

FORTINET®



The FortiGate
Cookbook
Recipes for Success with your FortiGate

FortiOS 5.2



Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

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	5
Introduction	6
Tips	7
Getting Started	9
Choosing your FortiGate's switch mode	10
Installing a FortiGate in NAT/Route mode	11
Installing a FortiGate in Transparent mode	17
Quick installation using DHCP	23
Redundant Internet connections	27
Troubleshooting your FortiGate installation	33
FortiGate registration and basic settings	37
Updating your FortiGate's firmware	42
Setting up FortiGuard services	45
FortiGuard troubleshooting	51
Logging FortiGate traffic	52
Troubleshooting FortiGate logging	56
Logging with FortiCloud	57
Creating security policies	62
Limited access administrator accounts	68
Port pairing in Transparent mode	73
Port forwarding	78
FortiGuard DDNS	84
SNMP monitoring	87
Packet capture	94
VDOM configuration	98
High Availability with two FortiGates	105
AirPlay for Apple TV	112
Protect a web server with DMZ	117

Traffic shaping for VoIP	122
Security	131
Blocking P2P traffic and YouTube applications	132
Blocking Windows XP traffic	139
Blocking and monitoring Tor traffic	144
Controlling access to Apple's App Store	149
Restricting online gaming to evenings	154
Preventing data leaks	160
Prevent credit card numbers from being leaked	165
Protecting a web server	169
Logging DNS domain lookups	174
Why you should use SSL inspection	179
Preventing certificate warnings	182
Blocking Facebook	194
Web rating overrides	199
Web filtering using quotas	204
Blocking Google access for consumer accounts	209
Overriding a web filter profile	212
Troubleshooting web filtering	218
WiFi	219
Setting up WiFi with FortiAP	220
Setting up a WiFi bridge with a FortiAP	225
Combining WiFi and wired networks with a software switch	229
WiFi network with external DHCP service	233
Providing remote access to the office and Internet	237
Extending WiFi range with mesh topology	243
Guest WiFi accounts	249
Captive portal WiFi access control	254
WP2A WiFi access control	259

WiFi with external RADIUS authentication	263
MAC access control	268
BYOD scheduling	273
BYOD for a user with multiple wireless devices	277
Explicit proxy with web caching	281
Authentication	287
User and device authentication	288
Excluding users from security scanning	295
FSSO in Polling mode	299
Two-factor authentication with FortiToken Mobile	306
VPNs	313
IPsec VPN for iOS devices	314
IPsec VPN with FortiClient	322
IPsec VPN with the native Mac OS client	328
Site-to-site IPsec VPN with two FortiGates	335
IPsec VPN to Microsoft Azure	341
Remote Internet browsing using a VPN	351
Remote browsing using site-to-site IPsec VPN	359
IPsec troubleshooting	366
SSL VPN for remote users	368
SSL VPN for Windows Phone 8.1	379
SSL VPN using FortiClient for iOS	385
SSL VPN troubleshooting	391
IPv6	393
Creating an IPv6 interface using SLAAC	394
Fortinet Integration	398
FortiExtender installation	399
Remotely accessing FortiRecorder through a FortiGate	405
Expert	417

Redundant architecture	418
BGP over a dynamic IPsec VPN	431
SLBC setup with one FortiController	438
SLBC Active-Passive setup with two FortiControllers	443
SLBC Active-Passive with two FortiControllers and two chassis	451
SLBC Dual Mode setup with two FortiControllers	465
SLBC Active-Passive with four FortiControllers and two chassis	473
Hub-and-spoke VPN using quick mode selectors	492
Glossary	503

Change Log

Date	Change description
May 12, 2015	Initial publication

Introduction

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

The FortiGate recipes is divided into the following sections:

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

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

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

Tips

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

Understanding the basics

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

Screenshots vs. text

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

Model and firmware

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

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

Ports

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

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

IP addresses and object names

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

Text elements

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

Selecting OK/Apply

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

IPv4 vs IPv6 policies

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

Turning on FortiOS features

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

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

Getting Started

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

Installation

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

Setting up your FortiGate

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

Common configurations

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

Choosing your FortiGate's switch mode

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

What is the internal switch mode?

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

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

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

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

Which mode is your FortiGate in by default?

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

How do you change the mode?

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

1. Command to change the FortiGate to switch mode:

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

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

Installing a FortiGate in NAT/Route mode

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

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

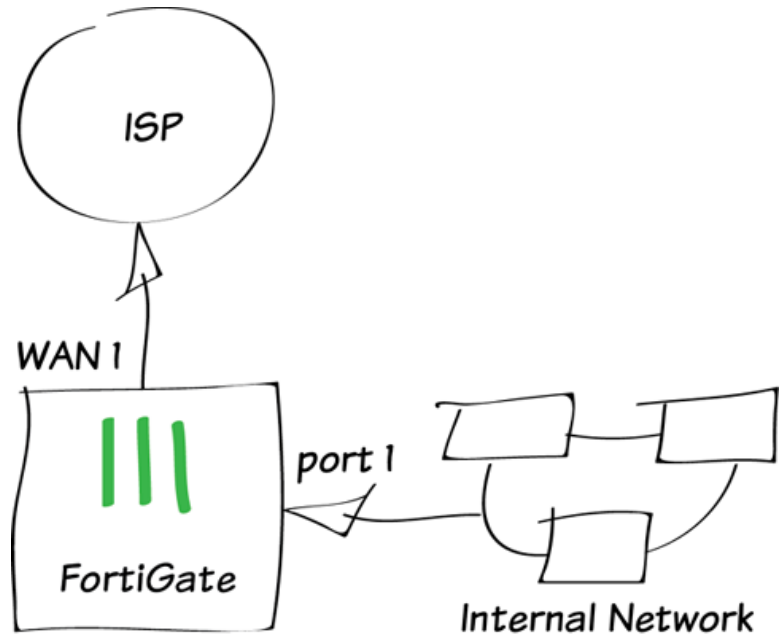
If you have not already done so, ensure that your FortiGate is using the correct internal switch mode. For more information, see [Choosing your FortiGate's switch mode](#).

A video of this recipe is available [here](#).

1. Connecting the network devices and logging onto the FortiGate

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

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



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

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

A screenshot of a web-based login interface. It features a light gray background with a subtle geometric pattern. In the center, there are two input fields. The first is labeled 'Name' and contains the text 'admin'. The second is labeled 'Password' and is empty. Below the input fields is a red button with the text 'Login' in white.

2. Configuring the FortiGate's interfaces

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

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

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

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

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

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

Interface Name	wan1(08:5B:0E:31:74:13)
Alias	<input type="text"/>
Link Status	Up
Type	Physical Interface
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicate to Extension Device
IP/Network Mask	<input type="text" value="192.168.0.12/255.255.255.0"/>

Interface Name	internal(08:5B:0E:31:74:12)
Alias	<input type="text"/>
Link Status	Up
Type	Physical Interface
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicate to Extension Device
IP/Network Mask	<input type="text" value="172.20.120.99/255.255.255.0"/>

3. Adding a default route

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

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

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

Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Device	<input type="text" value="wan1"/>
Gateway	<input type="text" value="192.168.0.1"/>
Distance	<input type="text" value="10"/> (1-255, Default=10)
Priority	<input type="text" value="0"/> (0-4294967295)
Comments	<input type="text" value="Write a comment..."/> 0/255

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

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

DNS Settings	
<input type="radio"/> Use FortiGuard Servers	<input checked="" type="radio"/> Specify
Primary DNS Server	<input type="text" value="208.91.123.53"/>
Secondary DNS Server	<input type="text" value="208.91.123.52"/>
Local Domain Name	<input type="text"/>

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

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

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

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

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

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

Incoming Interface	internal	+
Source Address	all	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	wan1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	
Firewall / Network Options		
<input checked="" type="checkbox"/> NAT		
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	Click to add...	

Logging Options

Log Allowed Traffic

Security Events

All Sessions

Capture Packets

6. Results

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

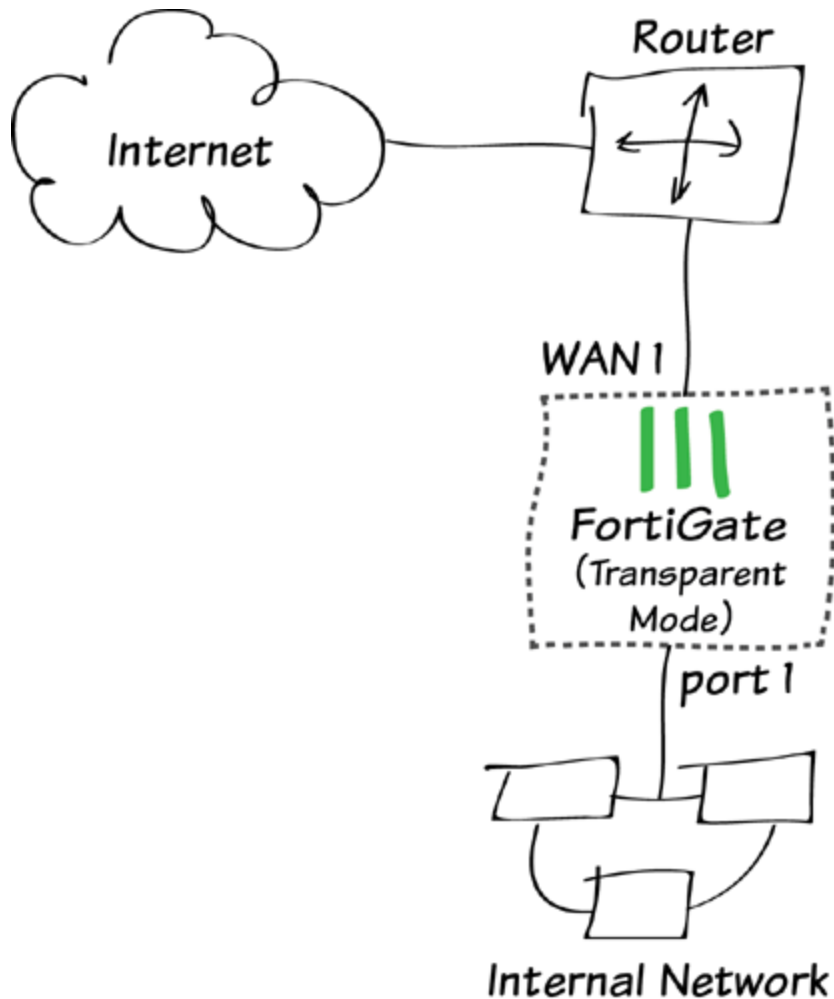
You can view information about the traffic being processed by your FortiGate by going to **System > FortiView > All Sessions** and finding traffic that has the **internal** interface as the **Src Interface** and the Internet-facing interface as the **Dst Interface**.

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

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

For further reading, check out [Installing a FortiGate in NAT/Route Mode in the FortiOS 5.2 Handbook](#).

Installing a FortiGate in Transparent mode



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

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

A video of this recipe is available [here](#).

