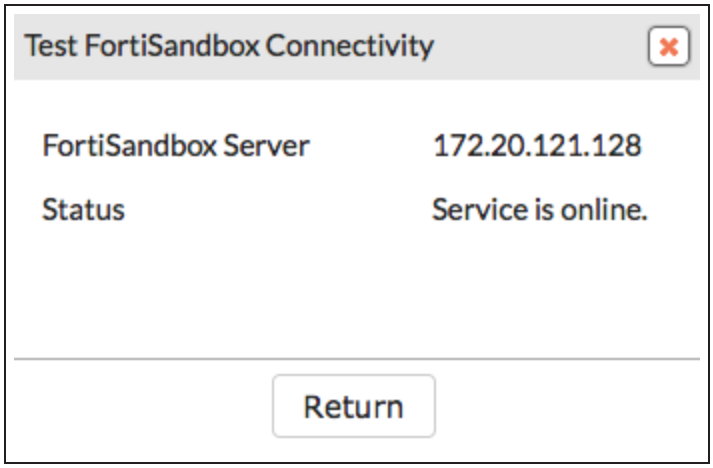


On the FortiSandbox, go to **File-based Detection > File Input > Device**. Edit the entry for the FortiGate.

Under **Permissions,** enable **Authorized**.



On the FortiGate, go to **System > FortiSandbox** and select **Test Connectivity**. The **Status** now shows that **Service is online**.

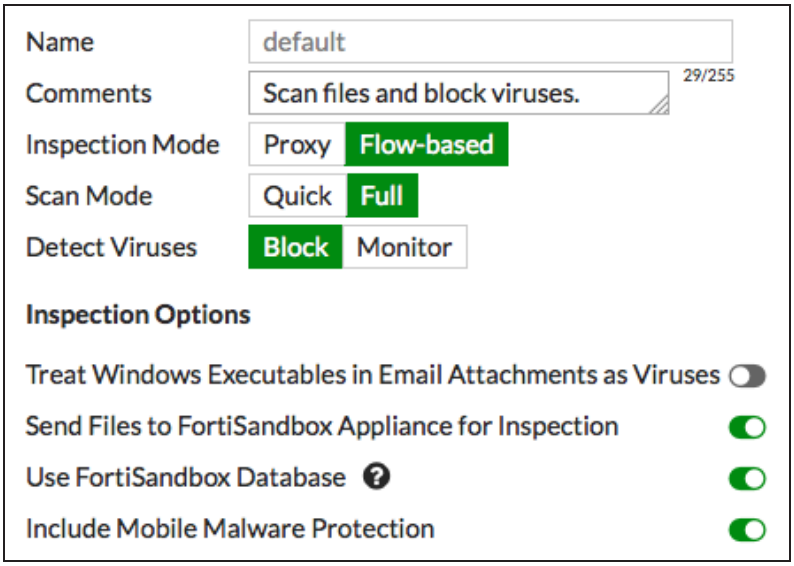


3. Configuring sandboxing in the default AntiVirus profile

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

Under **Inspection Options**, enable both **Send Files to FortiSandbox Appliance for Inspection** and **Use FortiSandbox Database**.

If FortiSandbox discovers a threat, it creates a signature for that file that is added to the FortiGate's AntiVirus signature database.

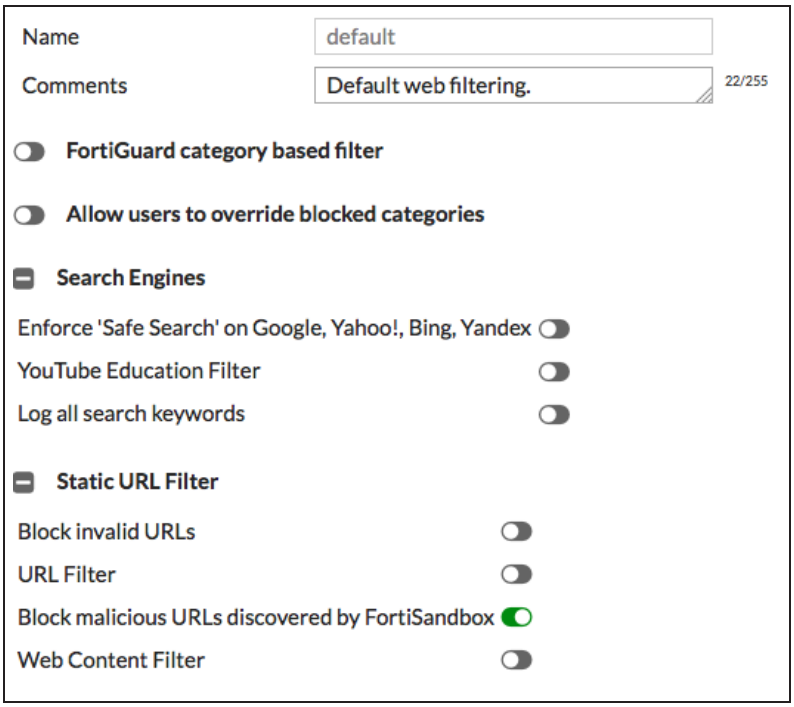


4. Configuring sandboxing in the default Web Filter profile

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

Under **Static URL Filter**, enable **Block malicious URLS discovered by FortiSandbox**.

If the FortiSandbox discovers a threat, the URL that threat came from will be added to the list of URLs that will be blocked by the FortiGate.

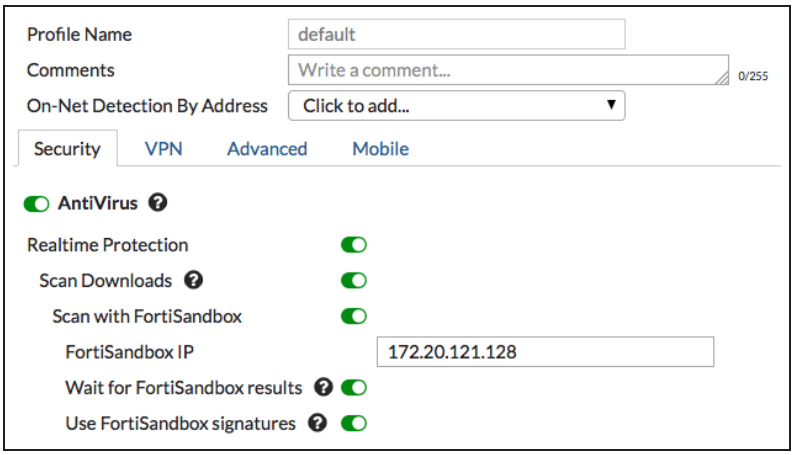


5. Configuring sandboxing in the default FortiClient profile

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

Under **AntiVirus**, enable **Realtime Protection**, then enable **Scan Downloads**, followed by **Scan with FortiSandbox**. Enter the IP of the FortiSandbox.

Decide if you want to wait for FortiSandbox results before sending files to the PC running FortiClient, or if you want downloaded files to be sent at the same time as they are being scanned by FortiSandbox.

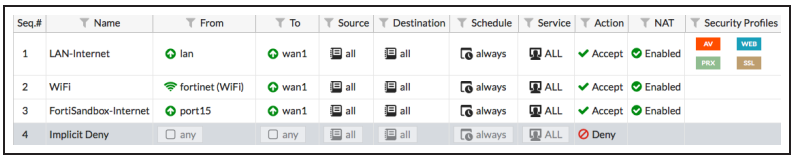


Enable **Use FortiSandbox signatures** to make sure new virus signatures and blocked URLs from the FortiSandbox are added to FortiClient's databases.

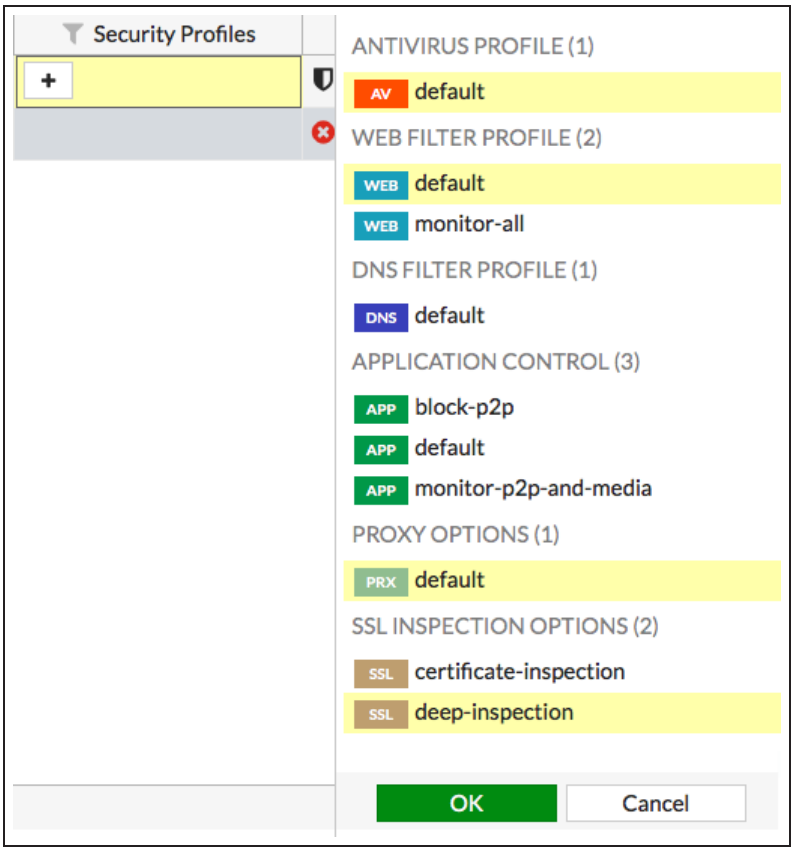
This profile will be pushed to any device running FortiClient that is registered to your FortiGate. These settings can also be configured from within FortiClient's **AntiVirus** settings.

6. Applying AntiVirus and Web Filter scanning to network traffic

Go to **Policy & Objects > IPv4 Policy** and view the policy list. If a policy has AntiVirus and web filtering scanning applied, the profiles will be listed in the **Security Profiles** column.



If scanning needs to be added to any security policy (excluding the **Implicit Deny** policy) select the **+** button in the **Security Profiles** column for that policy, then select the default **AntiVirus Profile**, the default **Web Filter Profile**, the appropriate **Proxy Options**, and the **deep-inspection** profile for **SSL Inspection Options** (to ensure that encrypted traffic is inspected). Then select **OK**.



7. Results

If your FortiGate discovers a suspicious file, it will now be sent to the FortiSandbox. To view information about the files that have been sent on the FortiGate, go to **FortiView > FortiSandbox** to see a list of file names and current status.

Add Filter | Files | Source | 5 minutes | 1 hour | 24 hours

Source	File Name	Status	Submitted
vickimartin (192.168.200.110)	Breakpoints.js	Clean	10/02/2015 09:40:00
vickimartin (192.168.200.110)	Corp_Reverb.css	Clean	10/02/2015 09:40:00
vickimartin (192.168.200.110)	FortiOS%205.2%20CLI_sx.js	Clean	10/02/2015 09:40:00
vickimartin (192.168.200.110)	Language.js	Clean	10/02/2015 09:40:00
vickimartin (192.168.200.110)	MadCapAll.js	Clean	10/02/2015 09:40:00
vickimartin (192.168.200.110)	Slideshow.css	Clean	10/02/2015 09:40:00
vickimartin (192.168.200.110)	Toc.js	Clean	10/02/2015 09:40:00
vickimartin (192.168.200.110)	Toc_Chunk6.js	Clean	10/02/2015 09:40:00
vickimartin (192.168.200.110)	Web.css	Clean	10/02/2015 09:40:00

You can also view results on the FortiSandbox by going to **System > Status** and viewing the **Scanning Statistics** widget.

There may be a delay before results appear on the FortiSandbox.

Scanning Statistics - Last 24 Hours

Scanning Files Statistics in Last 24 Hours

Rating	Sniffer	Device(s)	On Demand	Network	All
Malicious	0	0	0	0	0
Suspicious - High Risk	0	0	0	0	0
Suspicious - Medium Risk	0	0	0	0	0
Suspicious - Low Risk	0	0	0	0	0
Clean	0	35	0	0	35
Other	0	0	0	0	0
Processed	*0*	*35*	*0*	*0*	*35*
Pending	*0*	*0*	*0*	*0*	*0*
Processing	*0*	*0*	*0*	*0*	*0*
Total	*0*	*35*	*0*	*0*	*35*

Open FortiClient using a Windows PC on the internal network. Make sure it is registered to your FortiGate.

Go to **AntiVirus > Realtime Protection Enabled** and edit the settings. You will see that the **Realtime Protection** settings match the FortiClient Profile configured on the FortiGate. These settings cannot be changed using FortiClient.

Realtime Protection
Scheduled Scan
Exclusion List

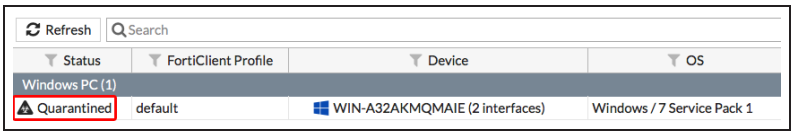
☑ Scan files as they are downloaded or copied to my system
☑ Extended scanning using FortiSandbox
FortiSandbox IP address: 172.20.121.128
☑ Wait for FortiSandbox results before allowing file access
☑ Identify malware & exploits using signatures or URLs received from FortiSandbox

On the FortiGate, go to **Monitor > FortiClient Monitor**. Select the FortiClient device, then select **Quarantine**.

Block | Quarantine | Unregister | Refresh | Search

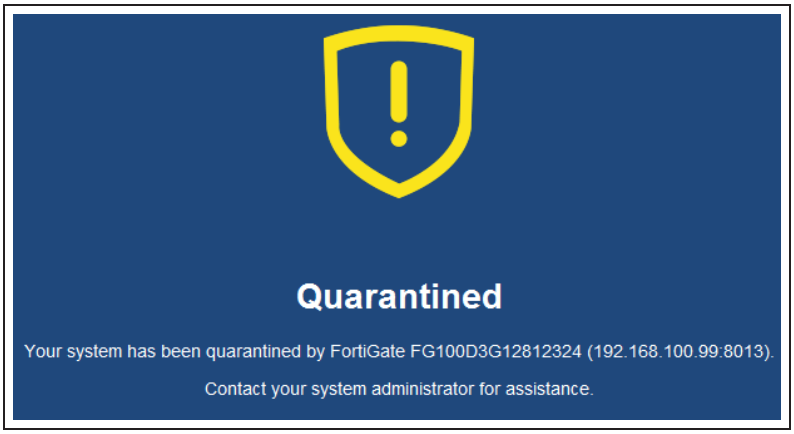
Status	FortiClient Profile	Device	OS
Windows PC (1)			
Registered - On-Net	default	WIN-A32AKMQMAIE (2 interfaces)	Windows / 7 Service Pack 1

The PC is now quarantined by FortiClient and cannot connect to the Internet or other network devices.



A message appears in FortiClient, telling the user to contact the system administrator.

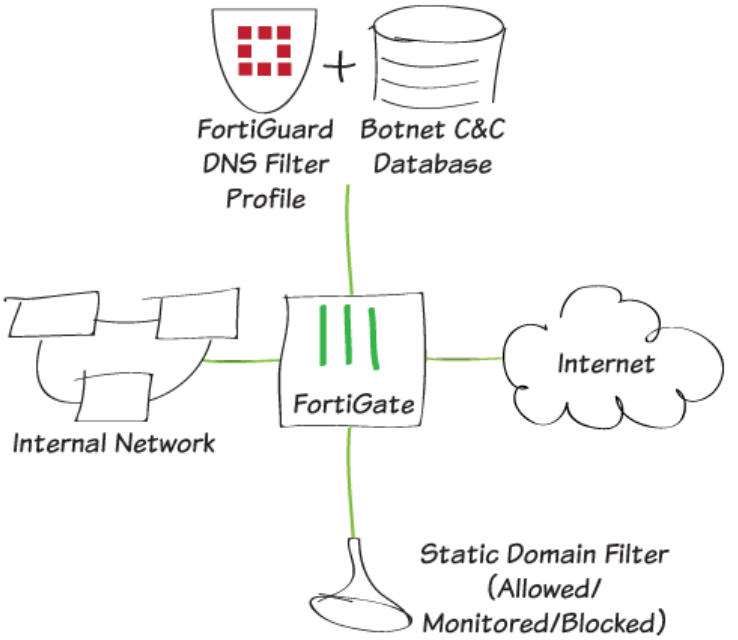
FortiClient cannot be shutdown on the PC. It can also not be uninstalled or unregistered from the FortiGate.



If the PC had downloaded a suspicious file that the FortiSandbox determined was malicious, quarantine would be applied automatically.

The quarantine can only be released from the FortiClient Monitor on the FortiGate.

Protection from Botnet C&C attacks



This recipe uses a new FortiGuard feature: the Botnet C&C (command and control) database to protect your network from Botnet C&C attacks.

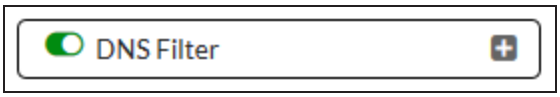
For this recipe, you will create a new DNS Filter Profile called Botnet&Facebook, block access to all known C&C addresses, and block access to the Social Networking FortiGuard category. In addition, you will enhance this with a Static Domain Filter in order to block access to www.facebook.com, and all of its affiliated subdomains.

For this recipe to work, your device must be licensed for the FortiGuard Web Filtering service. DNS filtering is only available when Inspection Mode is Proxy-based.

A video of this recipe is available here.

1. Enabling the DNS Filter Security Feature

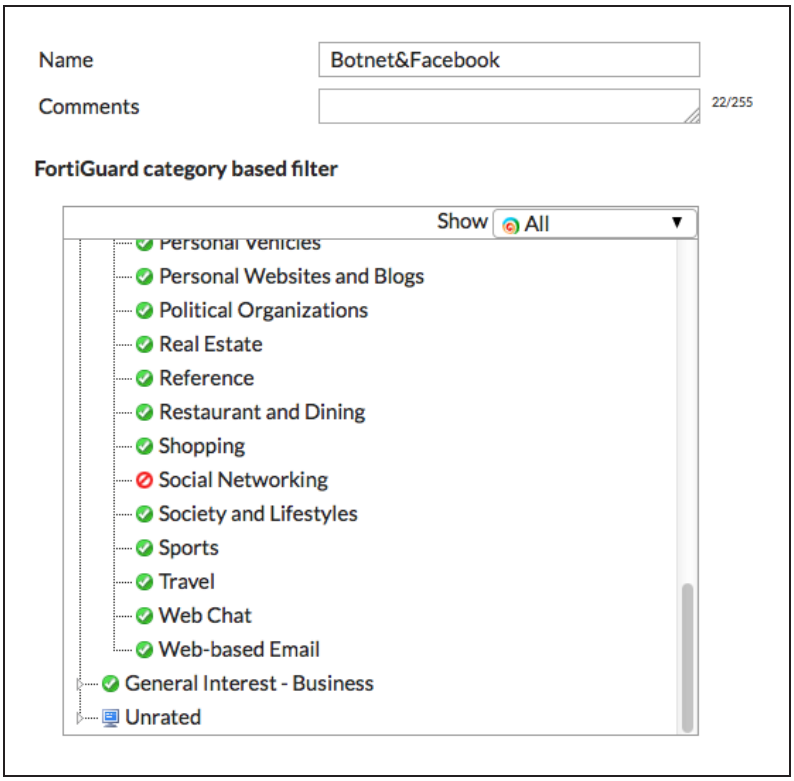
Go to **System > Feature Select**, and enable **DNS Filter** under **Security Features**. Select **Apply**.



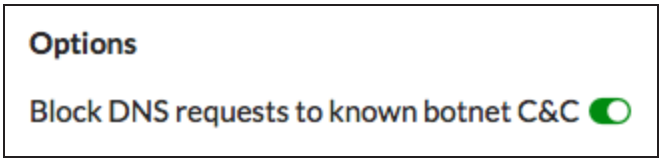
2. Creating the DNS Filter Profile and enabling Botnet C&C database

Go to **Security Profiles > DNS Filter**, and create a new profile called *Botnet&Facebook*.

Right-click and block the **Social Networking** category from the **FortiGuard category based filter** table.

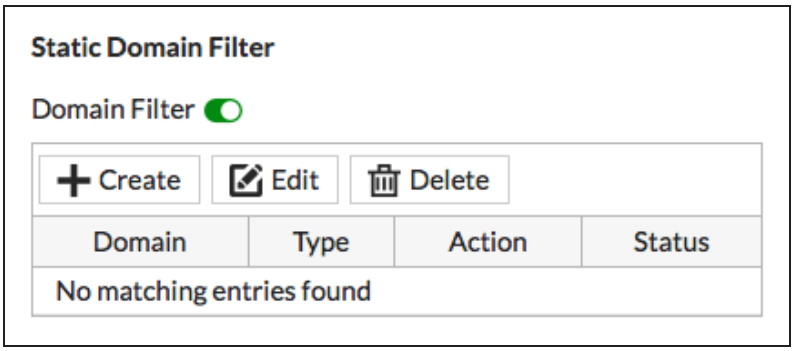


Under **Options**, enable **Block DNS requests to known botnet C&C**.



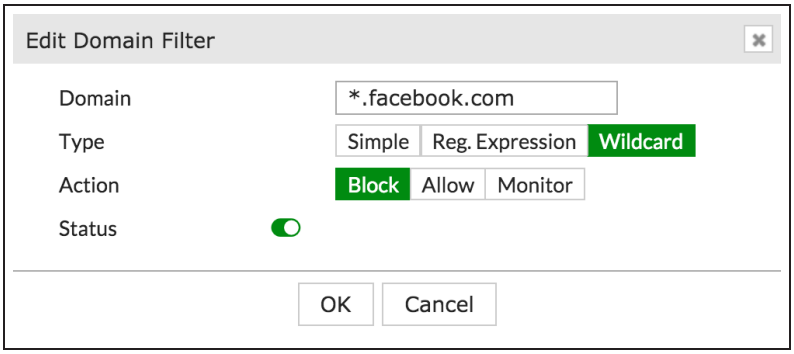
3. Configuring Static Domain Filter in DNS Filter Profile

In the DNS Filter Profile, enable **Domain Filter** under **Static Domain Filter**. You will now be able to add domains of your choosing.



Select **Create** and enter **.facebook.com*.

Set **Type** to **Wildcard**, and set **Action** to **Block**. Make sure **Status** is enabled. This will block access to Facebook, and all its other affiliated subdomains.



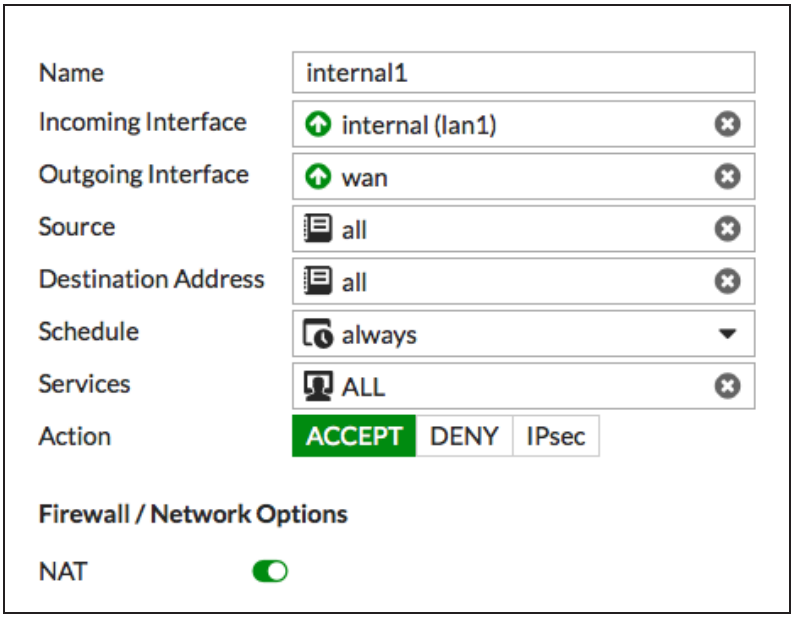
4. Creating a DNS Filtering firewall policy

Go to **Policy & Objects > IPv4 Policy**, and create a firewall policy that allows Internet access.

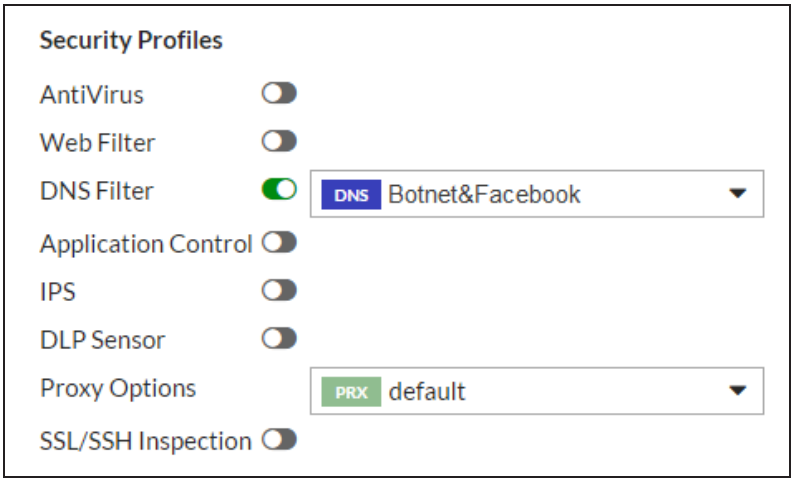
Set **Incoming Interface** to the internal interface and set **Outgoing Interface** to the external interface.

Set **Source** to **all** and set **Destination Address** to **all**.

Set **Schedule** to **always**, set **Services** to **ALL**, and make sure **NAT** is enabled.

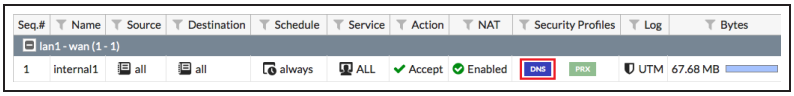


Under **Security Profiles**, enable **DNS Filter** and select the **Botnet&Facebook** DNS Filter profile – this will automatically enable **Proxy Options**.



5. Results

To confirm that the DNS Filter Profile has been added, go to **Policy & Objects > IPv4 Policy**. The policy will now have the DNS filter icon in the **Security Profiles** column.

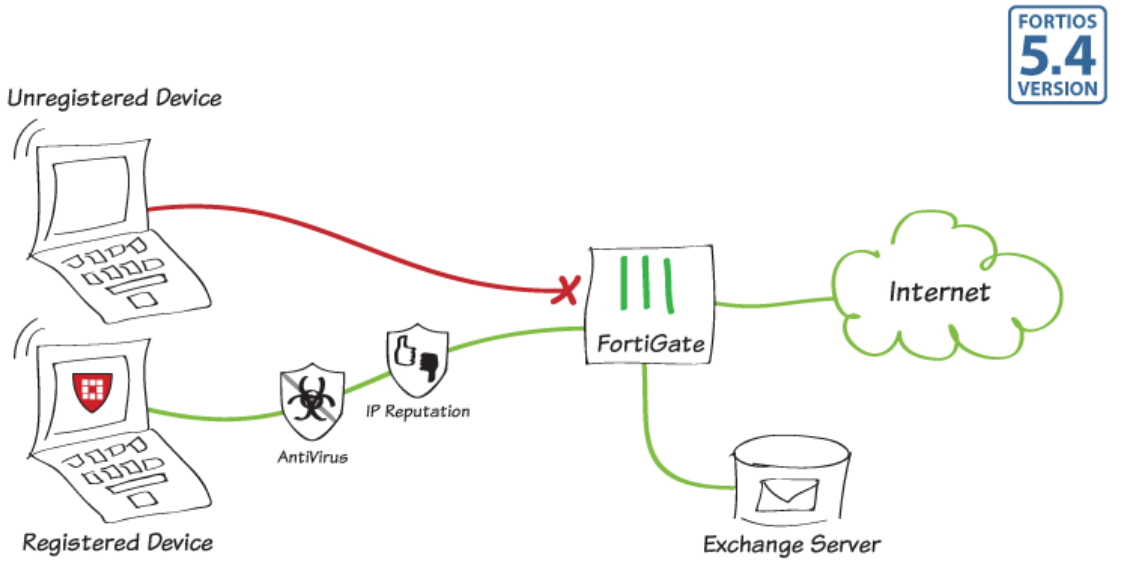


To confirm that the filter is working correctly, open a browser and attempt to browse to *www.facebook.com*. The DNS request will be blocked.

To confirm that the known Botnet C&C feature is working correctly, browse to a known Botnet site – the example is *nateve.us*. Again, the DNS request will be blocked.

Note that the blocked pages may look different on other web browsers.

Enforcing network security using a FortiClient Profile



In this recipe, you will learn how to enforce a FortiClient Profile on an internal network such that only internal devices registered with FortiClient can access the Internet and the corporate network. You will edit the default FortiClient Profile to enforce realtime antivirus protection and malicious website blocking.

This recipe requires you to enable FortiHeartBeat on a FortiGate interface. When you enable FortiHeartBeat on an interface, the option to enforce FortiClient registration becomes available. Devices connecting to that interface are forced to register to the FortiGate and install FortiClient before getting access to network services.

FortiGates come with a free FortiClient license allowing a limited number of devices to register to the FortiGate and download FortiClient. Your FortiGate gets the latest version of FortiClient for Mac and for Windows from FortiGuard. When devices register with the FortiGate they download and install one of these copies of FortiClient. You can see the status of your FortiClient licensing and purchase additional FortiClient licenses from the License Information Dashboard Widget.

This recipe was tested using FortiClient version 5.4.

A video of this recipe is available here.

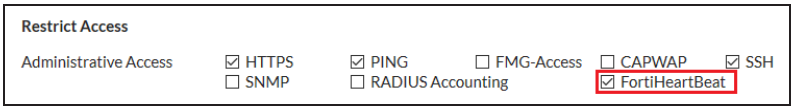
1. Enabling endpoint control on the FortiGate

On the FortiGate, go to **System > Feature Select** and make sure that **Endpoint Control** is enabled.

2. Enforcing FortiClient registration on the internal interface

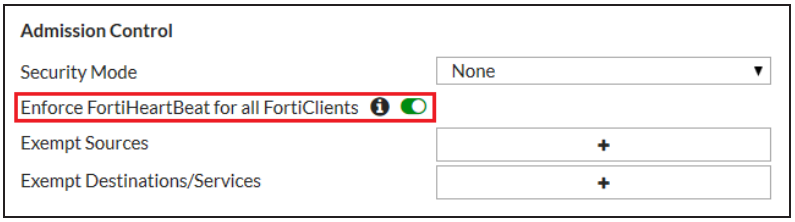
Go to **Network > Interfaces** and select the internal interface.

Under **Restrict Access**, enable **FortiHeartBeat**.



Under **Admission Control**, enable **Enforce FortiHeartBeat for all FortiClient.**

*You can also **Exempt Sources** and/or **Exempt Destinations/Services**. If you were to exempt a source device, that device would not require FortiClient registration to access network services or the Internet.*

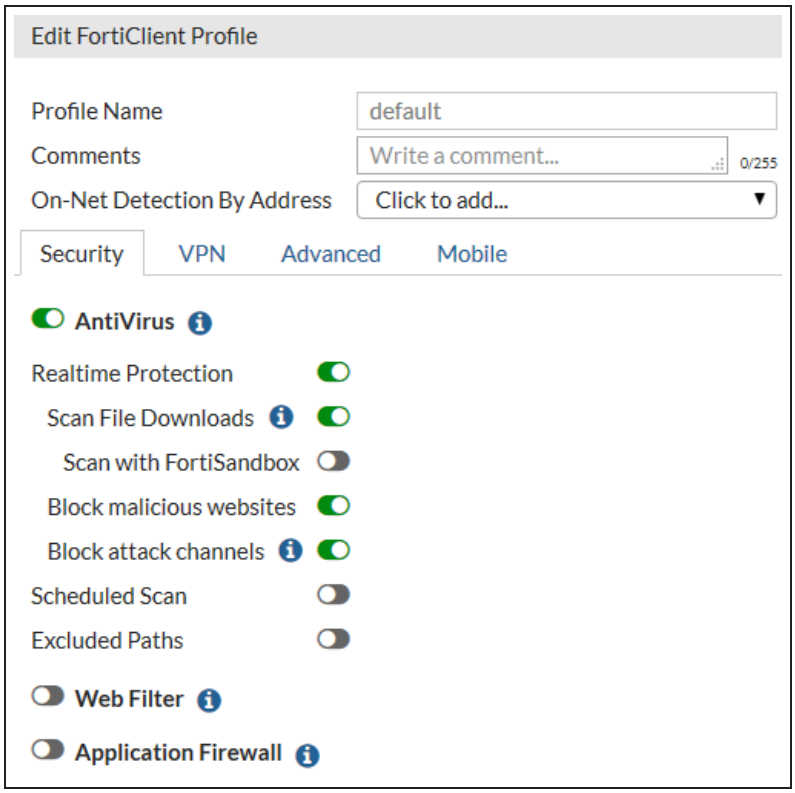


3. Configuring the FortiClient Profile

Configuring a FortiClient Profile allows you to control the security features enabled on the registered endpoint. The profile is automatically downloaded to FortiClient when it registers to the FortiGate.

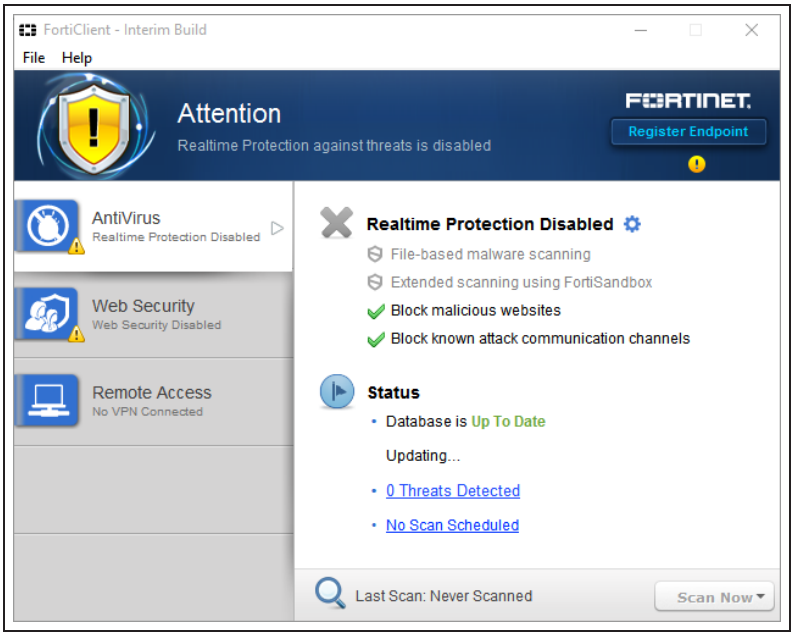
You can add additional FortiClient Profiles to define exceptions to the default profile. The configuration of the exception profiles includes devices, users, or addresses to which the exception applies.

Go to **Security Profiles > FortiClient Profiles** and edit the default profile to provide realtime antivirus protection that scans files as they are downloaded or copied to the device, block malicious websites and block attack channels.

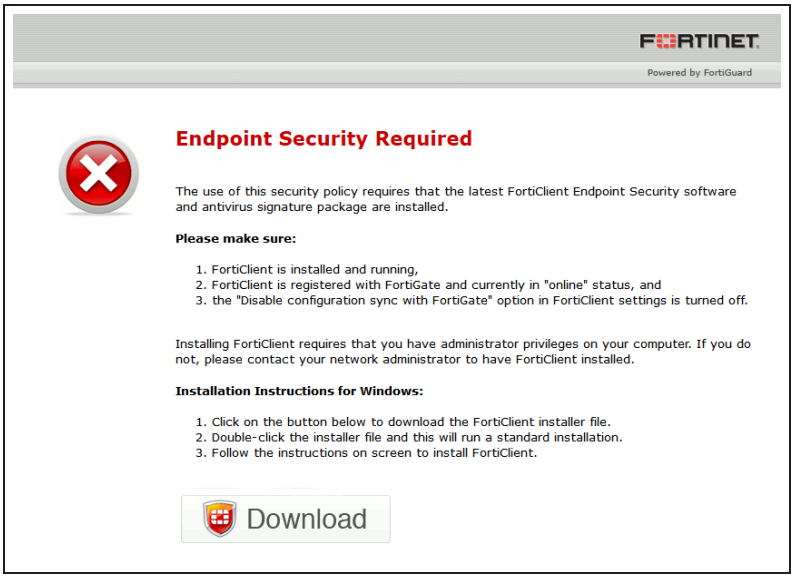


4. Results

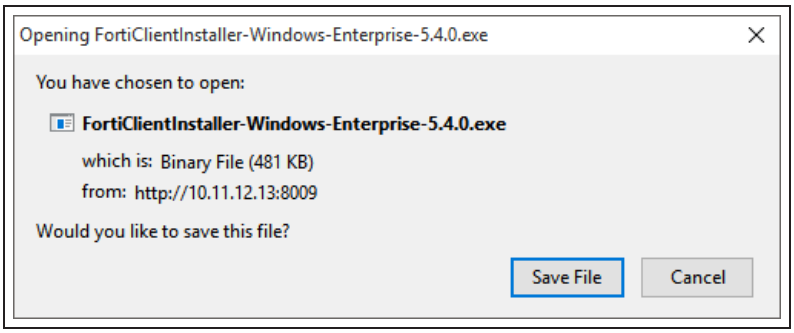
In this image, an internal device has FortiClient installed but not registered with a FortiGate. This is indicated by the **Attention** banner, and also because the option to **Register Endpoint** is available.



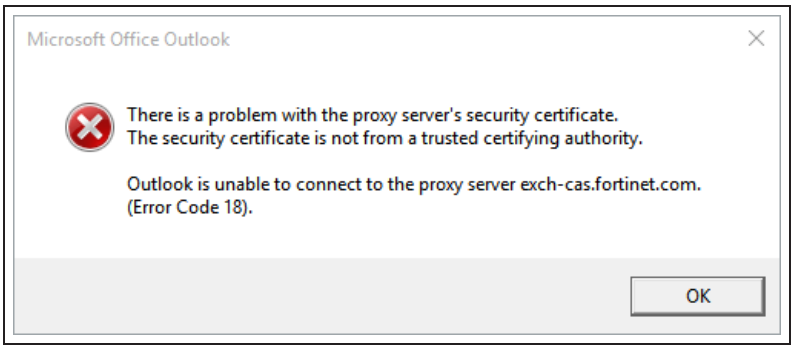
When a user on this device attempts to browse the Internet, an **Endpoint Security Required** page appears instructing the user to install and register endpoint security in the form of FortiClient.



A download link is provided at the bottom of the page. When the user clicks on this link, the FortiGate responds with a download of the latest FortiClient software.



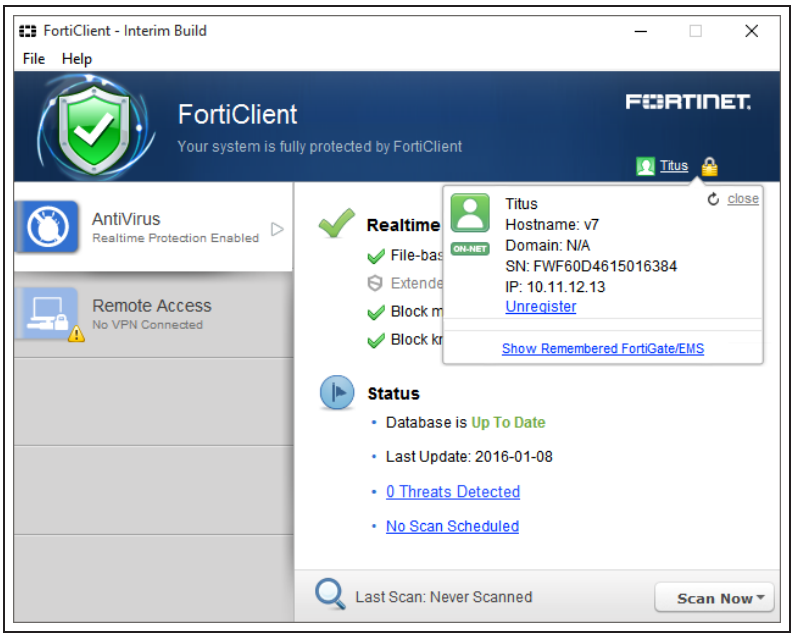
Similarly, since the device requires a registered FortiClient to access network services, internal servers (such as Exchange mail servers) will also be blocked, unless otherwise exempted– see Step 2.



By comparison, a registered device appears below. The device shows as registered, with a lock icon next to the device name in the upper right corner.

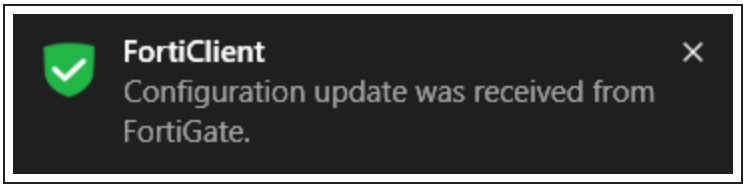
FortiClient should automatically attempt to register to the nearest FortiGate, provided that FortiHeartBeat has been enabled and registration enforced.

A user on this device can verify their registration status by clicking on the device name.

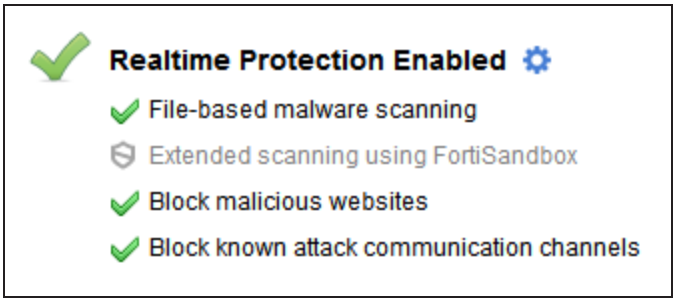


FortiClient displays the device's On-Net/Off-Net status, **Hostname**, **Domain**, registered FortiGate's serial number (**SN**), and **IP** address.

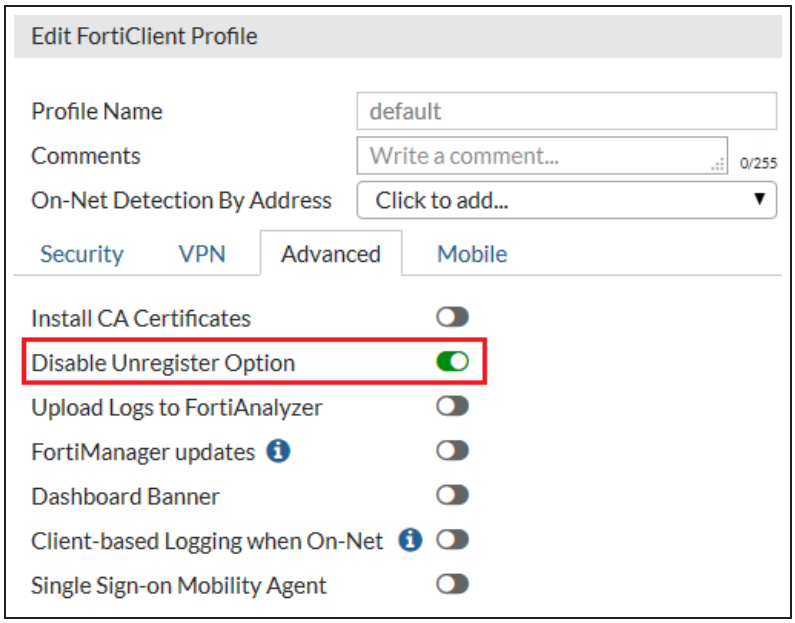
Upon registration, the FortiGate updates the FortiClient configuration to match the FortiClient Profile and downloads the latest FortiGuard antivirus database to the device.



You can verify that the registered configuration update matches the FortiClient Profile.



Depending on the FortiClient Profile, the user may also have the option to **Unregister** the device. This can be disabled on the FortiGate in **Security Profiles > FortiClient Profiles**, under the **Advanced** tab.



The registered device can now access corporate network services and browse the Internet.

To verify the status of the endpoints on the FortiGate, go to **User & Device > Device List**.

Note that this list also includes unregistered endpoints and any other connected device.

internal (4)				
Mac (1)				
Offline	drs		10.11.12.103	Mac OS X
Windows PC (3)				
Registered - Online - On-Net	abristow-PC	abristow	10.11.12.101	Windows / 7 Service
Registered - Online - On-Net	v7 (4 interfaces)	Titus	10.11.12.100	Windows / 10
Online	WIN-DNVK2JCJKR0		10.11.12.102	Windows 8.1 / 2012

By default, this list shows On-Net/Off-Net **Status**, endpoint **Device** (Hostname and device name), endpoint IP **Address**, and the device's operating system (**OS**).

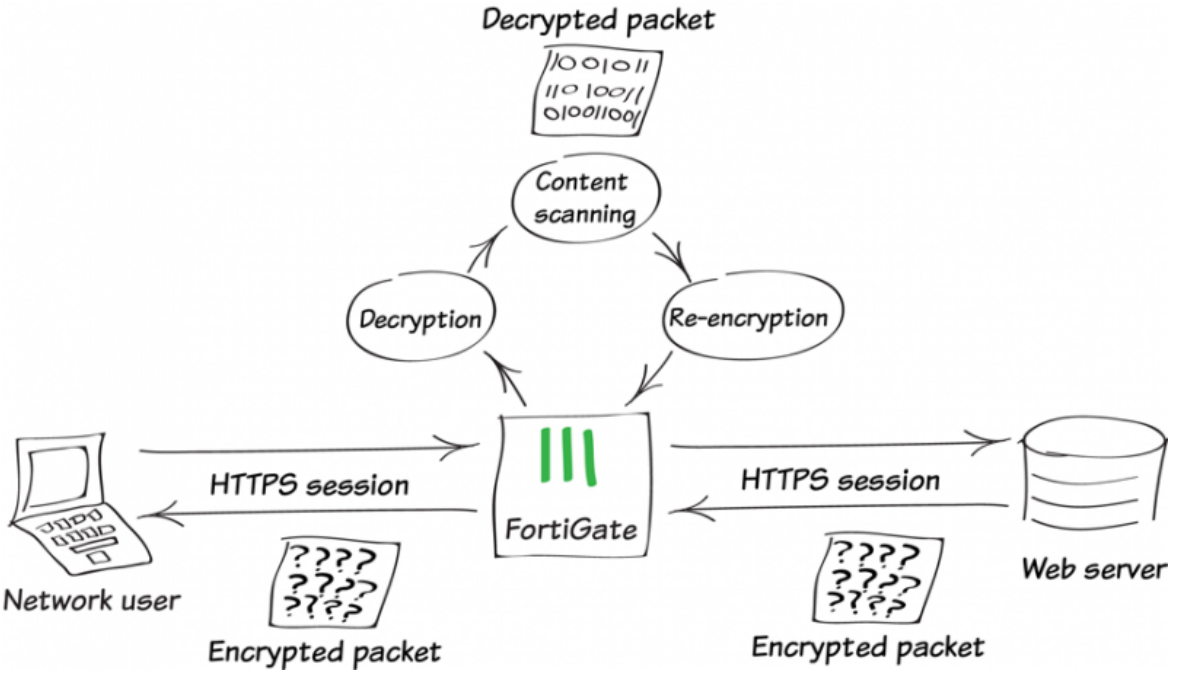
To view only the status of FortiClient connections, go to **Monitor > FortiClient Monitor**.

The FortiClient monitor shows both registered and unregistered FortiClients, including On-Net/Off-Net status.

internal (2)				
Registered - Online - On-Net (2)				
abristow-PC	abristow	10.11.12.101 (fortinet-us.com)	5.4.0	Microsoft Windows 7
v7 (4 interfaces)	Titus	10.11.12.100	5.4.0	Microsoft Windows 10

For further reading, check out the FortiClient 5.4 Administration Guide.

Why you should use SSL inspection



Most of us are familiar with Hypertext Transfer Protocol Secure (HTTPS) and how it protects a variety of activities on the Internet by applying Secure Sockets Layer (SSL) encryption to the web traffic.

The benefits of HTTPS are obvious, as encryption keeps your private data safe from prying eyes. However, there are risks associated with its use, since encrypted traffic can be used to get around your normal defenses.

For example, you might download a file containing a virus during an e-commerce session. Or you could receive a phishing email containing a seemingly harmless downloader file that, when launched, creates an encrypted session to a command and control (C&C) server and downloads malware onto your computer. Because the sessions in these attacks are encrypted, they might get past your network's security measures.

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

Full SSL inspection

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

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

There are two deployment methods for full SSL inspection:

1. Multiple Clients Connecting to Multiple Servers:

- Uses a CA certificate (which can be uploaded using the **Certificates** menu).
- Typically applied to outbound policies where destinations are unknown (i.e. normal web traffic).
- Address and web category whitelists can be configured to bypass SSL inspection.

2. Protecting SSL Server

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

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

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

SSL certificate inspection

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

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

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

Troubleshooting

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

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

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

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

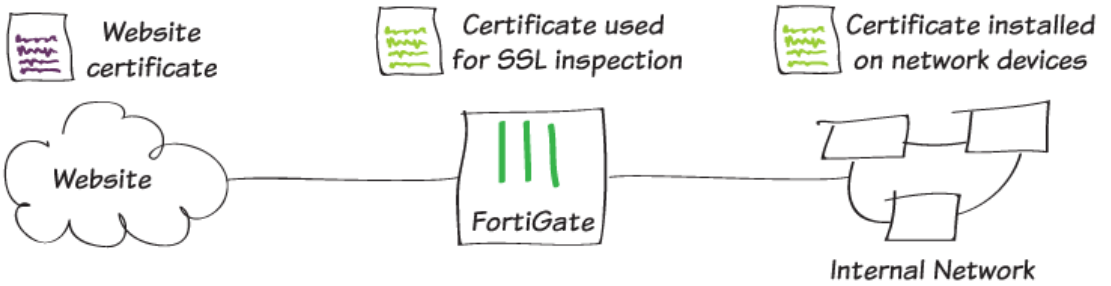
For corporate-owned mobile devices, MDM solutions like AirWatch, MobileIron, or Fiberlink, use Simple Certificate Enrollment Protocol (SCEP) to ease certificate enrollment.

Best practices

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

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

Preventing certificate warnings



In this recipe, you will prevent users from receiving a security certificate warning when your FortiGate applies full SSL inspection to incoming traffic.

When full SSL inspection is used, your FortiGate impersonates the recipient of the originating SSL session, then decrypts and inspects the content. The FortiGate then re-encrypts the content, creates a new SSL session between the FortiGate and the recipient by impersonating the sender, and sends the content to the end user. This is the same process used in "man-in-the-middle" attacks, which is why a user's device may show a security certificate warning.

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

Often, when a user receives a security certificate warning, they simply select **Continue** without understanding why the error is occurring. To avoid encouraging this habit, you can prevent the warning from appearing in the first place.

There are two methods for doing this, depending on whether you are using Using the default certificate or Using a self-signed certificate.

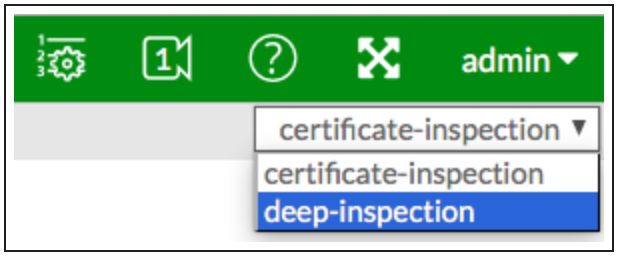
Using the default certificate

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

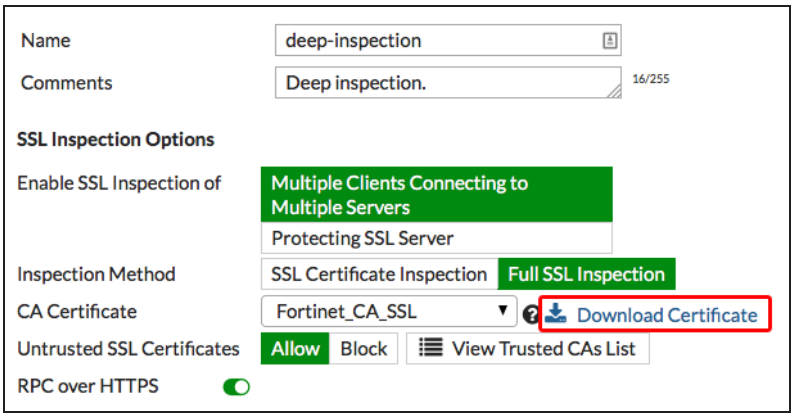
If you have the right environment, you can distribute the certificate and have it installed automatically.

1. Downloading the certificate used for full SSL inspection

Go to **Security Profiles > SSL/SSH Inspection**. Use the dropdown menu in the top right corner to select **deep-inspection**, the profile used to apply full SSL inspection.



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



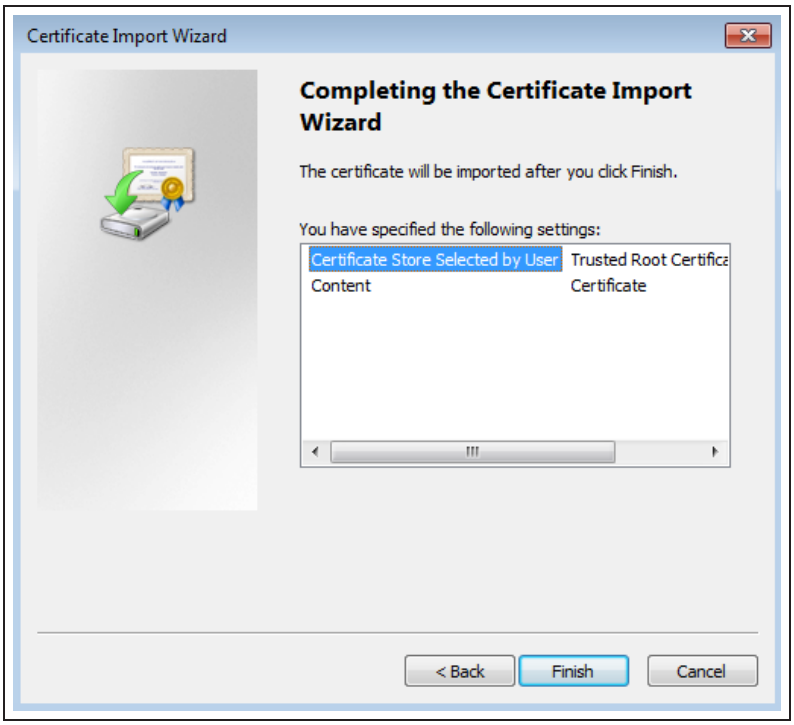
2. Installing the certificate on the user's browser

Internet Explorer, Chrome, and Safari (on Windows or Mac OS):

The above browsers use the operating system's certificate store for Internet browsing. If your users will be using these applications, you must install the certificate into the certificate store for your OS.

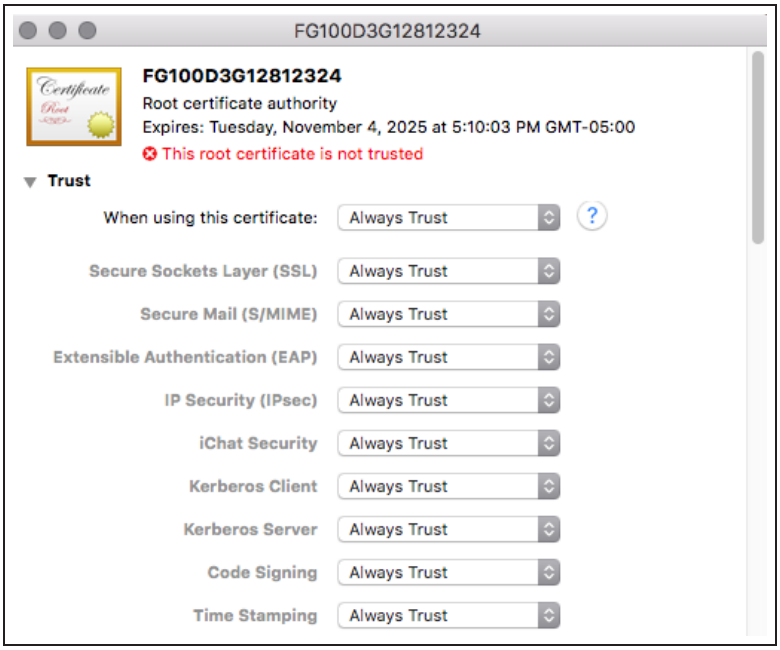
If you are using Windows 7/8/10, double-click on the certificate file and select **Open**. Select **Install Certificate** to launch the **Certificate Import Wizard**.

Use the wizard to install the certificate into the **Trusted Root Certificate Authorities** store. If a security warning appears, select **Yes** to install the certificate.



If you are using Mac OS X, double-click on the certificate file to launch **Keychain Access.**

Locate the certificate in the **Certificates** list and select it. Expand **Trust** and select **Always Trust**. If necessary, enter the administrative password for your computer to make this change.



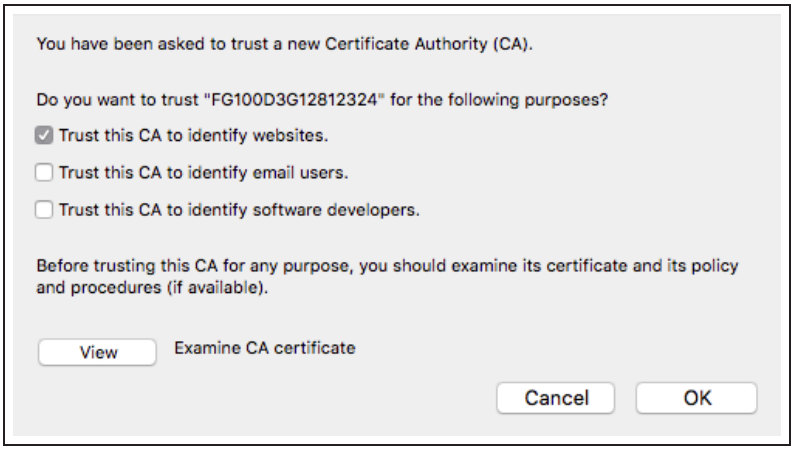
If you have the right environment, the certificate can be pushed to your users' devices. However, if Firefox is used, the certificate must be installed on each individual device, using the instructions below.

Firefox (on Windows or Mac OS)

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

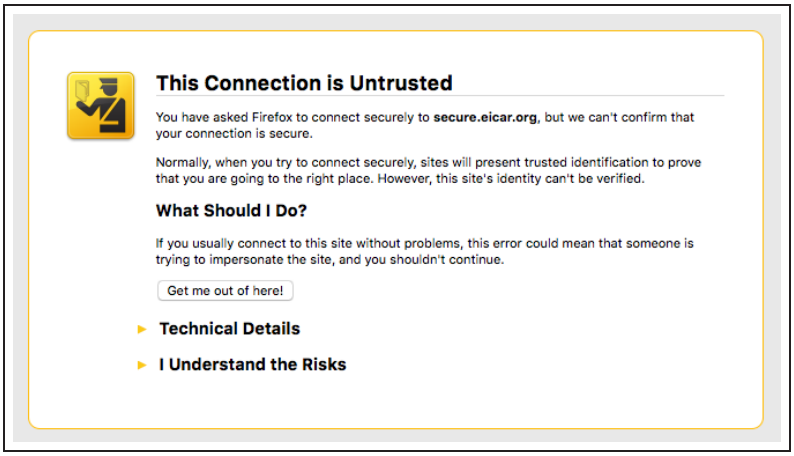
Go to **Tools > Options > Advanced** or **Firefox > Preferences > Advanced** and find the **Certificates** tab.

Select **View Certificates**, then select the **Authorities** list. **Import** the certificate and set it to be trusted for website identification.



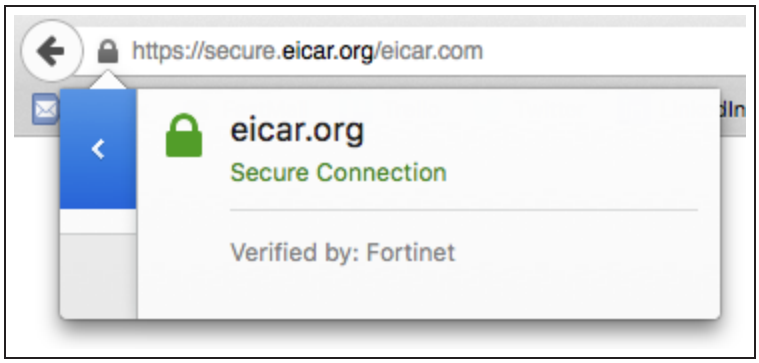
3. Results

Before installing the certificate, an error message would appear in the browser when a site that used HTTPS was accessed (the example shows an error message appearing in Firefox).



After you install the certificate, you should not experience a certificate security issue when you browse to sites on which the FortiGate unit performs SSL content inspection.

If you view information about the connection, you will see that it is verified by Fortinet.



Using a self-signed certificate

In this method, a self-signed certificate is created using OpenSSL. This certificate will then be installed on the FortiGate for use with SSL inspection.

In this recipe, OpenSSL for Windows version 0.9.8h-1 is used.

1. Creating a certificate with OpenSSL

If necessary, download and install Open SSL. Make sure that the file *openssl.cnf* is located in the *BIN* folder for OpenSSL.

Using Command Prompt (CMD), navigate to the BIN folder (in the example, the command is `cd c:\OpenSSL\openssl-0.9.8h-1-1bin\bin`.

Generate an RSA key with the following command:

```
OpenSSL genrsa -aes256 -out fgcaprivkey.pem 2048 -config openssl cnf
```

This RSA key uses AES 256 encryption and a 2058-bit key.

When prompted, enter a pass phrase for encrypting the private key.

Use the following command to launch OpenSSL, submit a new certificate request, and sign the request:

```
openssl req - new -x509 -days 3650 -extensions v3_ca -key fgcaprivkey.pem -
out fgcacert.pem - config openssl.cnf
```

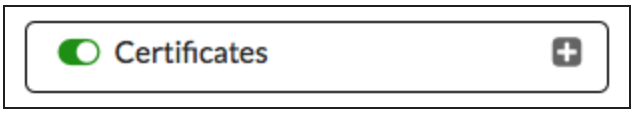
The result is a standard x509 binary certificate that is valid for 3,650 days (approx. 10 years)

When prompted, re-enter the pass phrase for encryption, then enter the details required for the certificate request, such as location and organization name.

Two new files have been created: a public certificate *(fgcacert.pem*) and a private key (in the example, *fgcaprivkey.pem*).

2. Enabling certificate configuration in the web-based manager

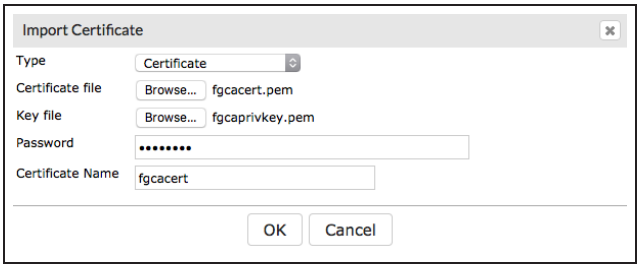
Go to **System > Feature Select**. Under **Additional Features**, enable **Certificates** and **Apply** the changes.



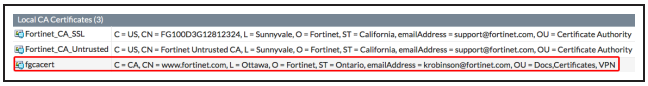
3. Importing the self-signed certificate

Go to **System > Certificates** and select **Import > Local Certificate**.

Set **Type** to **Certificate**, then select your **Certificate file** and **Key file**. Enter the **Password** used to create the certificate.

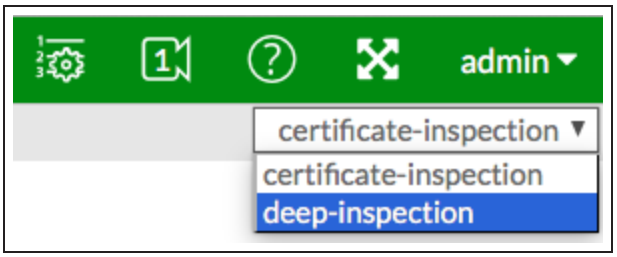


The certificate now appears on the **Local CA Certificates** list.



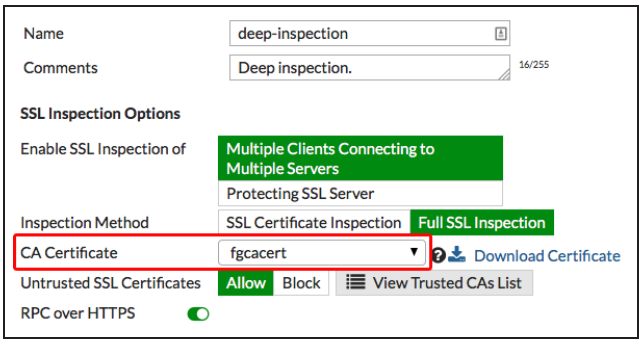
4. Edit the SSL inspection profile

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



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

Select **Download Certificate**, to download the certificate file needed in the next step.



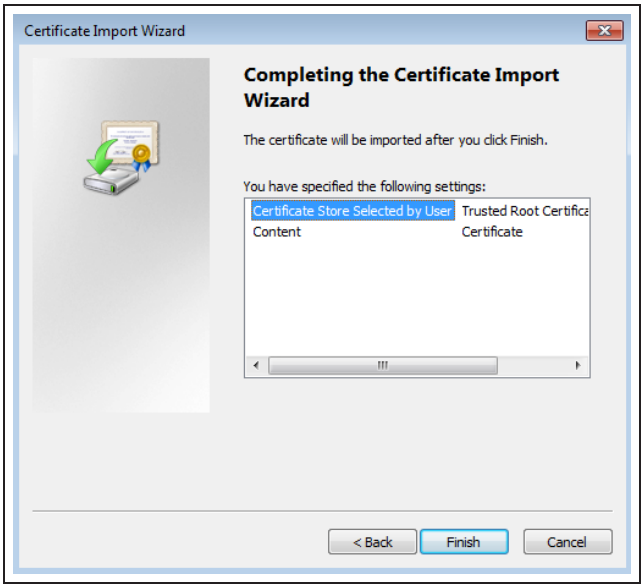
5. Importing the certificate into the web browser

Internet Explorer, Chrome, and Safari (on Windows or Mac OS):

The above browsers use the operating system's certificate store for Internet browsing. If your users will be using these applications, you must install the certificate into the certificate store for your OS.

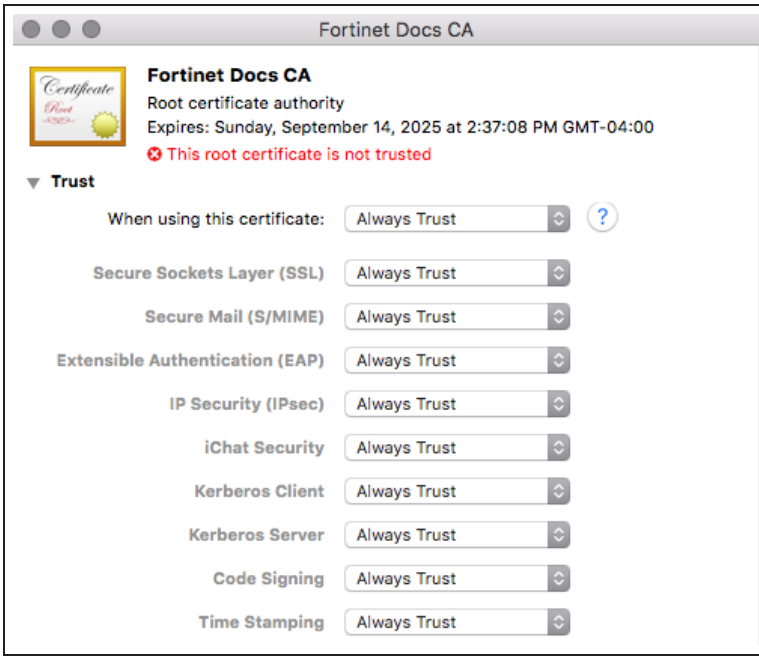
If you are using Windows 7/8/10, double-click on the certificate file and select **Open**. Select **Install Certificate** to launch the **Certificate Import Wizard**.

Use the wizard to install the certificate into the **Trusted Root Certificate Authorities** store. If a security warning appears, select **Yes** to install the certificate.



If you are using Mac OS X, double-click on the certificate file to launch **Keychain Access.**

Locate the certificate in the **Certificates** list and select it. Expand **Trust** and select **Always Trust**. If necessary, enter the administrative password for your computer to make this change.



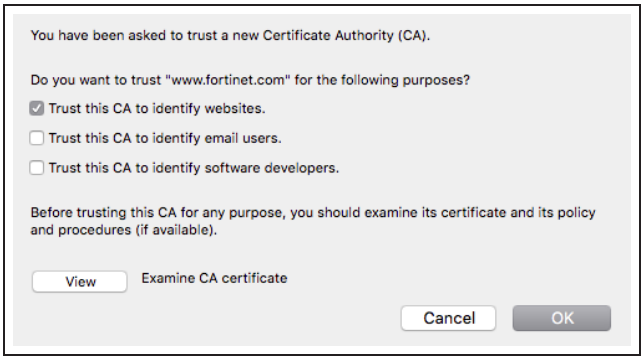
If you have the right environment, the certificate can be pushed to your users' devices. However, if Firefox is used, the certificate must be installed on each individual device, using the instructions below.

Firefox (on Windows or Mac OS)

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

Go to **Tools > Options > Advanced** or **Firefox > Preferences > Advanced** and find the **Certificates** tab.

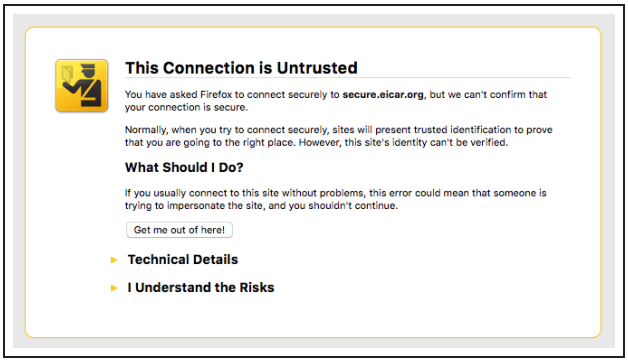
Select **View Certificates**, then select the **Authorities** list. **Import** the certificate and set it to be trusted for website identification.



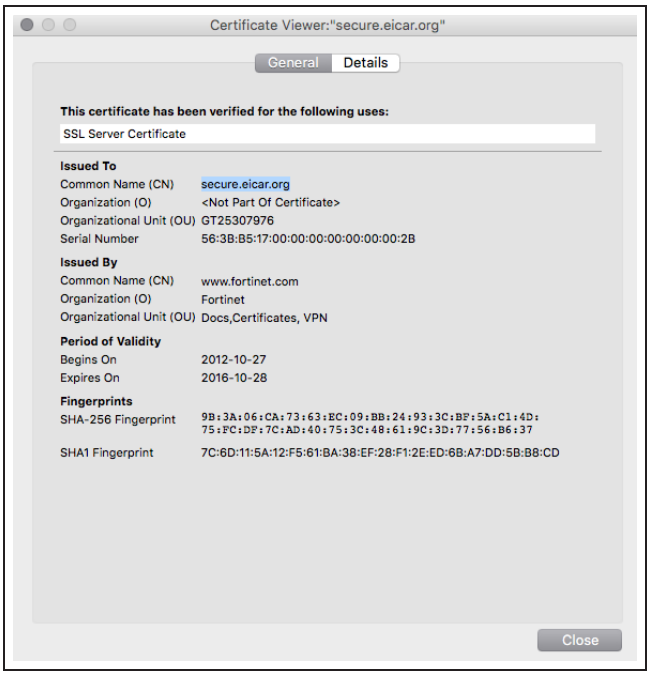
6. Results

Before installing the certificate, an error message would appear in the browser when a site that used HTTPS was accessed (the example shows an error message appearing in Firefox).

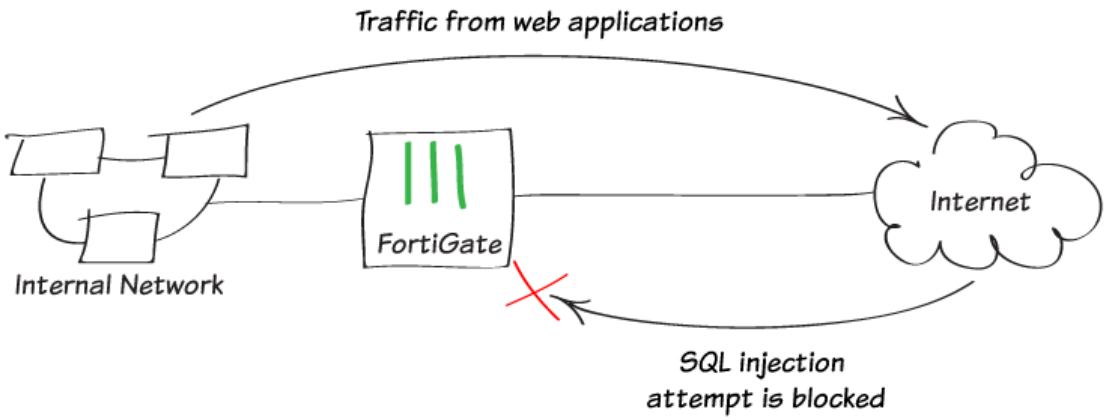
After you install the certificate, you should not experience certificate errors when you browse to sites on which the FortiGate unit performs SSL content inspection.



If you view information about the certificate in the browser, you will see that your self-signed certificate is used.



Protecting web applications



In this recipe, you will use a Web Application Firewall profile to protect web applications, such as Internet browsers, from being attacked. In this example, the default profile will be targeted to block SQL injection attempts, as well as generic attacks.

Web Application Firewall is only available when **Inspection Mode** is **Proxy-based**.

1. Enabling Web Application Firewall

Go to **System > Features** and enable **Web Application Firewall**. Select **Show More** and enable **Multiple Security Profiles**.

Apply your changes.

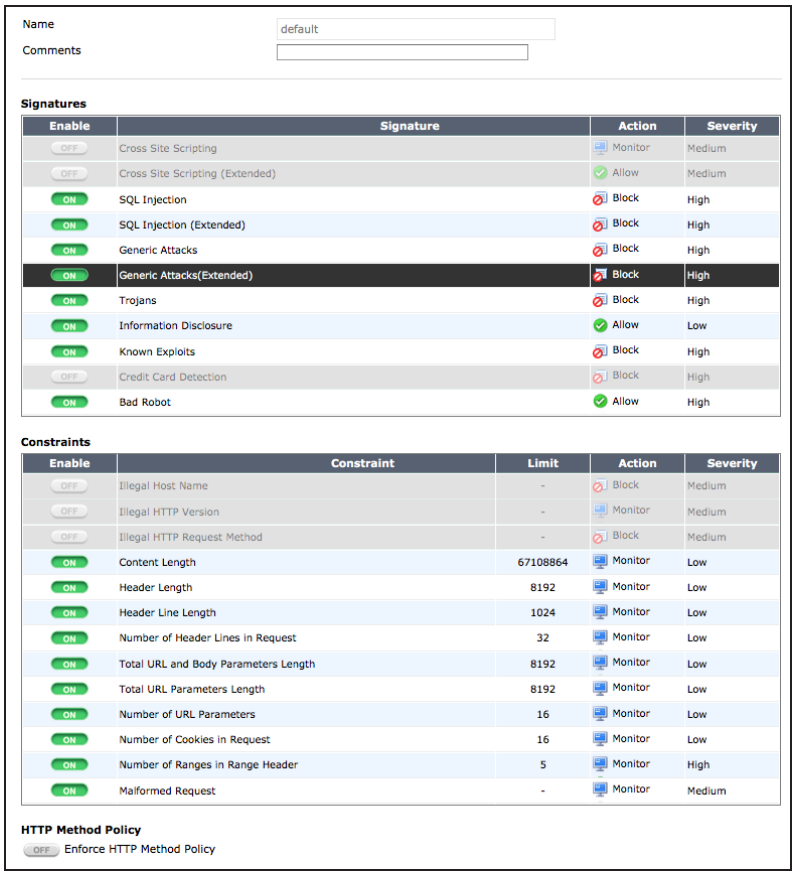
2. Editing the default Web Application Firewall profile

Web Application Firewall profiles are created with a variety of options, called **Signatures** and **Constraints**. Once these options are enabled, **Action** can be set to **Allow**, **Monitor**, or **Block**, and **Severity** can be set to **High**, **Medium**, or **Low**.

You can also use a Web Application Firewall profile to enforce an HTTP method policy, which controls the HTTP method allowed when accessing websites that match the specified pattern.

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

In this example, the signatures for **SQL Injection (Extended)** and **Generic Attacks (Extended)** have been enabled, with the **Action** set to **Block** and **Severity** set to **High**.



Name: default

Comments:

Signatures

Enable	Signature	Action	Severity
OFF	Cross Site Scripting	Monitor	Medium
OFF	Cross Site Scripting (Extended)	Allow	Medium
ON	SQL Injection	Block	High
ON	SQL Injection (Extended)	Block	High
ON	Generic Attacks	Block	High
ON	Generic Attacks(Extended)	Block	High
ON	Trojans	Block	High
ON	Information Disclosure	Allow	Low
ON	Known Exploits	Block	High
OFF	Credit Card Detection	Block	High
ON	Bad Robot	Allow	High

Constraints

Enable	Constraint	Limit	Action	Severity
OFF	Illegal Host Name	-	Block	Medium
OFF	Illegal HTTP Version	-	Monitor	Medium
OFF	Illegal HTTP Request Method	-	Block	Medium
ON	Content Length	67108864	Monitor	Low
ON	Header Length	8192	Monitor	Low
ON	Header Line Length	1024	Monitor	Low
ON	Number of Header Lines in Request	32	Monitor	Low
ON	Total URL and Body Parameters Length	8192	Monitor	Low
ON	Total URL Parameters Length	8192	Monitor	Low
ON	Number of URL Parameters	16	Monitor	Low
ON	Number of Cookies in Request	16	Monitor	Low
ON	Number of Ranges in Range Header	5	Monitor	High
ON	Malformed Request	-	Monitor	Medium

HTTP Method Policy

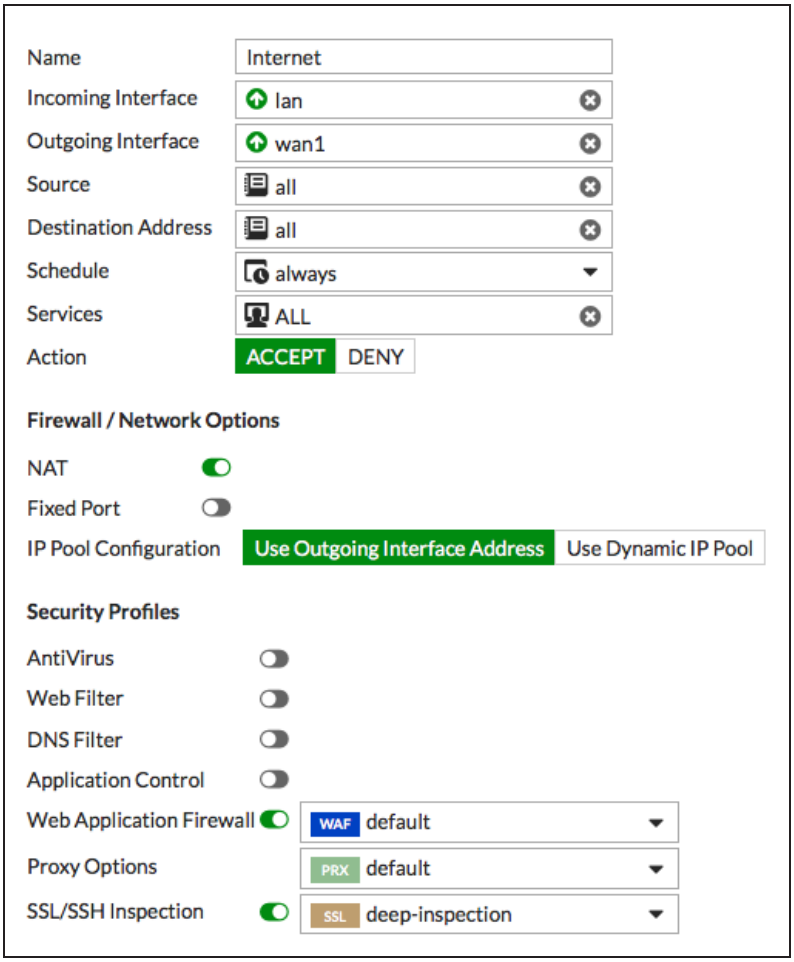
OFF Enforce HTTP Method Policy

3. Applying the profile to a security policy

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

Under **Security Profiles**, enable **Web Application Firewall** and set it to use the default profile. Set the appropriate **Proxy Option** and set **SSL/SSH Inspection** to use the **deep-inspection** profile.

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

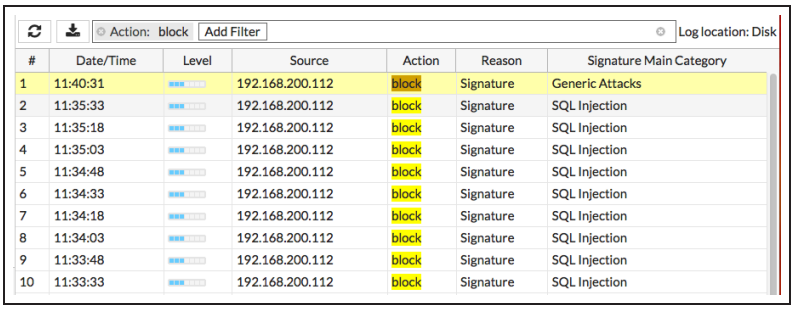


4. Results

Long URLs, such as this link, can be used to simulate an attack on your web browser.

After selecting one of these links, a replacement message will appear, stating that the transfer has been blocked by the Web Application Firewall.

Go to **Log & Report > Web Application Firewall** and filter for **Action: block** to view information about blocked traffic.



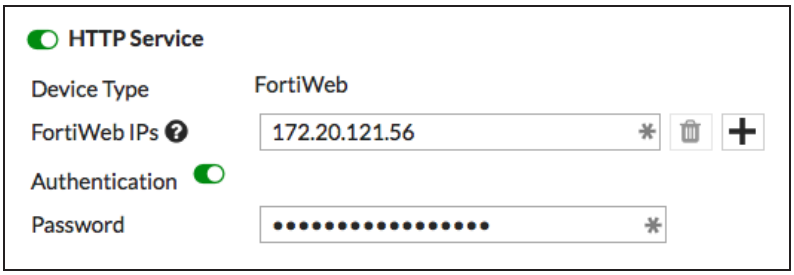
#	Date/Time	Level	Source	Action	Reason	Signature Main Category
1	11:40:31		192.168.200.112	block	Signature	Generic Attacks
2	11:35:33		192.168.200.112	block	Signature	SQL Injection
3	11:35:18		192.168.200.112	block	Signature	SQL Injection
4	11:35:03		192.168.200.112	block	Signature	SQL Injection
5	11:34:48		192.168.200.112	block	Signature	SQL Injection
6	11:34:33		192.168.200.112	block	Signature	SQL Injection
7	11:34:18		192.168.200.112	block	Signature	SQL Injection
8	11:34:03		192.168.200.112	block	Signature	SQL Injection
9	11:33:48		192.168.200.112	block	Signature	SQL Injection
10	11:33:33		192.168.200.112	block	Signature	SQL Injection

5. Offloading to a FortiWeb

If you have a FortiWeb, you may be able to offload the functions of the Web Application Control to your FortiWeb. To find out if this option is available, refer to the FortiOS or FortiWeb Release Notes for information about device compatibility.

Go to **System > External Security Devices** and enable **HTTP Service.** Enter your FortiWeb's IP address.

If necessary, enable **Authentication** and enter the FortiWeb's password.



Troubleshooting web filtering

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

The Web Filter option does not appear in the GUI.

Go to Feature Select and enable **Web Filter**.

New Web Filter profiles cannot be created.

Go to Feature Select and enable **Multiple Security Profiles**.

Web Filtering has been configured but is not working.

Make sure that web filtering is enabled in a policy. If it is enabled, check that the policy is the policy being used for the correct traffic. Also check that the policy is getting traffic by going to the policy list and adding the Sessions column to the list.