1. Changing the FortiGate's operation mode

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

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

System Information	
HA Status	Standalone [Configure]
Host Name	FG100D3G12812324 [Change]
Serial Number	FG100D3G12812324
Operation Mode	NAT [Change]
System Time	Tue Jul 15 09:04:33 2014 (FortiGuard) [Change]
Firmware Version	v5.2.0,build0589 (GA) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	19 day(s) 2 hour(s) 14 min(s)
Virtual Domain	Disabled [Enable]

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

Operation Mode	Transparent ▾
Management IP/Netmask	172.20.120.122/255.255.255.0
Default Gateway	172.20.120.2

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

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

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

DNS Settings	
<input type="radio"/> Use FortiGuard Servers	<input checked="" type="radio"/> Specify
Primary DNS Server	208.91.123.53
Secondary DNS Server	208.91.123.52
Local Domain Name	

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

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

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

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

Incoming Interface	port1	+
Source Address	all	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	any	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	

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

Logging Options	
<input checked="" type="checkbox"/>	Log Allowed Traffic
<input type="checkbox"/>	Security Events
<input checked="" type="checkbox"/>	All Sessions
<input type="checkbox"/>	Capture Packets

4. Connecting the network devices

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

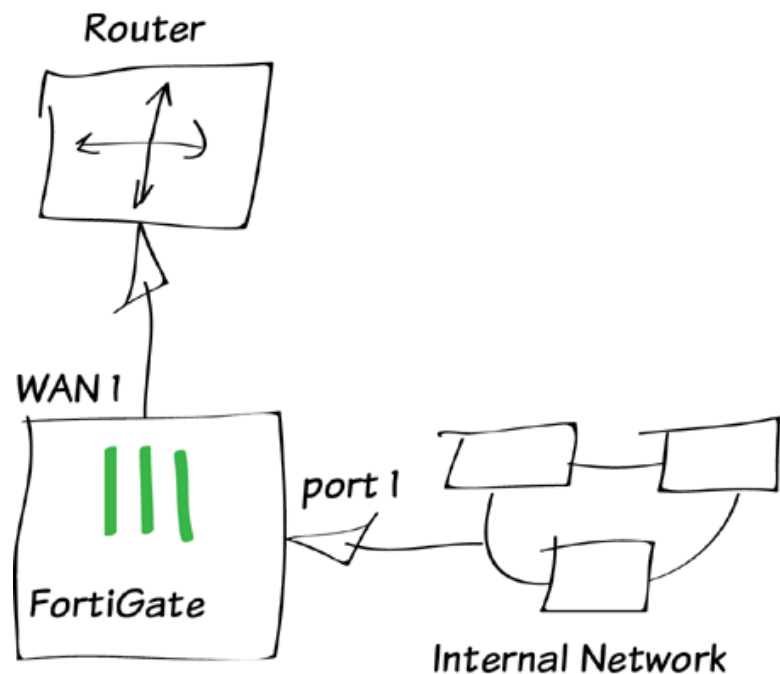
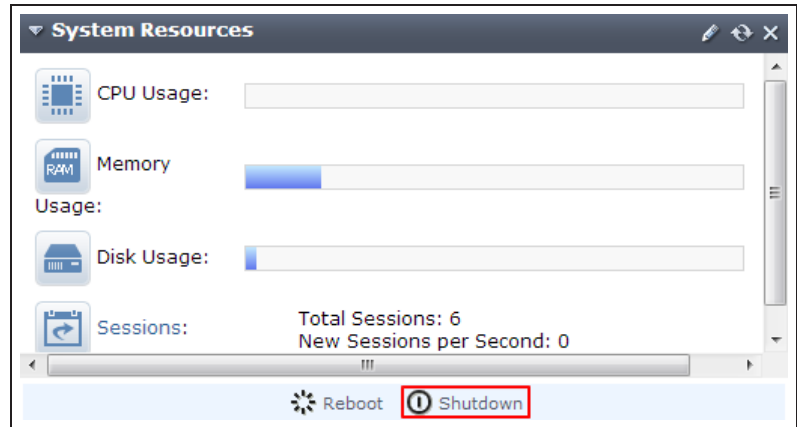
Alternatively, you can enter the following command in the **CLI Console** (also found by going to **System > Dashboard > Status**):
`execute shutdown`

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

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

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

Power on the FortiGate unit.



5. Results

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

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

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

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

Column Settings
✕

Available fields:

- Application
- Device
- Dst Address
- Dst NAT
- Dst NAT Address
- Dst NAT Port
- Dst Port
- Duration
- Policy ID
- Protocol
- Src
- Src Address
- Src NAT
- Src NAT Address
- Src NAT Port
- Src Port
- Timeout
- User Name

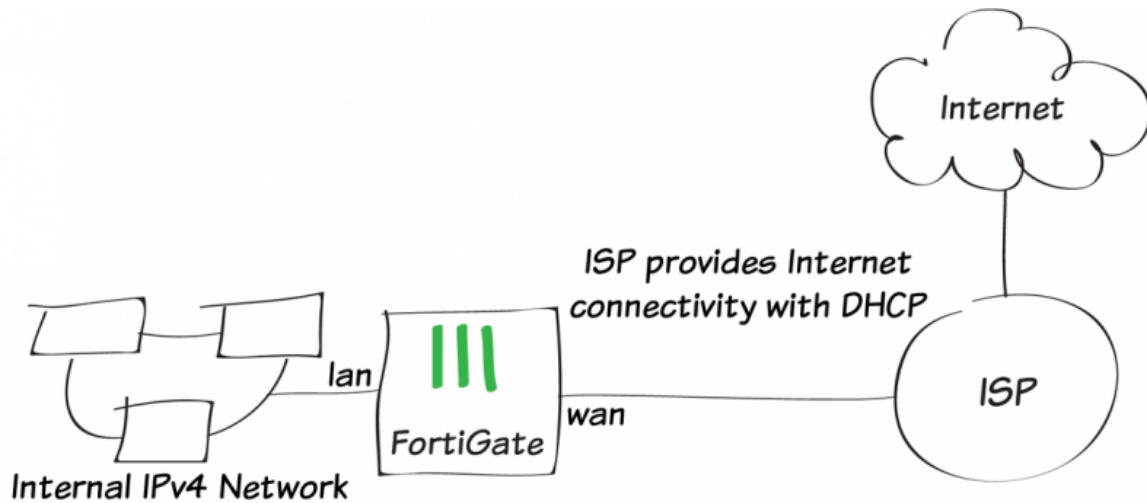
Show these fields in this order:

- Src Interface
- Dst Interface
- Dst
- Bytes

Default
OK
Cancel

For further reading, check out [Installation](#) in the [FortiOS 5.2 Handbook](#).

Quick installation using DHCP



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

This recipe has the following requirements:

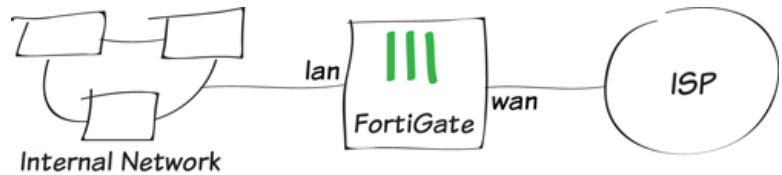
- An ISP that provides connectivity with DHCP and accepts DHCP requests without authentication.
- A FortiGate with a default configuration that includes a DHCP server on the lan (or internal) interface and a security policy that securely allows all sessions from the Internal network to reach the Internet.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

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

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

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

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



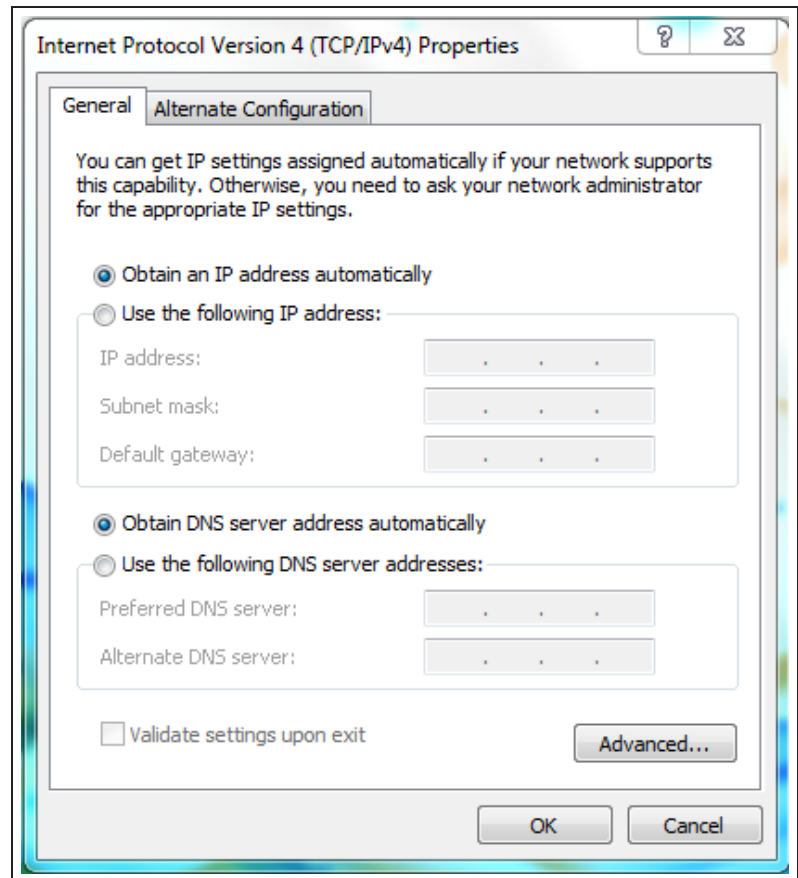
2. Configuring your PCs to use DHCP

Windows Vista/7/8:

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

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

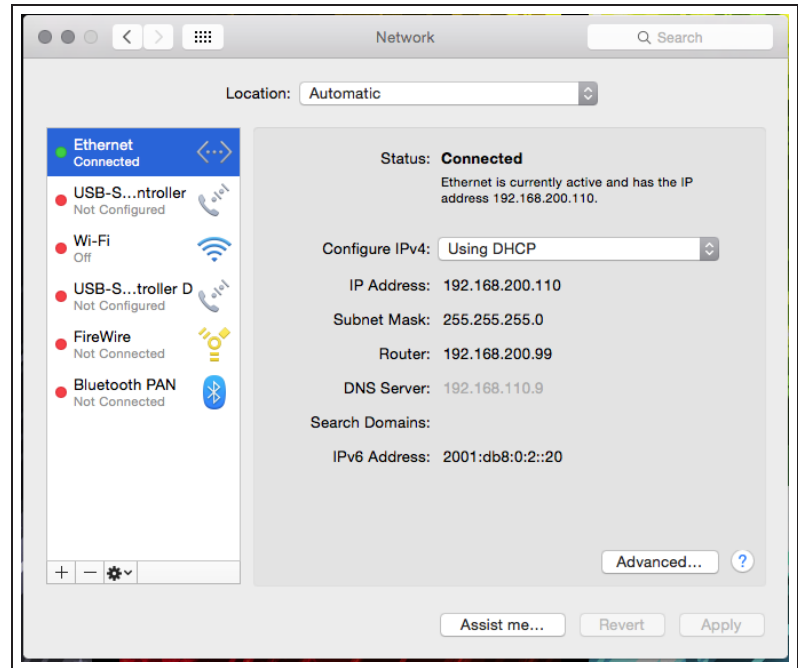
Select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.



Mac OS X

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

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



3. Results

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

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

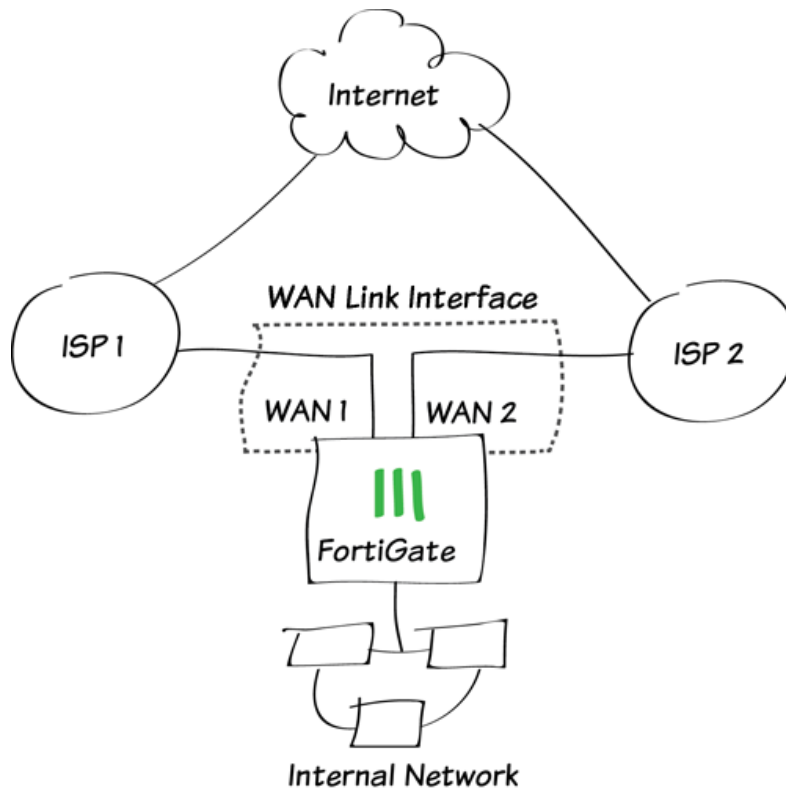
View the **Count** column, which displays the total amount of traffic that has used this policy since the FortiGate's last reboot. The column should display results, showing that the policy is being used for traffic.

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

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

For further reading, check out [Installation](#) in the [FortiOS 5.2 Handbook](#).

Redundant Internet connections



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

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

A video of this recipe can be found [here](#).

1. Connecting your ISPs to the FortiGate

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



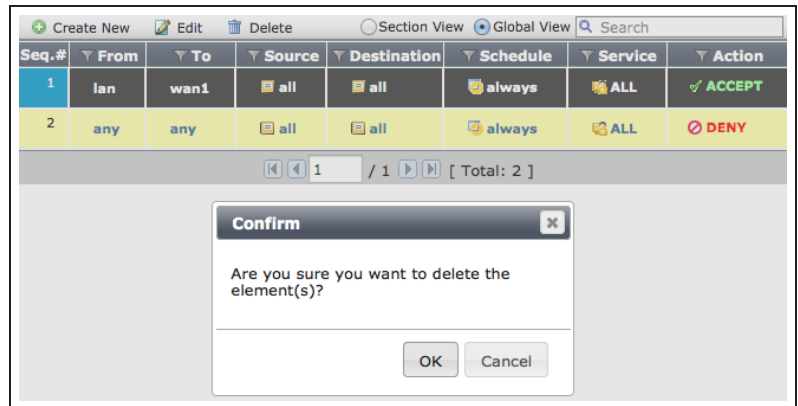
2. Deleting security policies and routes that use WAN1 or WAN2

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

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

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

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



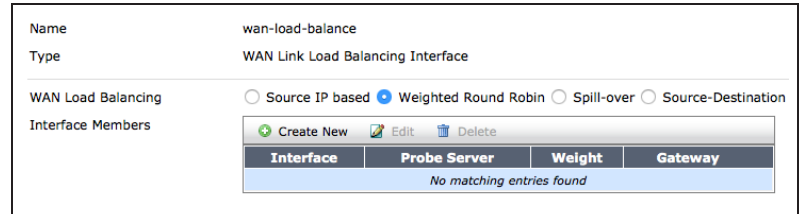
Go to **Router > Static > Static Routes** and delete any routes that use WAN1 or WAN2.



3. Creating a WAN link interface

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

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

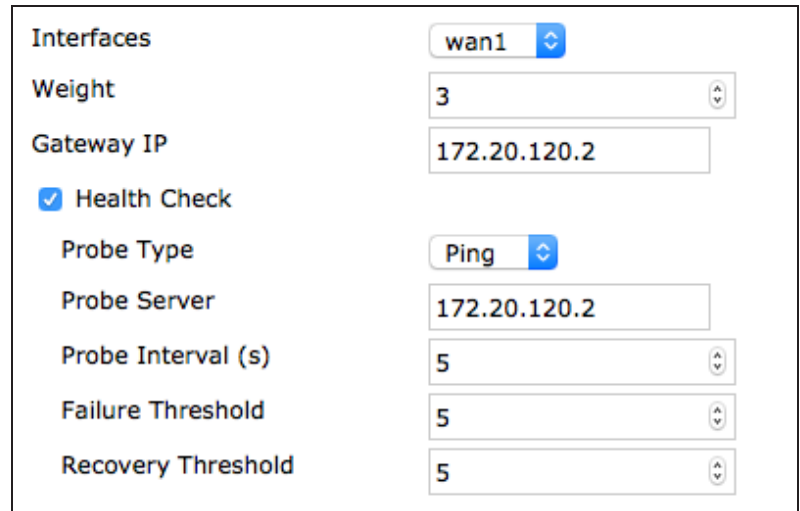


The screenshot shows the WAN Link Load Balancing configuration page. The Name is 'wan-load-balance' and the Type is 'WAN Link Load Balancing Interface'. Under WAN Load Balancing, 'Weighted Round Robin' is selected. The Interface Members section shows a table with columns for Interface, Probe Server, Weight, and Gateway, but it currently contains no entries.

Interface	Probe Server	Weight	Gateway
No matching entries found			

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

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



The screenshot shows the WAN Link Load Balancing configuration page with the following settings:

- Interfaces:** wan1
- Weight:** 3
- Gateway IP:** 172.20.120.2
- Health Check**
- Probe Type:** Ping
- Probe Server:** 172.20.120.2
- Probe Interval (s):** 5
- Failure Threshold:** 5
- Recovery Threshold:** 5

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

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

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

Interfaces	wan2
Weight	1
Gateway IP	182.20.120.2
<input checked="" type="checkbox"/> Health Check	
Probe Type	Ping
Probe Server	182.20.120.2
Probe Interval (s)	5
Failure Threshold	5
Recovery Threshold	5

4. Creating a default route for the WAN link interface

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

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

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	wan-load-balance
Distance	10 (1-255, Default=10)
Priority	0 (0-4294967295)
Comments	Write a comment... 0/255

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

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

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

Turn on **NAT**.

Incoming Interface: lan
Source Address: all
Source User(s): Click to add...
Source Device Type: Click to add...
Outgoing Interface: wan-load-balance
Destination Address: all
Schedule: always
Service: ALL
Action: ACCEPT

Firewall / Network Options
 NAT
 Use Destination Interface Address Fixed Port

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

Logging Options
 Log Allowed Traffic
 Security Events
 All Sessions
 Capture Packets

6. Results

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

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

The log shows traffic flowing through both WAN1 and WAN2.

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

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

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

For further reading, check out [Installing a FortiGate in NAT/Route Mode](#) in the [FortiOS 5.2 Handbook](#).

Troubleshooting your FortiGate installation

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

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

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

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

2. Check for equipment issues.

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

3. Check the physical network connections.

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

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

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

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

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

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

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

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

7. Verify the security policy configuration.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

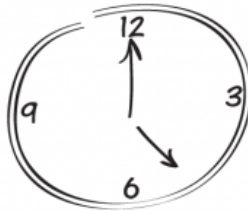
Resetting the FortiGate unit to factory defaults puts the unit back into NAT/Route mode.

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

FortiGate registration and basic settings



**Register your
FortiGate**



**Set the
system time**



**Configure the
admin account**

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

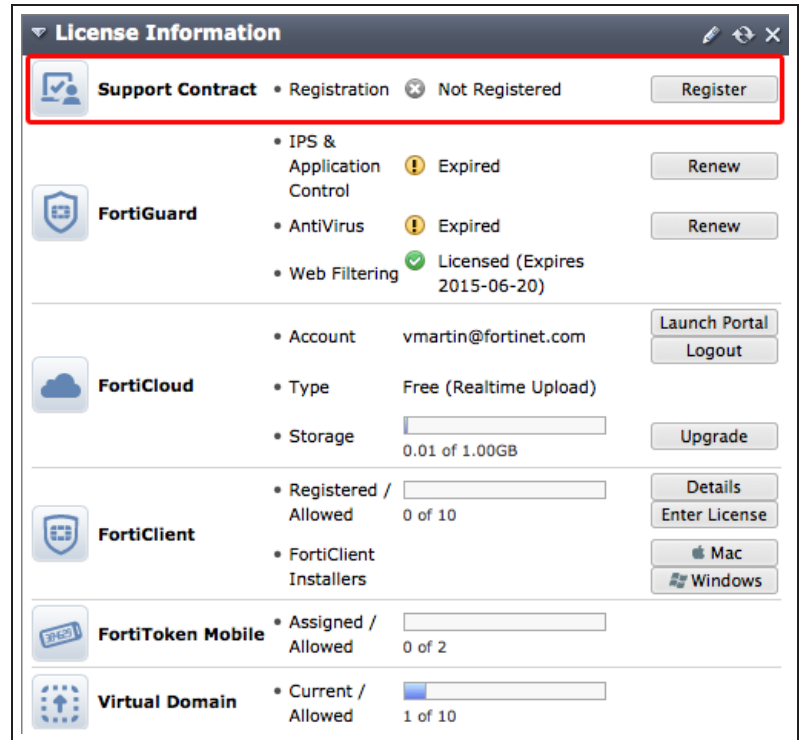
1. Registering your FortiGate

Registering your FortiGate allows you to receive FortiGuard updates and is required for firmware upgrades and access to [Fortinet Support](#).

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

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

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



Component	Status	Action
Support Contract	Registration: Not Registered	Register
FortiGuard	IPS & Application Control: Expired	Renew
	AntiVirus: Expired	Renew
	Web Filtering: Licensed (Expires 2015-06-20)	
FortiCloud	Account: vmartin@fortinet.com	Launch Portal / Logout
	Type: Free (Realtime Upload)	
	Storage: 0.01 of 1.00GB	Upgrade
FortiClient	Registered / Allowed: 0 of 10	Details / Enter License
	FortiClient Installers	Mac / Windows
FortiToken Mobile	Assigned / Allowed: 0 of 2	
Virtual Domain	Current / Allowed: 1 of 10	

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

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



Register this FortiGate

Register this FortiGate with FortiCare by logging in or creating a new account

Serial Number: FG100D3G12812324

Action: Login Create Account

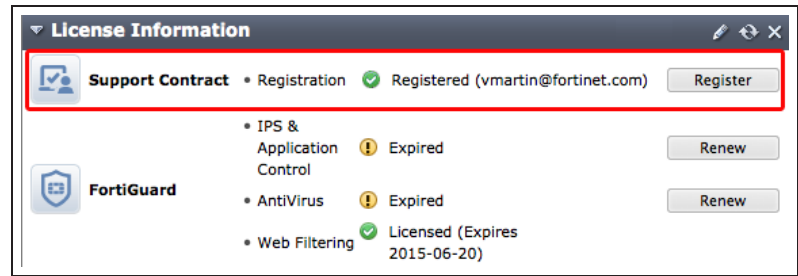
Email: vmartin@fortinet.com *

Password: ***** *

Country: Canada

Reseller: Other

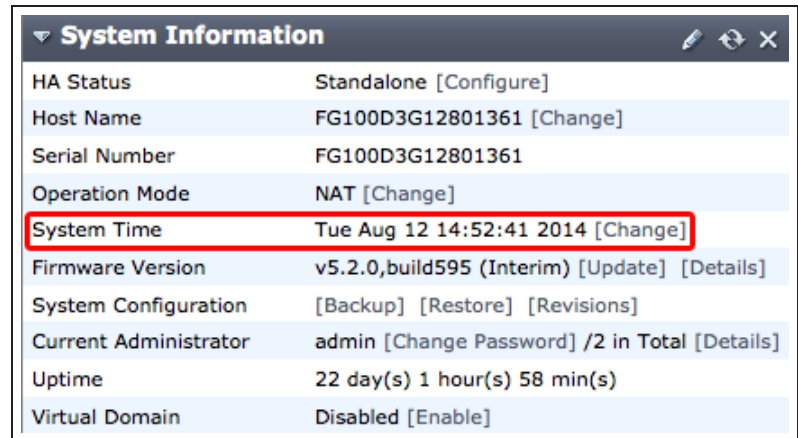
The **License Information** widget now displays the unit as **Registered**.