An active FortiGuard Web Filtering license displays as expired/unreachable.

If this occurs, make sure web filtering is enabled in one of your security policies. The FortiGuard service will sometimes show as expired when it is not being used, to save CPU cycles.

If web filtering is enabled in a policy, go to your **FortiGuard** settings and expand **Web Filtering**. Under **Port Selection**, select **Use Alternate Port (8888)**. Select **Apply** to save the changes. Check whether the license is shown as active. If it is still inactive/expired, switch back to the default port and check again.

WiFi

These recipes describe how to use FortiAPs to add WiFi (or Wi-Fi) services to your network.

FortiAPs, managed by FortiGates, provide a full suite of WiFi features. Small offices can use FortiAPs to quickly add WiFi. Enterprises and educational institutions can take advantage of FortiAP access control features. Each WiFi network, or SSID, is represented by a WiFi network interface to which you can apply firewall policies, security profiles, and other features in the same way you would for wired networks.

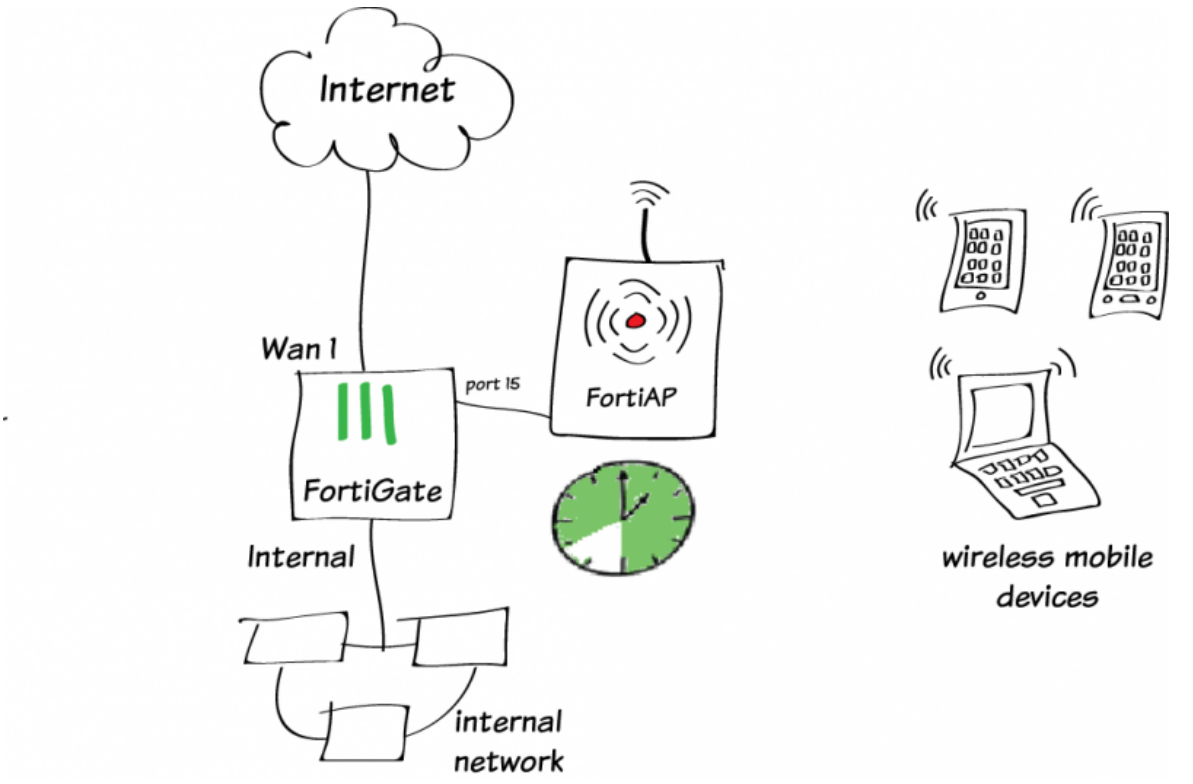
Getting started with WiFi

- WiFi network on a schedule
- Extending WiFi range with mesh topology

WiFi authentication

- Assigning WiFi users to VLANs dynamically
- WiFi RADIUS authentication with FortiAuthenticator

WiFi network on a schedule



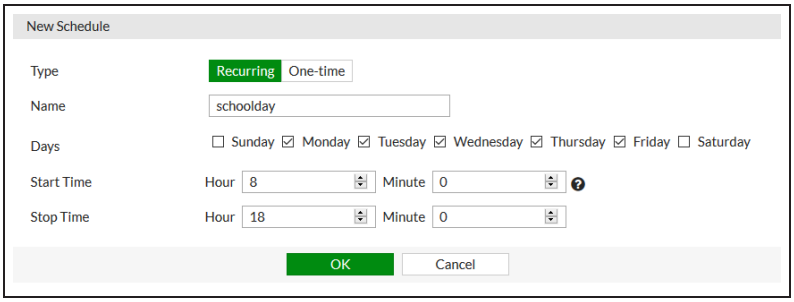
In this example, a school enables its WiFi network only during school hours. The school is open from 8am to 6pm Monday through Friday.

A schedule applied in the security policy would control access to the Internet, but outside of the scheduled period the SSID would still be visible and clients could associate with it. In this example, the schedule is applied in the SSID configuration. The SSID is available only during the scheduled hours.

This configuration was tested with FortiOS 5.4 Beta 3 and FortiAP v5.2-build0245.

1. Create the schedule

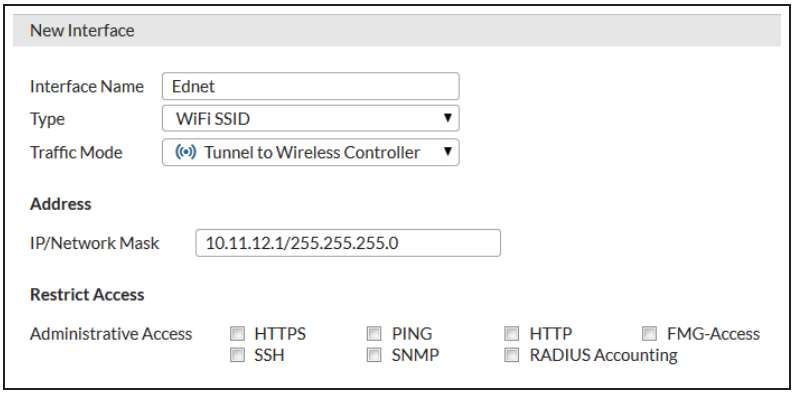
Go to **Policy & Objects > Schedules**. Create a recurring schedule for school hours (in the example, 8am-6pm, Monday through Friday).



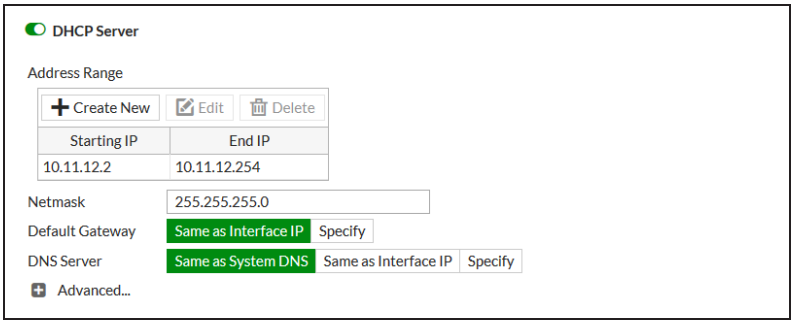
2. Create the SSID

Go to **WiFi Controller > SSID** and create the WiFi interface.

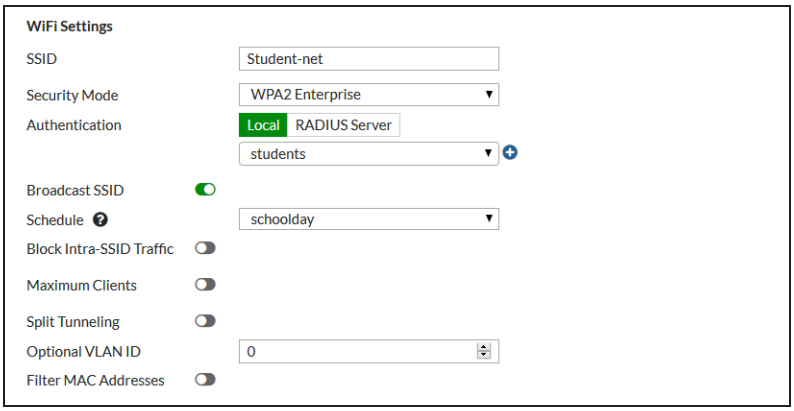
Set a **Name** and **IP/Network Mask** for the interface.



Enable **DHCP Server** to provide a range of IP addresses for your WiFi clients.



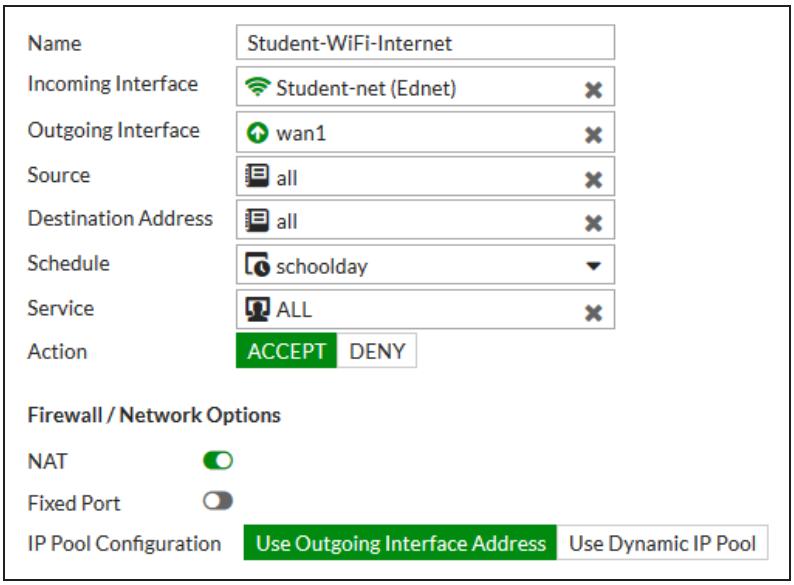
Set **Schedule** to the new schedule, and configure the other **WiFi Settings** as required.



3. Create the security policy

Go to **Policy & Objects > IPv4 Policy** and create a policy that allows Internet access for mobile devices on the Student-net wireless network. Give the policy a name that identifies what it is used for (in the example, *Student-WiFi-Internet*).

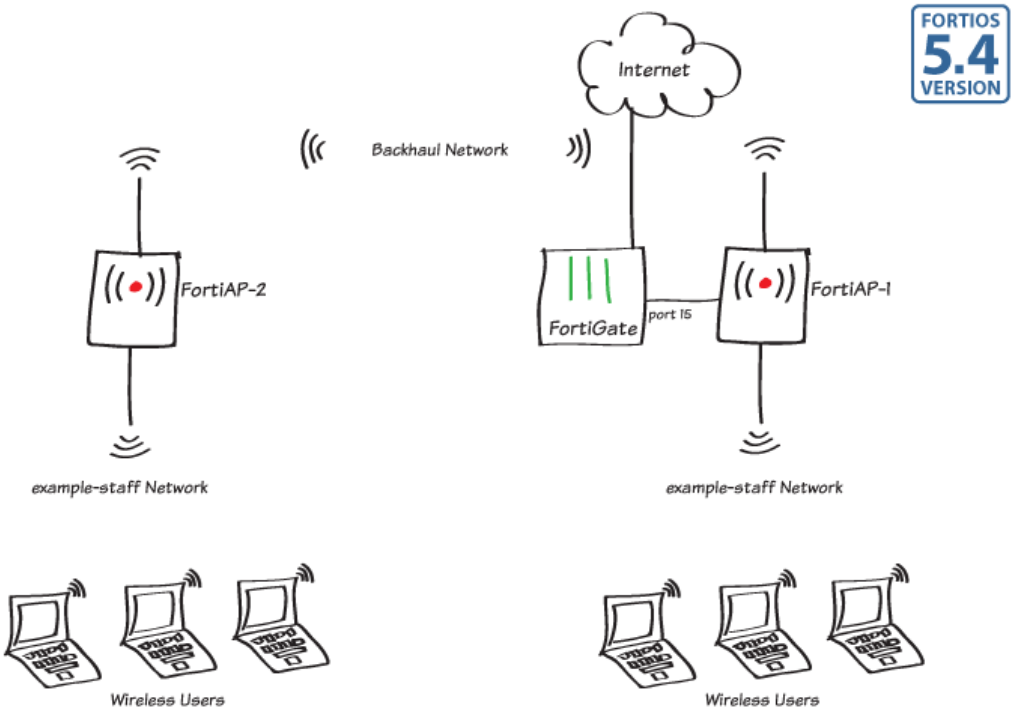
Set **Incoming Interface** to the wireless interface and **Outgoing Interface** to the Internet-facing interface. Set **Schedule** to the new schedule and make sure **NAT** is enabled.



Results

Verify that mobile devices can connect to the Internet outside of class time, when the schedule group is valid. Verify that the SSID is not available after scheduled times.

Extending WiFi range with mesh topology



In this example, a second FortiAP are used to extend the range of a WiFi network. The second FortiAP is connected to the FortiGate WiFi controller through a dedicated WiFi backhaul network.

In this example, both FortiAPs provide the example-staff network to clients that are in range.

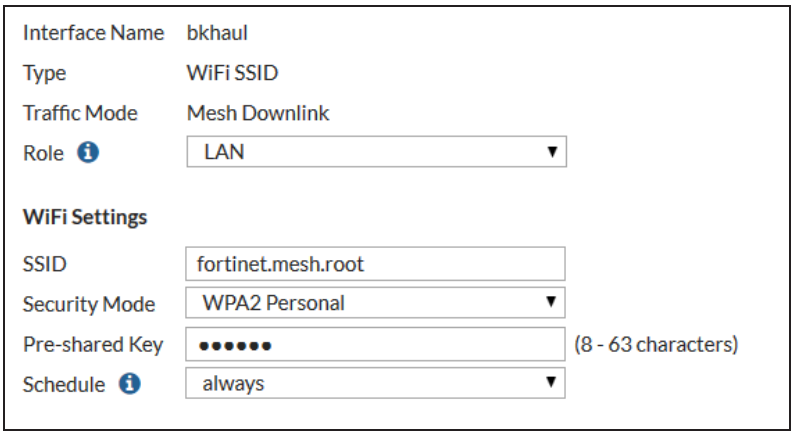
More mesh-connected FortiAPs could be added to further expand the coverage range of the network. Each AP must be within range of at least one other FortiAP. Mesh operation requires FortiAP models with two radios, such as the FortiAP-221C units used here.

1. Creating the backhaul SSID

Go to **WiFi Controller > SSID**.

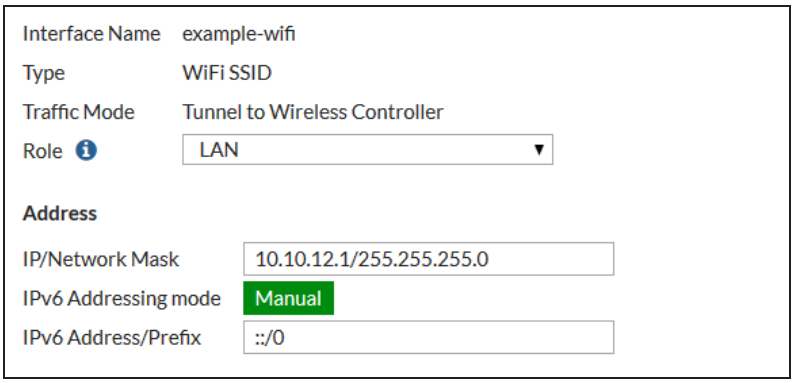
Create a new SSID. Set **Traffic Mode** to **Mesh Downlink**.

You will need the pre-shared key when configuring the mesh-connected FortiAP.

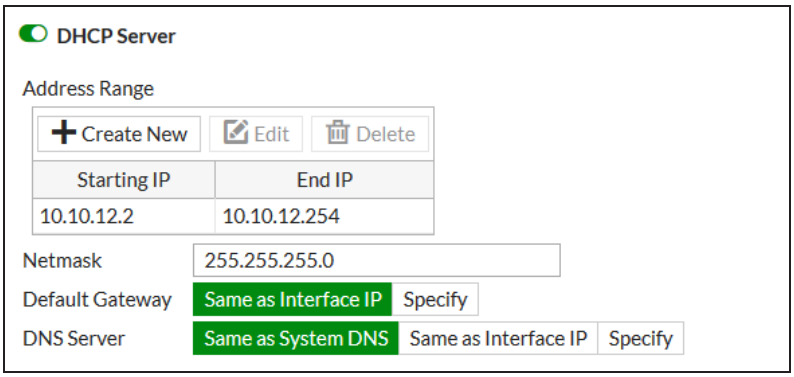


2. Creating the client SSID

Go to **WiFi Controller > SSID**. Create the WiFi network (SSID) that clients will use.



Configure DHCP to provide IP addresses for your clients.

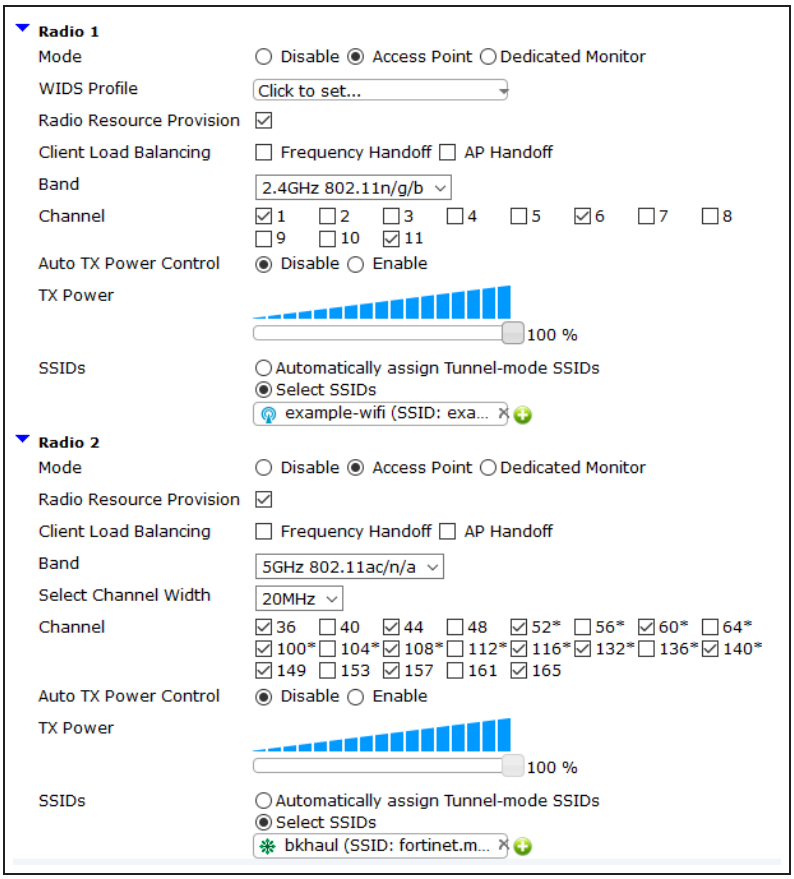


3. Creating the FortiAP Profile

Go to **WiFi Controller > FortiAP Profiles** and create a profile for the Platform (FortiAP model) that you are using.

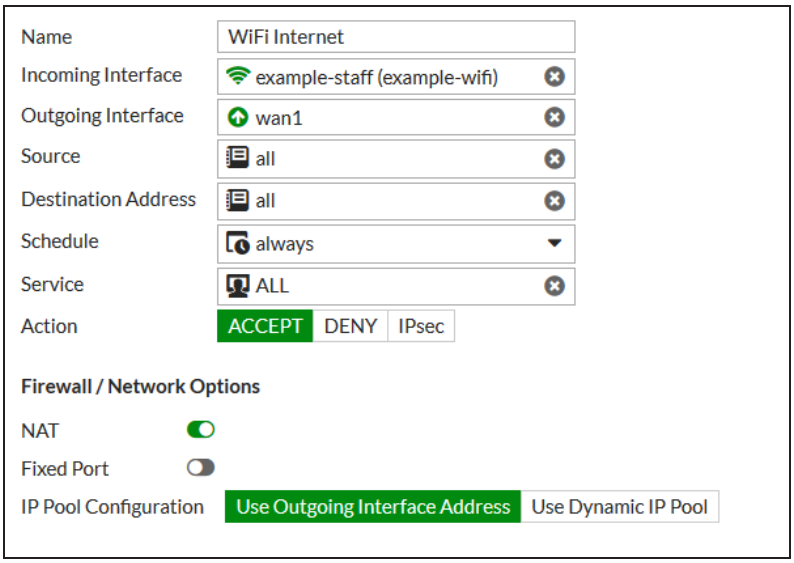
Configure Radio 1 for the client channel on the 2.4GHz 802.11n/g Band.

Configure Radio 2 for the backhaul channel on the 5GHz 802.11ac/n Band.



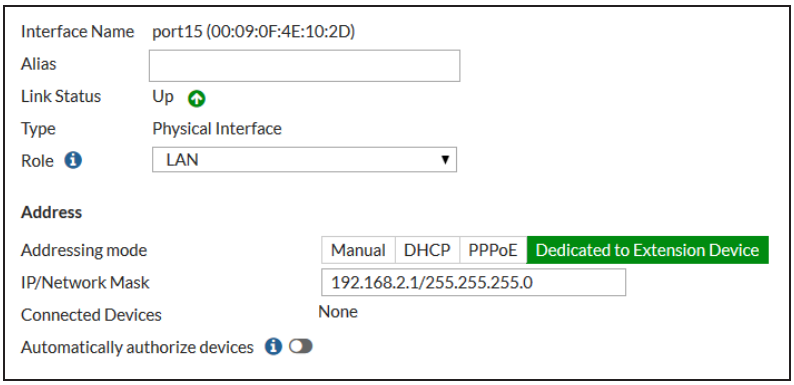
4. Configuring the security policy

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



5. Configuring an interface dedicated to FortiAP

Go to **Network > Interfaces** and edit an available interface (in this example, port 15). Set **Addressing mode** to **Dedicate to Extension Device**.

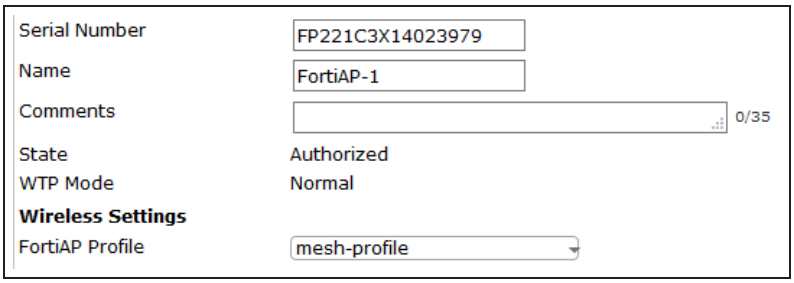


6. Preauthorizing FortiAP-1

Go to **WiFi Controller > Managed FortiAPs** and create a new entry.

Enter the serial number of the FortiAP unit and give it a name. Select the FortiAP profile that you created earlier.

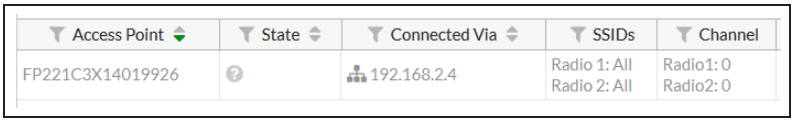
Doing this will allow FortiAP-1 to go online as soon as it is connected to the FortiGate. Optionally, you could connect the FortiAP to the FortiGate and then manually authorize it at that point, as will be done with FortiAP-2.



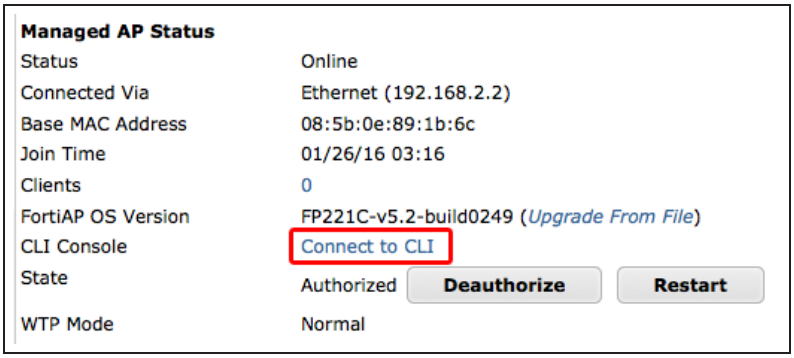
7. Configuring FortiAP-2 for mesh operation

Connect FortiAP-2's Ethernet port to the FortiGate network interface that you configured for FortiAPs.

Go to **WiFi Controller > Managed FortiAPs**. Click Refresh every 15 seconds until FortiAP-2 is listed. Select the AP, then select **Authorize**.



Edit FortiAP-2. Under **Managed AP Status**, select **Connect to CLI**.



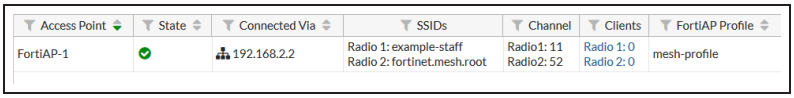
Log in with the username `admin`, then enter the following CLI commands, substituting your SSID and password where necessary:

```
cfg -a MESH_AP_TYPE=1
cfg -a MESH_AP_SSID=fortinet.mesh.root
cfg -a MESH_AP_PASSWD=hardtoguess
cfg -c
exit
```

Disconnect FortiAP-2 from the FortiGate.

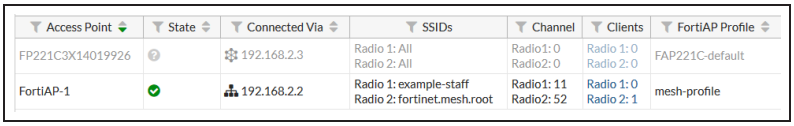
8. Connecting and authorizing the FortiAPs

Connect FortiAP-1. Go to **WiFi Controller > Managed FortiAPs**. Click Refresh every 15 seconds until FortiAP-1 is listed.



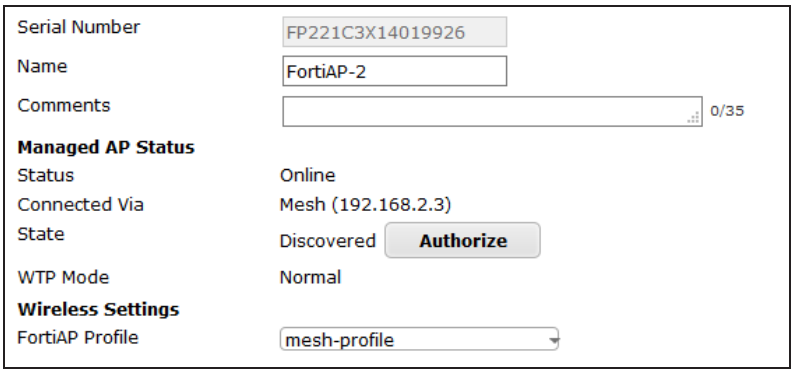
Access Point	State	Connected Via	SSIDs	Channel	Clients	FortiAP Profile
FortiAP-1	✔	192.168.2.2	Radio 1: example-staff Radio 2: fortinet.mesh.root	Radio1: 11 Radio2: 52	Radio 1: 0 Radio 2: 0	mesh-profile

Power up FortiAP-2. Periodically click Refresh. With a minute or two, Radio 2 of FortiAP-1 will indicate 1 client and FortiAP-2 will be listed as mesh-connected.

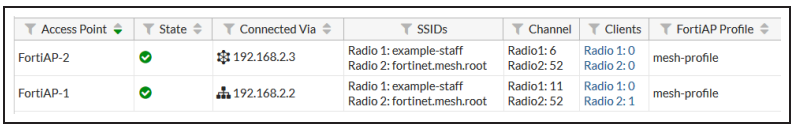


Access Point	State	Connected Via	SSIDs	Channel	Clients	FortiAP Profile
FP221C3X14019926	?	192.168.2.3	Radio 1: All Radio 2: All	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0	FAP221C-default
FortiAP-1	✔	192.168.2.2	Radio 1: example-staff Radio 2: fortinet.mesh.root	Radio1: 11 Radio2: 52	Radio 1: 0 Radio 2: 1	mesh-profile

Go to **WiFi Controller > Managed FortiAPs**. Edit FortiAP-2. Enter the **Name** and select the **FortiAP Profile** that you created earlier.



Click Refresh to update the display as needed. Within a minute or two, FortiAP-2 will be listed as Online.



Access Point	State	Connected Via	SSIDs	Channel	Clients	FortiAP Profile
FortiAP-2	✔	192.168.2.3	Radio 1: example-staff Radio 2: fortinet.mesh.root	Radio1: 6 Radio2: 52	Radio 1: 0 Radio 2: 0	mesh-profile
FortiAP-1	✔	192.168.2.2	Radio 1: example-staff Radio 2: fortinet.mesh.root	Radio1: 11 Radio2: 52	Radio 1: 0 Radio 2: 1	mesh-profile

9. Results

Go to **Monitor > WiFi Client Monitor**. Both backhaul and client SSIDs are shown. Click **Refresh** as needed to see updated information.

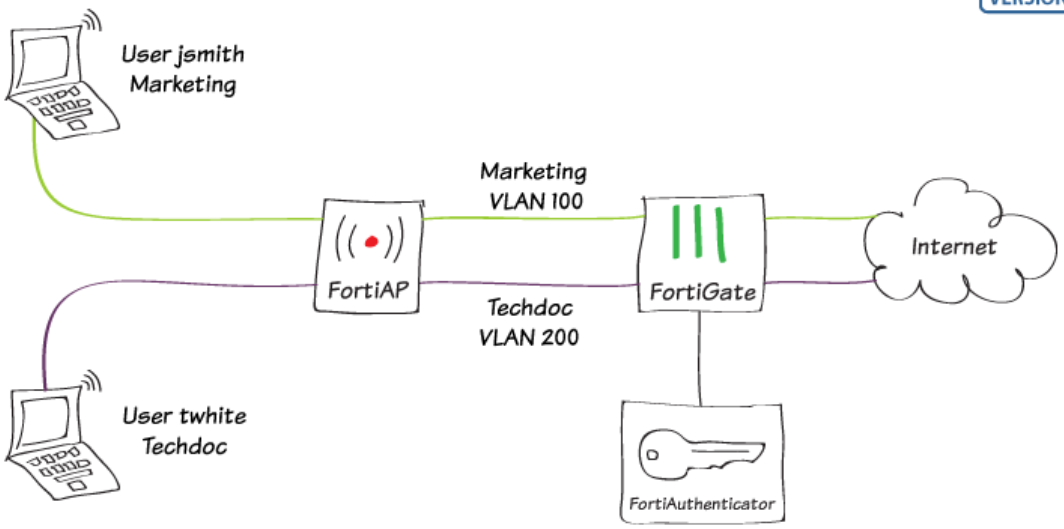
Connect to the network near FortiAP-2. The FortiAP column shows the client is associated with the mesh-connected FortiAP-2.

SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx	Signal
fortinet.mesh.root	FortiAP-1 (2)		192.168.2.3	7a:5b:0e:7f:52:fb	52	0 bps	20 dB
example-staff	FortiAP-2 (1)	rgreen	10.10.12.2	08:fd:0e:ff:0c:56	6	80 kbps	54 dB

Connect to the network near FortiAP-1. The FortiAP column shows the client is associated with FortiAP-1.

SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx	Signal
fortinet.mesh.root	FortiAP-1 (2)		192.168.2.3	7a:5b:0e:7f:52:fb	52	0 bps	23 dB
example-staff	FortiAP-1 (1)	rgreen	10.10.12.2	08:fd:0e:ff:0c:56	1	13 kbps	18 dB

Assigning WiFi users to VLANs dynamically

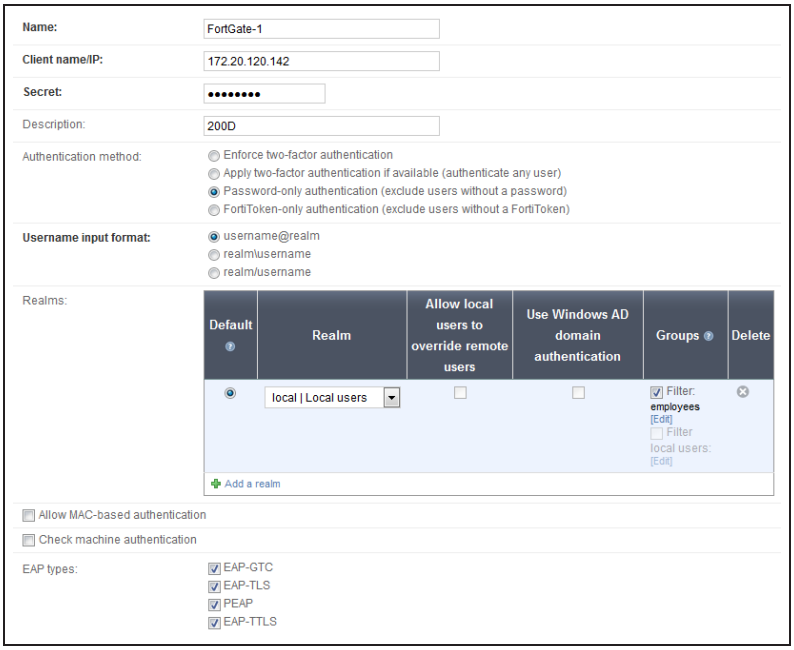


Virtual LANs (VLANs) are used to assign wireless users to different networks without requiring the use of multiple SSIDs. Each user's VLAN assignment is stored in the user database of the RADIUS server that authenticates the users.

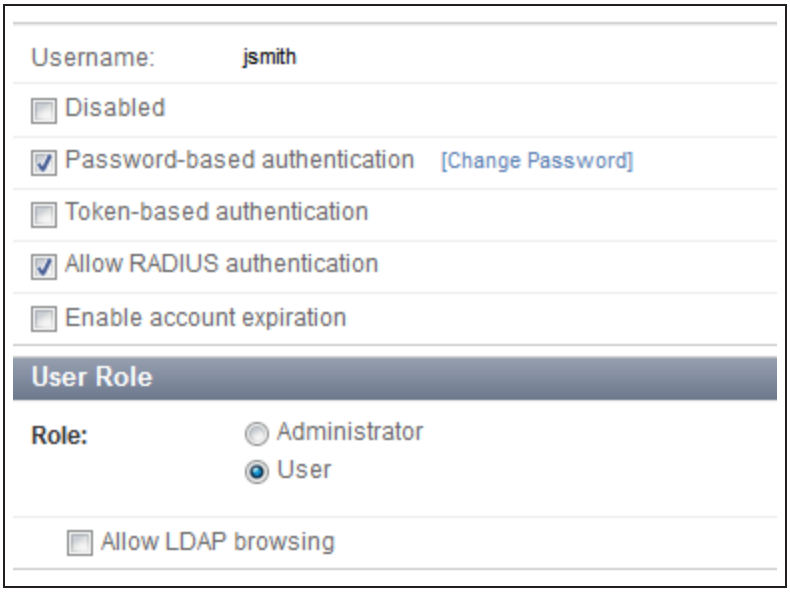
This example creates dynamic VLANs for the Techdoc and Marketing departments. The RADIUS server is a FortiAuthenticator.

1. Configure the FortiAuthenticator

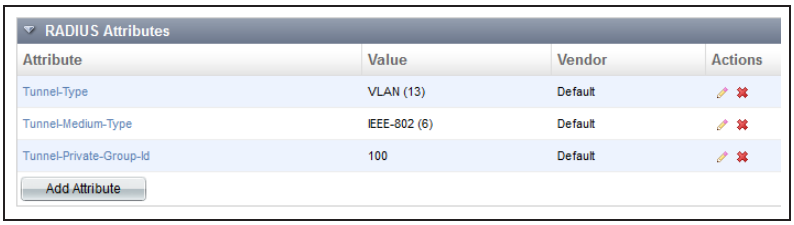
Go to **Authentication > RADIUS Service > Clients** to register the FortiGate as a client.
Enter a Secret (a password) and remember it. It will also be used in the FortiGate configuration.



Go to **Authentication > User Management > Local Users** and create local user accounts as needed.



For each user, add these RADIUS attributes which specify the VLAN information to be sent to the FortiGate. Tunnel-Private-Group-Id specifies the VLAN ID.

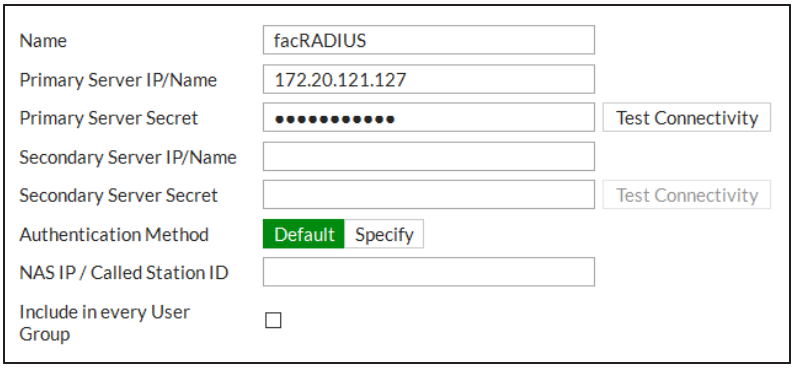


In this example, jsmith is assigned VLAN 100 and twhite is assigned VLAN 200.

2. Add the RADIUS server to the FortiGate configuration

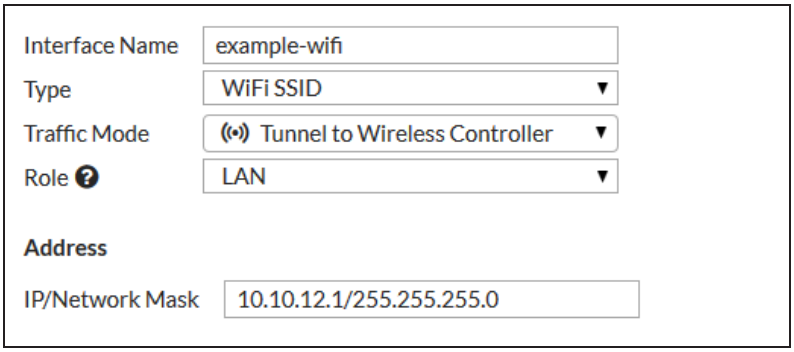
Go to **User & Device > RADIUS Servers**. Select Create New.

Enter the FortiAuthenticator IP address and the server secret that you entered on the FortiAuthenticator. Optionally, you can click Test Connectivity. Enter a RADIUS user's ID and password. The result should be "Successful".

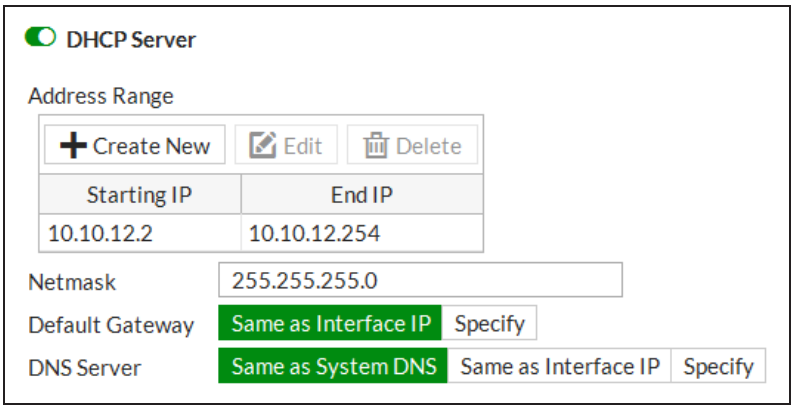


3. Create an SSID with dynamic VLAN assignment

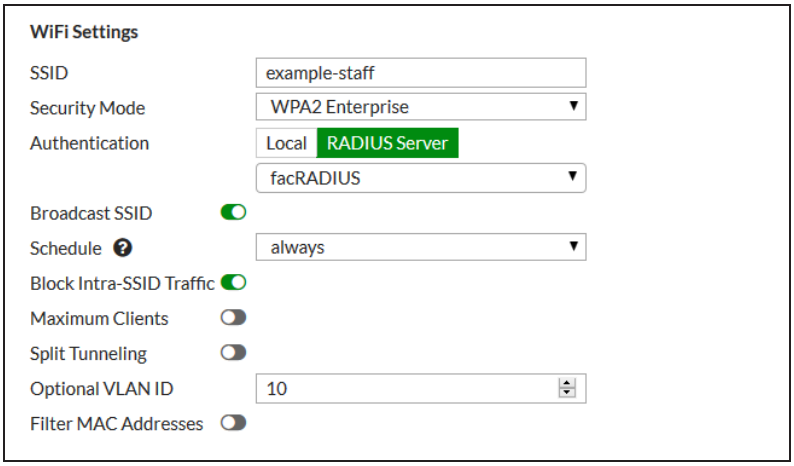
Go to **WiFi Controller > SSID**. Create a new SSID.



Set up DHCP service.



Select **WPA2 Enterprise** security and select your RADIUS server for authentication.
Set the default VLAN ID to 10. This VLAN is used when RADIUS doesn't assign a VLAN.