2. Setting the system time

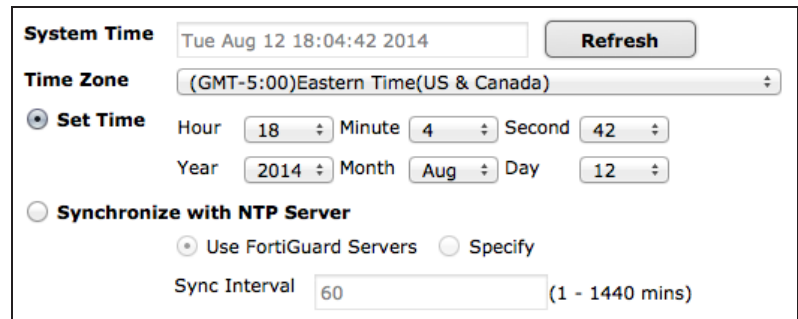
Go to **System > Dashboard > Status** and locate the **System Information** widget.

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



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

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



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

System Information	
HA Status	Standalone [Configure]
Host Name	FG100D3G12801361 [Change]
Serial Number	FG100D3G12801361
Operation Mode	NAT [Change]
System Time	Tue Aug 12 18:04:49 2014 [Change]
Firmware Version	v5.2.0,build595 (Interim) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /2 in Total [Details]
Uptime	22 day(s) 1 hour(s) 58 min(s)
Virtual Domain	Disabled [Enable]



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

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

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

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

If required, set additional trusted hosts.

<input checked="" type="checkbox"/> Restrict this Administrator Login from Trusted Hosts Only	
Trusted Host #1	<input type="text" value="192.168.220.110/32"/>
Trusted Host #2	<input type="text" value="0.0.0.0/0.0.0.0"/>
Trusted Host #3	<input type="text" value="0.0.0.0/0.0.0.0"/> 
IPv6 Trusted Host #1	<input "::="" 0"="" type="text" value=""/>
IPv6 Trusted Host #2	<input "::="" 0"="" type="text" value=""/>
IPv6 Trusted Host #3	<input "::="" 0"="" type="text" value=""/> 

4. Changing the default admin password

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

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

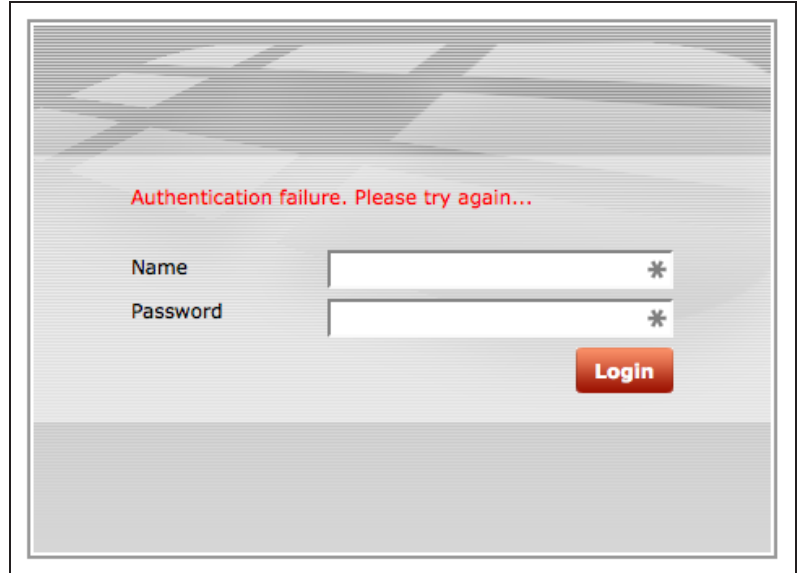
You will be automatically signed out after changing the password.

Administrator	admin
Old Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

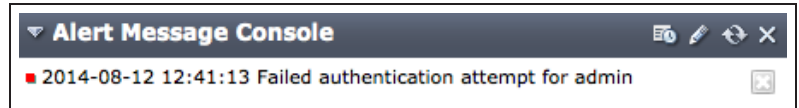
5. Results

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

Log in using the new password to access the FortiGate.



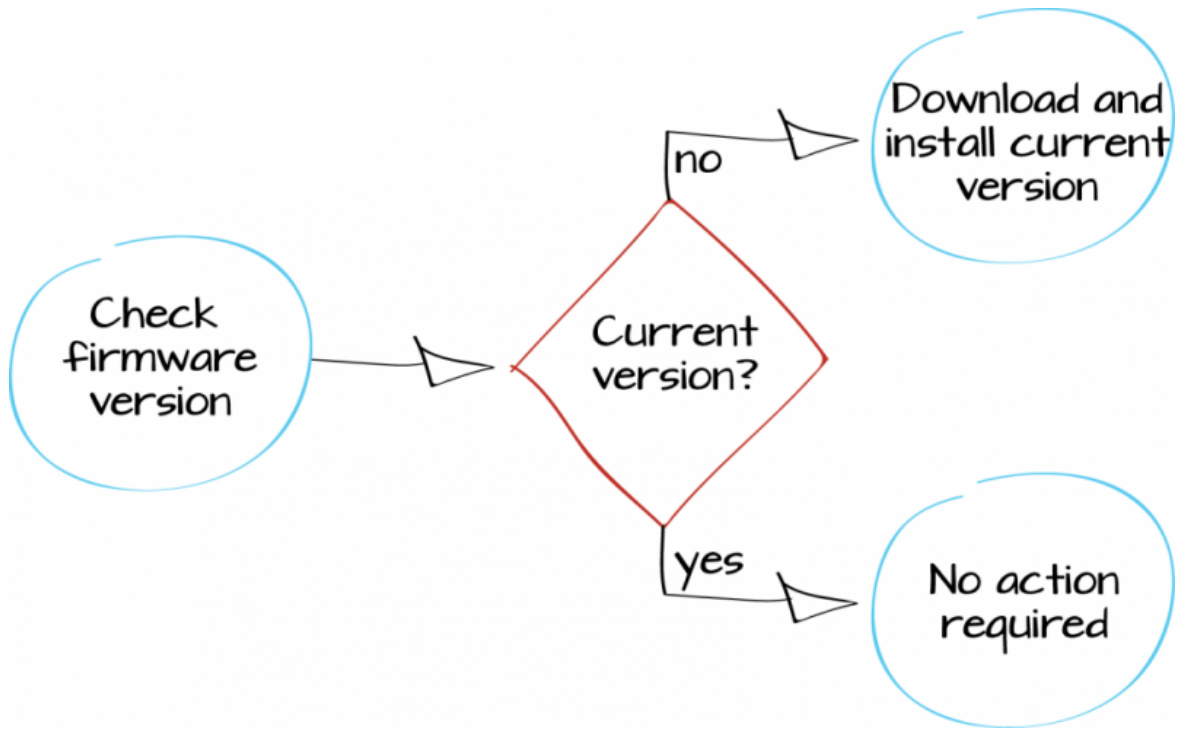
Go to **System > Dashboard > Status** and locate the **Alert Message Console** widget, which indicates the failed authentication attempt.



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

For further reading, check out [Basic Administration](#) in the [FortiOS 5.2 Handbook](#).

Updating your FortiGate's firmware

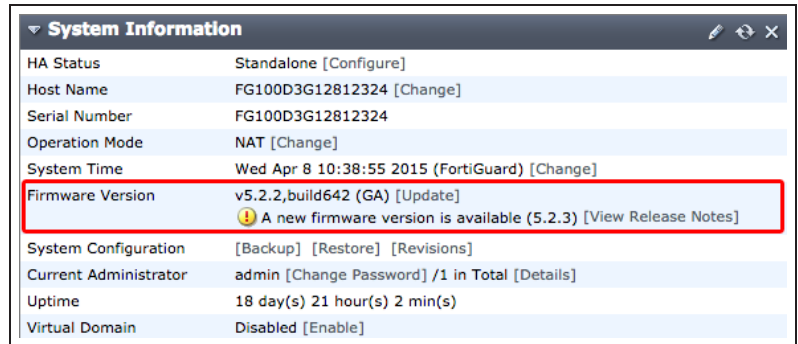


This example verifies the current version of FortiOS firmware and, if necessary, updates it to the latest version.

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

1. Checking the current FortiOS firmware

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



System Information	
HA Status	Standalone [Configure]
Host Name	FG100D3G12812324 [Change]
Serial Number	FG100D3G12812324
Operation Mode	NAT [Change]
System Time	Wed Apr 8 10:38:55 2015 (FortiGuard) [Change]
Firmware Version	v5.2.2,build642 (GA) [Update] ⚠ A new firmware version is available (5.2.3) [View Release Notes]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	18 day(s) 21 hour(s) 2 min(s)
Virtual Domain	Disabled [Enable]

2. Reviewing the Release Notes

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

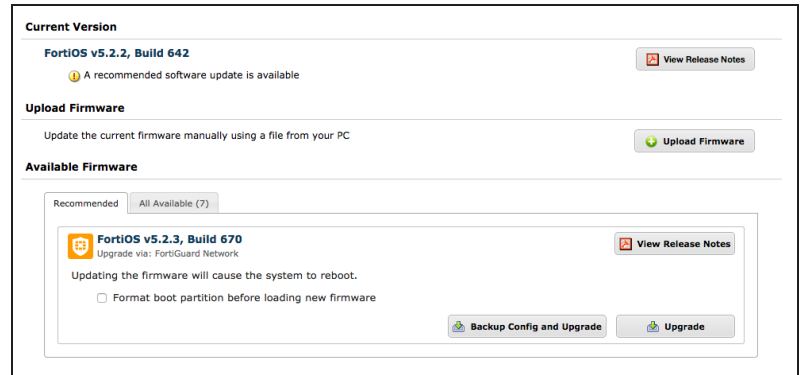
Pay extra attention to the **Upgrade Information** section, to find out if you can upgrade directly from your current firmware to the latest version. You should also check the **Supported Upgrade Paths** document, found at the [Fortinet Documentation Library](#).