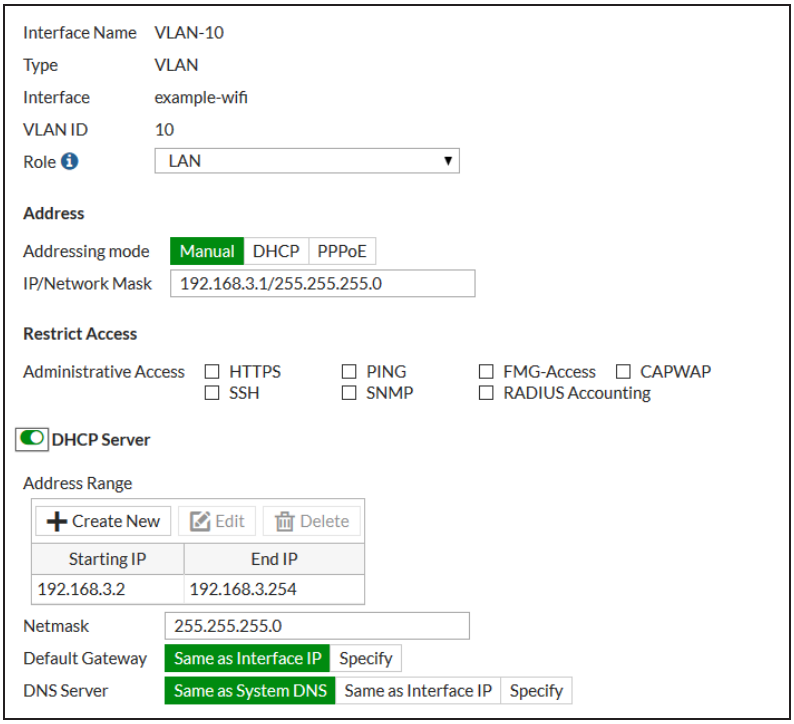
Go to the Dashboard and use the CLI Console to enable dynamic VLANs on the SSID.

```
config wireless-controller vap
 edit example-wifi
 set dynamic-vlan enable
 end
```

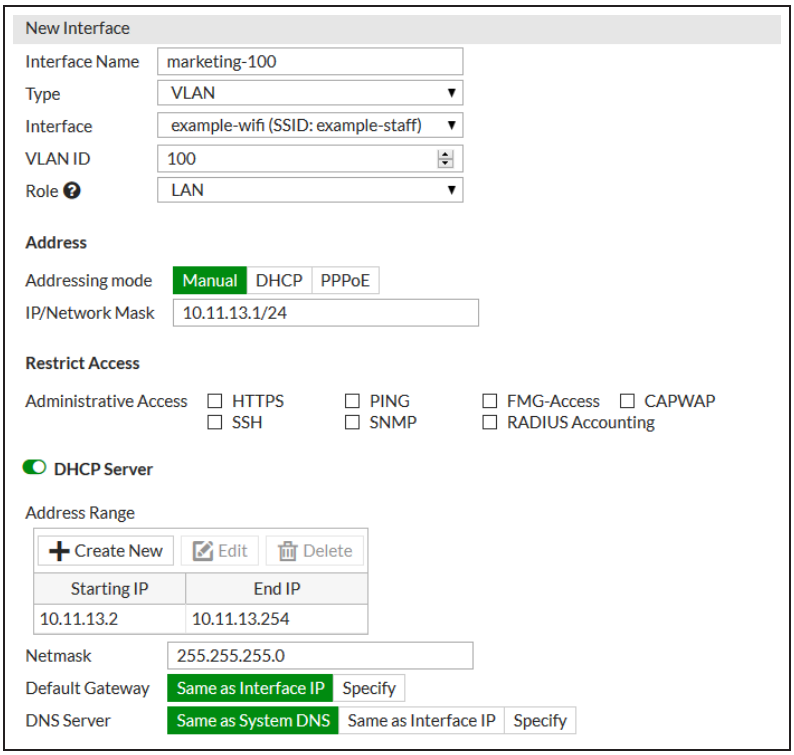
4. Create the VLAN interfaces

Go to **Network > Interfaces**.

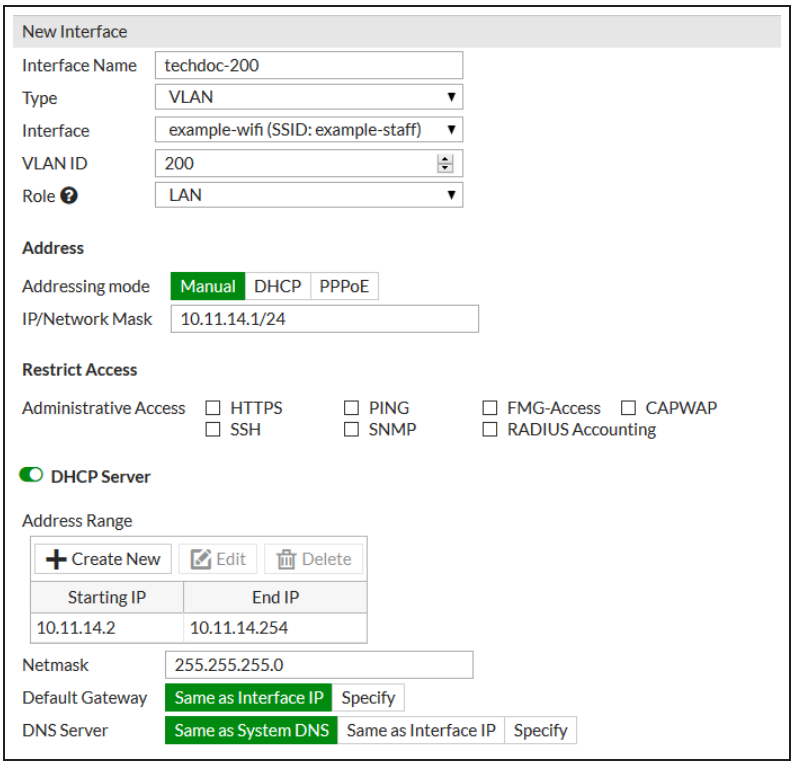
Create the VLAN interface for default VLAN-10 and set up DHCP service.



Create the VLAN interface for marketing-100 and set up DHCP service.



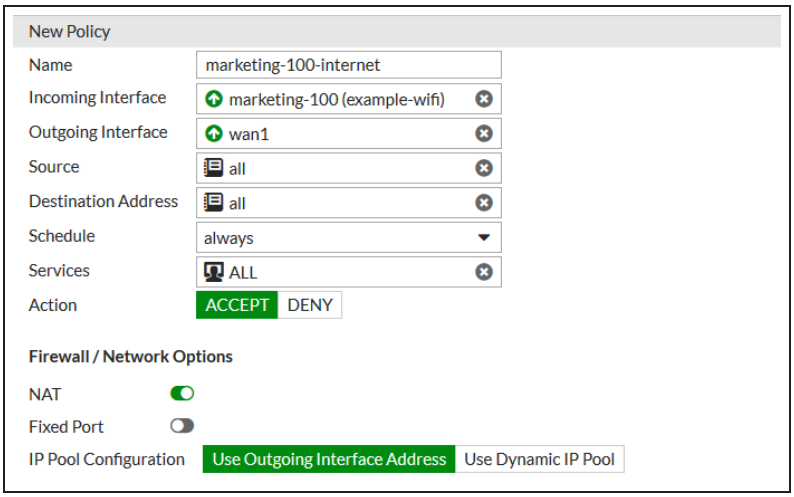
Create the VLAN interface for techdoc-200 and set up DHCP service.



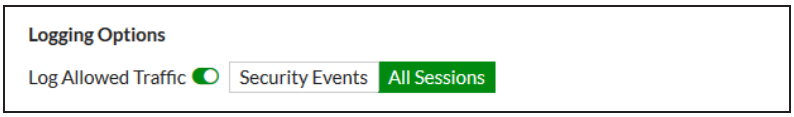
5. Create security policies

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

Create a policy that allows outbound traffic from marketing-100 to the Internet.

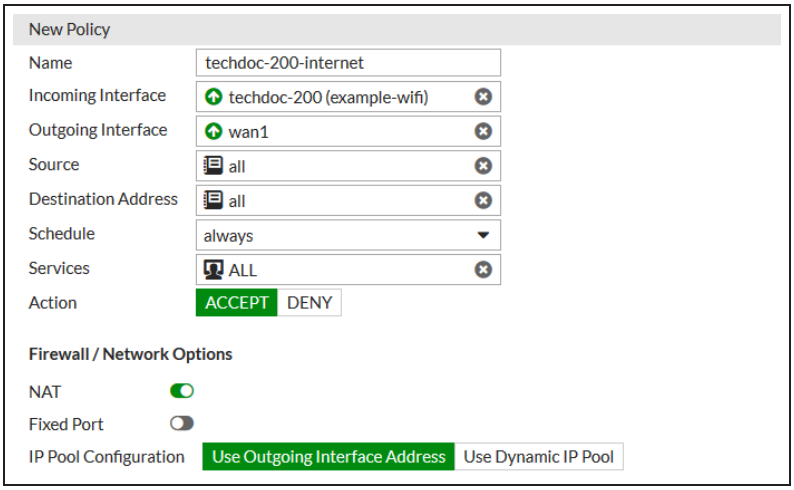


In **Logging Options**, enable logging for all sessions.



Create a policy that allows outbound traffic from techdoc-200 to the Internet.

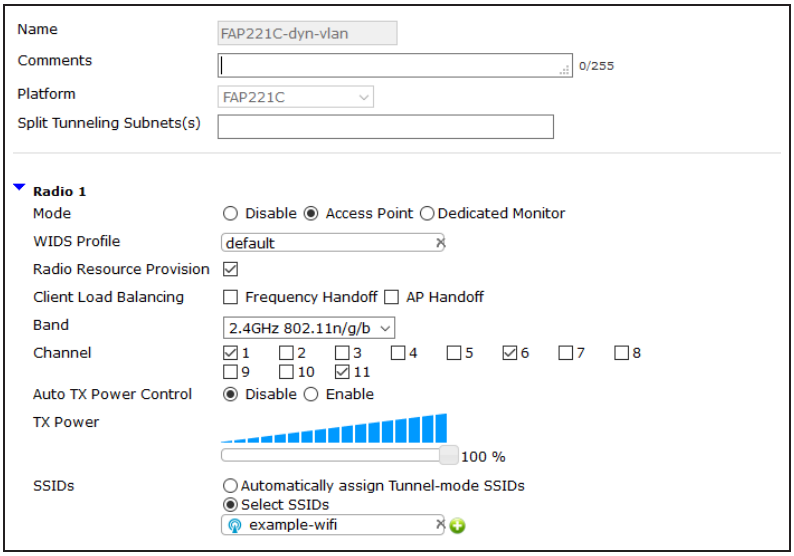
For this policy too, in Logging Options enable logging for all sessions.



6. Create the FortiAP Profile

Go to **WiFi Controller > FortiAP Profiles**.

Create a new profile for your FortiAP model and select the new SSID for both Radio 1 and Radio 2.



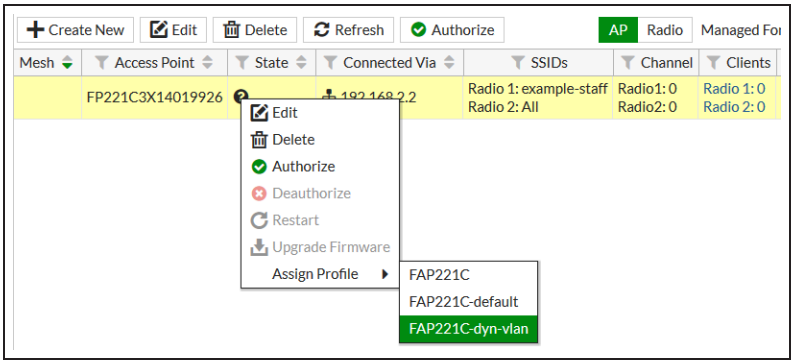
7. Connect and authorize the FortiAP

Go to **Network > Interfaces** and choose an unused interface. Set Addressing mode to *Dedicated to Extension Device*. Connect the FortiAP unit to the this interface and apply power.

Go to **WiFi Controller > Managed FortiAPs**.

Right-click on the FortiAP unit. Select **Authorize**.

Right-click on the FortiAP unit again. Select **Assign Profile** and select the FortiAP profile that you created.



Results

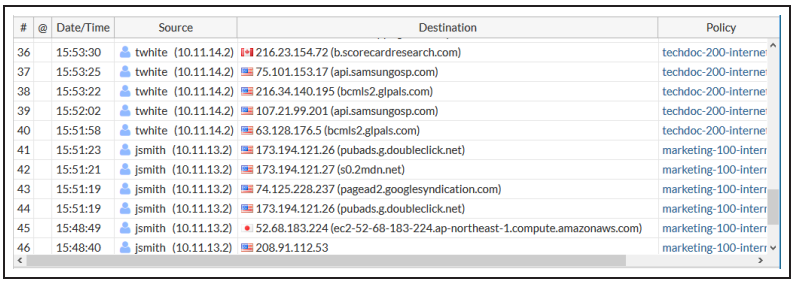
The SSID will appear in the list of available wireless networks on the users' devices. Both twhite and jsmith can connect to the SSID with their credentials and access the Internet. (If a certificate warning message appears, accept the certificate.)

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

Note that traffic for jsmith and twhite pass through
different policies.

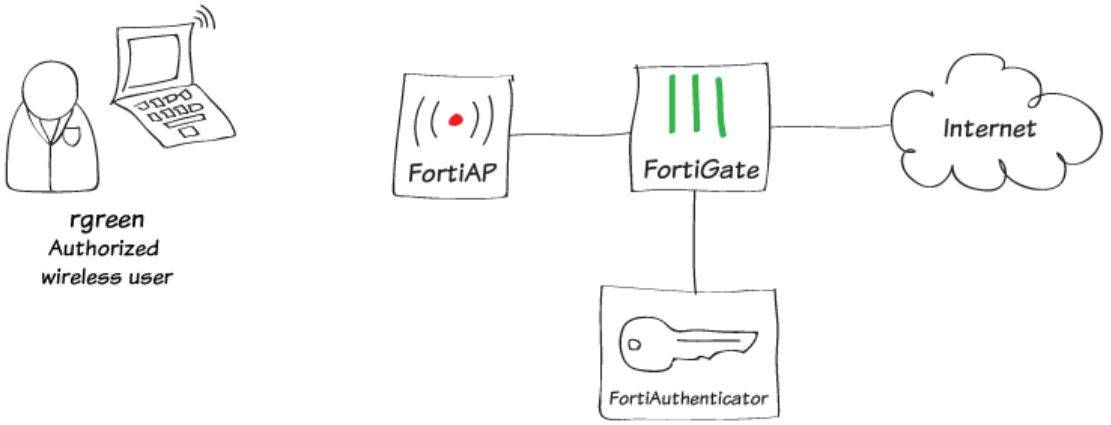
(The column selections were customized for clarity.)

The security policies could be made different so that Marketing and Techdoc departments were allowed different access, but didn't think that was fair.



#	@	Date/Time	Source	Destination	Policy
36		15:53:30	twhite (10.11.14.2)	216.23.154.72 (b.scorecardresearch.com)	techdoc-200-interne
37		15:53:25	twhite (10.11.14.2)	75.101.153.17 (api.samsungosp.com)	techdoc-200-interne
38		15:53:22	twhite (10.11.14.2)	216.34.140.195 (bcmls2.glpals.com)	techdoc-200-interne
39		15:52:02	twhite (10.11.14.2)	107.21.99.201 (api.samsungosp.com)	techdoc-200-interne
40		15:51:58	twhite (10.11.14.2)	63.128.176.5 (bcmls2.glpals.com)	techdoc-200-interne
41		15:51:23	jsmith (10.11.13.2)	173.194.121.26 (pubads.g.doubleclick.net)	marketing-100-intern
42		15:51:21	jsmith (10.11.13.2)	173.194.121.27 (s0.2mdn.net)	marketing-100-intern
43		15:51:19	jsmith (10.11.13.2)	74.125.228.237 (pagead2.googlesyndication.com)	marketing-100-intern
44		15:51:19	jsmith (10.11.13.2)	173.194.121.26 (pubads.g.doubleclick.net)	marketing-100-intern
45		15:48:49	jsmith (10.11.13.2)	52.68.183.224 (ec2-52-68-183-224.ap-northeast-1.compute.amazonaws.com)	marketing-100-intern
46		15:48:40	jsmith (10.11.13.2)	208.91.112.53	marketing-100-intern

WiFi RADIUS authentication with FortiAuthenticator



In this example, you use a RADIUS server to authenticate your WiFi clients.

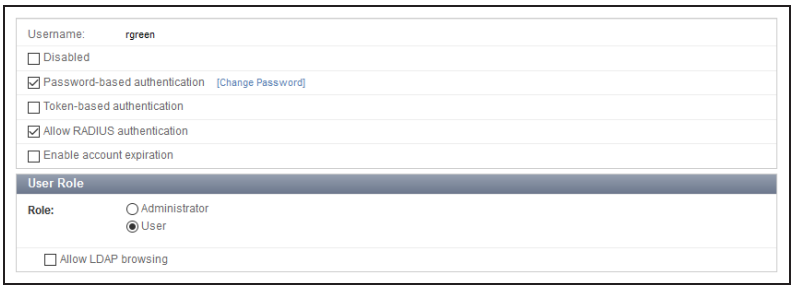
The RADIUS server is a FortiAuthenticator (v4.00-build0008) that is used authenticate users who belong to the employees user group.

1. Create the user accounts and user group on the FortiAuthenticator

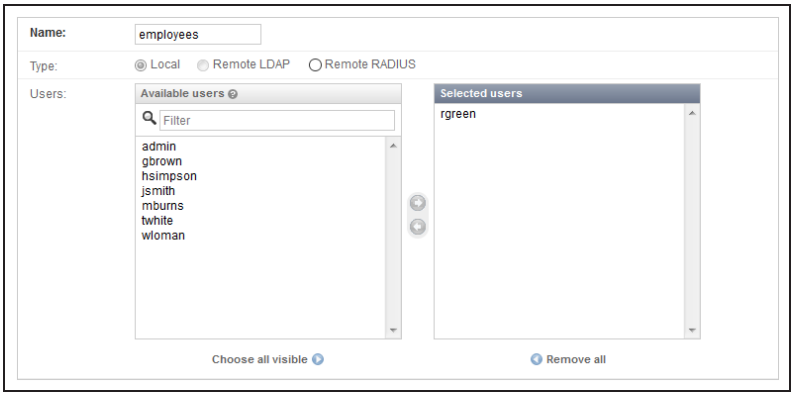
Go to **Authentication > User Management > Local Users** and create a user account.

User Role settings are available after you click OK.

Create additional user accounts as needed, one for each employee.



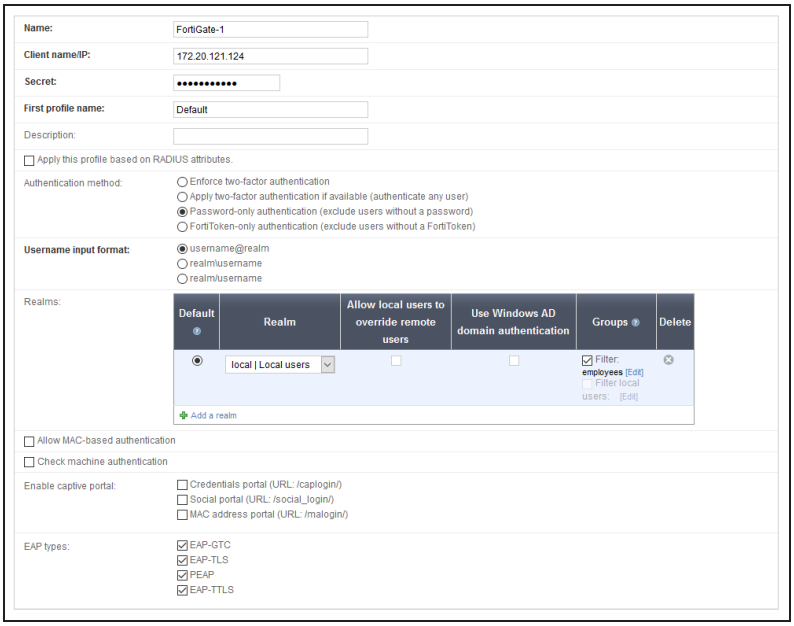
Go to **Authentication > User Management > User Groups** and create the local user group “employees” on the FortiAuthenticator.



2. Register the FortiGate as a RADIUS client on the FortiAuthenticator

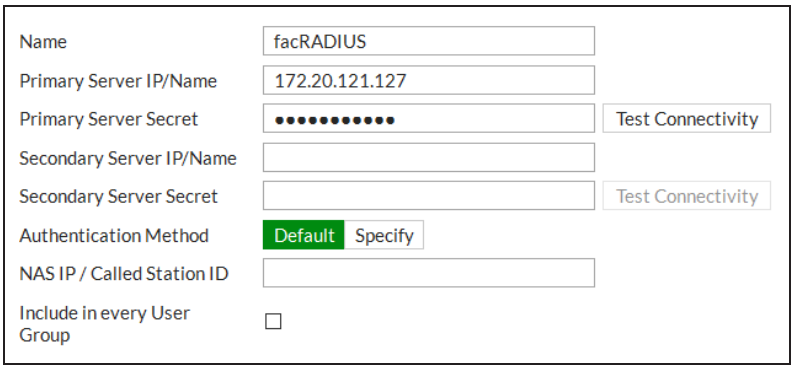
Go to **Authentication > RADIUS Service > Clients** and create a client account.

Enable all of the EAP types.



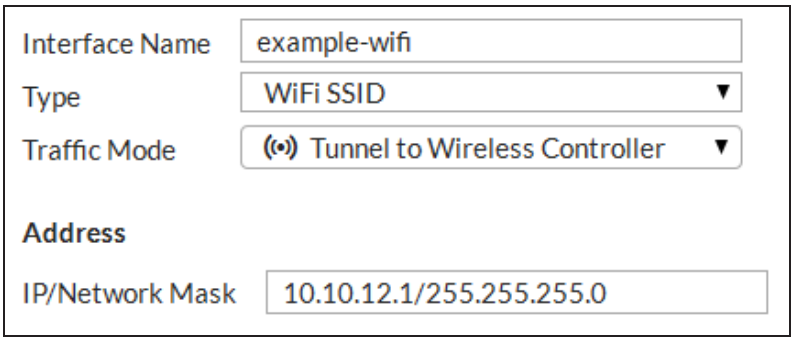
3. Configure FortiGate to use the RADIUS server

Go to **User & Device > RADIUS Servers** and add the FortiAuthenticator as a RADIUS server.

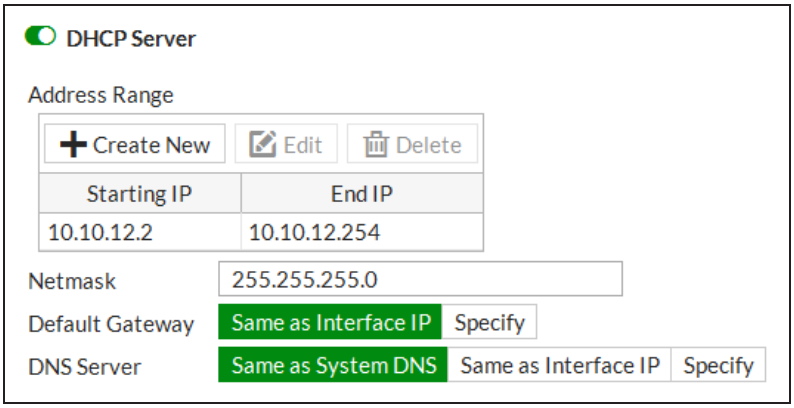


4. Create the SSID and set up authentication

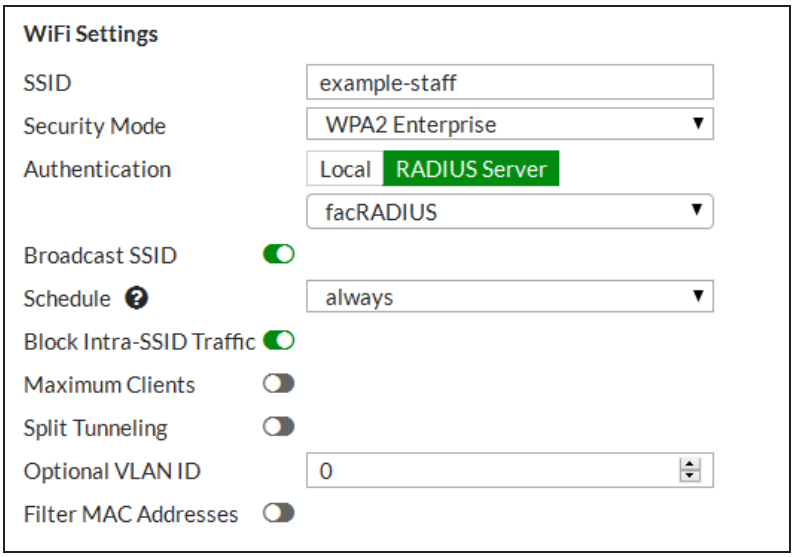
Go to **WiFi Controller > SSID** and define your wireless network.



Set up DHCP for your clients.

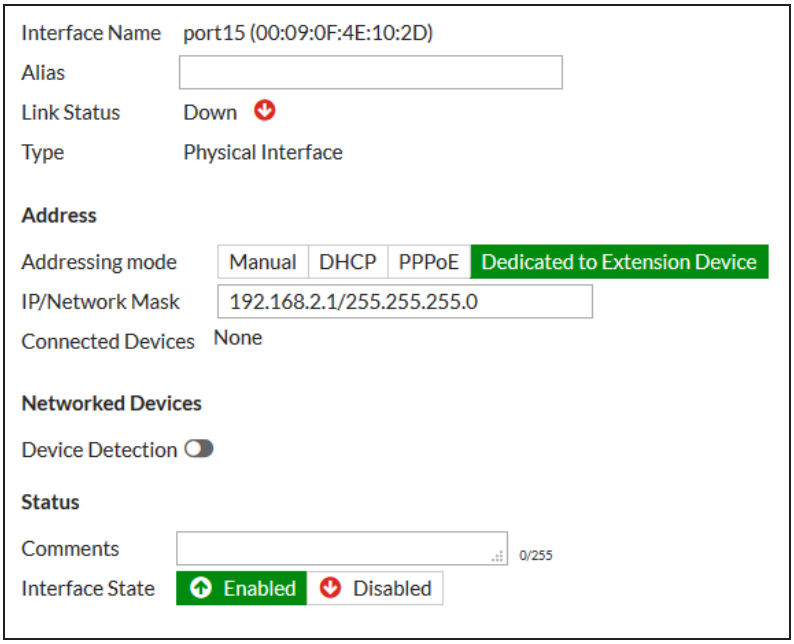


Configure WPA2 Enterprise security that uses the RADIUS server.

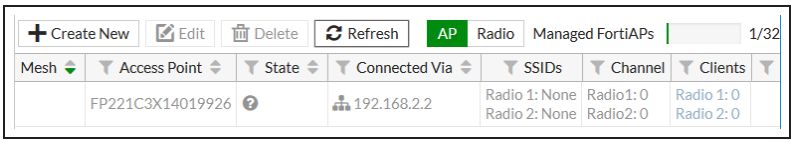


5. Connect and authorize the FortiAP

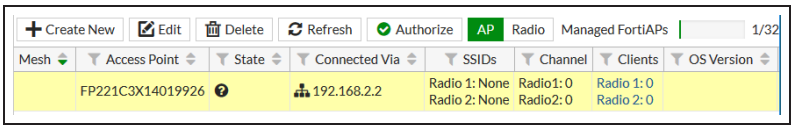
Go to **Network > Interfaces** and configure a dedicated interface for the FortiAP.



Connect the FortiAP unit. Go to **WiFi Controller > Managed FortiAPs**.



When the FortiAP is listed, select and authorize it.

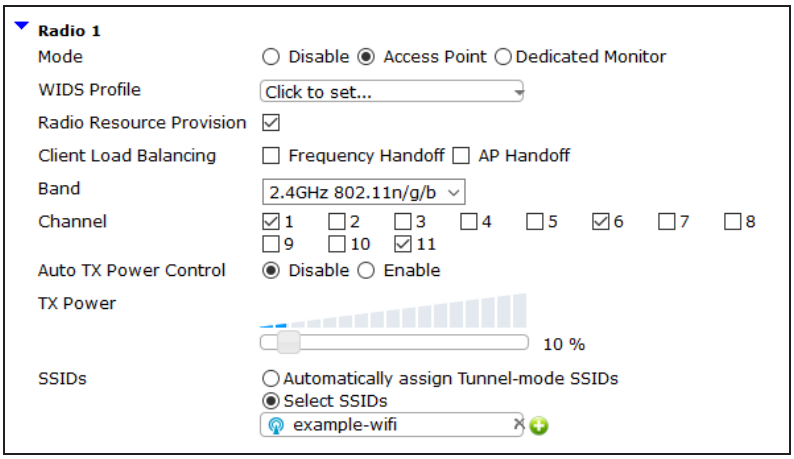


Go to **WiFi Controller > FortiAP Profiles** and edit the profile.

This example used a FortiAP-221C, so the FAP221C-default profile applies.

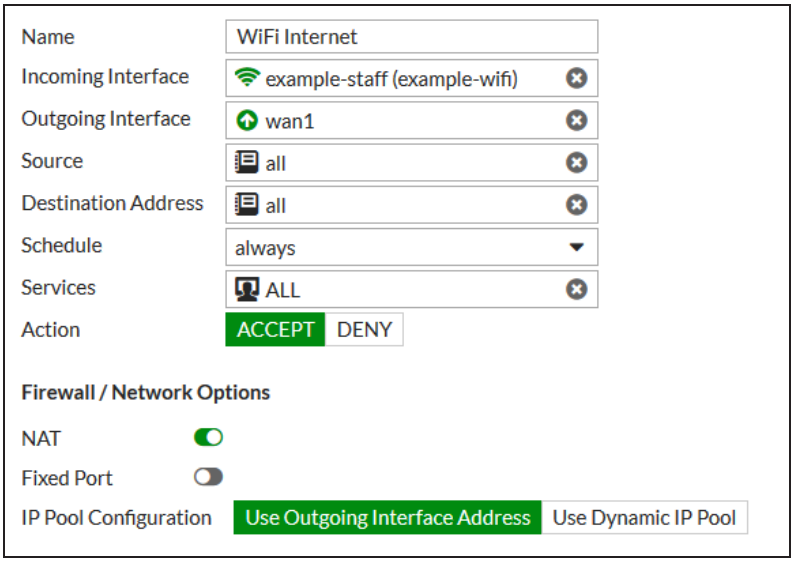
For each radio:

- Enable Radio Resource Provision.
- Select your SSID.



6. Create the security policy

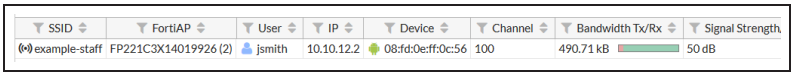
Go to **Policy & Objects > IPv4 Policy** and add a policy that allows WiFi users to access the Internet.



Results

Connect to the example-staff network and browse Internet sites.

Go to **Monitor > Client Monitor** to see that clients connect and authenticate.



SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength
example-staff	FP221C3X14019926 (2)	jsmith	10.10.12.2	08:fd:0e:ff:0c:56	100	490.71 kB	50 dB

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.

External authentication

- 802.1X with VLAN Switch interfaces on a FortiGate

WiFi authentication

- Assigning WiFi users to VLANs dynamically
- WiFi RADIUS authentication with FortiAuthenticator

802.1X with VLAN Switch interfaces on a FortiGate

This recipe follows on from the general introductory video, Managing FortiSwitch from FortiGate, which uses the FortiLink protocol.

Using 802.1X with VLAN Switch interfaces on the FortiGate secures the network at the switch port by requesting a connecting user to authenticate. In most deployments the user database will be external to the FortiGate.

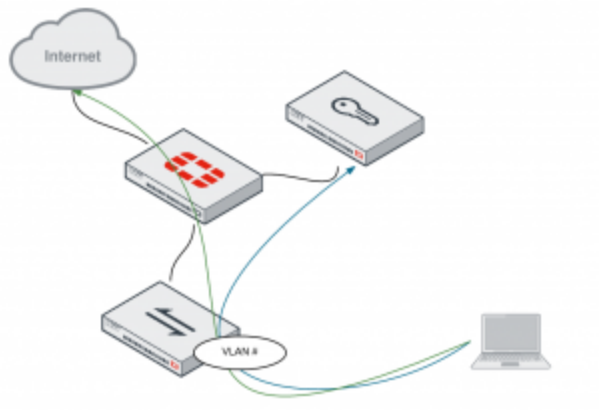
This example uses FortiAuthenticator for the RADIUS authentication server, however the example is generic enough to be adapted to any authentication server supported by the FortiGate and the EAP protocol. Also this example can be adapted for other products which make use of 802.1X, such as wireless access points.

In this example we will configure EAP-TTLS.

There are three elements to be configured:

- The supplicant, which identifies the client, in this case a Ubuntu host.
- The authenticator, which translates EAP to RADIUS messages, and vice-versa. This is the FortiGate switch controller.
- The authentication server, which processes the RADIUS messages. This is the FortiAuthenticator.

The topology is as shown:

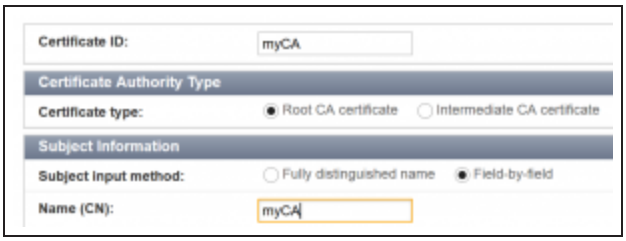


1. Configuring a CA

In this example we configure EAP-TTLS which requires, as a minimum, server certificate validation. To do this we use FortiAuthenticator, we create a CA root, self signed, and a service certificate for the authentication server. The supplicant requires access to the CA certificate in order to validate the server authentication.

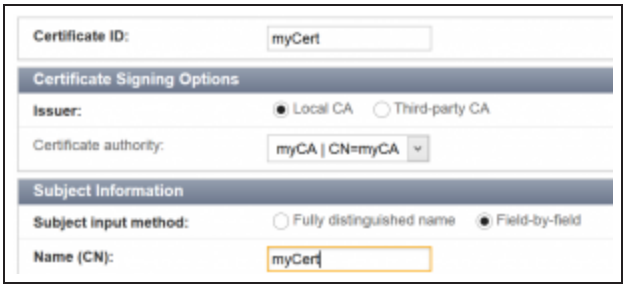
On FortiAuthenticator, go to **Certificate Management > Certificate Authorities > Local CAs** and create a new Local CA. Enter a **Certificate ID** and **Name (CN)**. Leave all other settings default.

This creates a root CA certificate that is self signed. This certificate must be copied to the supplicant.



Go to **Certificate Management > End Entities > Local Services** and create a new service. Enter a **Certificate ID**, **Issuer** (your local CA), and **Name (CN)**. Leave all other settings default.

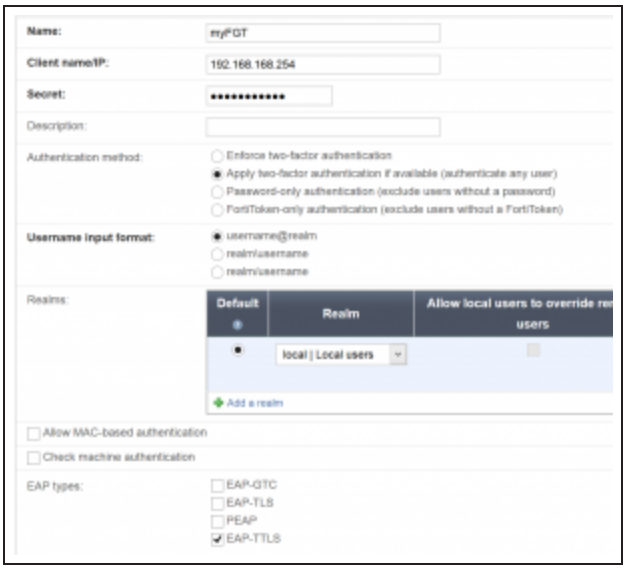
This creates a certificate for the authentication server.



2. Configuring RADIUS authentication

The FortiAuthenticator will be the RADIUS sever and the FortiGate the RADIUS client.

On the FortiAuthenticator, go to **Authentication > RADIUS Service > Clients** and create a new client. Enter the **Name**, **Client name/IP**, and shared **Secret**. For **Realms**, use the local user realm and set **EAP types** to use **EAP-TTLS**.

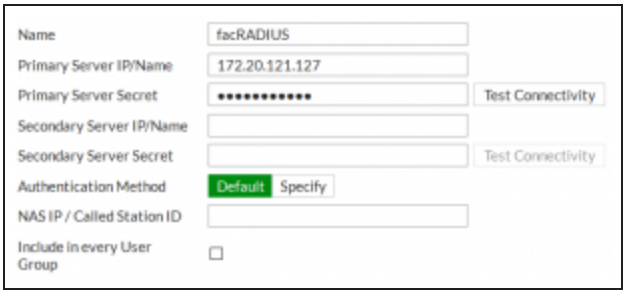


Go to **Authentication > User Management > Local Users** and create a local user and password.

This is your user account for 802.1X authentication.

Go to **Authentication > RADIUS Service > EAP** and select the local CA and local service certificates for the server's authentication.

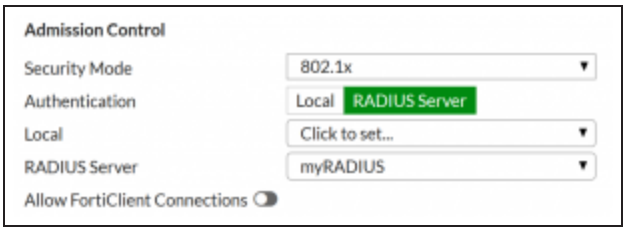
On the FortiGate, go to **User & Device > RADIUS Servers** and create a new server connection. Enter **Name**, **Primary Server IP/Name**, and **Primary Server Secret**.



Go to **WiFi & Switch Controller > VLANs**

Modify your VLAN and change the admission control authentication method to RADIUS, and select you RADIUS server.

(This example follows on from the local user configuration, given in the video.)



Test the RADIUS configuration from the the FortiGate CLI:

```
# diagnose test authserver radius myRADIUS mschap2 mike@local mypassword
authenticate 'mike@local' against 'mschap2' succeeded, server=primary assigned_
rad_session_id=790684157 session_timeout=0 secs idle_timeout=0 secs!
```

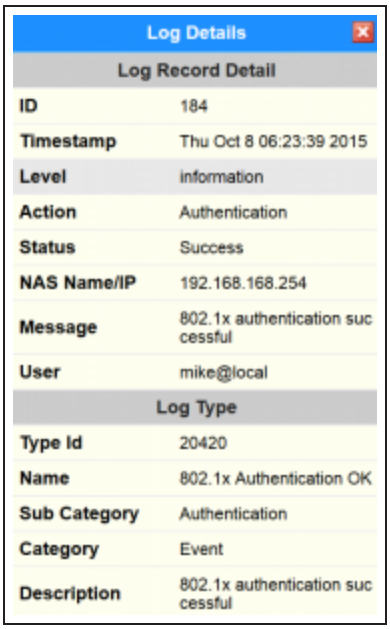
3. Configure the supplicant and test

We will configure the 802.1X supplicant settings on the wired interface of our Ubuntu host. Use the settings in the following screenshot to test your connection.

Edit your wired connection and select **802.1X security**. Chose **Tunneled TLS (TTLS)**, your **CA certificate**, **MSCAPv2** for **Inner authentication**, and the **Username.**

4. Results

Check FortiAuthenticator's log messages, look for *802.1x authentication successful*.



Log Details

Log Record Detail	
ID	184
Timestamp	Thu Oct 8 06:23:39 2015
Level	information
Action	Authentication
Status	Success
NAS Name/IP	192.168.168.254
Message	802.1x authentication successful
User	mike@local
Log Type	
Type Id	20420
Name	802.1x Authentication OK
Sub Category	Authentication
Category	Event
Description	802.1x authentication successful

Using *ifconfig,* you should see that you have been allocated an address from the DHCP server.

```
mike@ubuntu: ~
mike@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:92:23:01
          inet addr:10.10.10.2  Bcast:10.10.10.255  Mask:2
          inet6 addr: fe80::20c:29ff:fe92:2301/64 Scope:Li
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric
          RX packets:611 errors:0 dropped:23 overruns:0 fr
          TX packets:537 errors:0 dropped:0 overruns:0 car
          collisions:0 txqueuelen:1000
          RX bytes:518378 (518.3 KB)  TX bytes:69132 (69.1
```

If this does not work, check again the RADIUS client works using the *testauth* command. If that is ok, check your certificates, paying attention to the valid from date and time.

```
myFGT # diagnose test authserver radius myRADIUS mschap2 mike@local mypassword
authenticate 'mike@local' against 'mschap2' succeeded, server-primary assigned_rad
```

Certificate ID:	myCA [Edit]
Status:	Active
Version:	3
Serial number:	4D:36:80:C8:B5:1D:1D:3D
Issuer:	CN=myCA
Subject:	CN=myCA
Effective date:	Wed Oct 7 13:00:32 2015 GMT
Expiration date:	Sat Oct 4 13:00:32 2025 GMT

VPNs

This section contains information about configuring a variety of different Virtual Private Networks (VPNs), as well as different methods of authenticating VPN users. FortiGates support two types of VPNs: IPsec and SSL.

IPsec VPNs use Internet Protocol Security (IPsec) to create a VPN that extends a private network across a public network, typically the Internet. In order to connect to an IPsec VPN, users must install and configure an IPsec VPN client (such as FortiClient) on their PCs or mobile devices.

SSL VPNs use Secure Sockets Layer (SSL) to create a VPN that extends a private network across a public network, typically the Internet. Connections to an SSL VPN are done through a web browser and do not require any additional applications.