3. Updating to the latest firmware

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

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

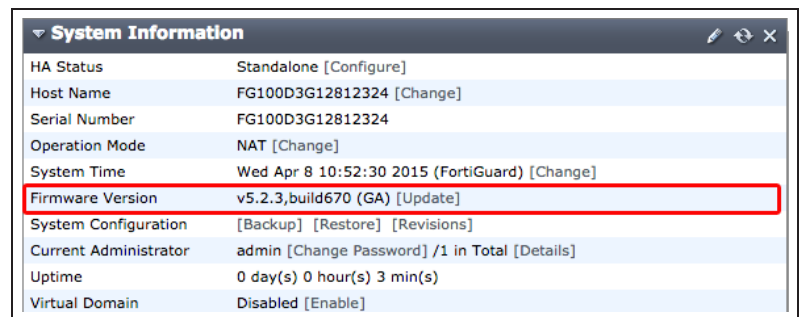
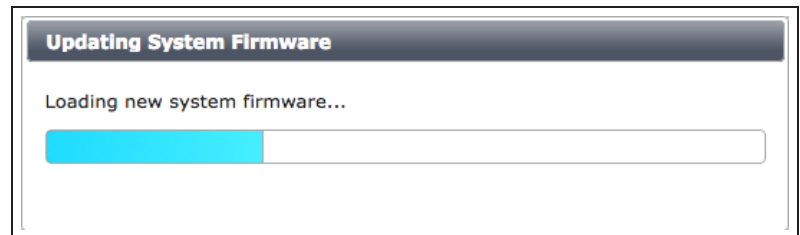


4. Results

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

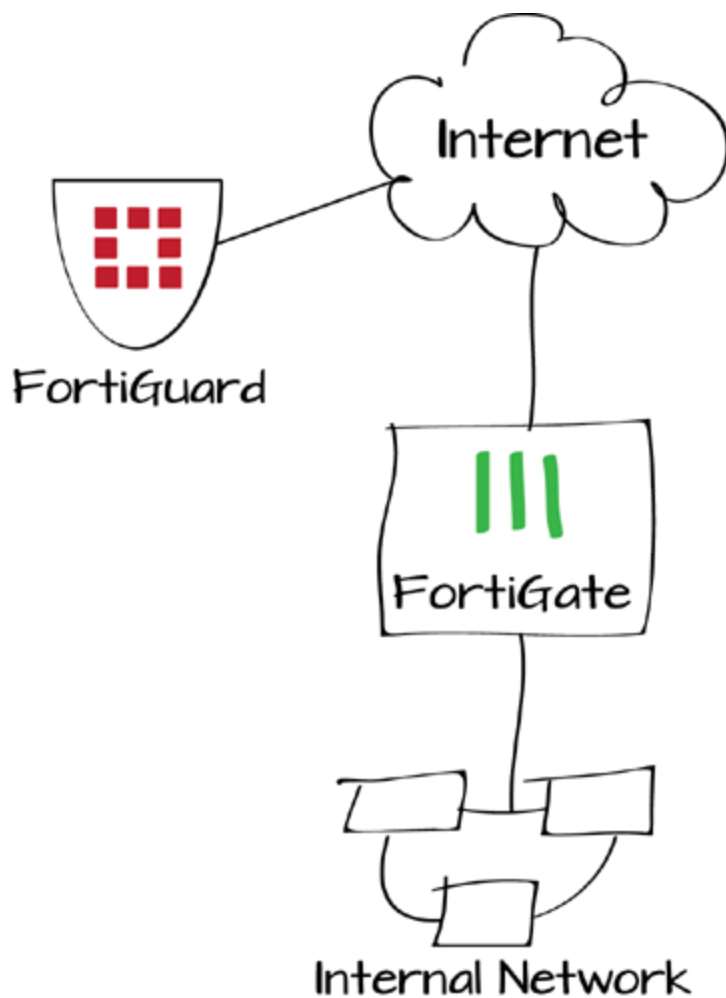
You may have to refresh your browser to see the FortiGate login.

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



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

Setting up FortiGuard services



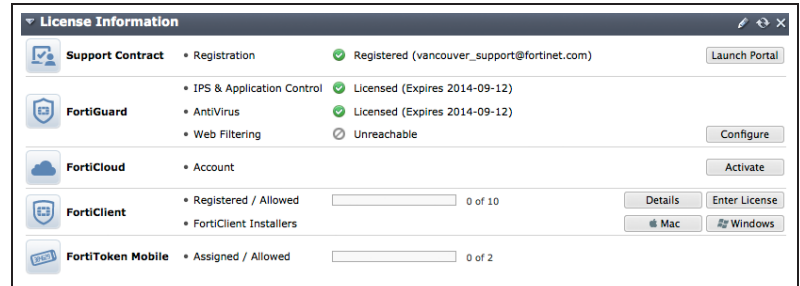
If you have purchased FortiGuard services and registered your FortiGate unit, the FortiGate should automatically connect to FortiGuard and display license information about your FortiGuard services. In this example, you will verify whether the FortiGate unit is communicating with the FortiGuard Distribution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

1. Verifying the connection

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

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

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



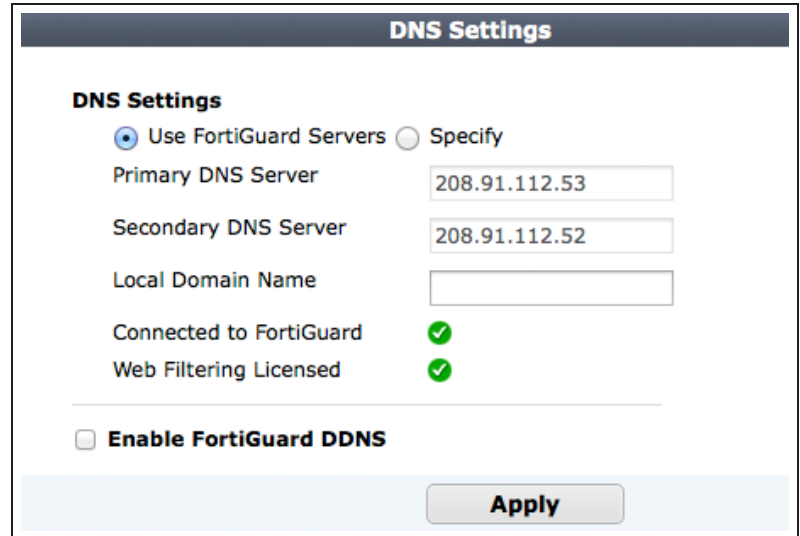
You can also view the FortiGuard connection status by going to **System > Config > FortiGuard**.

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

2. Troubleshooting communication errors

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

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



DNS Settings

DNS Settings

Use FortiGuard Servers Specify

Primary DNS Server

Secondary DNS Server

Local Domain Name

Connected to FortiGuard

Web Filtering Licensed

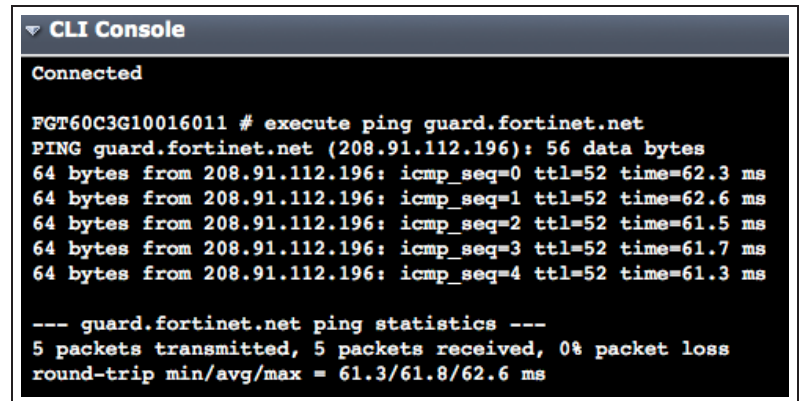
Enable FortiGuard DDNS

Apply

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

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

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



```
CLI Console
Connected
FGT60C3G10016011 # execute ping guard.fortinet.net
PING guard.fortinet.net (208.91.112.196): 56 data bytes
64 bytes from 208.91.112.196: icmp_seq=0 ttl=52 time=62.3 ms
64 bytes from 208.91.112.196: icmp_seq=1 ttl=52 time=62.6 ms
64 bytes from 208.91.112.196: icmp_seq=2 ttl=52 time=61.5 ms
64 bytes from 208.91.112.196: icmp_seq=3 ttl=52 time=61.7 ms
64 bytes from 208.91.112.196: icmp_seq=4 ttl=52 time=61.3 ms

--- guard.fortinet.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 61.3/61.8/62.6 ms
```

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

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

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

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

3. Results

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

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

The screenshot shows the FortiGate configuration page for FortiGuard and FortiToken Seed Server. The FortiGuard Availability is marked as 'Reachable' with a green checkmark. The FortiClient Version (Mac) is 5.2.0 (Updated 2014-07-15) and the FortiClient Version (Windows) is 5.2.0 (Updated 2014-07-15). The SSL-VPN Package Version is 4.0.2292 (Updated 2013-11-01). The FortiToken Seed Server Registration is marked as 'Reachable (0 Tokens Registered)' with a green checkmark. Under the 'Web Filtering and Email Filtering Options' section, 'Enable webfilter cache' and 'Enable antispam cache' are both checked. The TTL for the webfilter cache is 3600 and for the antispam cache is 1800. The 'Port Selection' section shows 'Use Alternate Port (8888)' selected, with a 'Test Availability' button next to it. A link is provided to re-evaluate URL category ratings.

FortiClient Information	
FortiGuard Availability	Reachable ✓
FortiClient Version (Mac)	5.2.0 (Updated 2014-07-15)
FortiClient Version (Windows)	5.2.0 (Updated 2014-07-15)

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

FortiToken Seed Server	
Registration	Reachable (0 Tokens Registered) ✓

AV & IPS Download Options

Web Filtering and Email Filtering Options

- Enable webfilter cache TTL: 3600
- Enable antispam cache TTL: 1800

Port Selection

Use Default Port (53) Use Alternate Port (8888) (FortiGuard services are reachable via ports 53 and 8888.) Test Availability

To have a URL's category rating re-evaluated, please [click here](#).

Apply

The screenshot shows the License Information widget in the FortiGate dashboard. It displays the status of various services and licenses. The Support Contract is registered. FortiGuard services (IPS & Application Control, AntiVirus, and Web Filtering) are all licensed and expire on 2014-09-12. FortiCloud account is active. FortiClient has 0 of 10 registered/allowed devices. FortiToken Mobile has 0 of 2 assigned/allowed devices.

Service	Status	Details
Support Contract	Registered ✓	(vancouver_support@fortinet.com) Launch Portal
FortiGuard	Licensed ✓	IPS & Application Control (Expires 2014-09-12)
FortiGuard	Licensed ✓	AntiVirus (Expires 2014-09-12)
FortiGuard	Licensed ✓	Web Filtering (Expires 2014-09-12)
FortiCloud	Account	Activate
FortiClient	Registered / Allowed	0 of 10 Details Enter License
FortiToken Mobile	Assigned / Allowed	0 of 2 Mac Windows

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

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

Support Contract		
Registration	Registered (Login ID: vancouver_support@fortinet.com) [Login Now]	✓
Hardware	8 x 5 support (Expires: 2014-09-12)	✓
Firmware	8 x 5 support (Expires: 2014-09-12)	✓
Enhanced Support	24 x 7 support (Expires: 2014-09-12)	✓
Comprehensive Support	24 x 7 support (Expires: 2014-09-12)	✓
FortiGuard Services		
Next Generation Firewall		
IPS & Application Control	Licensed (Expires 2014-09-12)	✓
IPS Definitions	4.00444 (Updated 2014-03-26 via Manual Update) [Update]	
IPS Engine	3.00038 (Updated 2014-06-11 via Manual Update)	
ATP Services		
AntiVirus	Licensed (Expires 2014-09-12)	✓
AV Definitions	1.00000 (Updated 2012-10-17 via Manual Update) [Update]	
AV Engine	5.00154 (Updated 2014-06-11 via Manual Update)	
Web Filtering	Licensed (Expires 2014-09-12)	✓
Other Services		
Vulnerability Scan	Licensed (Expires 2014-09-12)	✓
VCM Plugins	1.00366 (Updated 2014-07-09 via Manual Update) [Update]	
Email Filtering	Licensed (Expires 2014-09-12)	✓
Messaging Services	Licensed (Expires 2014-09-12)	✓
FortiClient Information		
FortiGuard Availability	Reachable	✓
FortiClient Version (Mac)	5.2.0 (Updated 2014-07-16)	
FortiClient Version (Windows)	5.2.0 (Updated 2014-07-16)	
SSL-VPN Package Information		
SSL-VPN Package Version	4.0.2292 (Updated 2013-11-01)	
FortiToken Seed Server		
Registration	Reachable (0 Tokens Registered)	✓

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

FortiGuard troubleshooting

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

FortiGuard services appear as expired/unreachable.

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

Services are active but still appear as expired/unreachable.

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

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

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

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

Communication errors remain.