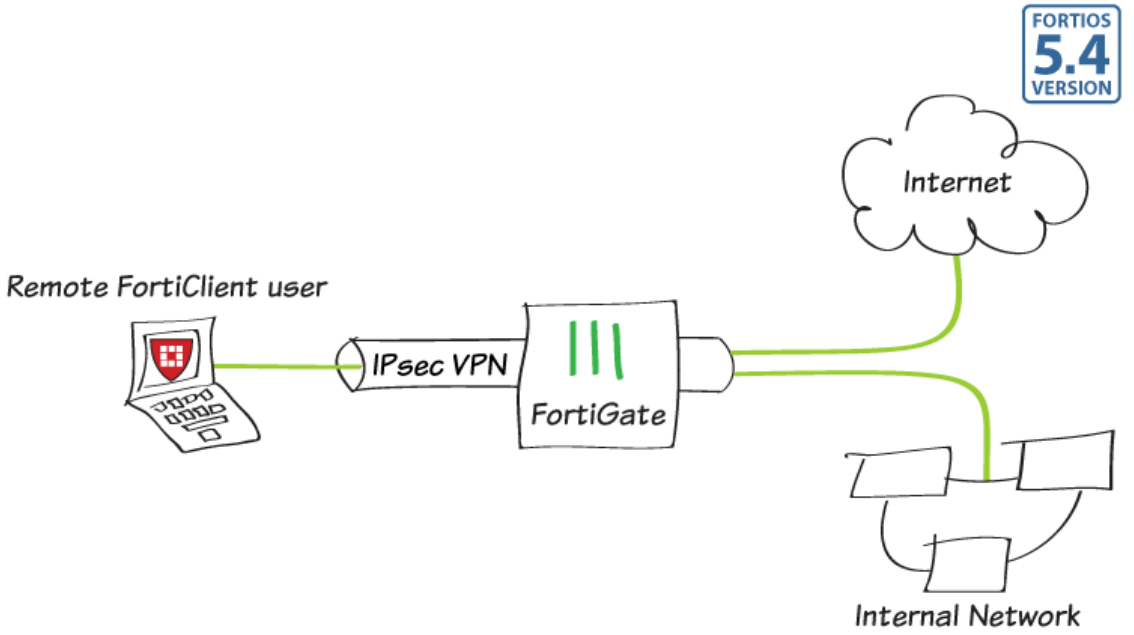
IPsec

- IPsec VPN with FortiClient
- Site-to-site IPsec VPN with two FortiGates
- IPsec troubleshooting

SSL

- SSL VPN using web and tunnel mode
- SSL VPN troubleshooting

IPsec VPN with FortiClient

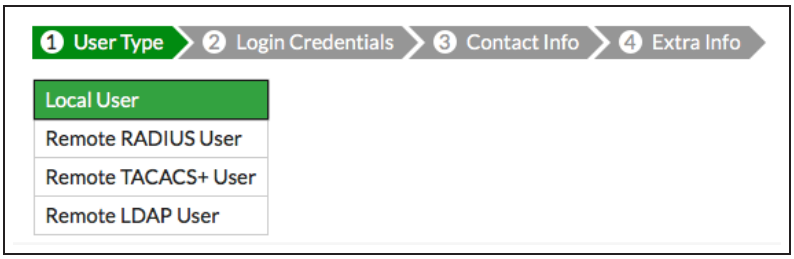


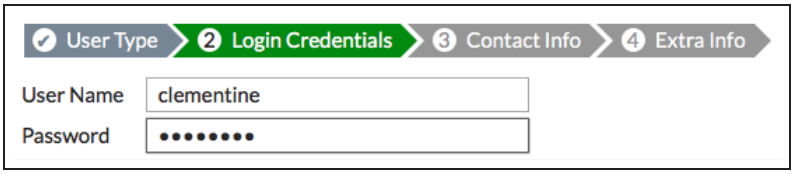
In this example, you will allow remote users to access the corporate network using an IPsec VPN that they connect to using FortiClient for Mac OS X, Windows, or Android. Traffic to the Internet will also flow through the FortiGate, to apply security scanning.

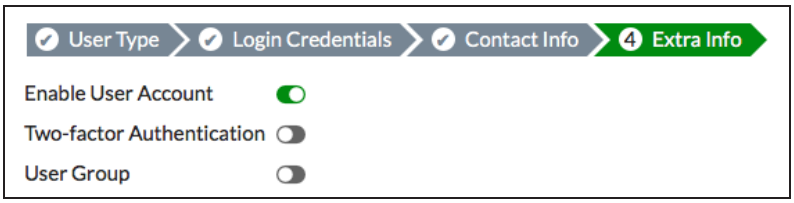
In this example, FortiClient 5.4.0.493 for Mac OS X is used.

1. Creating a user group for remote users

Go to **User & Device > User Definition**. Create a local user account for an IPsec VPN user.





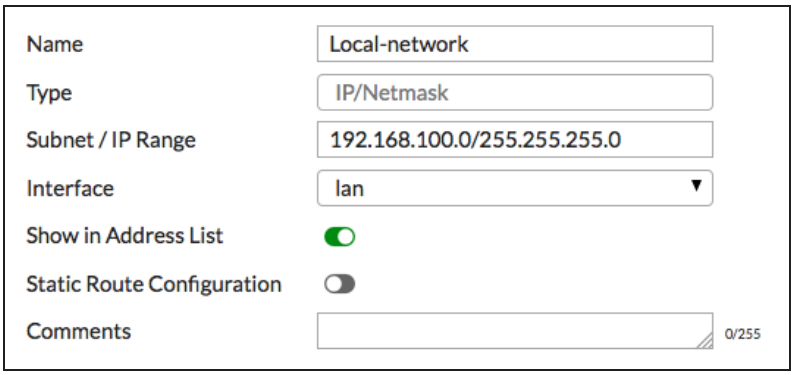


Go to **User & Device > User Groups**. Create a user group for IPsec VPN users and add the new user account.

2. Adding a firewall address for the local network

Go to **Policy & Objects > Addresses** and create an address for the local network.

Set **Type** to **IP/Netmark, Subnet/IP Range** to the local subnet, and **Interface** to an internal port.



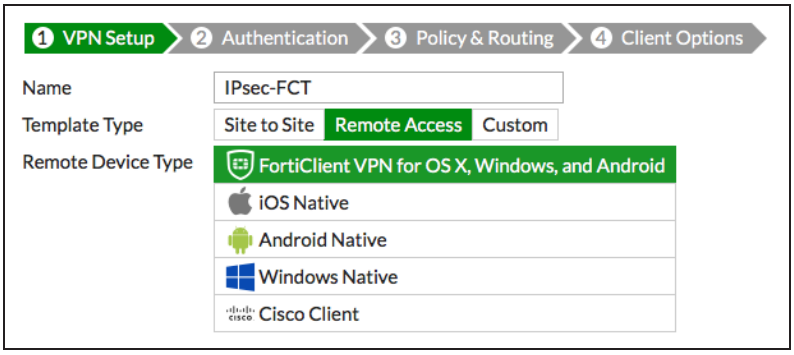
3. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to **VPN > IPsec Wizard** and create a new tunnel using a pre-existing template.

Name the VPN connection.

The tunnel name may not have any spaces in it and should not exceed 13 characters.

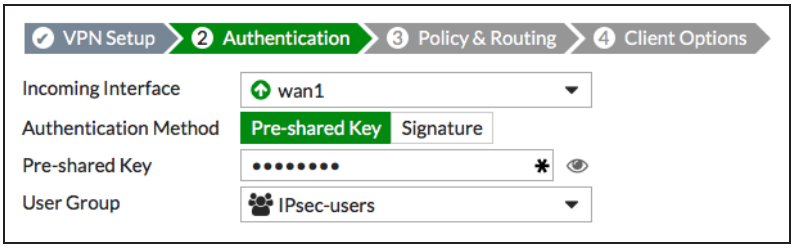
Set **Template** to **Remote Access**, and set **Remote Device Type** to **FortiClient VPN for OS X, Windows, and Android**.



Set the **Incoming Interface** to the internet-facing interface and **Authentication Method** to **Pre-shared Key**.

Enter a pre-shared key and select the new user group, then click **Next**.

The pre-shared key is a credential for the VPN and should differ from the user's password.



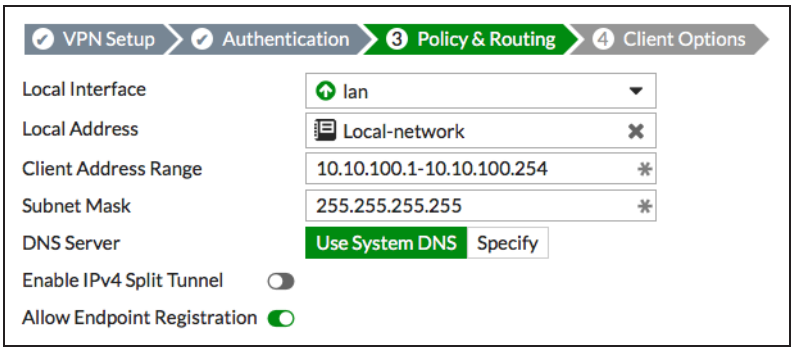
Set **Local Interface** to an internal interface (in the example, *lan*) and set **Local Address** to the local LAN address.

Enter an **Client Address Range** for VPN users.

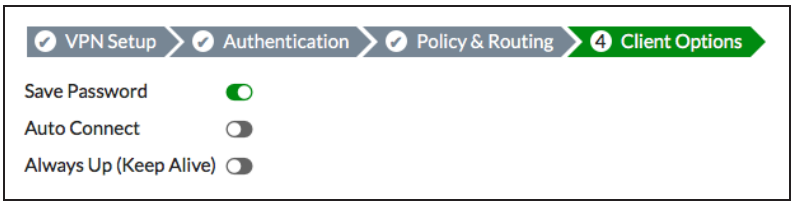
The *IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the _range suffix (in the example, IPsec-FCT_range).*

Make sure **Enable IPv4 Split Tunnel** is *not* selected, so that all Internet traffic will go through the FortiGate.

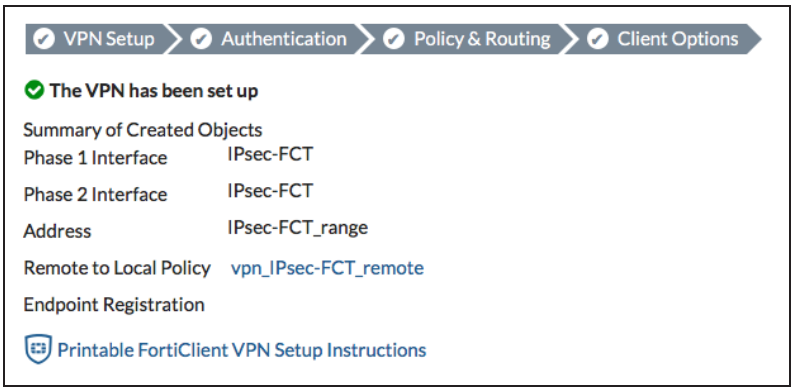
*If you do select **Enable Split Tunneling**, traffic not intended for the corporate network will not flow through the FortiGate or be subject to the corporate security profiles.*



Select **Client Options** as desired.



After you create the tunnel, a summary page appears listing the objects which have been added to the FortiGate's configuration by the wizard.



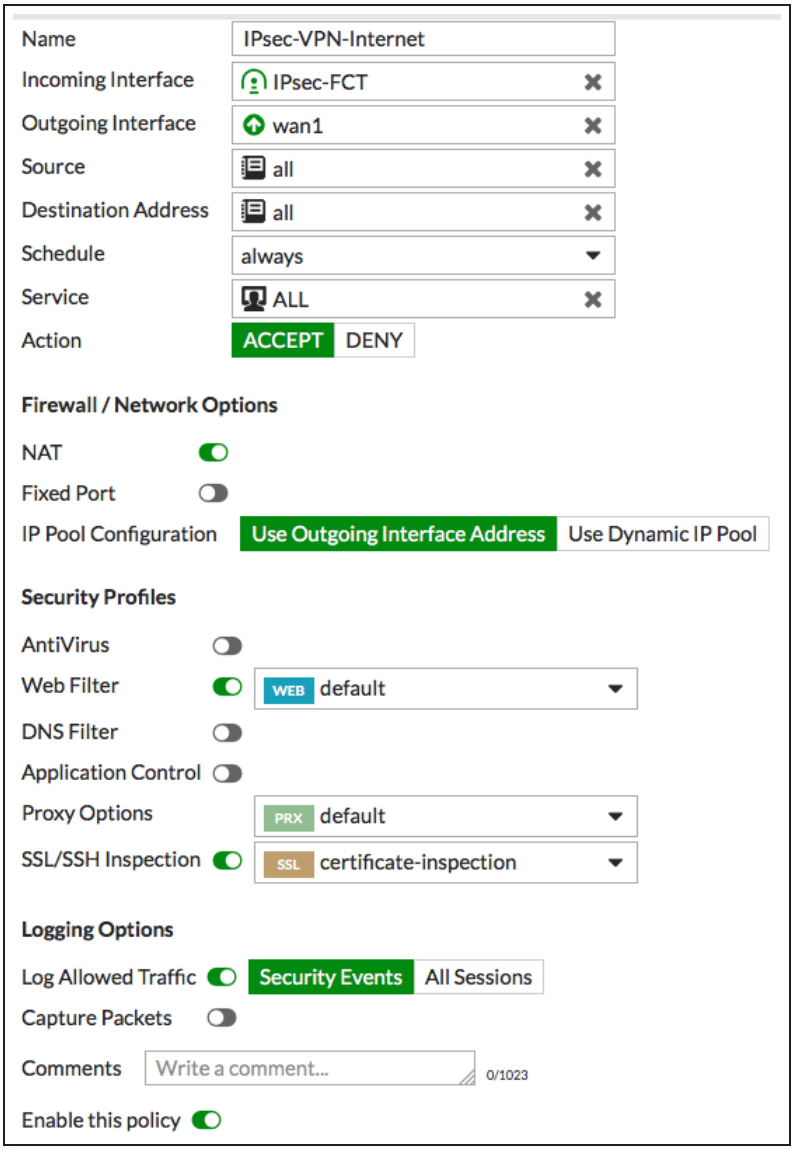
4. Creating a security policy for access to the Internet

The IPsec wizard automatically created a security policy allowing IPsec VPN users to access the internal network. However, since split tunneling is disabled, another policy must be created to allow users to access the Internet through the FortiGate.

Go to **Policy & Objects > IPv4 Policies** and create a new policy. Set a policy name that will identify what this policy is used for (in the example, *IPsec-VPN-Internet)*

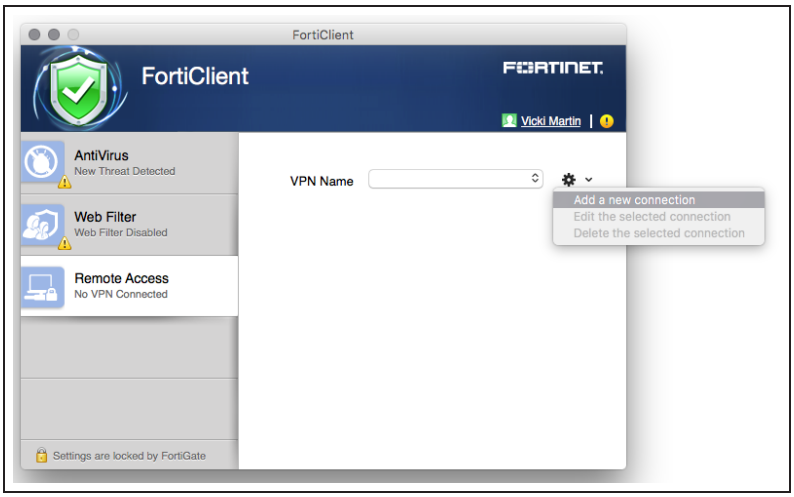
Set **Incoming Interface** to the tunnel interface and **Outgoing Interface** to **wan1**. Set **Source** to the IPsec client address range, **Destination Address** to **all**, **Service** to **ALL,** and enable **NAT**.

Configure any remaining firewall and security options as desired.



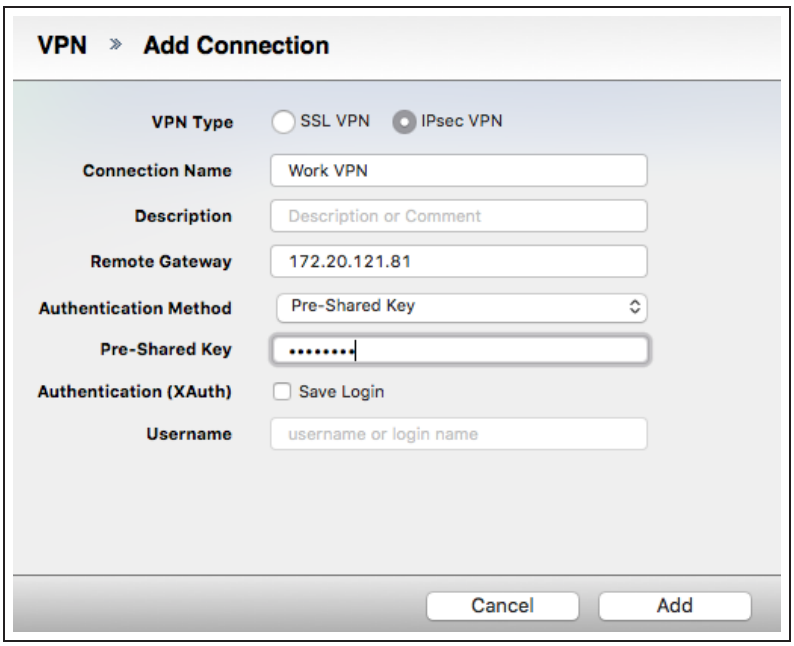
5. Configuring FortiClient

Open FortiClient, go to **Remote Access** and **Add a new connection**.



Set the **Type** to **IPsec VPN** and **Remote Gateway** to the FortiGate IP address.

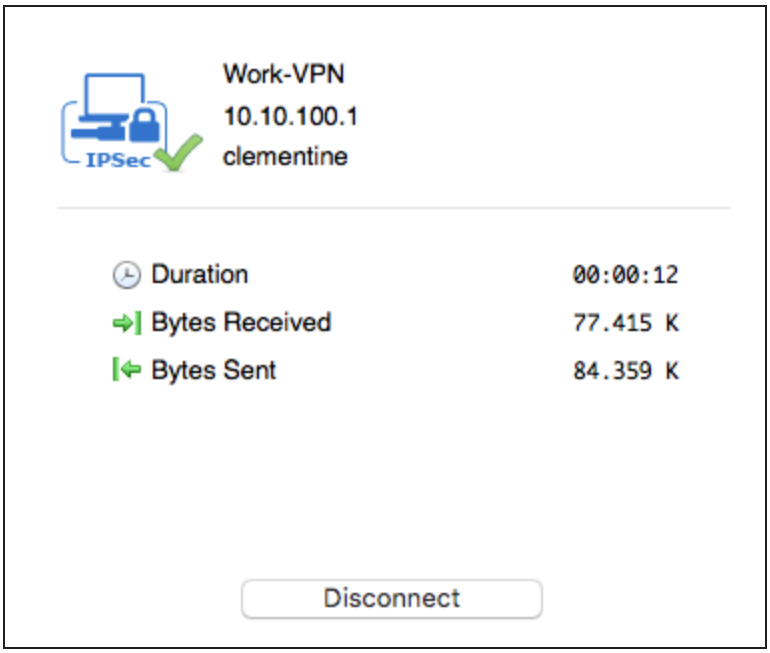
Set **Authentication Method** to **Pre-Shared Key** and enter the key below.



6. Results

On FortiClient, select the VPN, enter the username and password, and select **Connect**.

Once the connection is established, the FortiGate assigns the user an IP address and FortiClient displays the status of the connection, including the IP address, connection duration, and bytes sent and received.



On the FortiGate unit, go to **Monitor > IPsec Monitor** and verify that the tunnel **Status** is **Up**.

The monitor also shows the IP address of the FortiClient user, under **Remote Gateway**.

Name	Type	Remote Gateway	Username	Status
IPsec-FCT_0	Dialup - FortiClient (Windows, Mac OS, Android)	172.20.121.46		Up

Browse the Internet, then go to **FortiView > Policies** and select the **now** view. You can see traffic flowing through the **IPsec-VPN-Internet** policy.

Policy	Source Interface	Destination Interface	Bytes (Sent/Received)	Sessions	Bandwidth
IPsec-VPN-Internet	IPsec-FCT_0	wan1	449.18 kB	137	176.55 kbps

Right-click on the policy, then select **Drill Down to Details**. You can see more information about the traffic.

Summary of IPsec-VPN-Internet

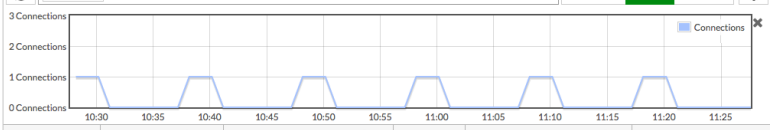
Policy Name :	IPsec-VPN-Internet
Policy ID :	3
Source Interface :	IPsec-FCT
Destination Interface :	wan1
Bytes (Sent/Received) :	442.44 kB
Bandwidth :	15.02 kbps
Sessions :	129
Time Period :	Realtime

Sources | Destinations | Applications | Countries | Sessions

Source	Device	Source Interface	Bytes (Sent/Received)	Sessions	Bandwidth
10.10.100.1		IPsec-FCT_0	444.28 kB	129	15.02 kbps

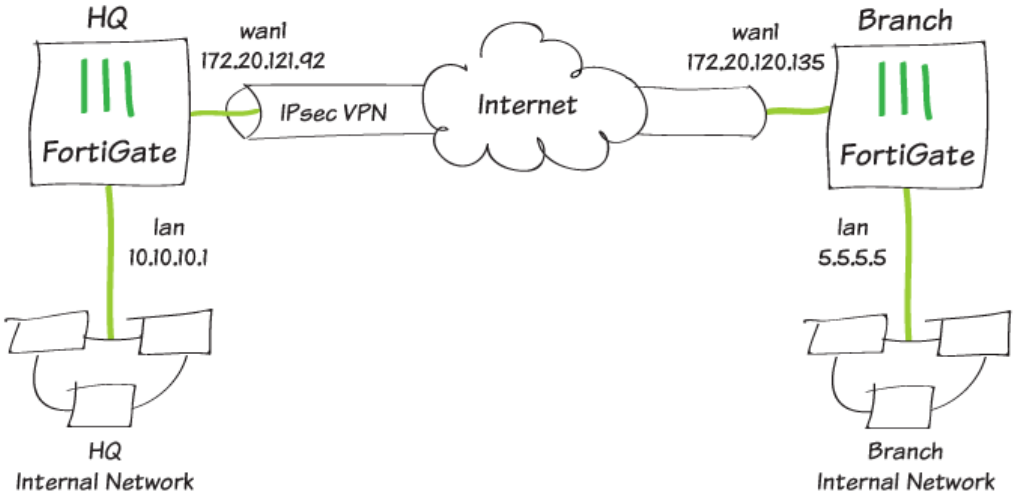
Go to **FortiView > VPN** to see which users have connected to the VPN.

Add Filter | 5 minutes | 1 hour | 24 hours



User	Connections	Last Connection Time	VPN Type	Bytes (Sent/Received)	Duration
clementine	1	2016-01-21, 8:38:23 AM	ipsec	15.56 MB	1h 59m 54s

Site-to-site IPsec VPN with two FortiGates



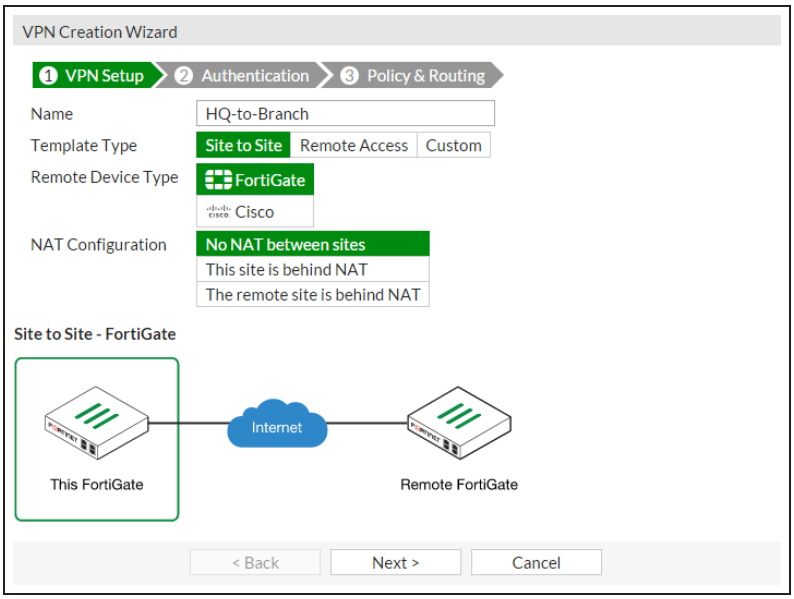
In this example, you will allow transparent communication between two networks that are located behind different FortiGates at different offices using route-based IPsec VPN. The VPN will be created on both FortiGates by using the VPN Wizard's **Site to Site - FortiGate** template.

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

1. Configuring the HQ IPsec VPN

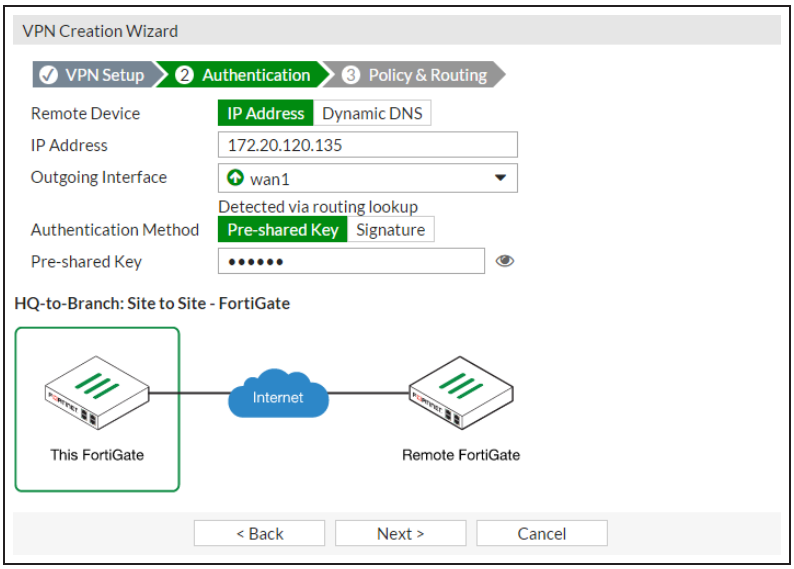
On the HQ FortiGate, go to **VPN > IPsec Wizard**.

Select the **Site to Site** template, and select **FortiGate**.

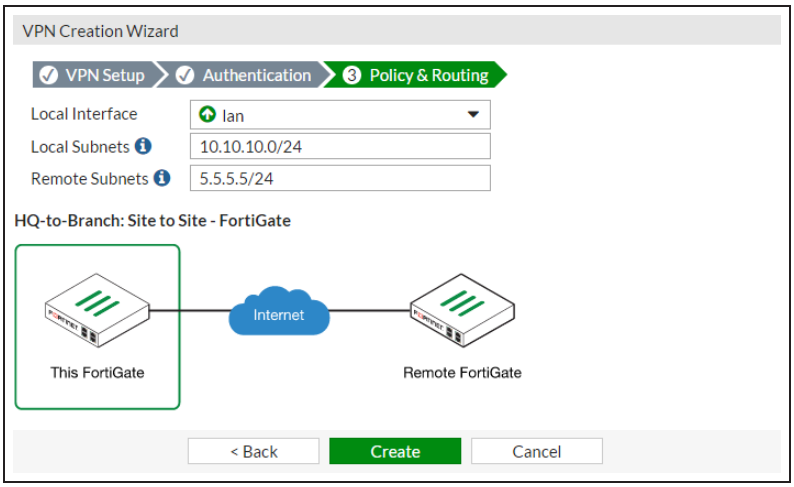


In the **Authentication** step, set **IP Address** to the IP of the Branch FortiGate (in the example, *172.20.120.135*). After you enter the gateway, an available interface will be assigned as the **Outgoing Interface**. If you wish to use a different interface, select **Change**.

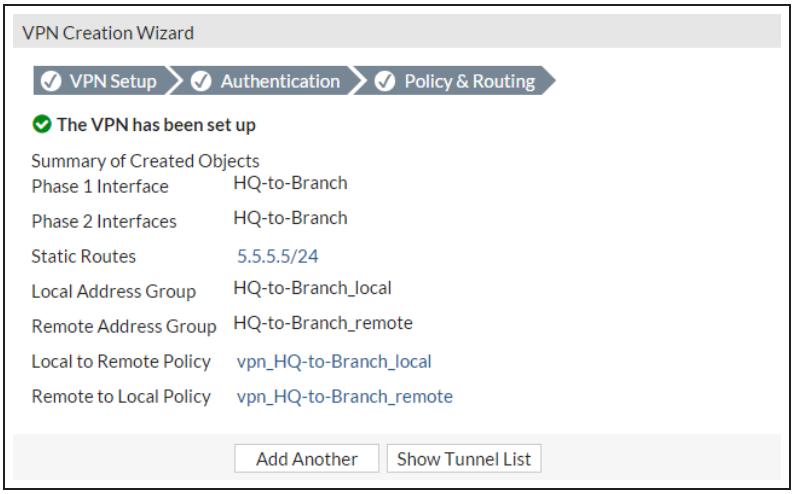
Set a secure **Pre-shared Key**.



In the **Policy & Routing** step, set the **Local Interface**. The **Local Subnets** will be added automatically. Set **Remote Subnets** to the Branch FortiGate's local subnet (in the example, 5.5.5.5/*24*).



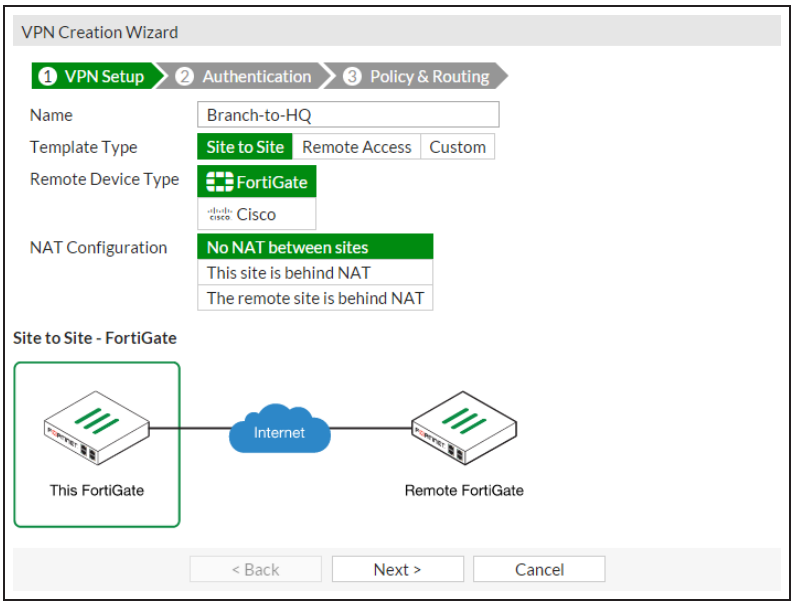
A summary page shows the configuration created by the wizard, including firewall addresses, firewall address groups, a static route, and security policies.



2. Configuring the Branch IPsec VPN

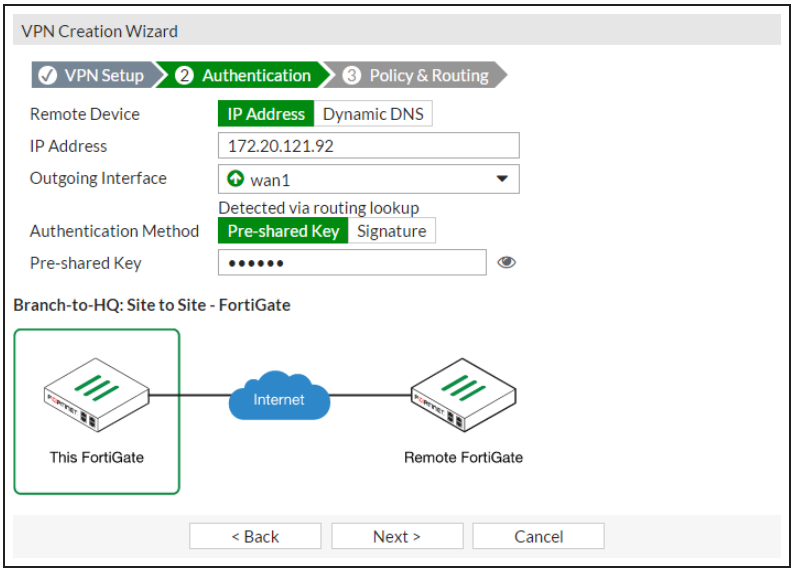
On the Branch FortiGate, go to **VPN > IPsec Wizard**.

Select the **Site to Site** template, and select **FortiGate**.

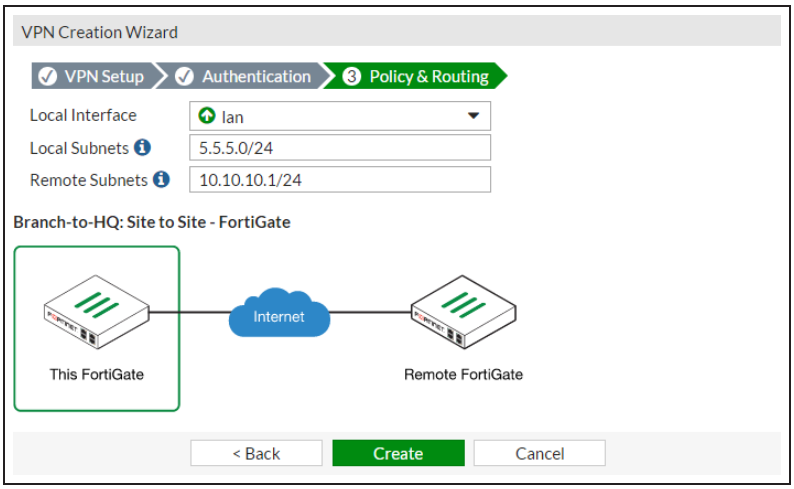


In the **Authentication** step, set **IP Address** to the IP of the HQ FortiGate (in the example, *172.20.121.92*). After you enter the gateway, an available interface will be assigned as the **Outgoing Interface**. If you wish to use a different interface, select **Change**.

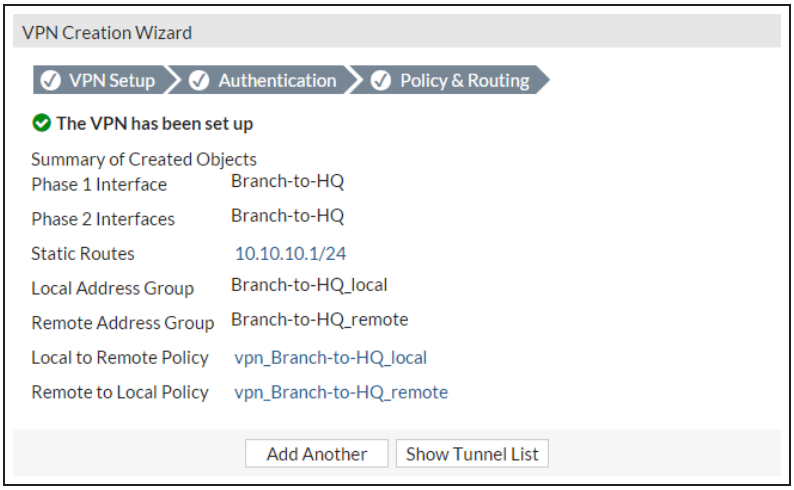
Set the same **Pre-shared Key** that was used for HQ's VPN.



In the **Policy & Routing** step, set the **Local Interface**. The **Local Subnets** will be added automatically. Set **Remote Subnets** to the HQ FortiGate's local subnet (in the example, 10.10.10.1/*24*).

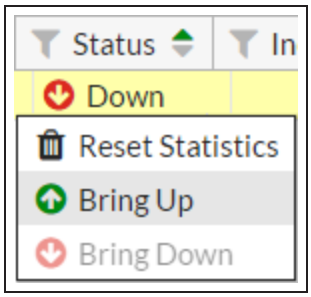


A summary page shows the configuration created by the wizard, including firewall addresses, firewall address groups, a static route, and security policies.



3. Results

On either FortiGate, go to **Monitor > IPsec Monitor** to verify the status of the VPN tunnel. Right-click under **Status** and select **Bring Up**.



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

If you need to generate traffic to test the connection, ping the Branch FortiGate's internal interface from the HQ's internal network.

IPsec troubleshooting

This page contains tips to help you with some common challenges of IPsec VPNs.

The options to configure policy-based IPsec VPN are unavailable.

Go to Feature Select and enable **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 following diagnostic command in the CLI:

```
diag debug application ike -1
diag debug enable
```

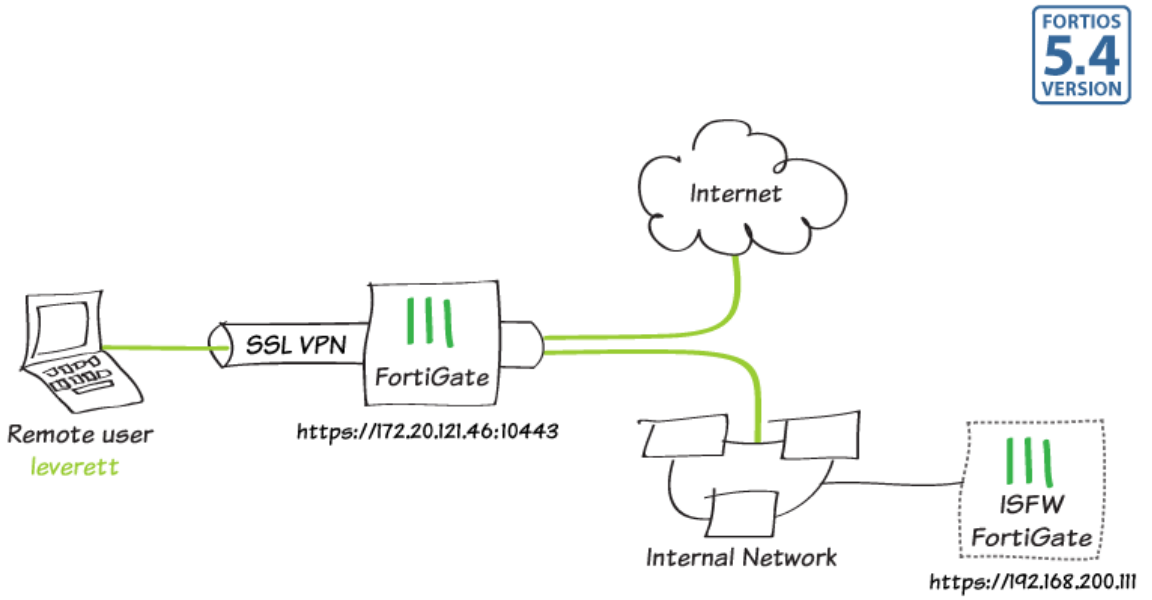
The resulting output may indicate where the problem is occurring. When you are finished, disable the diagnostics by using the following command:

```
diag debug reset
diag debug disable
```

The VPN tunnel goes down frequently.

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

SSL VPN using web and tunnel mode



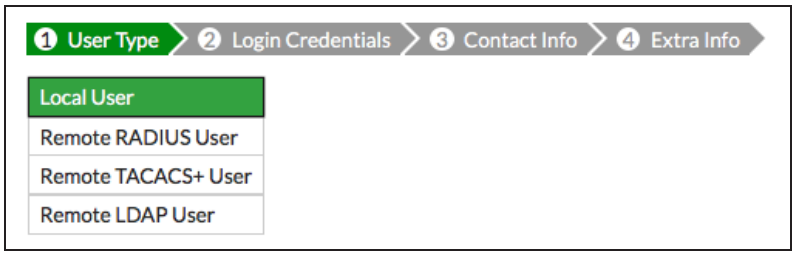
In this example, you will allow remote users to access the corporate network using an SSL VPN, connecting either by web mode or tunnel mode and with FortiClient. This allows users to access network resources, such as the Internal Segmentation Firewall (ISFW) used in this example.

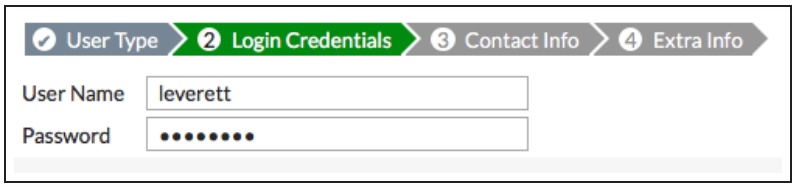
For users connecting via tunnel mode, traffic to the Internet will also flow through the FortiGate, to apply security scanning to this traffic.

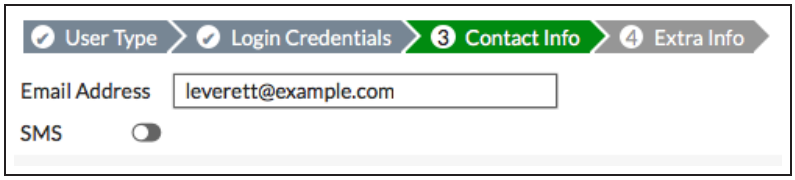
During the connecting phase, the FortiGate will also verify that the remote user's antivirus software is installed and up-to-date.

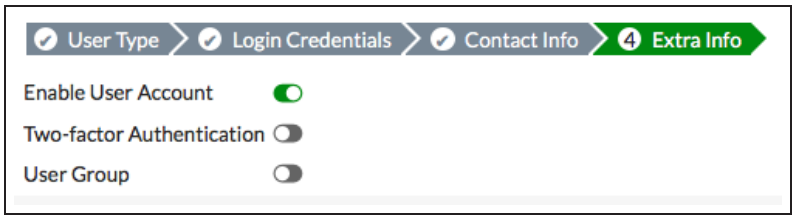
1. Creating a user and a user group

Go to **User & Device User Definition**. Create a local user account for a SSL VPN user.

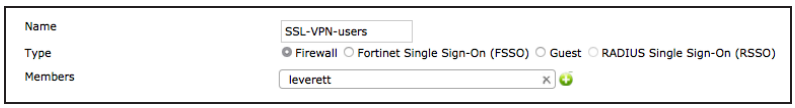








Go to **User & Device > User Groups**. Create a user group for SSL VPN users and add the new user account.



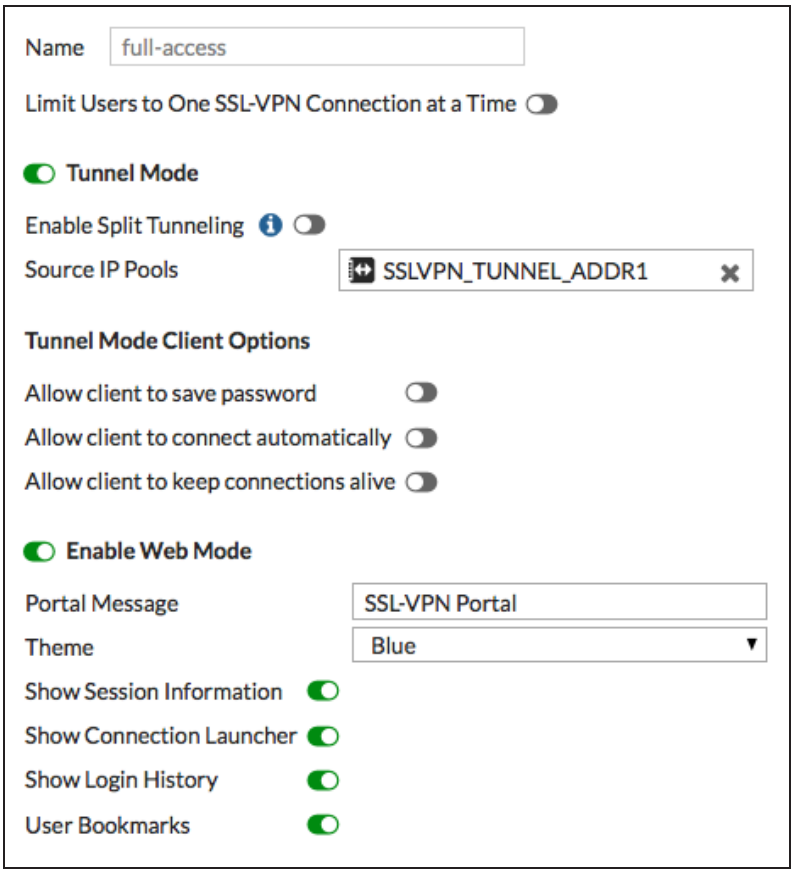
2. Creating an SSL VPN portal for remote users

Go to **VPN > SSL-VPN Portals**. Edit the **full-access** portal. The full-access portal allows the use of tunnel mode and/or web mode.

Make sure Enable **Split Tunneling** is *not* selected, so that all Internet traffic will go through the FortiGate.

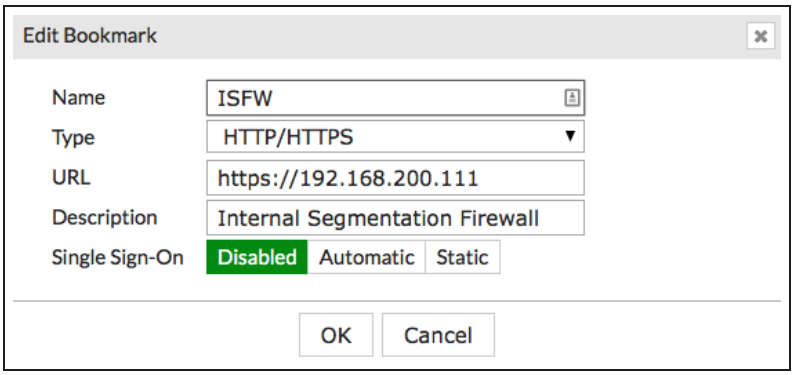
*If you do select **Enable Split Tunneling**, traffic not intended for the corporate network will not flow through the FortiGate or be subject to the corporate security profiles. You will also have to set your corporate network's address as the **Routing Address**.*

Set **Source IP Pools** to use the default IP range **SSLVPN_TUNNEL-ADDR1.**



Under **Predefined Bookmarks**, select create new to add a new bookmark. Bookmarks are used as links to internal network resources.

In the example, a bookmark is added to connect to a FortiGate being used as an ISFW, which can be accessed at *https://192.168.200.111*.



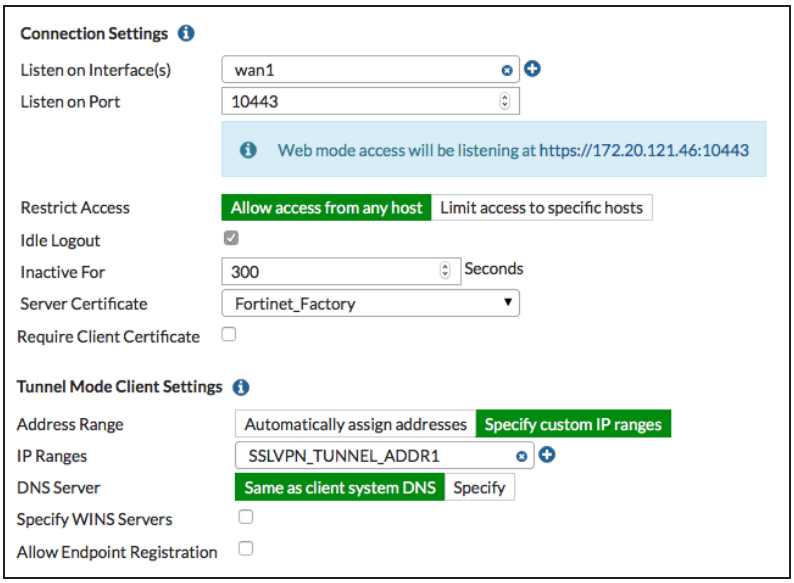
3. Configuring the SSL VPN tunnel

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

To avoid port conflicts, set **Listen on Port** to **10443**. Set **Restrict Access** to **Allow access from any host**.

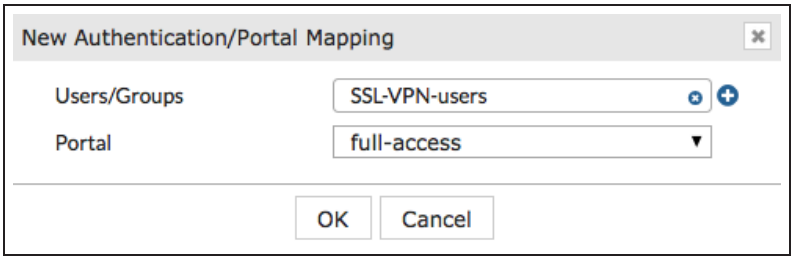
In the example, the **Fortinet_Factory** certificate is used as the **Server Certificate**. It is, however, recommended that you purchase a certificate for your domain and upload it for use with an SSL VPN.

Under **Tunnel Mode Client Settings**, set **IP Ranges** to use the default IP range **SSLVPN_TUNNEL-ADDR1.**



Under **Authentication/Portal Mapping**, add the SSL VPN user group and map it to the **full-access** portal.

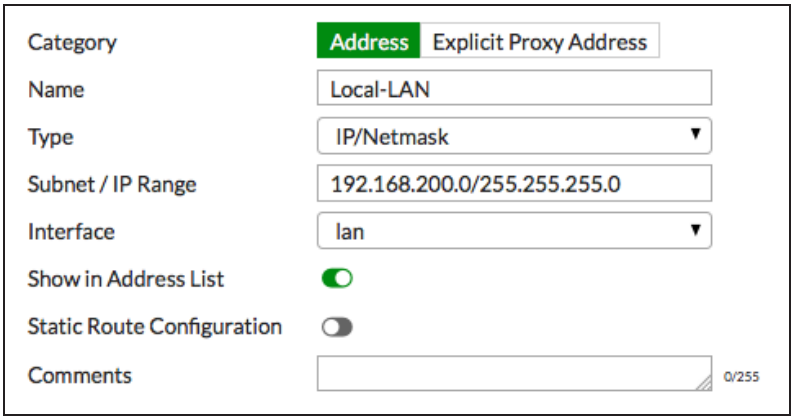
If necessary, map a portal for **All Other Users/Groups**.



4. Adding an address for the local network

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

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

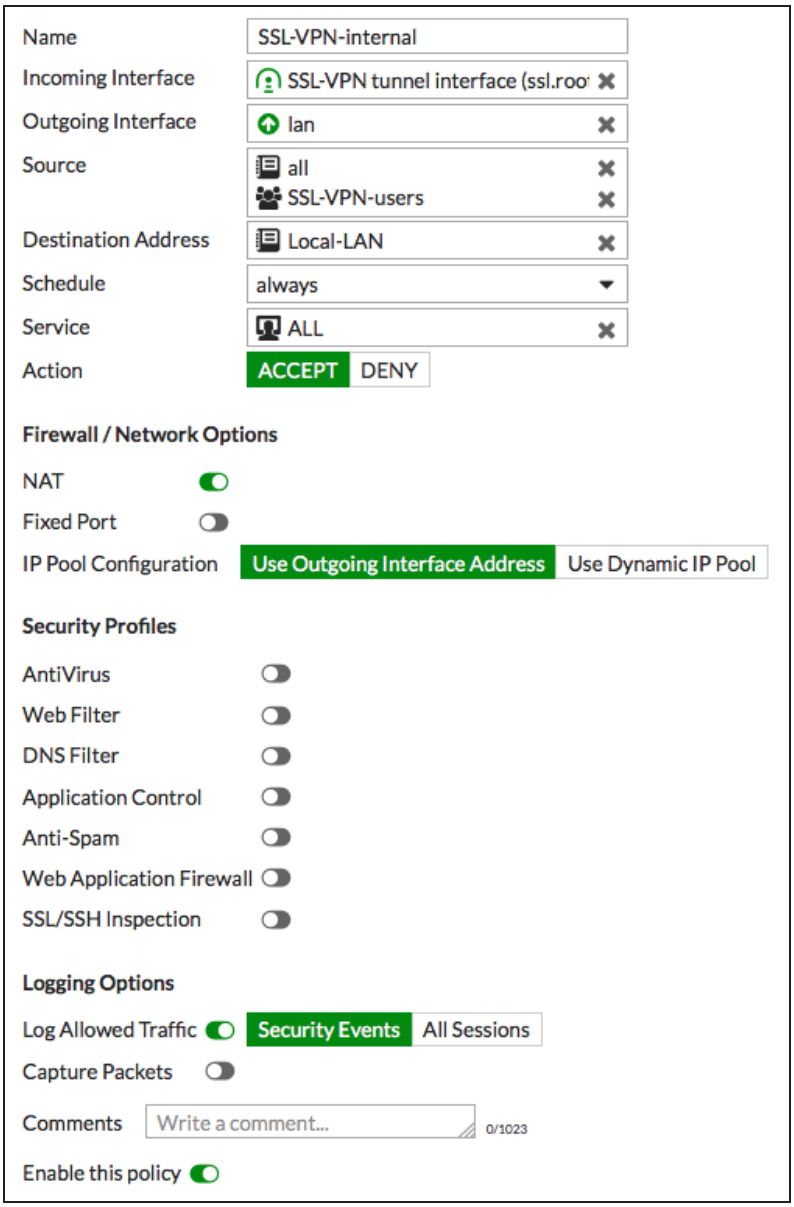


5. Adding security policies for access to the internal network and Internet

Go to **Policy & Objects > IPv4 Policy**. Add a security policy allowing access to the internal network through the VPN tunnel interface. Set a policy name that will identify what this policy is used for (in the example, *SSL-VPN-internal)*

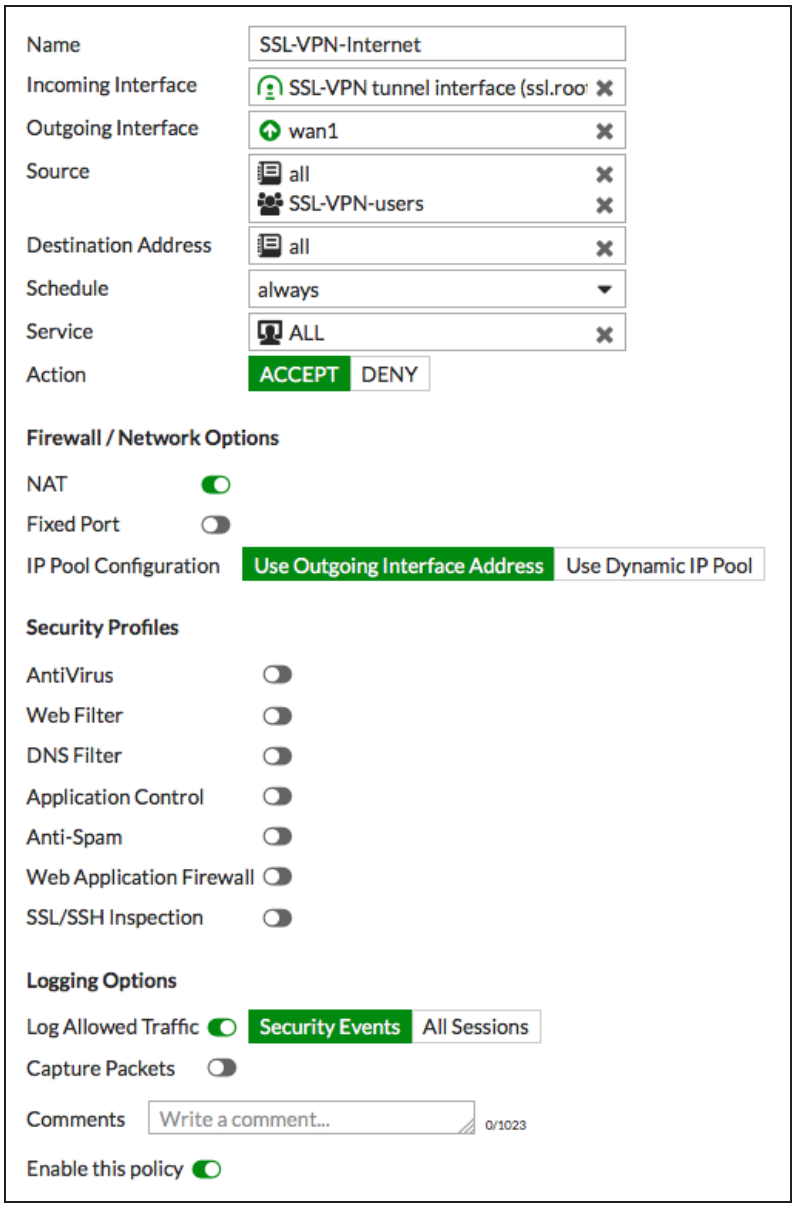
Set **Incoming Interface** to **ssl.root** and **Outgoing Interface** to the local network interface. Select **Source** and set **Address** to **all** and **Source User** to the SSL-VPN user group. Set **Destination Address** to the local network address, **Service** to **ALL**, and enable **NAT.**

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**, **Outgoing Interface** is set to **wan1**, and **Destination** is set to **all**.



6. Setting the FortiGate unit to verify users have current AntiVirus software

Go to the **Dashboard**. In the **CLI Console** widget, enter the following commands to enable the host to check for compliant AntiVirus software on the remote user's computer:

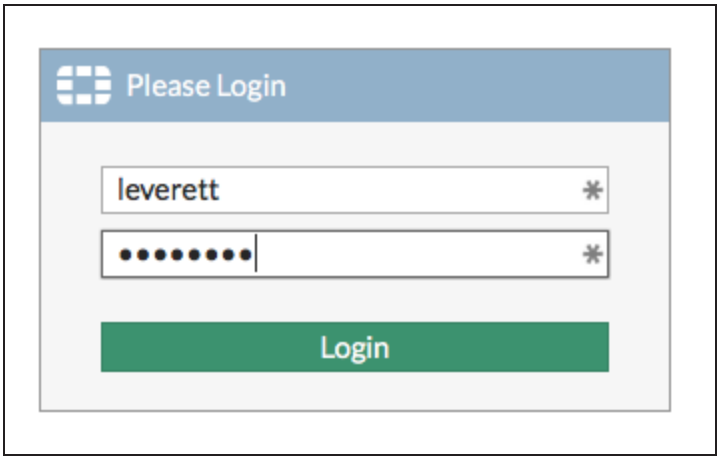
```
config vpn ssl web portal
   edit full-access
       set host-check av
   end
```

7. Results

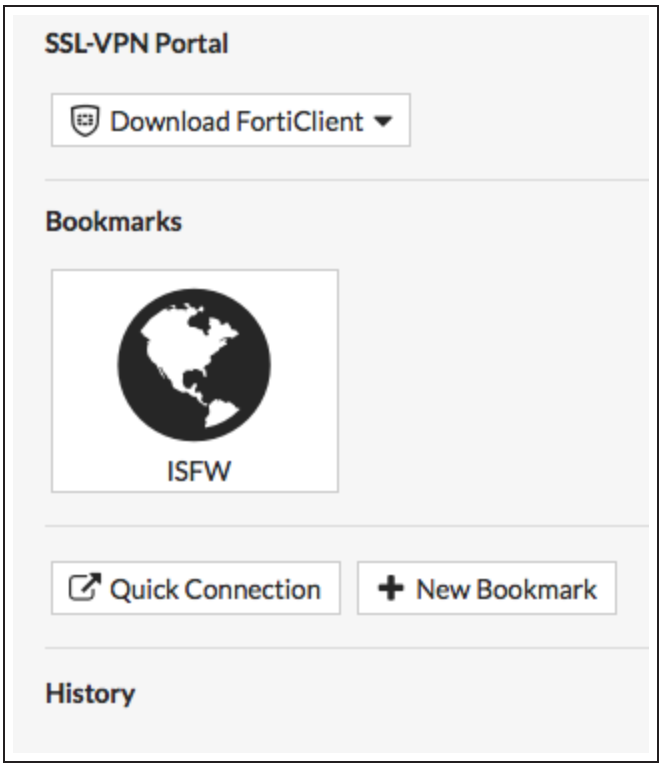
Web mode:

Using a supported Internet browser, connect to the SSL VPN web portal using the remote gateway configured in the SSL VPN settings (in the example, *172.20.121.46:10443*)

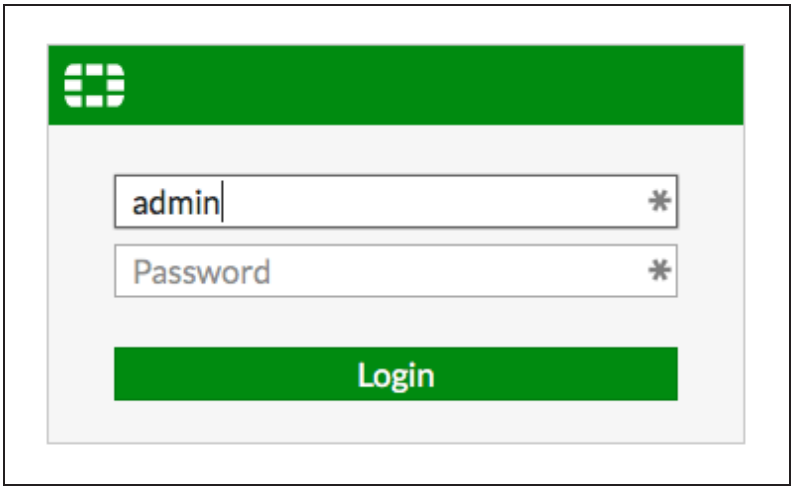
Use the SSL VPN user's credentials to authenticate.



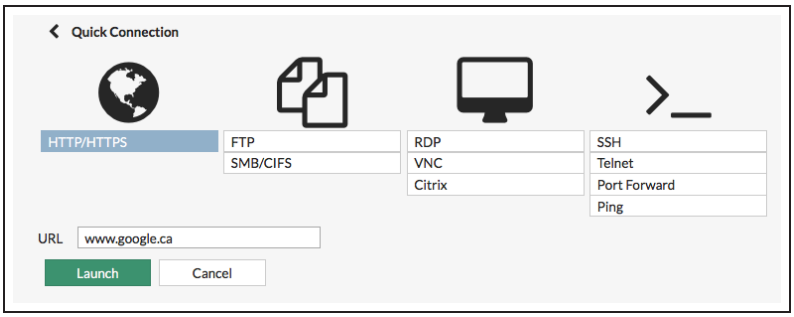
The web portal appears.



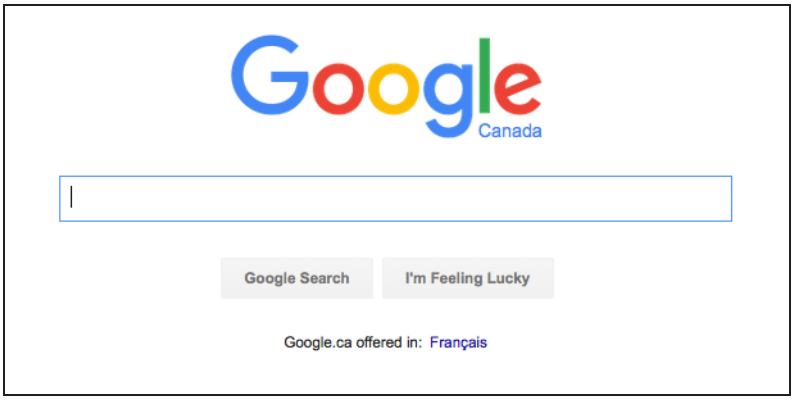
In this example, selecting the **ISFW Bookmark** allows you to connect to the ISFW FortiGate.



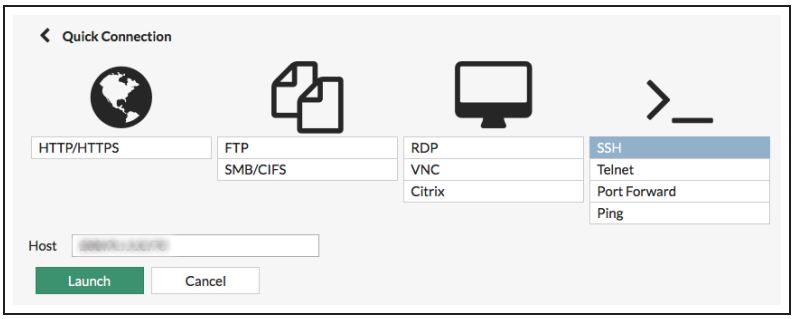
To connect to the Internet, select **Quick Connection**. Select **HTTP/HTTPS**, then enter the **URL** and select **Launch**.



The website will launch.

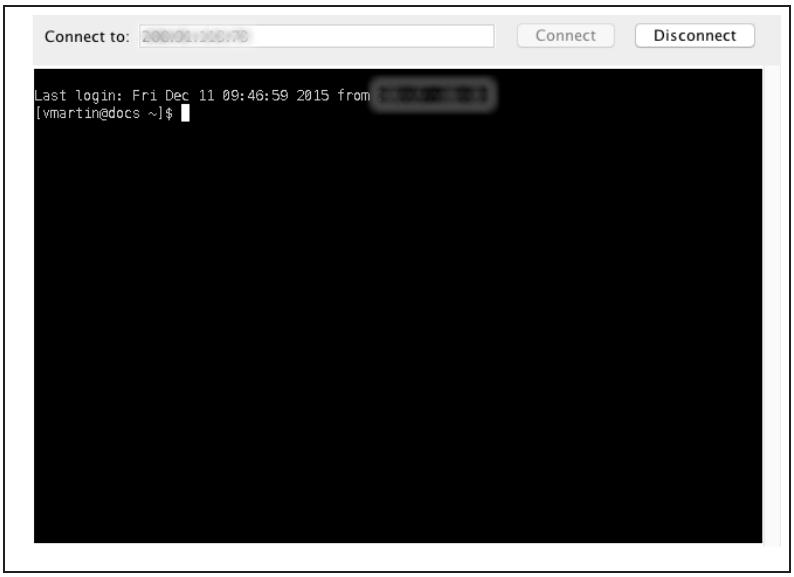


You can also use the **Quick Connection** for other allowed types of traffic, such as **SSH**.

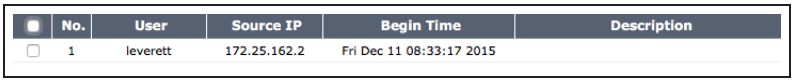


An SSH connection will open in your browser, connecting to the requested Host.

Java is required for an SSH connection.



On the FortiGate, go to **Monitor > SSL-VPN Monitor**. The user is connected to the VPN.



	No.	User	Source IP	Begin Time	Description
☐	1	leverett	172.25.162.2	Fri Dec 11 08:33:17 2015	

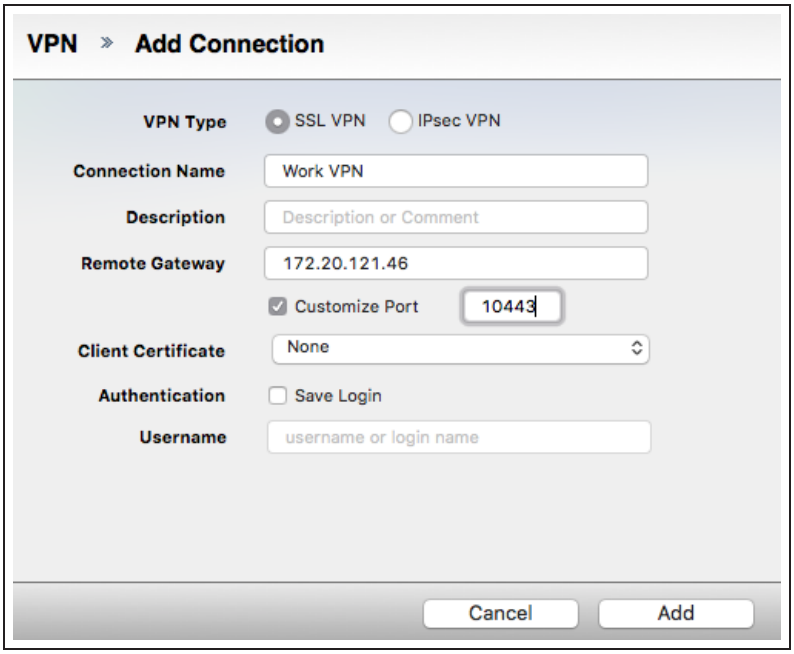
Tunnel mode:

If you have not done so already, download FortiClient from www.forticlient.com.

Open the FortiClient Console and go to **Remote Access**. Add a new connection.

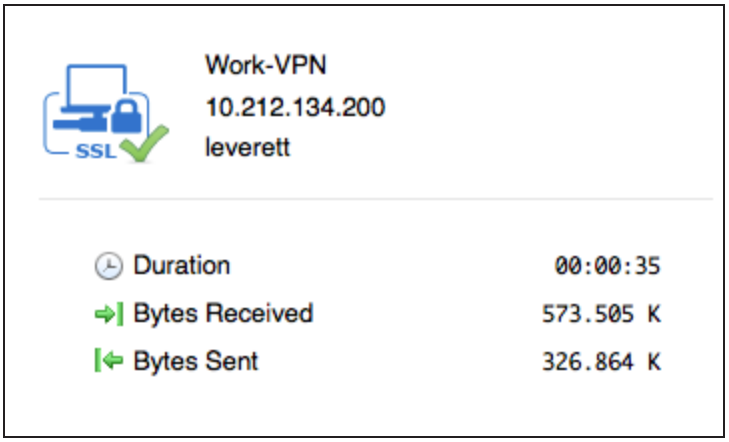
Set **VPN Type** to **SSL VPN**, set **Remote Gateway** to the IP of the listening FortiGate interface (in the example, *172.20.121.46*). Select **Customize Port** and set it to **10443**.

Select **Add**.

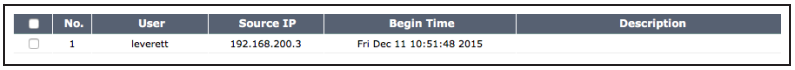


Connect to the VPN using the SSL VPN user's credentials.

You are able to connect to the VPN tunnel.



On the FortiGate, go to **Monitor > SSL-VPN Monitor**. The user is connected to the VPN.



No.	User	Source IP	Begin Time	Description
1	leverett	192.168.200.3	Fri Dec 11 10:51:48 2015	

SSL VPN troubleshooting

This page contains tips to help you with some common challenges for SSL VPN.

There is no response from the SSL VPN URL.

Go to VPN **Settings** and check the SSL VPN port assignment. Also, verify that the SSL VPN policy is configured correctly.

You receive an error stating that the web page cannot be found.

Check the URL you are attempting to connect to. It should follow this pattern:

https*://<FortiGate IP>:<Port>/remote/login*

Ensure that you are using the correct port number in the URL.

FortiClient cannot connect.

Read the Release Notes to ensure that the version of FortiClient you are using is compatible with your version of FortiOS.

When you attempt to connect using FortiClient or in Web mode, you receive the following error message: “Unable to logon to the server. Your user name or password may not be configured properly for this connection. (-12).”

Ensure that cookies are enabled in your browser. Also, if you are using a remote authentication server, ensure that the FortiGate is able to communicate with it.

The tunnel connects but there is no communication.

Make sure that there is a static route to direct packets destined for the tunnel users to the SSL VPN interface.

You can connect remotely to the VPN tunnel but are unable to access the network resources.

Examine the policy allowing VPN access to the local network. If the destination address is set to **all**, create a firewall address for the internal network. Change the destination address and attempt to connect remotely again.

Users are unable to download the SSL VPN plugin.

Go to the VPN **Portal** to make sure that the option to **Limit Users to One SSL-VPN Connection at a Time** is disabled. This allows users to connect to the resources on the portal page while also connecting to the VPN through FortiClient.

Users are being assigned to the wrong IP range.

Ensure that the same IP Pool is used in **VPN Portal** and **VPN Settings** to avoid conflicts. If there is a conflict, the portal settings will be used.

Expert

FortiGate units can be deployed in many ways to meet a wide range of advanced requirements. This section contains recipes and articles (which discuss topics in greater depth than a recipe) about a variety of these configurations.

Recipes and articles in this section are intended for users with a high degree of background knowledge about FortiGates and computer networking, such as users who have completed Fortinet's Network Security Expert (NSE) 4 level of training.

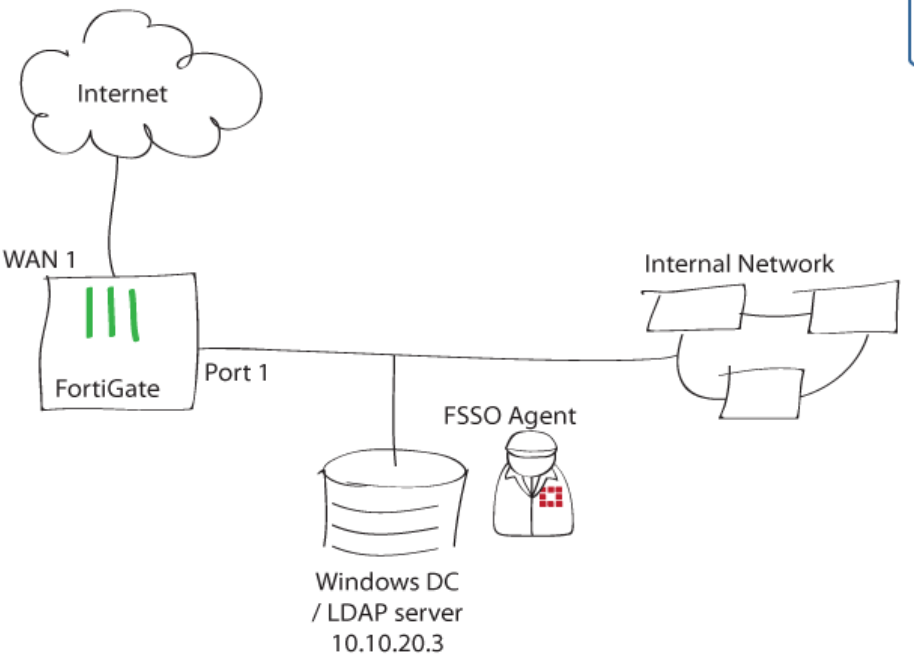
Authentication

- Single Sign-On using LDAP and FSSO agent in advanced mode
- Single Sign-On using FSSO agent in advanced mode and FortiAuthenticator
- SSO using a FortiGate, FortiAuthenticator, and DC Polling

VPN

- Configuring ADVPN in FortiOS 5.4

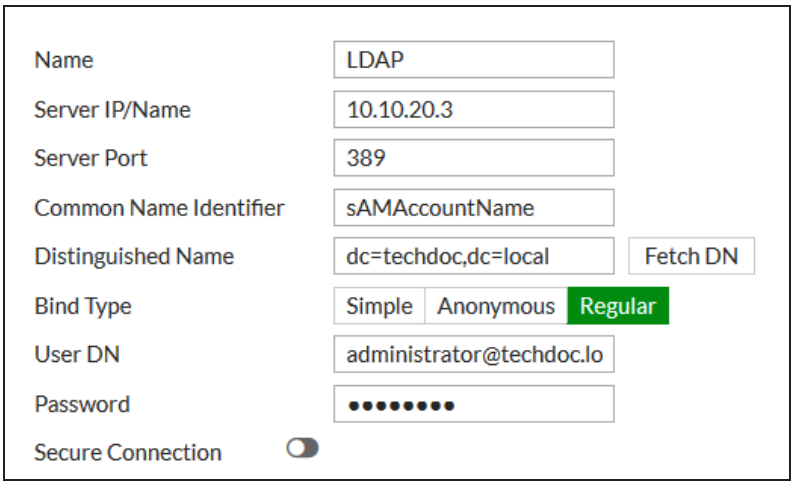
Single Sign-On using LDAP and FSSO agent in advanced mode



This recipe illustrates FortiGate user authentication with FSSO and a Windows DC LDAP server. In this example, user authentication controls Internet access.

1. Integrating the FortiGate with the Windows DC LDAP server

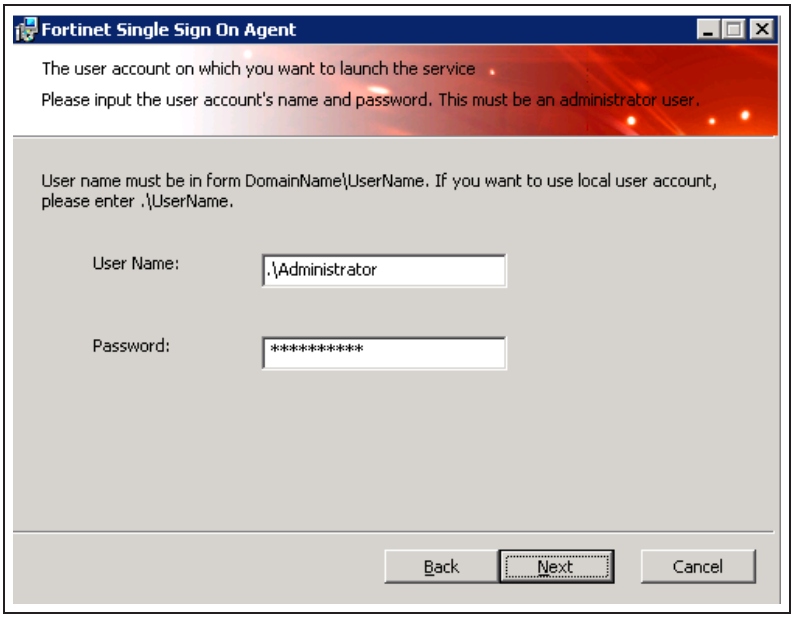
Go to **User & Device > LDAP Servers** to configure the LDAP server.



2. Installing FSSO agent on the Windows DC server

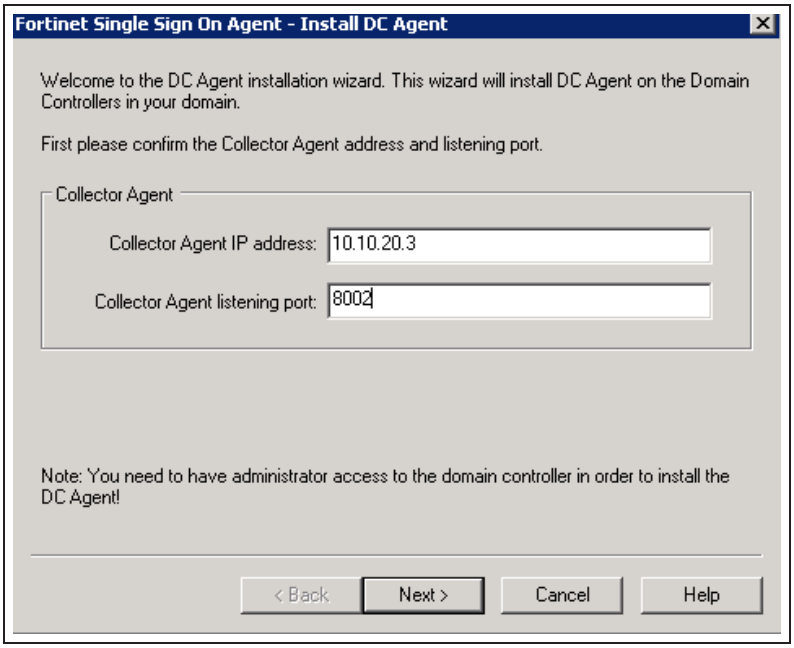
Accept the license and follow the Wizard.

Enter the Windows AD administrator password.

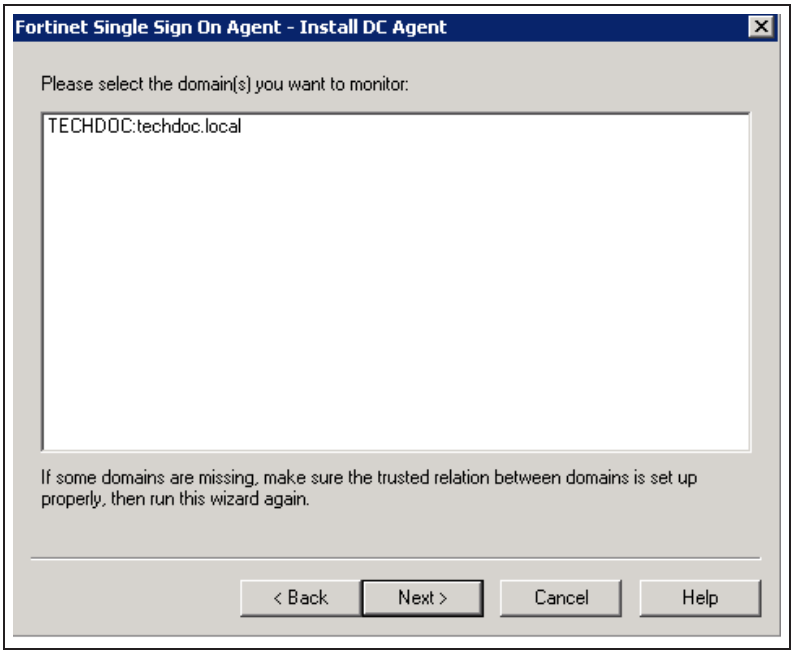


Select the **Advanced** Access method.

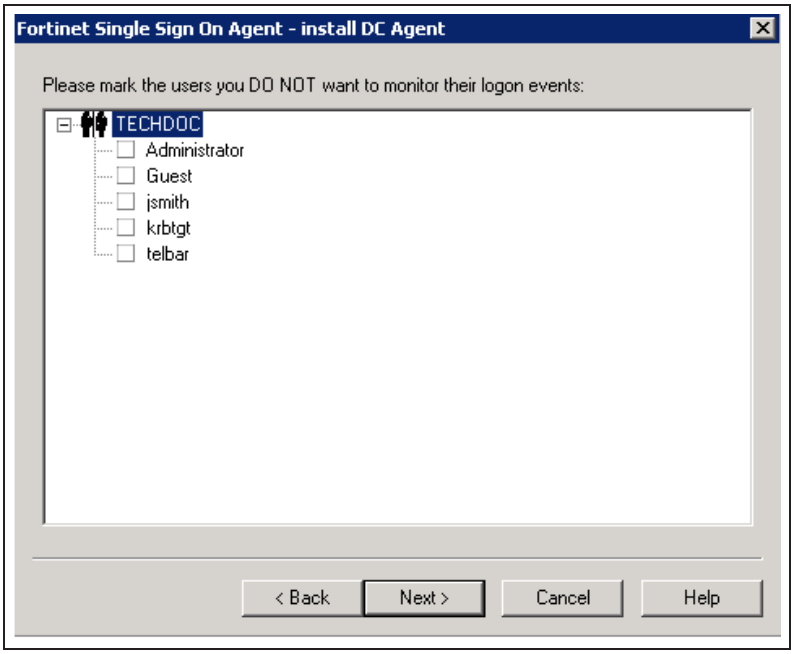
In the **Collector Agent IP address** field, enter the IP address of the Windows AD server.



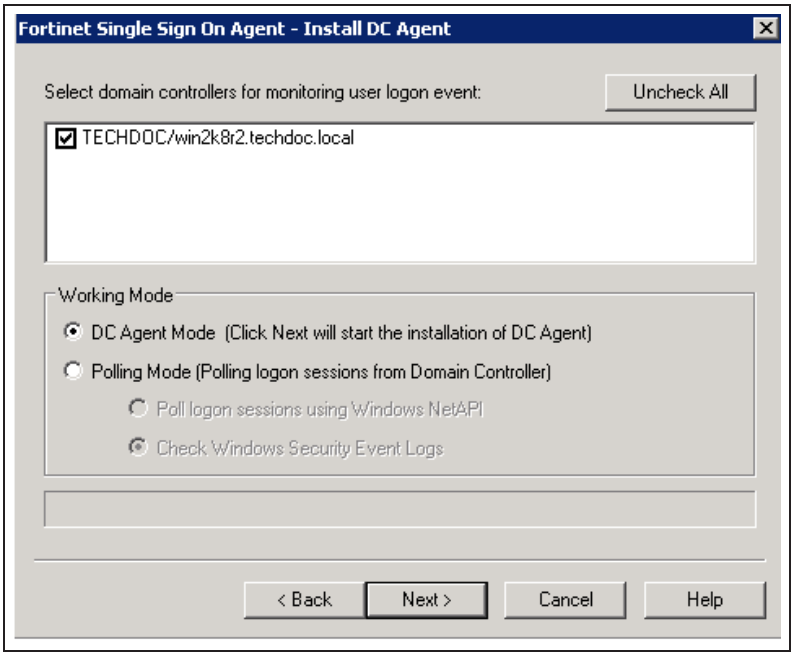
Select the domain you wish to monitor.



Next, select the users you do not wish to monitor.



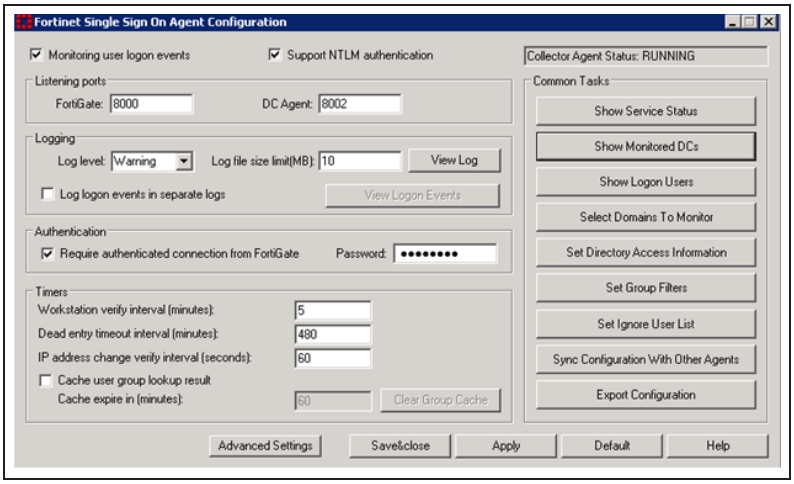
Under **Working Mode**, select **DC Agent Mode**.