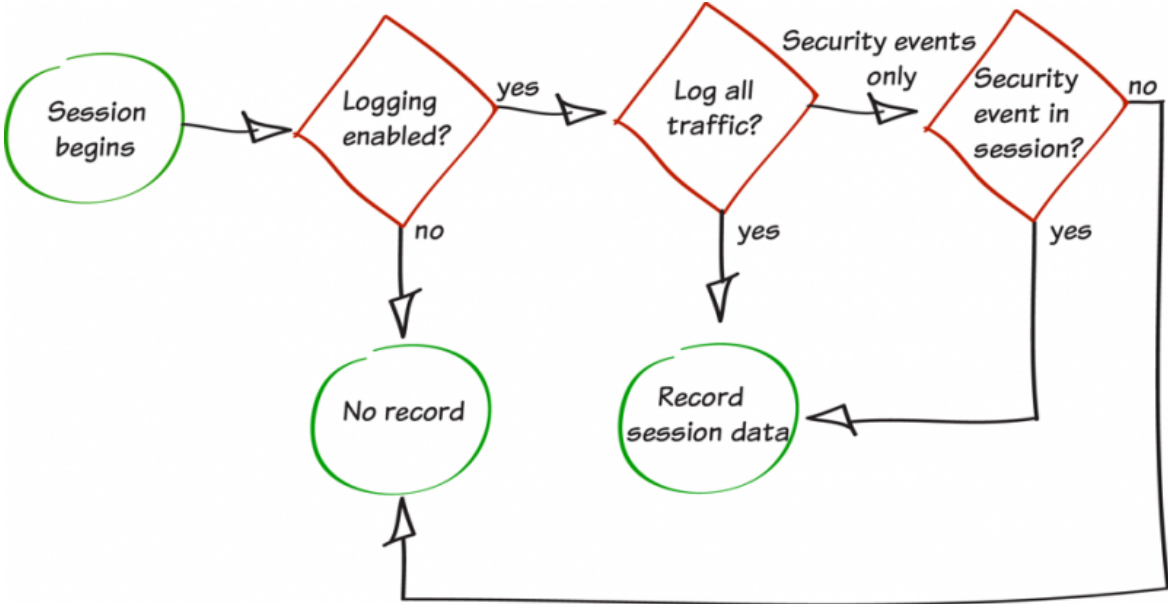
FortiGate units contact the FortiGuard Network by sending UDP packets with typical source ports of 1027 or 1031, and destination ports of 53 or 8888. The FDN reply packets would then have a destination port of 1027 or 1031. If your ISP blocks UDP packets in this port range, the FortiGate unit cannot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

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

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

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

Logging FortiGate traffic



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

1. Recording log messages and enabling event logging

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

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

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

Log Settings

Logging and Archiving

Send Logs to FortiAnalyzer/FortiManager
IP Address:

Send Logs to FortiCloud
Account:

Upload Option

Realtime

Event Logging

Enable All

WiFi activity event System activity event User activity event

Router activity event VPN activity event Explicit web proxy event

GUI Preferences

Display Logs From:

Resolve Hostnames (Using reverse DNS lookup)

Resolve Unknown Applications (Using remote application database)

2. Enabling logging in the security policies

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

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

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

Destination Address: all
Schedule: always
Service: ALL
Action: ACCEPT

Firewall / Network Options
 ON NAT
 Use Destination Interface Address Fixed Port
 Use Dynamic IP Pool

Security Profiles
 OFF AntiVirus
 OFF Web Filter
 OFF Application Control
 OFF SSL Inspection

Traffic Shaping
 OFF Shared Shaper
 OFF Reverse Shaper
 OFF Per-IP Shaper

Logging Options
 ON Log Allowed Traffic
 Security Events
 All Sessions

3. Results

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

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

For further reading, check out [Logging and reporting overview](#) in the [FortiOS 5.2 Handbook](#).

Troubleshooting FortiGate logging

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

No log messages appear.

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

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

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

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

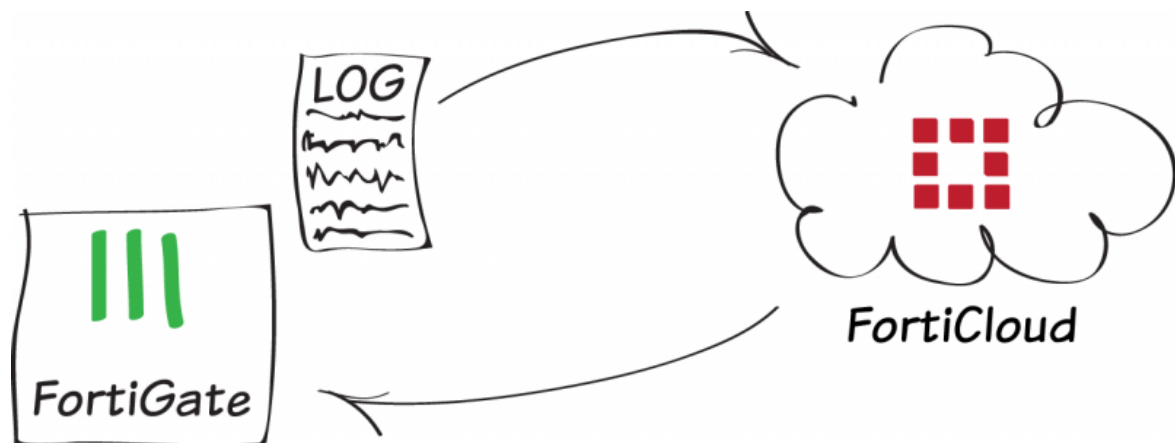
The FortiGate unit's performance level has decreased since enabling disk logging.

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

Logging to a FortiAnalyzer unit is not working as expected.

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

Logging with FortiCloud

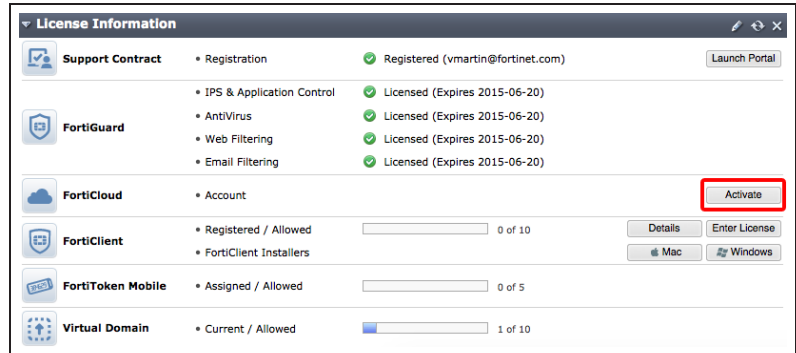


In this example, you will use FortiCloud, an online logging service provided by Fortinet, to store the logs of your FortiGate unit's traffic. You will also access logs using the [FortiCloud website](#).

Before you can use FortiCloud, you must register your FortiGate. For more information, see [FortiGate registration and basic settings](#).

1. Activating FortiCloud

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



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

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

Activate FortiCloud

Activate FortiCloud by logging in or creating a new account

Action: Login Create Account

Email: test@example.com

Confirm Email: test@example.com

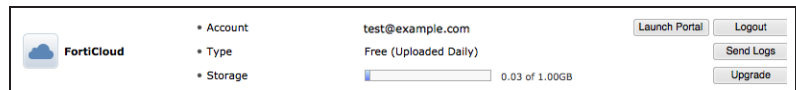
Password: *****

Confirm Password: *****

I agree to the FortiCloud terms & conditions (View)

OK Cancel

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



2. Sending logs to FortiCloud

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

Send Logs to FortiCloud

Account: test@example.com (Test Connectivity)

Upload Option: Realtime

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

FortiCloud Connection Summary

Disk Quota	1024 MB
Quota Used	29 MB
DLP Archive	<input checked="" type="checkbox"/>

Close

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

Event Logging

Enable All

Endpoint event

Router activity event

WiFi activity event

VPN activity event

System activity event

HA event

User activity event

Explicit web proxy event

GUI Preferences

Display Logs From: FortiCloud

Resolve Hostnames (Using reverse DNS lookup)

Resolve Unknown Applications (Using remote application database)

3. Enabling logging in your Internet access security policy

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

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

Logging Options

Log Allowed Traffic

Security Events

All Sessions

Capture Packets

4. Results


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

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

Log location: FortiCloud

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

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



FG100D3G1281232
FG100D3G12812324 | FortiOS 5.2.0

[Setup Wizard](#)

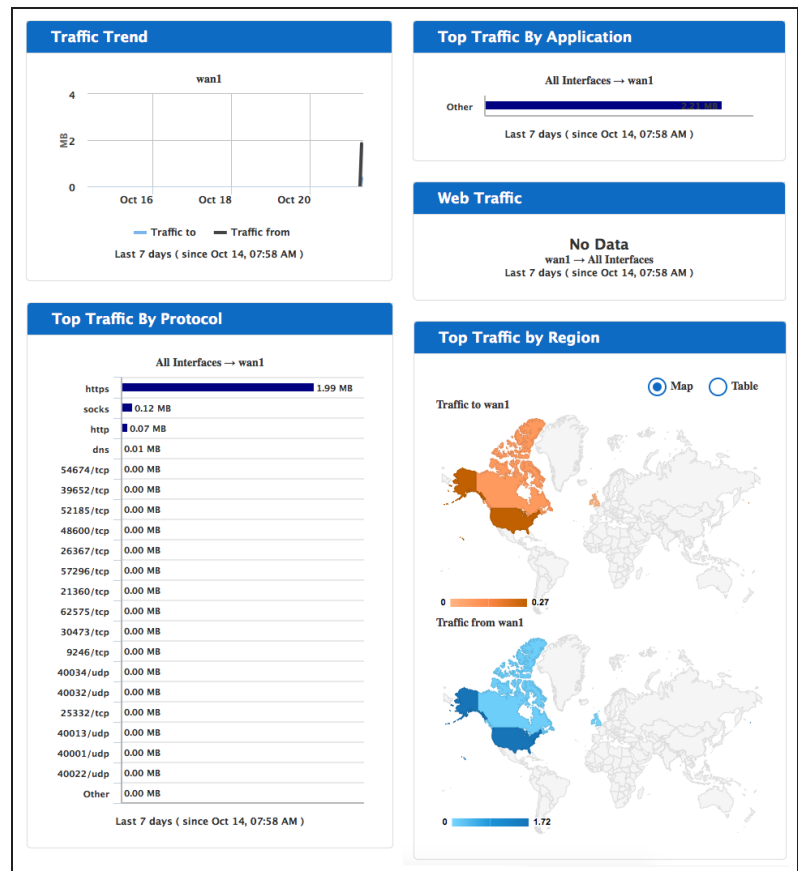
Last log upload : No upload
2% used [Manage Quota](#)
Free trial 1GB [Subscribe](#)

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

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

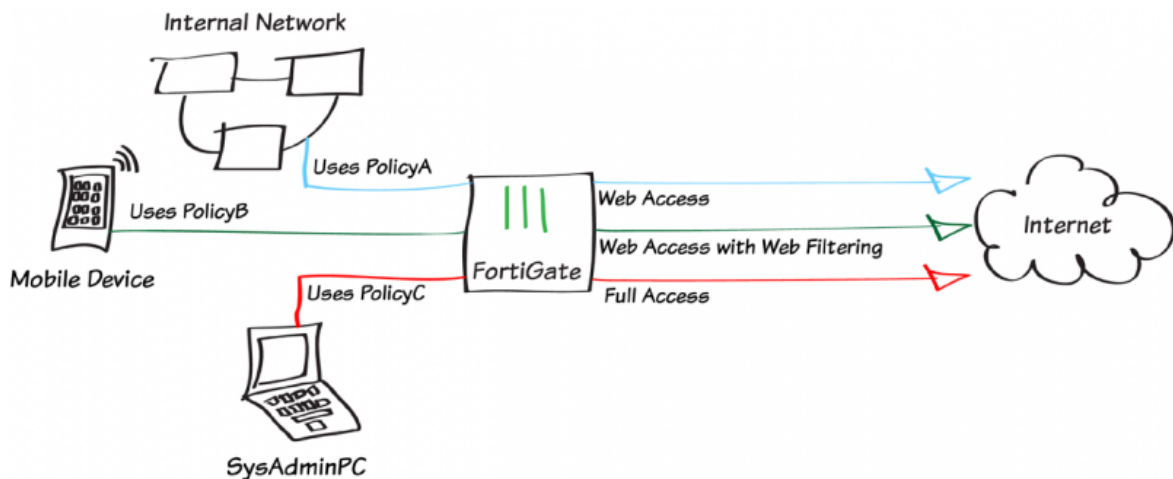
From the portal, you can also access options for **FortiView**, **Drilldown**, **Reports**, and **Management**.