Reboot the Domain Controller.

Upon reboot, the collector agent will start up.

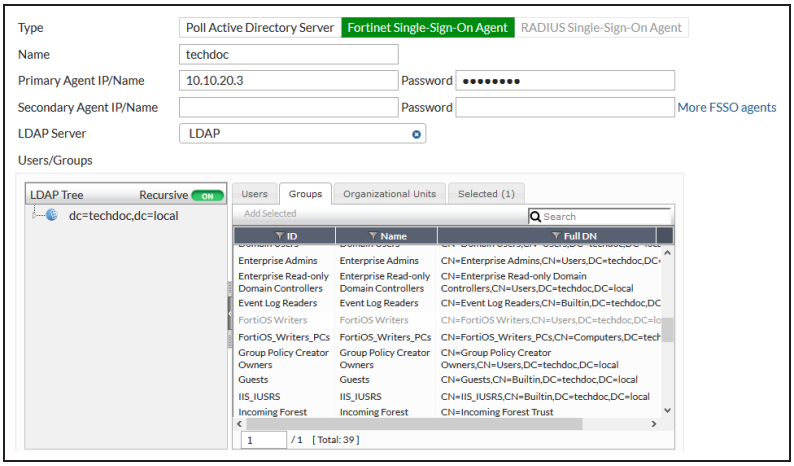
You can choose to **Require authenticated connection from FortiGate** and set a **Password**.



3. Configuring Single Sign-On on the FortiGate

Go to **User & Device > Single Sign-On** and create a new SSO server.

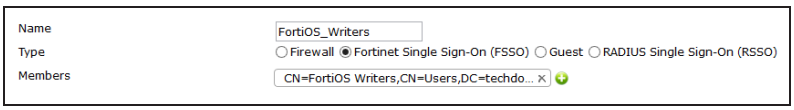
Under the **Groups** tab, select the user groups to be monitored. In this example, the "FortiOS Writers" group is used.



4. Adding a user group to the FortiGate

Go to **User & Device > User Groups** to create a new **FSSO** user group.

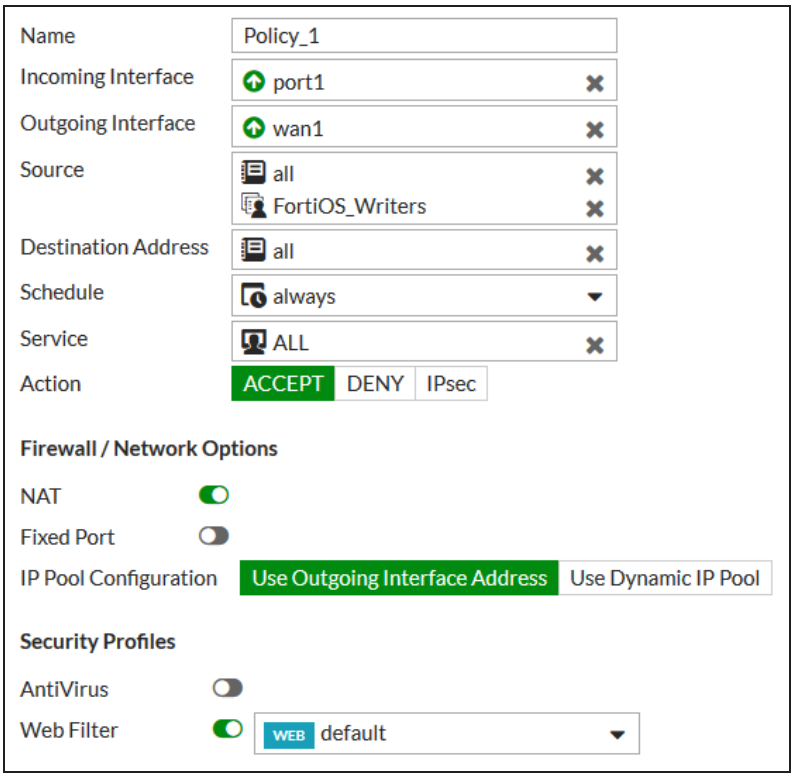
Under **Members**, select the "FortiOS Writers" group.



5. Adding a policy to the FortiGate

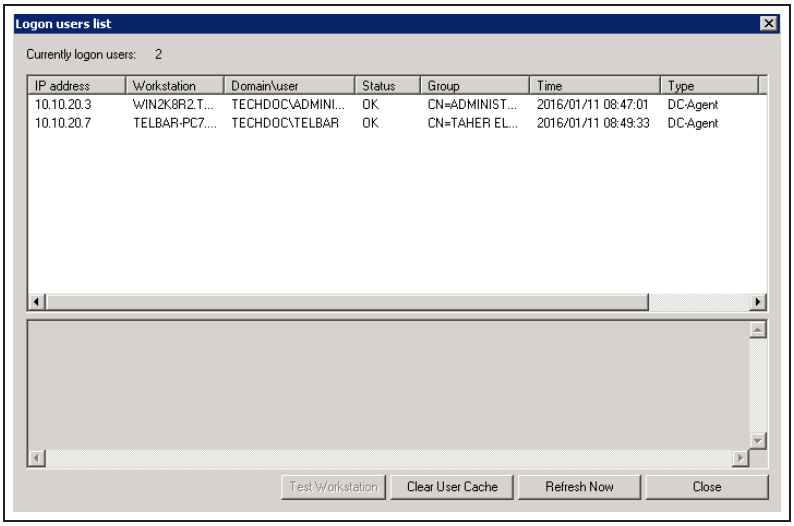
Go to **Policy & Objects > IPv4 Policy** and create a policy allowing "FortiOS_Writers" to navigate the Internet with appropriate security profiles.

The default **Web Filter** security profile is used in this example.



9. Results

Have users log on to the domain, go to the FSSO agent, and select **Show Logon Users.**

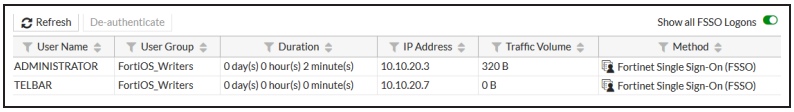


From the FortiGate, go to **Dashboard** to look for the **CLI Console** widget and type this command for more detail about current FSSO logons:

diagnose debug authd fsso list

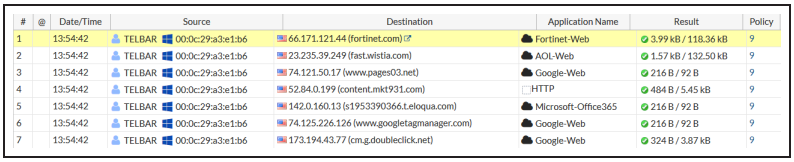
----FSSO logons----
IP: 10.10.20.3 User: ADMINISTRATOR Groups: CN=FORTIOS WRITERS,CN=USERS,DC=TECHDOC,DC=LOCAL Workstation: WIN2K8R2.TECHDOC.LOCAL MemberOf: FortiOS_Writers
IP: 10.10.20.7 User: TELBAR Groups: CN=FORTIOS WRITERS,CN=USERS,DC=TECHDOC,DC=LOCAL Workstation: TELBAR-PC7.TECHDOC.LOCAL MemberOf: FortiOS_Writers
Total number of logons listed: 2, filtered: 0
----end of FSSO logons----

From the FortiGate, go to **Monitor > Firewall User Monitor** and verify FSSO Logons.



Have users go to the Internet and the security profiles will be applied accordingly.

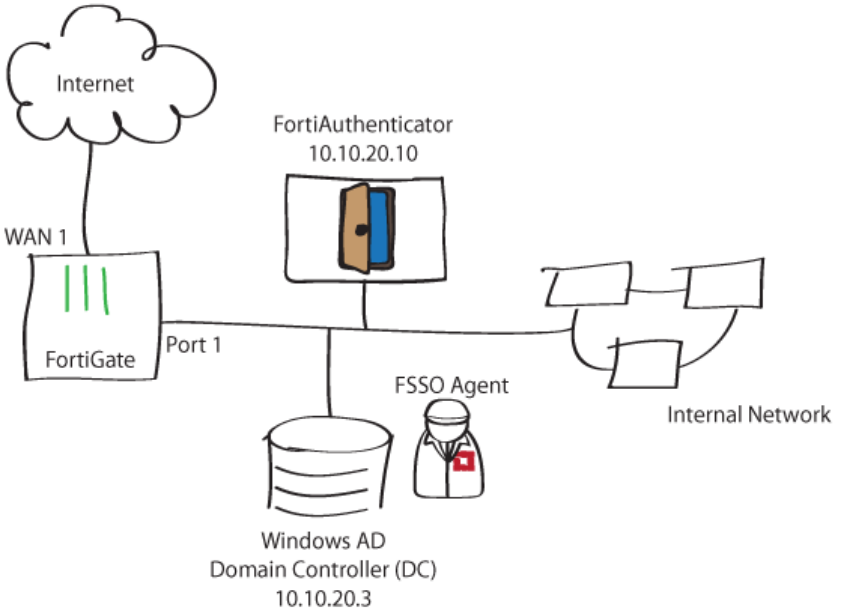
Go to **Log & Report > Forward Traffic** to verify the log.



Select an entry for details.

#	1	**Action**	Accept: session close
Application Category	unscanned	**Date/Time**	13:54:42
Destination	66.171.121.44 (fortinet.com)	**Destination Country**	United States
Destination Interface	wan1	**Destination Port**	80
Device	00:0c:29:a3:e1:b6	**Device Type**	Windows PC
Duration	103	**Group**	FortiOS_Writers
LAN In	3989	**LAN Out**	118365
Level		**Log ID**	13
Master Src MAC	00:0c:29:a3:e1:b6	**OS Name**	Windows
OS Version	7 or 8	**Policy**	9
Policy Type	policy	**Policy UUID**	1014caf4-3541-51e5-8733-9d89455a30ff
Protocol	tcp	**Protocol Number**	6
Received Bytes	118365	**Received Packets**	91
Sent Bytes	3989	**Sent Packets**	74
Service	HTTP	**Session ID**	799920
Source	TELBAR 00:0c:29:a3:e1:b6	**Source Country**	Reserved
Source Interface	port1	**Source Port**	56180
Src NAT IP	172.20.120.22	**Src NAT Port**	56180
Sub Type	forward	**Timestamp**	1/11/2016, 1:54:42 PM
Tran Display	snat	**User**	TELBAR
Virtual Domain	root	**WAN In**	118365
WAN Out	3989		

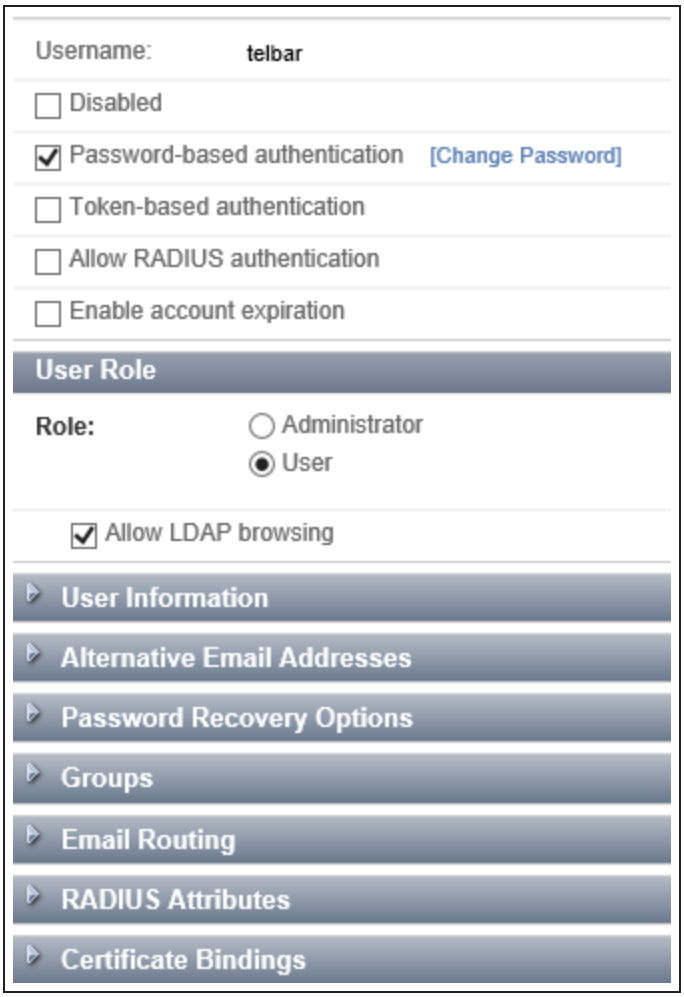
Single Sign-On using FSSO agent in advanced mode and FortiAuthenticator



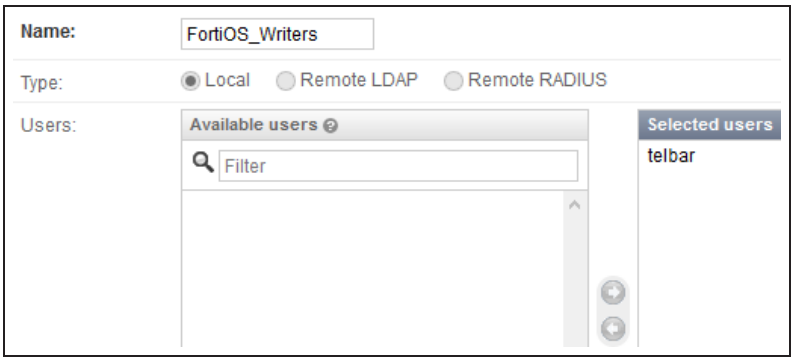
This recipe demonstrates FortiGate user authentication with FSSO agent installed on a Windows Domain Controller, and the use of a FortiAuthenticator as an LDAP server. In this example, user authentication controls Internet access.

1. Configuring an LDAP directory on the FortiAuthenticator

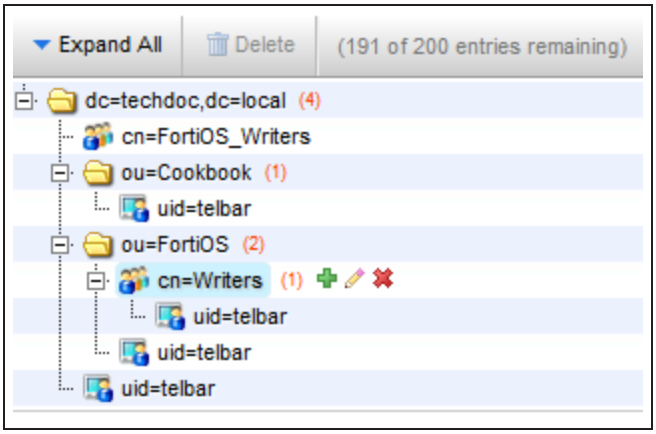
Go to **Authentication > User Management > Local Users** to create a user list. Make sure to enable **Allow LDAP browsing**.



Go to **Authentication > User Management > User Groups** to create a user group and add users to it. "FortiOS_Writers" user group is used in this example.

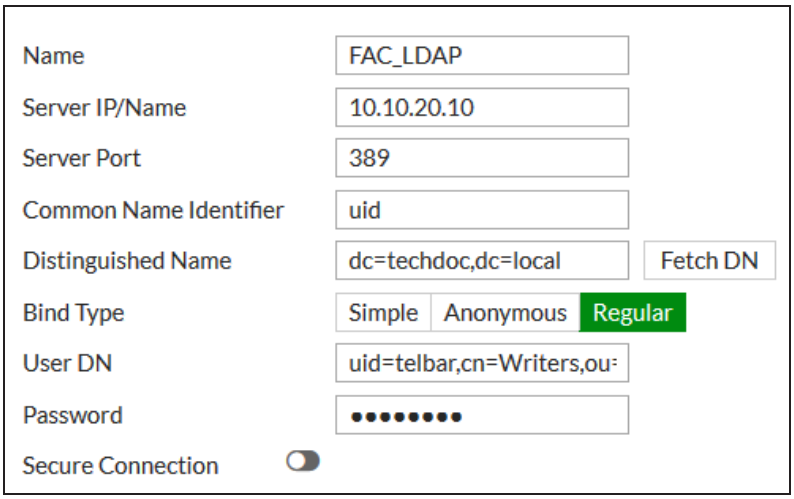


Go to **Authentication > LDAP Service > Directory tree** and configure the LDAP directory tree.



2. Integrating the FortiGate with the FortiAuthenticator

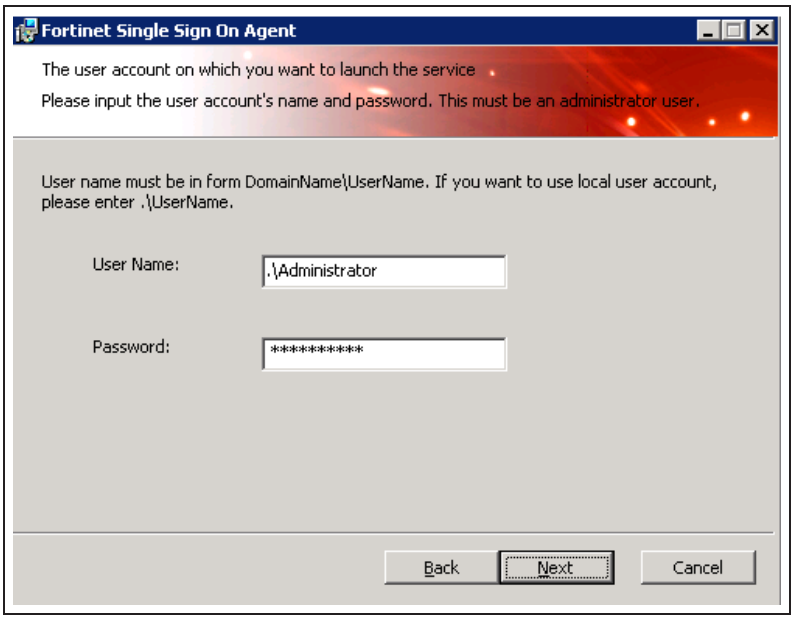
On the FortiGate, go to **User & Device > LDAP Servers** to configure the LDAP server.



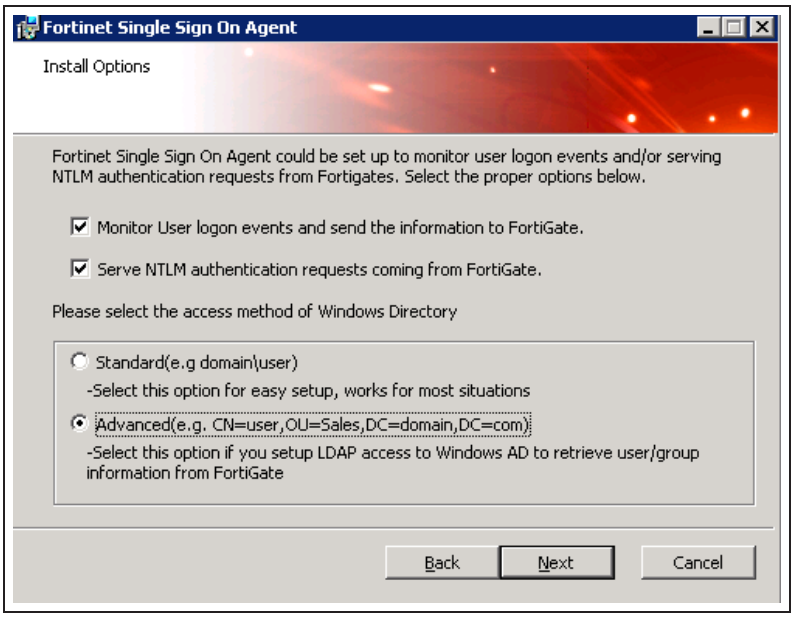
3. Installing FSSO agent on the Windows DC

Accept the license and follow the Wizard.

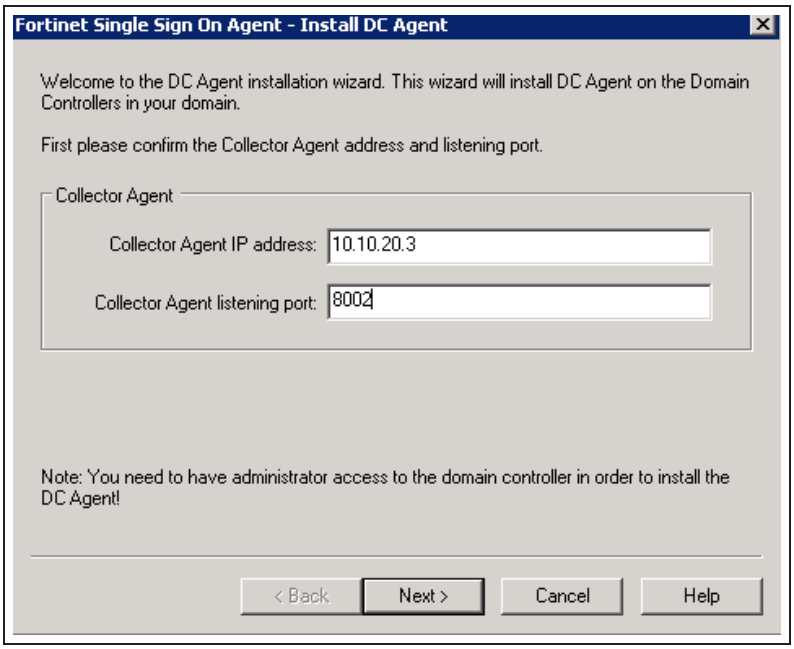
Enter the Windows AD administrator password.



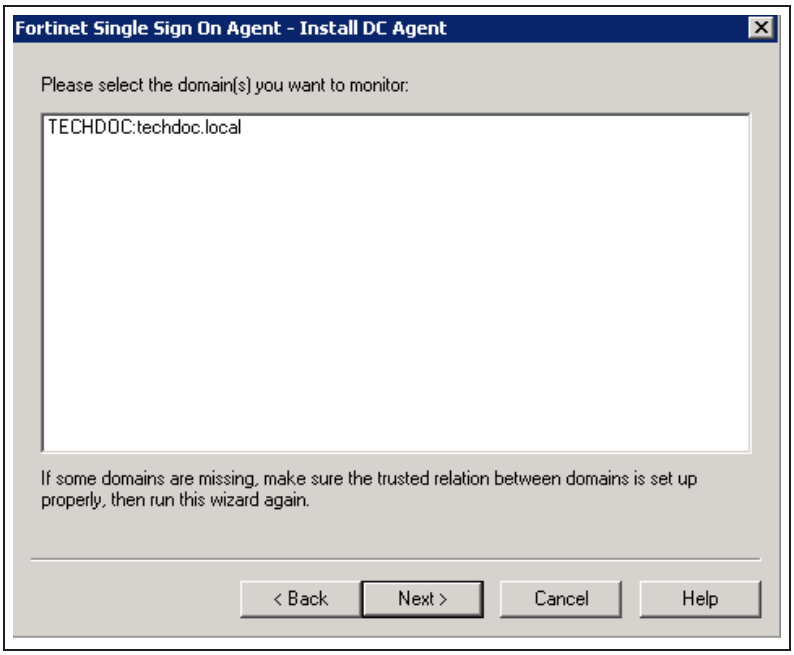
Select the **Advanced** access method for Windows Directory.



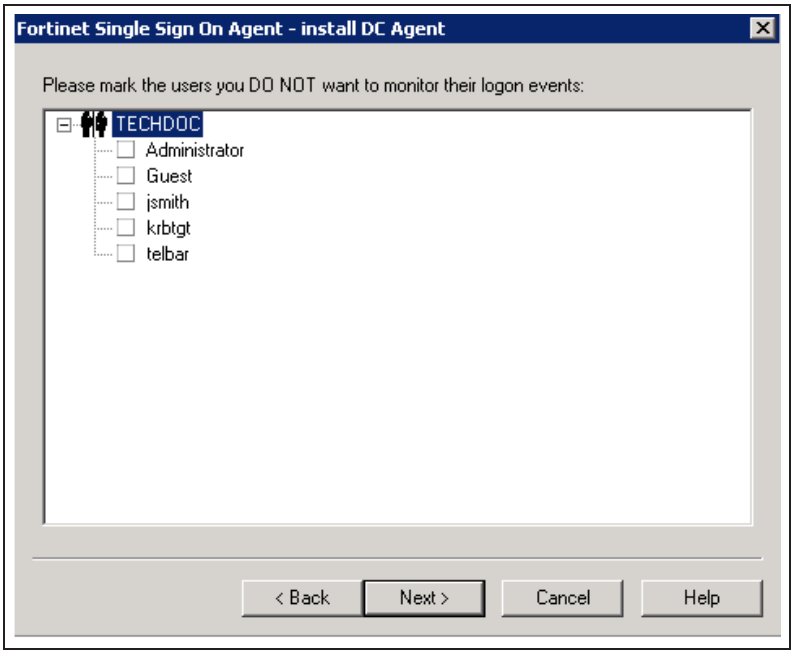
In the **Collector Agent IP address** field, enter the IP address of the Windows AD server.



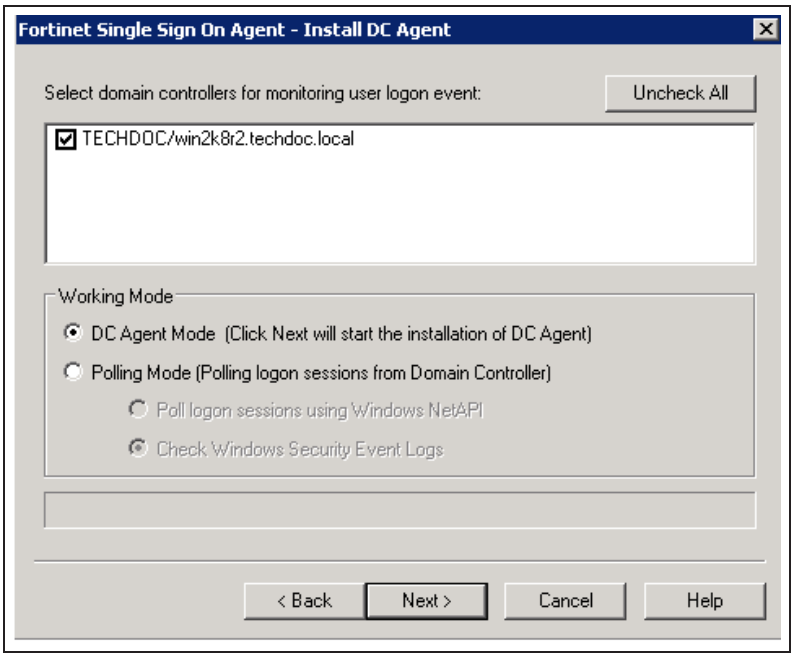
Select the domain you wish to monitor.



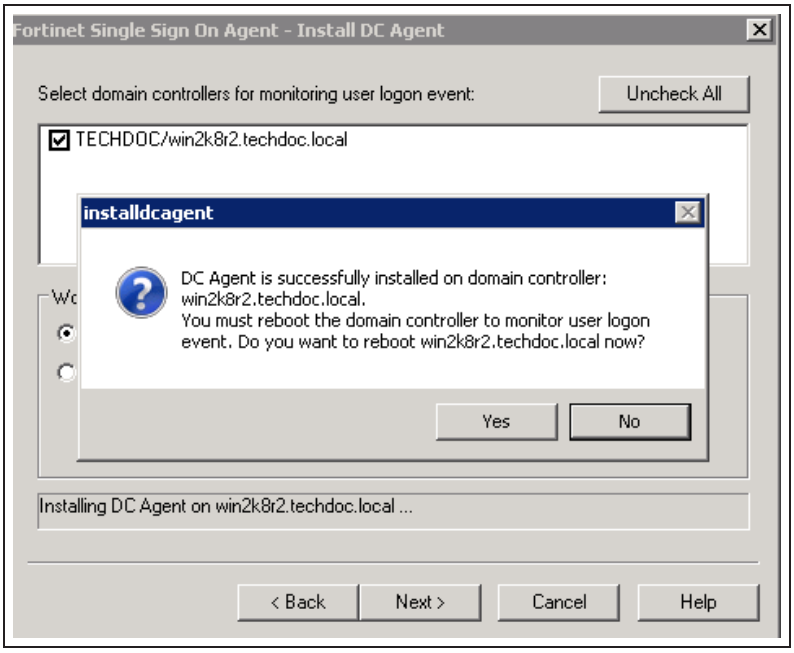
Next, select the users you do not wish to monitor.



Under **Working Mode**, select **DC Agent Mode**.

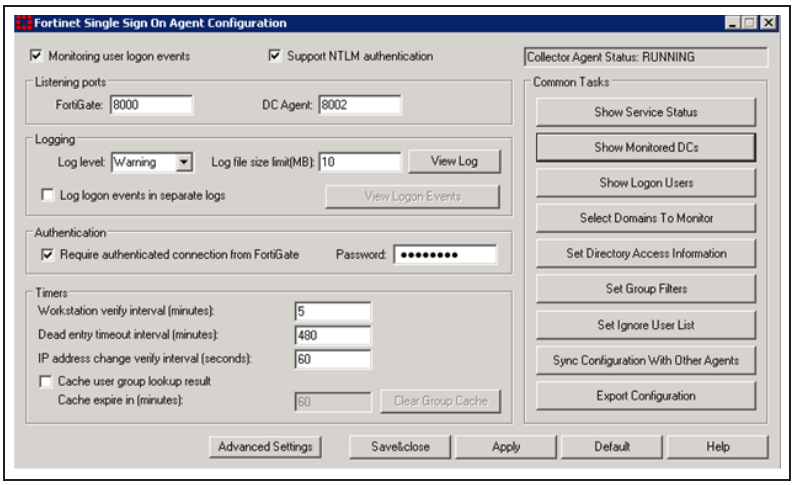


When prompted, select **Yes** to reboot the Domain Controller.



Upon reboot, the collector agent will start up.

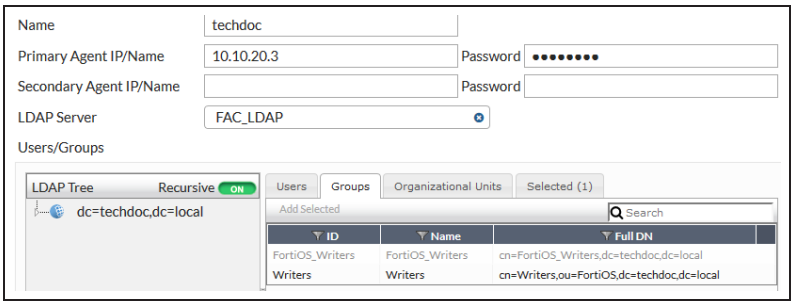
You can choose to **Require authenticated connection from FortiGate** and set a **Password** which will be used in step 4.



4. Configuring Single Sign-On on the FortiGate

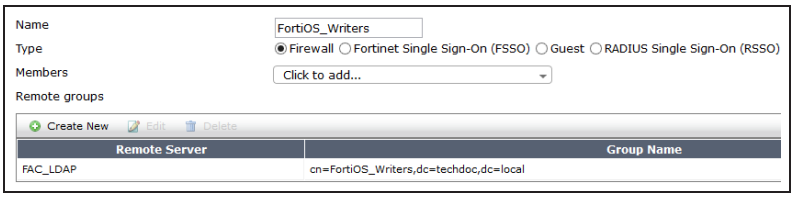
Go to **User & Device > Single Sign-On** and create a new SSO server. In the **Primary Agent IP/Name** field, enter the **Collector Agent IP Address** used in step 3. Likewise, enter the **Password** required for authentication.

Under the **Groups** tab, select the user groups to be monitored. In this example, the "FortiOS_Writers" group is used.



5. Adding a user group to the FortiGate

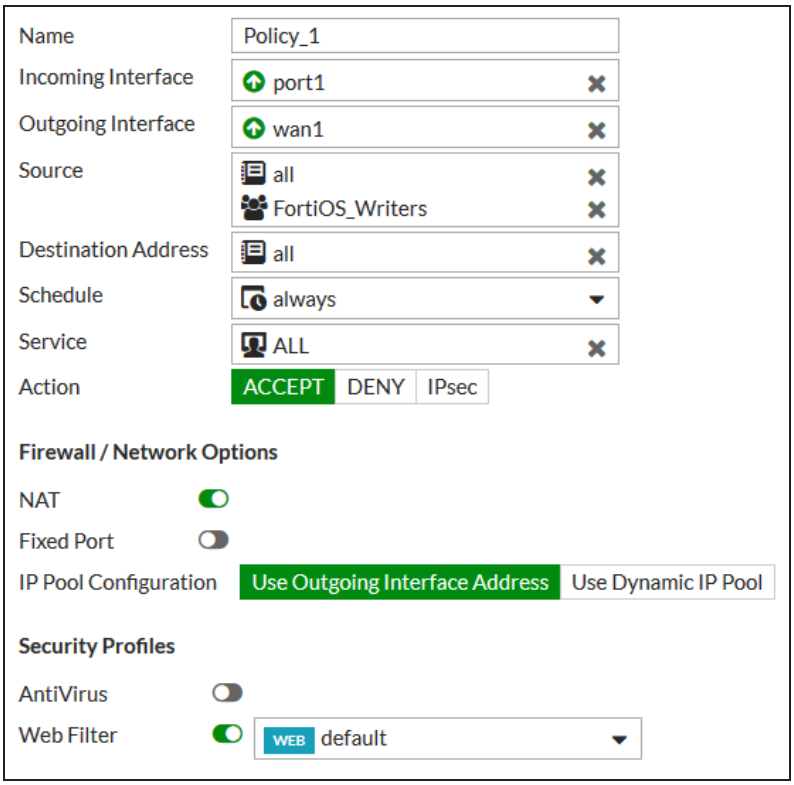
Go to **User & Device > User Groups** to create new user group. Under **Remote groups**, add the remote LDAP server created earlier in the FortiAuthenticator (in this example it's called "FAC_LDAP").



6. Adding a policy to the FortiGate

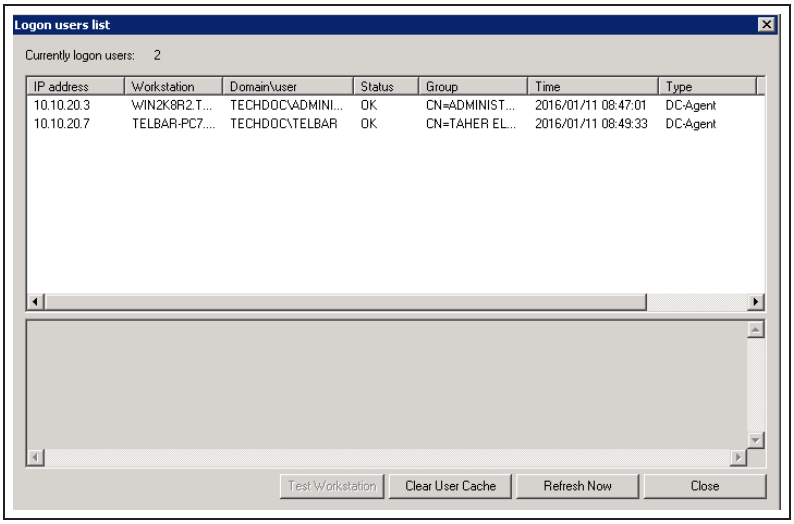
Go to **Policy & Objects > IPv4 Policy** and create a policy allowing "FortiOS_Writers" to navigate the Internet with appropriate security profiles.

The default **Web Filter** security profile is used in this example.



7. Results

Have users log on to the domain, go to the FSSO agent, and select **Show Logon Users.**



From the FortiGate, go to **Dashboard** to look for the **CLI Console** widget and type this command for more detail about current FSSO logons:

diagnose debug authd fsso list

----FSSO logons----
IP: 10.10.20.3 User: ADMINISTRATOR Groups: CN=FORTIOS WRITERS,CN=USERS,DC=TECHDOC,DC=LOCAL Workstation: WIN2K8R2.TECHDOC.LOCAL MemberOf: FortiOS_Writers
IP: 10.10.20.7 User: TELBAR Groups: CN=FORTIOS WRITERS,CN=USERS,DC=TECHDOC,DC=LOCAL Workstation: TELBAR-PC7.TECHDOC.LOCAL MemberOf: FortiOS_Writers
Total number of logons listed: 2, filtered: 0
----end of FSSO logons----

Have users belonging to the "FortiOS_ Writers" user group navigate the Internet. An authentication portal is presented to allow only authorized users. Security profiles will be applied accordingly.

Upon successful authentication, from the FortiGate, go to **Monitor > Firewall User Monitor** and verify FSSO Logons.

User Name	User Group	Duration	IP Address	Traffic Volume	Method
telbar	FortiOS_Writers	0 day(s) 0 hour(s) 0 minute(s)	10.10.20.7	849.04 kB	Firewall

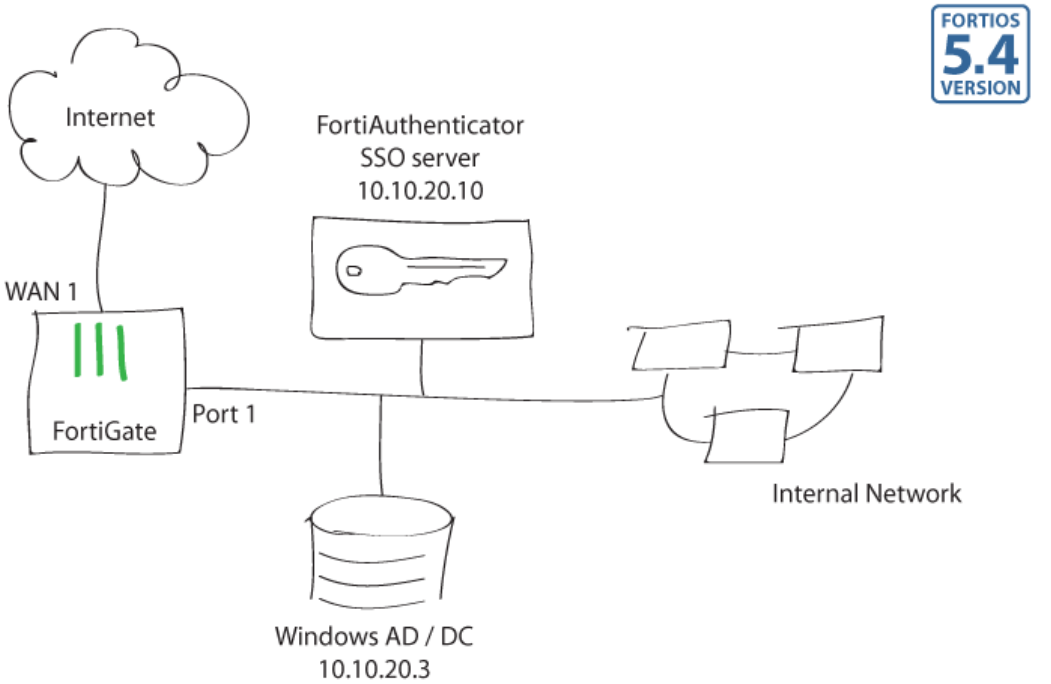
Go to **Log & Report > Forward Traffic** to verify the log.

#	@	Date/Time	Source	Destination	Application Name	Result	Policy
1		14:57:07	ADMINISTRATOR WIN2K8R2	8.8.8.8 (google-public-dns-a.google.com)	Google-DNS	85 B / 138 B	9
2		14:56:50	ADMINISTRATOR WIN2K8R2	8.8.8.8 (google-public-dns-a.google.com)	Google-DNS	80 B / 80 B	9
3		14:56:50	telbar 00:0c:29:a3:e1:b6	64.4.54.165 (urs.microsoft.com.nsatc.net)	HTTPS	1.69 kB / 6.71 kB	9
4		14:56:49	telbar 00:0c:29:a3:e1:b6	13.107.5.80 (api-bing-com.e-0001.e-msedge.net)	HTTP	1.96 kB / 3.12 kB	9
5		14:56:48	telbar 00:0c:29:a3:e1:b6	64.4.54.165 (urs.microsoft.com.nsatc.net)	HTTPS	1.56 kB / 6.68 kB	9

Select an entry for details.

#	3	**Action**	Accept: session close
Application Category	unscanned	**Date/Time**	14:56:50
Destination	64.4.54.165 (urs.microsoft.com.nsatc.net)	**Destination Country**	United States
Destination Interface	wan1	**Destination Port**	443
Device	00:0c:29:a3:e1:b6	**Device Type**	Windows PC
Duration	2	**Group**	FortiOS_Writers
Level		**Log ID**	13
Master Src MAC	00:0c:29:a3:e1:b6	**OS Name**	Windows
OS Version	7 or 8	**Policy**	9
Policy Type	policy	**Policy UUID**	1014caf4-3541-51e5-8733-9d89455a30ff
Protocol	tcp	**Protocol Number**	6
Received Bytes	6707	**Received Packets**	8
Sent Bytes	1685	**Sent Packets**	11
Service	HTTPS	**Session ID**	806372
Source	telbar 00:0c:29:a3:e1:b6	**Source Country**	Reserved
Source Interface	port1	**Source Port**	57084
Src NAT IP	172.20.120.22	**Src NAT Port**	57084
Sub Type	forward	**Timestamp**	1/11/2016, 2:56:50 PM
Tran Display	snat	**User**	telbar
Virtual Domain	root		

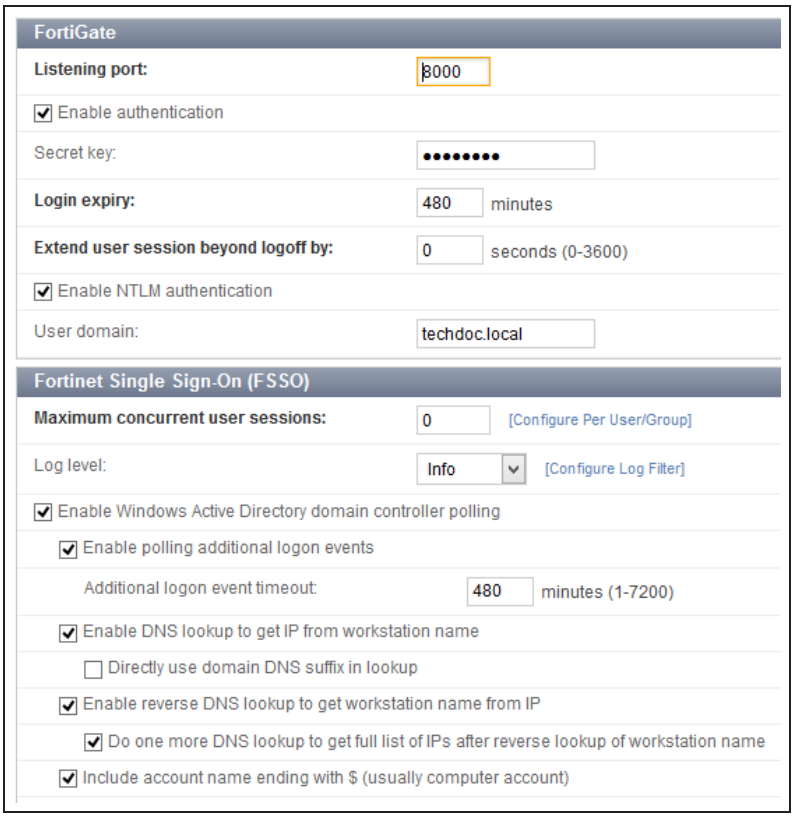
SSO using a FortiGate, FortiAuthenticator, and DC Polling



This recipe demonstrates FortiGate user authentication with a FortiAuthenticator as a Single Sign-On server. In this example, the FortiAuthenticator is configured to collect the user logon by polling the Domain Controller logs. User authentication controls Internet access.