For more information about using FortiCloud, see the [FortiCloud FAQ](#)



For further reading, check out [FortiCloud](#) in the [FortiOS 5.2 Handbook](#).

Creating security policies



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

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

In this example, a wireless network has already been configured that is in the same subnet as the wired LAN. For information about this configuration, see [Setting up a WiFi bridge with a FortiAP](#).

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

A video of this recipe can be found [here](#).

1. Configuring PolicyA to allow general web access

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

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

Ensure that you have enabled **NAT**.

Incoming Interface: lan

Source Address: all

Source User(s): Click to add...

Source Group(s): Click to add...

Source Device Type: Click to add...

Outgoing Interface: wan1

Destination Address: all

Schedule: always

Service: HTTP, HTTPS, DNS

Action: ACCEPT

Firewall / Network Options

NAT

Use Destination Interface Address Fixed Port

Use Dynamic IP Pool

Use Central NAT Table

Web Cache

WAN Optimization

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

Logging Options

Log Allowed Traffic

Security Events

All Sessions

Capture Packets

2. Creating PolicyB to allow access for mobile devices

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

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

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

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

Enable **NAT**.

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

Incoming Interface	lan
Source Address	all
Source User(s)	Click to add...
Source Group(s)	Click to add...
Source Device Type	Mobile Devices
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	HTTP HTTPS DNS
Action	ACCEPT
Firewall / Network Options	
<input checked="" type="checkbox"/> NAT	
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...
<input type="radio"/> Use Central NAT Table	
<input type="checkbox"/> Web Cache	
<input type="checkbox"/> WAN Optimization	
<input type="checkbox"/> Compliant with FortiClient Profile	
Security Profiles	
<input type="checkbox"/> AntiVirus	default
<input checked="" type="checkbox"/> Web Filter	default
<input type="checkbox"/> Application Control	default
<input type="checkbox"/> IPS	default
<input type="checkbox"/> Email Filter	default
<input type="checkbox"/> DLP Sensor	default
<input type="checkbox"/> VoIP	default
<input type="checkbox"/> ICAP	default
Proxy Options	default
<input checked="" type="checkbox"/> SSL/SSH Inspection	default

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

Logging Options

Log Allowed Traffic

Security Events

All Sessions

Capture Packets

3. Defining SysAdminPC

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

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

Alias	<input type="text" value="SysAdminPC"/>
MAC Address	<input type="text" value="c4:2c:03:21:af:04"/>
Additional MACs	<input type="text" value="Click to add..."/>
Device Type	<input type="text" value="Mac"/>

4. Configuring PolicyC to allow access for SysAdminPC

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

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

Enable **NAT**.

Incoming Interface	<input type="text" value="lan"/>
Source Address	<input type="text" value="all"/>
Source User(s)	<input type="text" value="Click to add..."/>
Source Group(s)	<input type="text" value="Click to add..."/>
Source Device Type	<input type="text" value="SysAdminPC"/>
Outgoing Interface	<input type="text" value="wan1"/>
Destination Address	<input type="text" value="all"/>
Schedule	<input type="text" value="always"/>
Service	<input type="text" value="ALL"/>
Action	<input type="text" value="ACCEPT"/>

Firewall / Network Options

NAT

Use Destination Interface Address Fixed Port

Use Dynamic IP Pool

Use Central NAT Table

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

Logging Options

ON Log Allowed Traffic

Security Events

All Sessions

Capture Packets

5. Ordering the policy table

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

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

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

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

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

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

6. Results

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

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

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

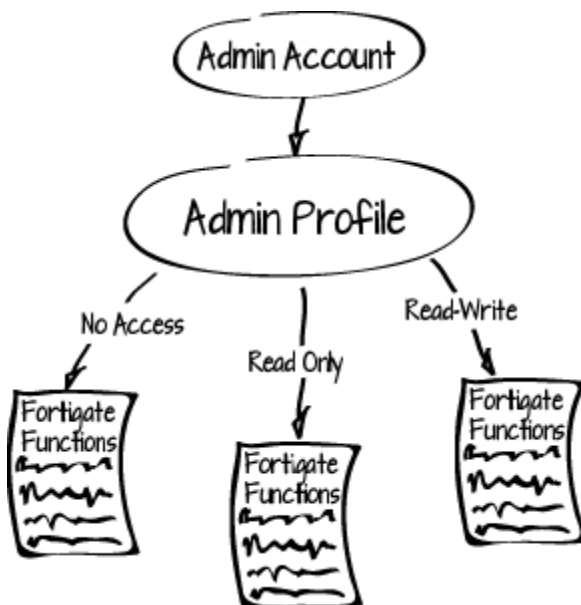
Policy ID is automatically assigned to a policy when it is created, and so, in the example, the ID for PolicyA is 1, PolicyB is 2, and PolicyC is 3.

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

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

For further reading, check out [Firewall policies](#) in the [FortiOS 5.2 Handbook](#).

Limited access administrator accounts



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

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

1. Creating a new administrator profile

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

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

Profile Name:

Comments: 95/255

Access Control	<input type="checkbox"/> None	<input type="checkbox"/> Read Only	<input type="checkbox"/> Read-Write
System Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Network Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Administrator Users	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
FortiGuard Update	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Maintenance	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Router Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ Firewall Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▶ Security Profile Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
VPN Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
User & Device	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
WAN Opt & Cache	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Endpoint Security	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
WiFi Controller	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
▼ Log & Report	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Configuration	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Data Access	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Report Access	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Threat Weight	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

2. Adding a new administrator and assigning the profile

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

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

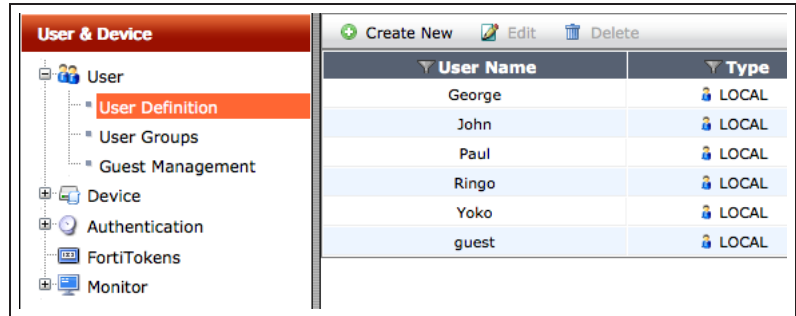
Add an IP address to at least one of the **Trusted Host** fields to control where the administrator can log in from. In the example the administrator can log in only from the 172.20.120.0 network.

Administrator	<input type="text" value="t.white"/>
Type	<input checked="" type="radio"/> Regular <input type="radio"/> Remote <input type="radio"/> PKI
Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>
Comments	<input type="text" value="User and device admin account"/> 29/255
Administrator Profile	<input type="text" value="User-Device-Config"/>
Contact Info	
<input checked="" type="checkbox"/> Email Address	<input type="text" value="t.white@example.com"/>
<input type="checkbox"/> SMS	<input checked="" type="radio"/> FortiGuard Messaging Service <input type="radio"/> Custom
	Country/Region <input type="text" value="Click to add..."/>
	Phone Number <input type="text"/>
<input type="checkbox"/> Enable Two-factor Authentication	
<input checked="" type="checkbox"/> Restrict this Administrator Login from Trusted Hosts Only	
Trusted Host #1	<input type="text" value="172.20.120.0/24"/>
Trusted Host #2	<input type="text" value="0.0.0.0/0.0.0.0"/>
Trusted Host #3	<input type="text" value="0.0.0.0/0.0.0.0"/> <input type="button" value="+"/>

3. Results

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

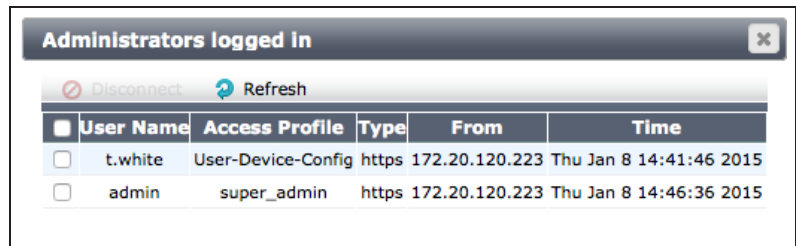
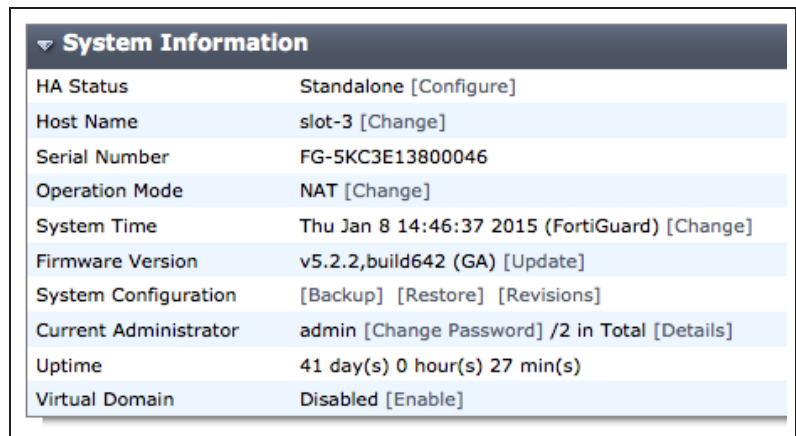
t.white should be able to change user and device authentication settings and view log messages and reports.



Log in from another browser window with the admin account.

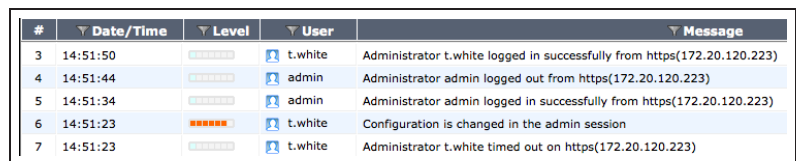
Go to **System > Dashboard > Status**, and view the **System Information** widget. It should show two administrators.

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



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

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

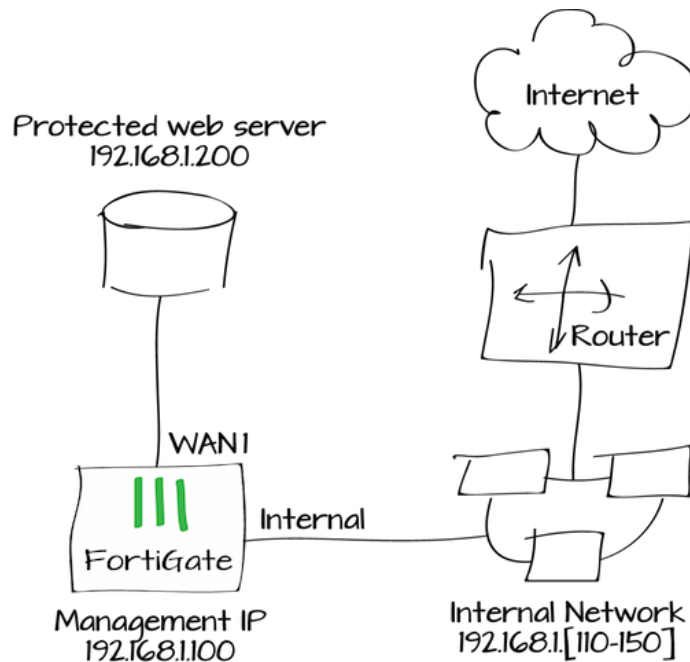


should be within the Trusted Hosts network address.