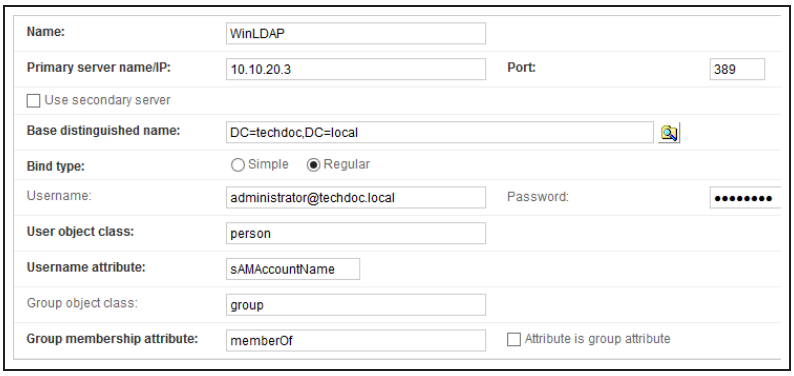
1. Configuring the FortiAuthenticator

Go to **Fortinet SSO Methods > SSO > General** and configure these general settings.



Go to **Fortinet SSO Methods > SSO > Domain Controllers** and add the Windows DC to the FortiAuthenticator.

Go to **Authentication > Remote Auth. Servers > LDAP** to set the Windows AD as an LDAP server. This will be useful to import **SSO Filtering Objects** from Windows AD to the FortiAuthenticator.

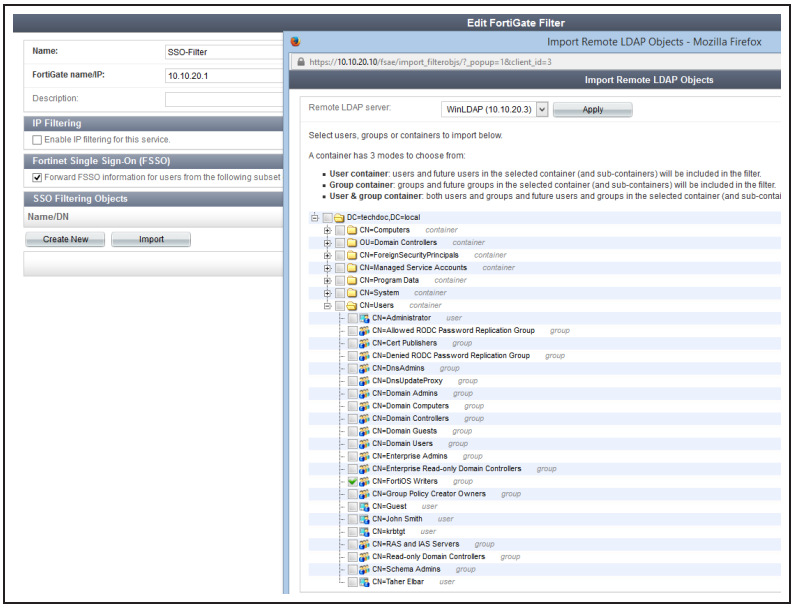


Go to **Fortinet SSO Methods > SSO > FortiGate Filtering** and create a new FortiGate Filter.

Under **Fortinet Single Sign-On (FSSO)**, enable **Forward FSSO information for users from the following subset of users/groups/containers only.**

Under **SSO Filtering Objects**, select **Import.** In the **Remote LDAP Server** field, select the LDAP server created in the previous step (WinLDAP in this example) and select **Apply**.

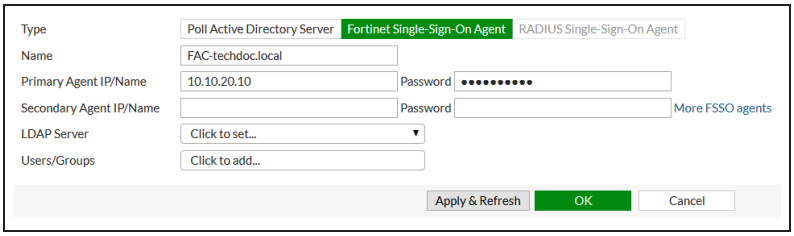
Next, select groups or containers to be imported, controlled, and monitored by the FortiAuthenticator. In this example, the "FortiOS Writers" user group is selected.



2. Configuring SSO on the FortiGate

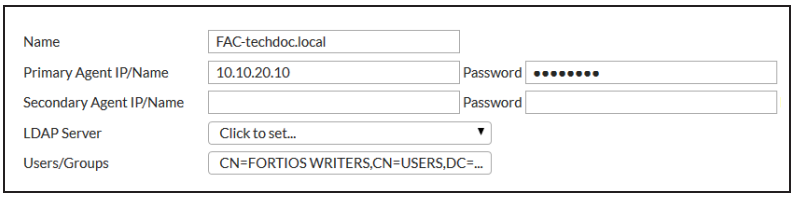
Go to **User & Device > Single Sign-On** and create a new SSO server.

In the **Type** field, select **Fortinet Single-Sign-On Agent** and set the **Name**, the **Primary Agent IP/Name,** the **Password** and select **Apply & Refresh**.



When selecting the **Users/Groups** field, the SSO user groups initially polled by the FortiAuthenticator from the Domain Controller appear.

In this example, only the "FortiOS Writers" group appears because of the **FortiGate Filtering** configuration in the previous step.



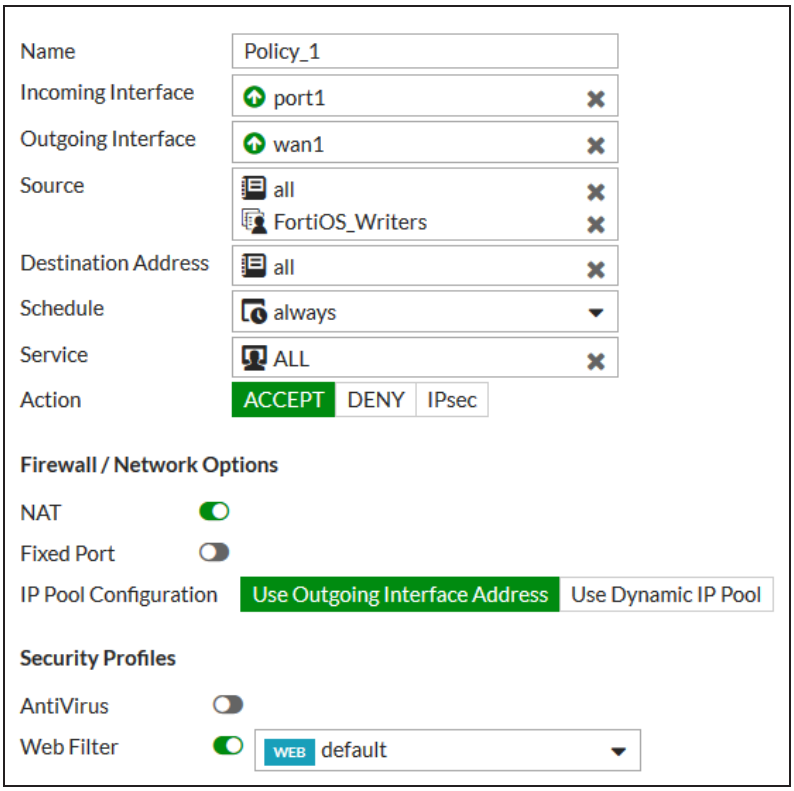
3. Creating a user group on the FortiGate

Go to **User & Device > User Groups** and create a new Fortinet Single Sign-On (FSSO) user group. Under **Members,** select the user group to be monitored. In this example only "FortiOS Writers" appears because of the **FortiGate Filtering** configured earlier.

4. Adding a policy on the FortiGate

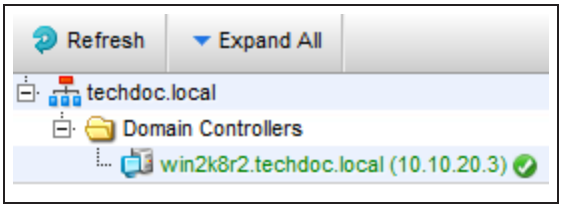
Go to **Policy & Objects > IPv4 Policy** and create a policy allowing "FortiOS_ writers" to navigate the Internet with appropriate security profiles.

The default **Web Filter** security profile is used in this example.



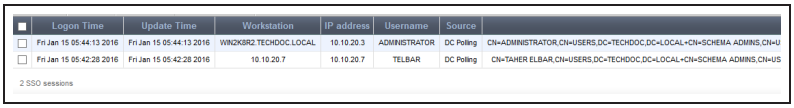
5. Results from the FortiAuthenticator

Go to **Monitor > SSO > Domains** to verify monitored domains. In this example "techdoc.local" is monitored by the FortiAuthenticator.



Have users log on to the domain.

Go to **Monitor > SSO > SSO Sessions** to verify SSO sessions.



Logon Time	Update Time	Workstation	IP address	Username	Source	
Fri Jan 15 05:44:13 2016	Fri Jan 15 05:44:13 2016	WIN2K8R2.TECHDOC.LOCAL	10.10.20.3	ADMINISTRATOR	DC Polling	CN=ADMINISTRATOR,CN=USERS,DC=TECHDOC,DC=LOCAL+CN=SCHEMA ADMINS,CN=U
Fri Jan 15 05:42:28 2016	Fri Jan 15 05:42:28 2016	10.10.20.7	10.10.20.7	TELBAR	DC Polling	CN=TAHER ELBAR,CN=USERS,DC=TECHDOC,DC=LOCAL+CN=SCHEMA ADMINS,CN=US

2 SSO sessions

Go to **Logging > Log Access > Logs** to verify logs.

15486	Wed Jan 13 15:42:08 2016	information	Event	Authentication	20994	Login	Success		Local administrator authentication with no token successful
15477	Wed Jan 13 11:43:45 2016	information	Event	Authentication	20001	Authentication	Success	FAC_LDAP	Local user authentication(chap) with no token successful
15476	Wed Jan 13 11:43:45 2016	information	Event	Authentication	20001	Authentication	Success	FAC_LDAP	Local user authentication(chap) with no token successful
15475	Wed Jan 13 11:43:44 2016	information	Event	Authentication	20001	Authentication	Success	FAC_LDAP	Local user authentication(chap) with no token successful

Select an entry for details.

Log Details

Log Record Detail	
ID	15477
Timestamp	Wed Jan 13 11:43:45 2016
Level	information
Action	Authentication
Status	Success
NAS Name/IP	FAC_LDAP
Message	Local user authentication(chap) with no token successful
User	telbar
Log Type	
Type Id	20001
Name	Authentication OK No FTK
Sub Category	Authentication
Category	Event
Description	Authentication successful without FortiToken

You can also verify FSSO users in the **User Inventory** widget under **System > Dashboard > Status.**

User Inventory

Users	Used: 2	Maximum allowed: 100	Available: 98	Disabled: 0
Groups	Used: 2	Maximum allowed: 10	Available: 8	
FortiToken 200	Used: 0	Populated: 0	Available: 0	Disabled: 0
FortiToken Mobile	Used: 0	Populated: 2	Available: 2	Disabled: 0
FSSO Users	Logged-in: 2	Max. allowed: 100	Available: 98	
FortiClient Workstations	Logged-in: 0	Maximum allowed: 5	Available: 5	

6. Results from the FortiGate

Upon successful authentication, go to **Monitor > Firewall User Monitor** and verify FSSO Logons.

User Name	User Group	Duration	IP Address	Traffic Volume	Method
ADMINISTRATOR	FortiOS_Writers	0 day(s) 0 hour(s) 16 minute(s)	10.10.20.3	4.17 kB	Fortinet Single Sign-On (FSSO)
TELBAR	FortiOS_Writers	0 day(s) 0 hour(s) 9 minute(s)	10.10.20.7	21.55 kB	Fortinet Single Sign-On (FSSO)

Have authenticated users navigate the Internet. Security profiles will be applied accordingly.

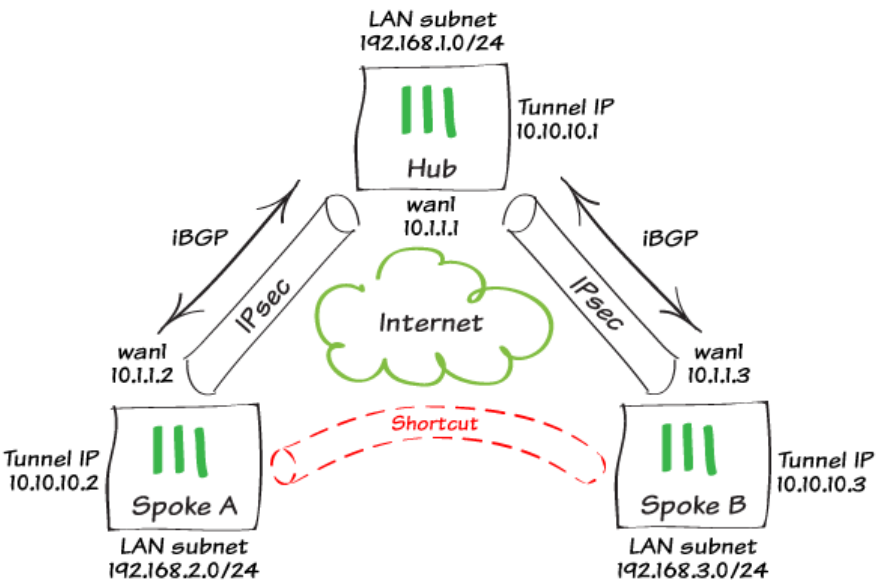
Go to **Log & Report > Forward Traffic** to verify the log.

#	@	Date/Time	Source	Destination	Application Name	Result	Policy
1		10:55:28	TELBAR 00:0c:29:a3:e1:b6	184.150.152.168 (www.google.ca)	Google-Web	680 B / 2.27 kB	9
2		10:55:24	TELBAR 00:0c:29:a3:e1:b6	184.150.152.168 (www.google.ca)	Google-Web	906 B / 3.03 kB	9
3		10:55:19	TELBAR 00:0c:29:a3:e1:b6	23.34.199.187 (e10088.dspb.akamaiedge.net)	Microsoft-Web	274 B / 248 B	9
4		10:55:19	TELBAR 00:0c:29:a3:e1:b6	184.150.158.11 (a.adroll.com)	HTTP	552 B / 454 B	9
5		10:55:19	TELBAR 00:0c:29:a3:e1:b6	13.107.5.80 (api.bing.com)	HTTP	1.31 kB / 1.55 kB	9
6		10:55:11	ADMINISTRATOR WIN2K8R2	8.8.8.8 (google-public-dns-a.google.com)	Google-DNS	73 B / 168 B	9
7		10:55:03	TELBAR 00:0c:29:a3:e1:b6	184.106.30.104 (distillery.wistia.com)	HTTP	856 B / 75 B	9

Select an entry for details.

#	2	**Action**	Accept: session close
Application Category	unscanned	**Date/Time**	10:55:24
Destination	184.150.152.168 (www.google.ca)	**Destination Country**	Canada
Destination Interface	wan1	**Destination Port**	80
Device	00:0c:29:a3:e1:b6	**Device Type**	Windows PC
Duration	110	**Group**	FortiOS_Writers
LAN In	906	**LAN Out**	3030
Level		**Log ID**	13
Master Src MAC	00:0c:29:a3:e1:b6	**OS Name**	Windows
OS Version	7 or 8	**Policy**	9
Policy Type	policy	**Policy UUID**	1014caf4-3541-51e5-8733-9d89455a30ff
Protocol	tcp	**Protocol Number**	6
Received Bytes	3030	**Received Packets**	9
Sent Bytes	906	**Sent Packets**	11
Service	HTTP	**Session ID**	469908
Source	TELBAR 00:0c:29:a3:e1:b6	**Source Country**	Reserved
Source Interface	port1	**Source Port**	60827
Src NAT IP	172.20.120.22	**Src NAT Port**	60827
Sub Type	forward	**Timestamp**	1/15/2016, 10:55:24 AM
Tran Display	snat	**User**	TELBAR
Virtual Domain	root	**WAN In**	3030
WAN Out	906		

Configuring ADVPN in FortiOS 5.4



In this recipe, we will explore a new VPN feature introduced in FortiOS 5.4.0: ADVPN.

ADVPN (Auto Discovery VPN) is an IPsec technology based on an IETF RFC draft (https://tools.ietf.org/html/draft-sathyanarayan-ipsecme-advpn-03). In simple terms, ADVPN allows a traditional hub and spoke VPN's spokes to establish dynamic, on-demand direct tunnels between each other so as to avoid routing through the topology's hub device. ADVPN requires the use of dynamic routing in order to function and FortiOS 5.4 supports both BGP and RIP. This recipe will focus on using BGP and its route-reflector mechanism as the dynamic routing solution to use with ADVPN.

ADVPN's primary advantages is that it provides the full meshing capabilities to a standard hub and spoke topology, greatly reducing the provisioning effort required for full spoke to spoke low delay reachability and addressing the scalability issues associated with very large fully meshed VPN networks.

BGP (and specifically, iBGP) is a natural fit for ADVPN as its route reflector mechanism resides on the VPN hub device and mirrors routing information from each spoke peer to each other. Furthermore, dynamic group peers result in near zero-touch hub provisioning when a new spoke is introduced in the topology.

As pictured, while the static configuration will involve both spoke FortiGate units to connect to our circular hub FortiGate, Spoke A will be able to establish a dynamic on-demand shortcut IPSec tunnel to Spoke B (and vice versa) if a host behind either spoke attempts to reach a host behind the other spoke. We will complete the configuration below and our verification step below will include reachability from 192.168.2.1 (spoke A) to 192.168.3.1 (spoke B) over the dynamically created shortcut link.

This recipe is documented in CLI as configuration such as BGP and ADVPN are best done using the command line interface. We are assuming basic IP and default routing configuration has been completed on the devices.

1. Configure the Hub FortiGate

Using the CLI, configure phase 1 parameters.

The auto-discovery commands enable the sending and receiving of shortcut messages to spokes (the hub is responsible for lettings the spokes know that they should establish those tunnels).

Note: aggressive mode is **not** supported currently for ADVPN.

```
config vpn ipsec phase1-interface
   edit "ADVPN"
       set type dynamic
       set interface "wan1"
       set proposal aes128-sha1
       set add-route disable
       set dhgrp 2
       set auto-discovery-sender enable
       set psksecret fortinet
   next
end
```

Configure the phase2 parameters.

This is a standard phase 2 configuration.

```
config vpn ipsec phase2-interface
   edit "ADVPN-P2"
       set phase1name "ADVPN"
       set proposal aes128-sha1
   next
end
```

Configure the tunnel interface IP.

ADVPN

```
config system interface
   edit "ADVPN"
       set vdom "root"
       set ip 10.10.10.1 255.255.255.255
       set type tunnel
       set remote-ip 10.10.10.254
       set interface "wan1"
   next
```

requires that tunnel IPs be configured on each device connecting to the topology. Those IP addresses need to be unique for each peer. A particularity of the hub is that it needs to define a bogus remote-IP address (10.10.10.254 in our example). This address should be unused in the topology and it will not be actually considered as part of the configuration for the hub.

```
end
```

Configure iBGP and route-reflection.

iBGP will be our overlay protocol of choice for enabling ADVPN communications. We are using an arbitrary private AS number (65000) in our example,

```
config router bgp
   set as 65000
   set router-id 10.10.10.1
   config neighbor-group
       edit "ADVPN-PEERS"
          set remote-as 65000
          set route-reflector-client enable
       next
   end
   config neighbor-range
       edit 1
          set prefix 10.10.10.0 255.255.255.0
          set neighbor-group "ADVPN-PEERS"
       next
   end
   config network
       edit 1
```

and configuring a dynamic client group to reduce provisioning requirements.

```
            set prefix 192.168.1.0 255.255.255.0
        next
    end
end
```

While we are advertising our LAN network directly ("config network" command), route redistribution is a perfectly valid alternative.

Configure basic policies to allow traffic to flow between the local network and the ADVPN VPN topology. As we generally desire traffic to be allowed between spokes in an ADVPN setup, we must remember to create a policy allowing spoke to spoke communications.

```
config firewall policy
    edit 0
        set name "OUT ADVPN"
        set srcintf "lan"
        set dstintf "ADVPN"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set status enable
    next
    edit 0
        set name "IN ADVPN"
        set srcintf "ADVPN"
        set dstintf "lan"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set status enable
    next
    edit 0
        set name "ADVPNtoADVPN"
        set srcintf "ADVPN"
        set dstintf "ADVPN"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
```

```
        set status enable
    next
end
```

2. Configure the Spoke FortiGates

Using the CLI, configure phase 1 parameters.

Note that we are configuring only one of the spokes in this example - the parameters that need to change for each spoke are highlighted in red.

```
config vpn ipsec phase1-interface
    edit "ADVPN"
        set interface "wan1"
        set proposal aes128-sha1
        set add-route disable
        set dhgrp 2
        set auto-discovery-receiver enable
        set remote-gw 10.1.1.1
        set psksecret fortinet
    next
end
```

Configure the phase2 parameters.

```
config vpn ipsec phase2-interface
    edit "ADVPN-P2"
        set phase1name "ADVPN"
        set proposal aes128-sha1
        set auto-negotiate enable
    next
end
```

Configure the tunnel interface IP.

Notice that on the spokes, the remote IP is actually used and points to the IP defined on the hub.

```
config system interface
    edit "ADVPN"
        set vdom "root"
        set ip 10.10.10.2 255.255.255.255
        set type tunnel
        set remote-ip 10.10.10.1
        set interface "wan1"
    next
end
```

Config iBGP.

```
config router bgp
    set as 65000
```

This is a static standard configuration and as stated for the hub, redistribution could be used instead of explicit route advertisement.

```
    set router-id 10.10.10.2
    config neighbor
        edit "10.10.10.1"
            set soft-reconfiguration enable
            set remote-as 65000
        next
    end
    config network
        edit 1
            set prefix 192.168.2.0 255.255.255.0
        next
    end
end
```

Configure a static route for the tunnel IP subnet.

This is an important special step for the spokes as they need a summary route that identifies all tunnel IP used over your topology to point towards the ADVPN interface. In our example, we use 10.10.10.0/24 (if our network planning expects less than 255 sites). Be sure to adequately plan this IP range as it needs to be hardcoded in the spokes.

```
config router static
    edit 3
        set dst 10.10.10.0 255.255.255.0
        set device "ADVPN"
    next
end
```

Configure policies.

```
config firewall policy
   edit 0
       set name "OUT ADVPN"
       set srcintf "lan"
       set dstintf "ADVPN"
       set srcaddr "all"
       set dstaddr "all"
       set action accept
       set schedule "always"
       set service "ALL"
       set status enable
   next
   edit 0
       set name "IN ADVPN"
       set srcintf "ADVPN"
       set dstintf "lan"
       set srcaddr "all"
       set dstaddr "all"
       set action accept
       set schedule "always"
       set service "ALL"
       set status enable
   next
end
```

Results

We can validate the behaviour of our configuration using a few commands. We are going to run these commands from SPOKE A.

get router info routing-table bgp will at a minimum display the learned routes from the topology. Note

```
B 192.168.1.0/24 [200/0] via 10.0.0.1, ADVPN, 22:30:21
B 192.168.3.0/24 [200/0] via 10.0.0.3 (recursive via 10.0.0.1), 22:30:21
```

the recursive routing - a result of our spoke's required static route. In this case, there has not been any traffic between our local subnet (192.168.2.0/24) and the other spoke's subnet, as the routes are both going through the hub.

However once we initiate a ping between both spokes, we obtain a different display of routing information - routing now goes through a newly established dynamic tunnel directly through the remote spoke rather than through the hub. The ping hiccup that occurs is the tunnel rerouting through a newly negotiated tunnel to the other spoke.

```
FG # exec ping-options source 192.168.2.1

FG # exec ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1): 56 data bytes
64 bytes from 192.168.3.1: icmp_seq=0 ttl=254 time=38.3 ms
64 bytes from 192.168.3.1: icmp_seq=1 ttl=254 time=32.6 ms
Warning: Got ICMP 3 (Destination Unreachable)
64 bytes from 192.168.3.1: icmp_seq=2 ttl=255 time=43.0 ms
64 bytes from 192.168.3.1: icmp_seq=3 ttl=255 time=31.7 ms
64 bytes from 192.168.3.1: icmp_seq=4 ttl=255 time=31.2 ms
--- 192.168.3.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 31.2/35.3/43.0 ms

FG # get router info routing-table bgp

B       192.168.1.0/24 [200/0] via 10.0.0.1, ADVPN, 22:34:13
B       192.168.3.0/24 [200/0] via 10.0.0.3, ADVPN_0, 00:02:28
```

Our routing

information now displays the remote subnet as being available through the spoke directly, through interface ADVPN_0, a dynamically instantiated interface going to that spoke.

Some additional data can be obtained using the very useful **diag vpn tunnel list** command. We are highlighting the aspects in the output which convey data specific to ADVPN, in this case the auto-discovery flag and the child-parent relationship of new instantiated dynamic tunnel interfaces.

```
FG # diag vpn tunnel list
list all ipsec tunnel in vd 0
-----------------------------------------------------
name=ADVPN_0 ver=1 serial=a 10.1.1.2:0->10.1.1.3:0
bound_if=6 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/0
  parent=ADVPN index=0
proxyid_num=1 child_num=0 refcnt=19 ilast=3 olast=604 auto-discovery=2
stat: rxp=7 txp=7 rxb=1064 txb=588
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=ADVPN-P2 proto=0 sa=1 ref=2 serial=1 auto-negotiate adr
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=3 options=2f type=00 soft=0 mtu=1438 expire=42680/0B
replaywin=2048 seqno=8 esn=0
  life: type=01 bytes=0/0 timeout=43152/43200
  dec: spi=9a487db3 esp=aes key=16 55e53d9fbc8dbeaa6df1032fbc80c4f6
  ah=sha1 key=20 a1470452c6a444f26a070add087f0d970c18e3a7
  enc: spi=3c37fea7 esp=aes key=16 8fd62a6745a9ba4fda062d4504b76851
  ah=sha1 key=20 44c606f1ef1bf5739ba62f6572031aa956974d0a
  dec:pkts/bytes=7/588, enc:pkts/bytes=7/1064
-----------------------------------------------------
name=ADVPN ver=1 serial=9 10.1.1.2:0->10.1.1.1:0
bound_if=6 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/0
proxyid_num=1 child_num=1 refcnt=22 ilast=8 olast=8 auto-discovery=2
stat: rxp=3120 txp=3120 rxb=399536 txb=191970
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=12
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=ADVPN-P2 proto=0 sa=1 ref=2 serial=1 auto-negotiate adr
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA: ref=3 options=2f type=00 soft=0 mtu=1438 expire=4833/0B
```

```
replaywin=2048
seqno=5ba esn=0
  life: type=01 bytes=0/0 timeout=43148/43200
  dec: spi=9a487db2 esp=aes key=16 4f70d27edad656cfcacbae61b23d4b11
  ah=sha1 key=20 b19ea87c90dd92d1cab58cbf24ae8fe12ee927cb
  enc: spi=b3dde355 esp=aes key=16 efbb4440df75018610b4ba8f5756167d
  ah=sha1 key=20 81cc9cee3bee1c2dba0eb1e7ac66e9d34b67bde9
  dec:pkts/bytes=1465/90152, enc:pkts/bytes=1465/187560
-------------------------------------------------------
```

Glossary

BGP: Border Gateway Protocol is primarily used to connect the networks of large organizations that have two or more ISP connections, or between other autonomous systems. If used in such a situation, a FortiGate can use BGP for routing.

BYOD: Bring Your Own Device (also called device management) is the practice of allowing network users to access an organization's (usually wireless) network with their own computers, smart phones, tablets and other devices. BYOD has a major impact on networks with large and diverse user bases, such as educational institutions, but also affects large and small business networks.

CA: A certificate authority (CA) is an entity that issues digital certificates, which are used to establish secure connections over a network, typically the Internet. The CA acts as a trusted third-party by verifying the identity of a certificate's owner: for example, the certificate found when you go to https://www.facebook.com is verified as belonging to Facebook.

Certificates: In networking, certificates (including public key certificates, digital certificates, and identity certificates) provide digital signatures for websites or other electronic communication and allow you to verify whether a digital identity is legitimate.. A FortiGate can use certificates for many things, including SSL inspection and user authentication.

CLI: The Command Line Interface is a text-based interface used to configure a FortiGate unit. Most steps in the FortiGate Cookbook use the Graphical User Interface (see GUI), but some configuration options are only available using the CLI.

DHCP: Dynamic Host Configuration Protocol is a networking protocol that allows devices to request network parameters, such as IP addresses, automatically from a DHCP server, reducing the need to assign these settings manually. A FortiGate can function as a DHCP server for your network and can also receive its own network parameters from an external DHCP server.

Dial-up/dynamic VPN: A dial-up VPN, also called a dynamic VPN, is a type of IPsec VPN where one of the endpoints has a dynamic IP address.

DMZ: A Demilitarized Zone is an interface on a FortiGate unit that provides external users with secure access to a protected subnet on the internal network without giving them access to other parts of the network. This is most commonly done for subnets containing web servers, which must be accessible from the Internet. The DMZ interface will only allow traffic that has been explicitly allowed in the FortiGate's configuration. FortiGate models that do not have a DMZ interface can use other interfaces for this purpose.

DNS: Domain Name System is used by devices connecting to the Internet to locate websites by mapping a domain name to a website's IP address. For example, a DNS server maps the domain name www.fortinet.com to the IP address 66.171.121.34. Your FortiGate unit controls which DNS servers the network uses. A FortiGate can also function as a DNS server.

DSR: In a typical load balancing scenario, server responses to client requests are routed through a load balancer on their way back to the client. The load balancer examines the headers of each response and can insert a cookie before sending the server response on to the client. In a Direct Server Return (DSR) configuration, the server receiving a client request responds directly to the client IP, bypassing the load balancer. Because the load balancer only processes incoming requests, load balancing performance is dramatically improved when using

DSR in high bandwidth applications. In such applications, it is not necessary for the load balancer to receive and examine the server's responses. So the client makes a request and the server simply streams a large amount of data to the client.

Dynamic IP address: A dynamic IP address is one that can change without the device's user having to do anything. Dynamic IP addresses allow networks to control the IP addresses of devices that connect to them. This allows you to connect portable devices to different networks without needing to manually change their IP addresses.

Dynamic IP addresses are set by network protocols, most often DHCP.

ECMP: Equal Cost Multipath Routing allows next-hop packet forwarding to a single destination to occur over multiple best paths that have the same value in routing metric calculations. ECMP is used by a FortiGate for a variety of purposes, including load balancing.

Explicit Proxy: Explicit proxy is a type of configuration where all clients are configured to allow requests to go through a proxy server, which is a server used as an intermediary for requests from clients seeking resources from other servers. When a FortiGate uses explicit proxy, the clients sending traffic are given the IP address and port number of the proxy server.

FortiAP: A FortiAP unit is a wireless Access Point that can be managed by a FortiGate. Most FortiAP functions can also been accomplished using a FortiWiFi unit.

FortiClient: The FortiClient software provides a variety of features, including antivirus, web filtering, firewall, and parental controls, to individual computers and mobile devices. It can also be used to connect to a FortiGate using either an SSL or IPsec VPN.

FortiClient is available for Windows, Mac OSX, iOS, and Android, and can be set up quickly. After being installed, it automatically updates its virus definition files, does a full system scan once per week, and much more.

FortiClient can be downloaded at www.forticlient.com.

FortiOS: FortiOS is the operating system used by FortiGate and FortiWiFi units. It is also referred to as firmware.

FTP: File Transfer Protocol is a standard protocol used to transfer computer files from one host to another host over a computer network, usually the Internet, using FTP client and server applications.

Gateway: A gateway is the IP address that traffic is sent to if it needs to reach resources that are not located on the local subnet. In most FortiGate configurations, a default route using a gateway provided by an Internet service provider must be set to allow Internet traffic.

GUI: The Graphical User Interface, also known as the web-based manager, is a graphics-based interface used to configure a FortiGate unit and is an alternative to using the Command Line Interface (see CLI). You can connect to the GUI using either a web browser or FortiExplorer. Most steps in the FortiGate Cookbook use the GUI.

Hardware switch: A hardware switch is a virtual interface that groups different interfaces together, allowing a FortiGate to treat the group as a single interface. Many FortiGate models have a default hardware switch, called either lan or internal.

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.

ISFW: An Internal Segmentation Firewall (ISFW) is a FortiGate in that sits at strategic internal points of the internal network, rather than on the network edge. This allows extra security measures to be taken around key network components, such a servers that contain valuable intellectual property.

IP address: An Internet Protocol address is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication. FortiGate units can use IP addresses to filter traffic and determine whether to allow or deny traffic. Both IP version 4 and IP version 6 (see IPv4 and IPv6) are supported by your FortiGate.

IPsec: Internet Protocol Security is used to for securing IP communications by authenticating and encrypting each packet of a session. A FortiGate primarily uses this protocol to secure virtual private networks (see VPN).

IPv4: Internet Protocol version 4 is the fourth version of the Internet Protocol (IP), the main protocol used for communication over the Internet. IPv4 addresses are 32-bit and can be represented in notation by 4 octets of decimal digits, separated by a period: for example, 172.16.254.1.

IPv6: Internet Protocol version 6 is the sixth version of the Internet Protocol (IP), the main protocol used for communication over the Internet (IPv5 never became an official protocol). IPv6 was created in response to the depletion of available IPv4 addresses. IPv6 addresses are 128-bit and can be represented in notation by 8 octets of hexadecimal digits, separated by a colon: for example, 2001:db8:0000:0000:0000:0000:0000:0000. IPv6 addresses can be shortened if all the octets are 0000; for example, the previous address can also be written as 2001:db8::

LAN/internal: The LAN/internal interface is an interface that some FortiGate models have by default. This interface contains a number of physical ports that are all treated as a single interface by the FortiGate unit. This allows you to configure access for the entire Local Area Network at the same time, rather than configuring each port individually.

LDAP: Lightweight Directory Access Protocol is a protocol used for accessing and maintaining distributed directory information services over a network. LDAP servers are commonly used with a FortiGate for user authentication.

MAC address: A Media Access Control address is a unique identifier assigned to a network interface used for network communication. A MAC address is assigned to a device by the manufacturer and so this address, unlike an IP address, is not normally changed. MAC addresses are represented in notation by six groups of two hexadecimal digits, separated by hyphens or colons: for example, 01:23:45:67:89:ab. Your FortiGate can identify network devices using MAC addresses.

Multicast: Multicast is a method of group communication where information is addressed to a group of destinations simultaneously. A FortiGate can use multicast traffic to allow communication between network devices.

NAT: Network Address Translation is a process used to modify, or translate, either the source or destination IP address or port in a packet header. The primary use for NAT is to allow multiple network devices on a private network to be represented by a single public IP address when they browse the internet. FortiGate also supports many other uses for NAT.

Packet: A packet is a unit of data that is transmitted between communicating devices. A packet contains both the message being sent and control information, such as the source address (the IP address of the device that sent the packet) and the destination address (the IP address of the device the packet is being sent to).

Ping: Ping is a utility used to test whether devices are connected over a IP network and to measure how long it takes for a reply to be received after the message is sent, using a protocol called Internet Control Message Protocol (ICMP). If ICMP is enabled on the destination interface, you can ping the IP address of a FortiGate interface to test connectivity between your computer and the FortiGate. You can also use the CLI command `execute ping` to test connectivity between your FortiGate and both internal and external devices.

Ports: See Interfaces and Port Numbers.

Port numbers: Port numbers are communication endpoints used to allow network communication. Different ports are used for different application-specific or process-specific purposes; for example, HTTP protocol commonly uses port 80.

Pre-shared key: In cryptography, a pre-shared key is a character string (like a password) known by two parties, and used by those parties to identify each other. Pre-shared keys are commonly used for granting access to IPsec VPNs and WiFi networks.

Pre-shared keys are different from regular passwords because they are not normally associated with a specific individual's credentials.

RADIUS: Remote Authentication Dial In User Service is a protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service. RADIUS servers are commonly used with a FortiGate for user authentication, including single-sign on.

RTSP: The Real Time Streaming Protocol is a media control protocol that is used for controlling streaming audio and video streams. RTSP has a wide range of uses and is often leveraged by other media-related services such as SIP. It most commonly uses TCP and UDP port 554 but additional ports are used by the actual media controlled by RTSP.

FortiOS includes an RSTP session helper that opens the ports used by individual RTSP-controlled streams. FortiRecorder and FortiCamera use RTSP for video streaming.

SCTP: The Stream Control Transmission Protocol is a transport layer protocol (protocol number 132) used most often for sending telephone signalling messages over carrier IP networks.

Session: A session is the dialogue between two or more communicating devices that include all messages that pass between the devices; for example, a session is created when a user browses to a specific website on the Internet for all communication between the user's computer and the web server that hosts the site. Sessions are tracked by a FortiGate unit in order to create logs about the network traffic.

SIP: Session Initiation Protocol is used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol networks. FortiGate units use this protocol for voice over IP (see VoIP).

Site-to-site VPN: A site-to-site VPN allows two networks that are each behind a VPN gateway (for example, a FortiGate unit), to establish secure connections with each other over a public network, typically the Internet.

Site-to-site VPNs most often use IPsec and can be established between two FortiGates, or between a FortiGate and any other IPsec VPN gateway, such as a Cisco ASA or Microsoft Azure.

SLAAC: Stateless Address Autoconfiguration is a feature of IPv6 that allows devices on an IPv6 network to automatically get IPv6 addresses. SLAAC is similar to DHCP except that DHCP requires you to run and configure a DHCP server. SLAAC is built into IPv6 and requires only minor additional configuration. SLAAC is defined by RFC 2462.

SNMP: Simple Network Management Protocol is a protocol that monitors hardware on your network. A FortiGate can use SNMP to monitor events such as high CPU usage, VPN tunnels going down, or hardware becoming disconnected.

SSH: Secure Shell is a protocol used for secure network services between two devices, including remote command-line access. SSH can be used to access a FortiGate's command line interface (CLI).

SSID: A Service Set Identifier is the name that a wireless access point broadcasts to wireless users. Wireless users select this name to join a wireless network.

SSL: Secure Sockets Layer is a protocol for encrypting information that is transmitted over a network, including the Internet. SSL can be used for secure communications to a FortiGate, as well as for encrypting Internet traffic (see HTTPS) and for allowing remote users to access a network using SSL virtual private network (see VPN).

SSL inspection: Secure Sockets Layer inspection is used by your FortiGate to scan traffic or communication sessions that use SSL for encryption, including HTTPS protocol.

SSO: Single Sign-On is a feature that allows a user to login just once and remembers the credentials to re-use them automatically if additional authentication is required. A FortiGate supports both Fortinet single sign-on (FSSO) and single sign-on using a RADIUS server (RSSO).

Static IP address: Static IP addresses require user intervention to change. Normally a device that always has a wired connection to an Ethernet network has a static IP address.

Static route: A static route is a manually-configured routing entry that is fixed and does not change if the network is changed or reconfigured.

Subnet: A subnetwork, or subnet, is a segment of the network that is separated physically by routing network devices and/or logically by the difference in addressing of the nodes of the subnet from other subnets. Dividing the network into subnets helps performance by isolating traffic from segments of the network where it doesn't need to go, and it aids in security by isolating access. The addressing scope of a subnet is defined by its IP address and subnet mask and its connection to other networks is achieve by the use of gateways.

Subnet Mask: A subnet mask is the part of an IP address that is used to determine if two addresses are on the same subnet by allowing any network enabled device, such as a FortiGate, to separate the network address and the host address. This lets the device determine if the traffic needs to be sent through a gateway to an external network or if it is being sent to host on the local network.

URL: A Uniform Resource Locator is a text string that refers to a network resource. The most common use for URLs is on the Internet, where they are also known as web addresses.

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

VDOM: Virtual Domains are used to divide a single FortiGate unit into two or more virtual instances of FortiOS that function separately and can be managed independently.

VLAN: Virtual Local Area Networks are used to logically divide a single local area network (LAN) into different parts that function independently. A FortiGate uses VLANs to provide different levels of access to users connecting to the same LAN.

VoIP: Voice over Internet Protocol is a protocol that is used to allow voice communications and multimedia sessions over Internet Protocol sessions, including the Internet. VoIP protocol is used by a FortiGate when traffic needs to reach a connected VoIP phone or FortiVoice unit.

VPN: A Virtual Private Network is a private network that acts as a virtual tunnel across a public network, typically the Internet, and allows remote users to access resources on a private network. There are two main types of VPNs that can be configured using a FortiGate unit: IPsec VPN (see IPsec) and SSL VPN (see SSL).

WAN/WAN 1: The WAN or WAN1 port on your FortiGate unit is the interface that is most commonly used to connect the FortiGate to a Wide Area Network, typically the Internet. Some FortiGate models have a WAN2 port, which is commonly used for redundant Internet connections.

The FortiGate Cookbook contains a variety of step-by-step examples of how to integrate a FortiGate unit into your network and apply features such as security profiles, wireless networking, and VPN.

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

Written for FortiOS 5.4

Fortinet.com