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

For further reading, check out [Administrators](#) in the [FortiOS 5.2 Handbook](#).

Port pairing in Transparent mode



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

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

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

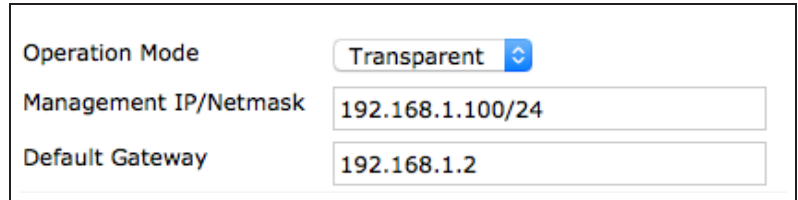
1. Switching the FortiGate unit to transparent mode and adding a static route

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

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

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

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



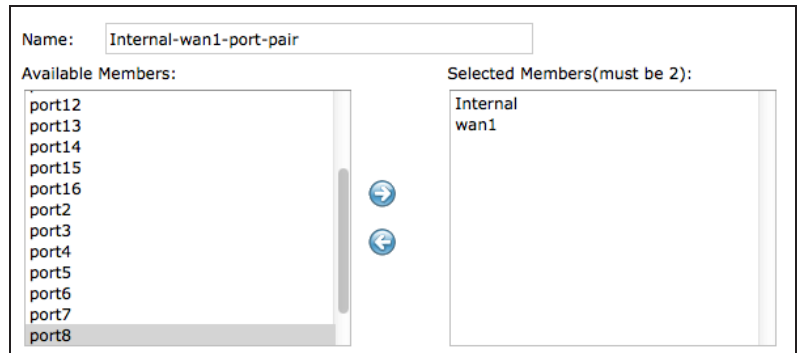
Operation Mode	Transparent
Management IP/Netmask	192.168.1.100/24
Default Gateway	192.168.1.2

2. Creating an internal and wan1 port pair

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

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

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



Name:	Internal-wan1-port-pair
Available Members:	Selected Members(must be 2):
port12 port13 port14 port15 port16 port2 port3 port4 port5 port6 port7 port8	Internal wan1

3. Creating security policies

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

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

Incoming Interface	Internal	+
Source Address	all	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	wan1	+
Destination Address	Web-Server	+
Schedule	always	
Service	HTTP	X +
	HTTPS	X
Action	ACCEPT	

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

Incoming Interface	wan1	+
Source Address	Web-Server	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	Internal	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	

4. Results

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

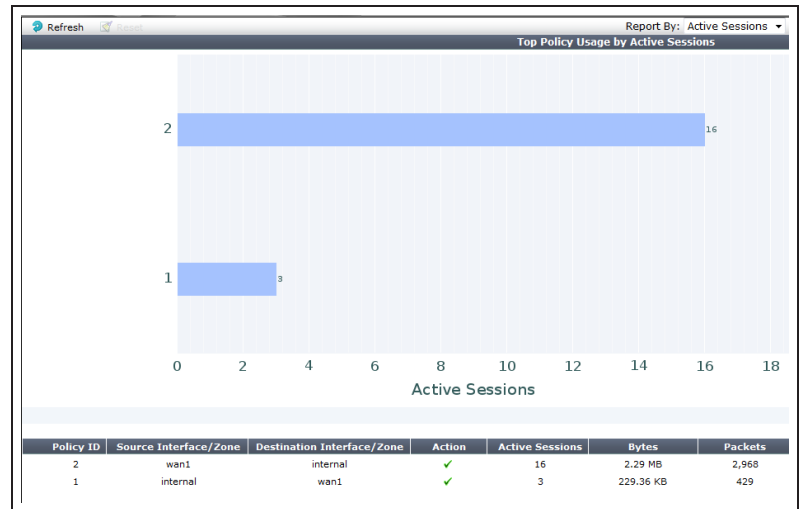
Go to **Log & Report > Traffic Log > Forward Traffic** to verify that there is traffic from the internal to wan1 interface.

Select an entry for details.

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

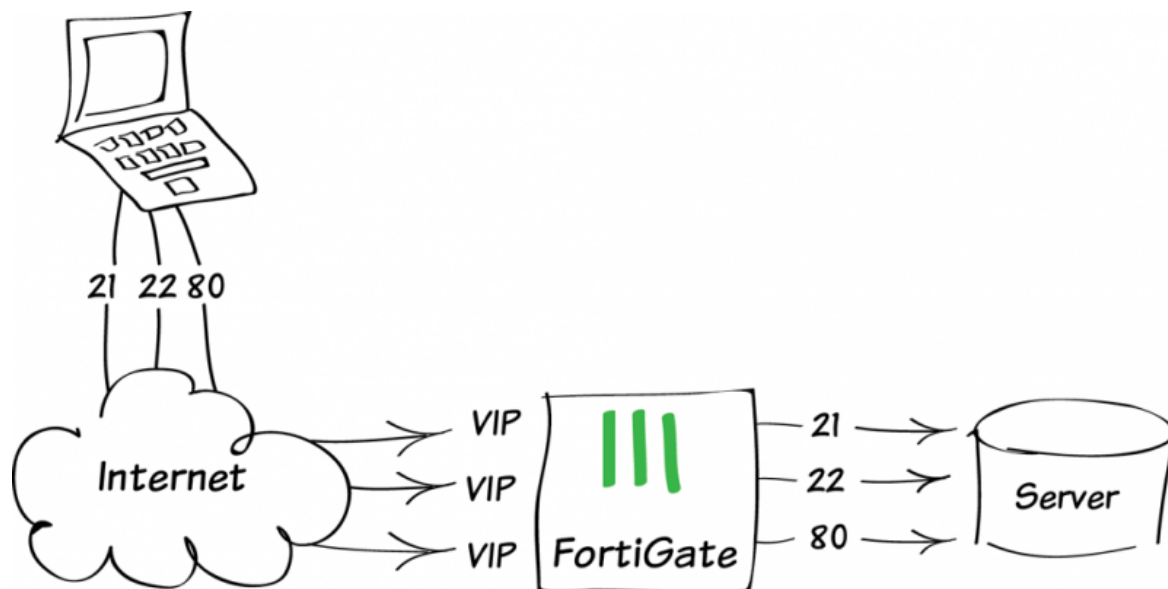
Dst	74.125.225.223	Virtual Domain	root
Received	9296	Source Country	Reserved
Application Name	SSL	Sent / Received	1.04 KB / 9.08 KB
Duration	17	Sent	1067
Application Details		Service	HTTPS
Protocol	6	Destination Country	United States
Application Control List	default	Dst Port	443
roll	65531	Status	close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

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



For further reading, check out [Interfaces](#) in the [FortiOS 5.2 Handbook](#).

Port forwarding



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

A video of this recipe can be found [here](#).

1. Creating three virtual IPs

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

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

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

The screenshot shows the configuration for a Virtual IP named 'webserver-80'. The 'VIP Type' is set to 'IPv4 VIP'. The 'Name' field contains 'webserver-80'. The 'Interface' is 'wan2'. The 'Type' is 'Static NAT'. The 'Port Forwarding' checkbox is checked. The 'Protocol' is 'TCP'. The 'External Service Port' and 'Map to Port' are both set to 80. The 'Mapped IP Address/Range' is 192.168.111.99. The 'External IP Address/Range' is also 192.168.111.99. The 'Source Address Filter' checkbox is unchecked.

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

The screenshot shows the configuration for a Virtual IP named 'webserver-ssh'. The 'VIP Type' is set to 'IPv4 VIP'. The 'Name' field contains 'webserver-ssh'. The 'Interface' is 'Any'. The 'Type' is 'Static NAT'. The 'Port Forwarding' checkbox is checked. The 'Protocol' is 'TCP'. The 'External Service Port' and 'Map to Port' are both set to 22. The 'Mapped IP Address/Range' is 192.168.111.99. The 'External IP Address/Range' is also 192.168.111.99. The 'Source Address Filter' checkbox is unchecked.

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

The screenshot shows the configuration for a Virtual IP (VIP) named 'webserver-ftp'. The 'VIP Type' is set to 'IPv4 VIP'. The 'Name' field contains 'webserver-ftp'. The 'Interface' is 'wan2'. The 'Type' is 'Static NAT'. The 'Port Forwarding' checkbox is checked. The 'Protocol' is 'TCP'. The 'External Service Port' and 'Map to Port' are both set to '21'. The 'Mapped IP Address/Range' is '192.168.111.99'.

2. Adding virtual IPs to a VIP group

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

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

The screenshot shows the configuration for a Virtual IP Group named 'Webserver'. The 'Type' is 'IPv4 VIP Group'. The 'Name' field contains 'Webserver'. The 'Interface' is 'wan2'. The 'Members' list includes 'webserver-80', 'webserver-ftp', and 'webserver-ssh'.

3. Creating a security policy

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

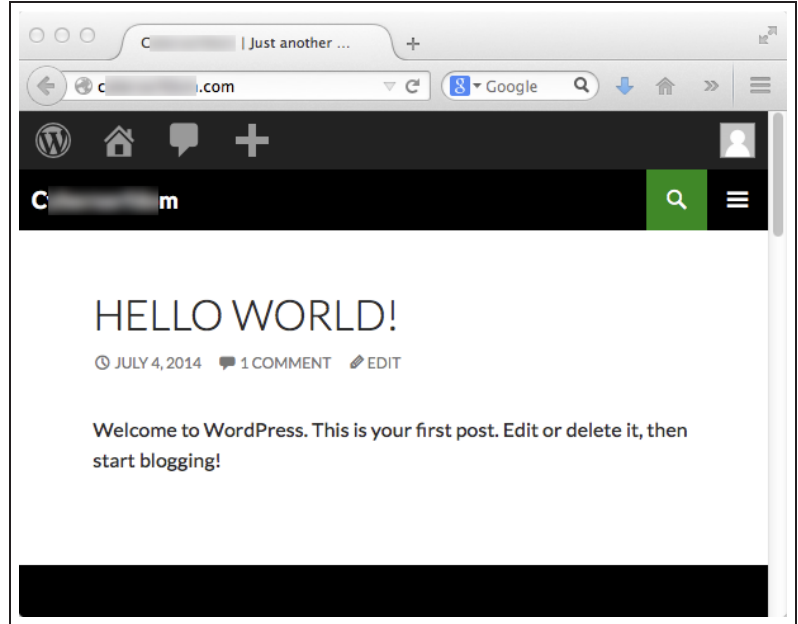
Set **Incoming Interface** to your Internet-facing interface, **Outgoing Interface** to the interface connected to the server, and **Destination Address** to the VIP group. Set **Service** to allow **HTTP**, **FTP**, and **SSH** traffic.

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

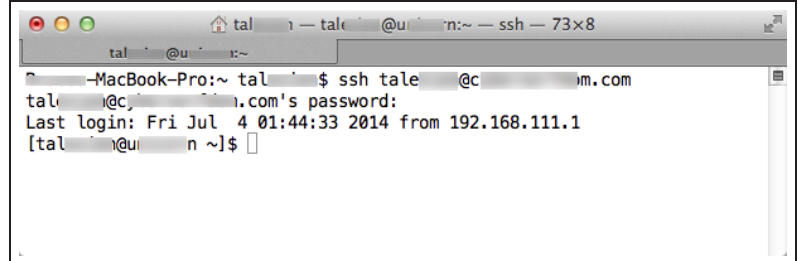
Incoming Interface	wan2	+
Source Address	all	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	internal1	+
Destination Address	Webserver	+
Schedule	always	
Service	HTTP	X +
	FTP	X
	SSH	X
Action	ACCEPT	
Firewall / Network Options		
<input type="checkbox"/> NAT		
<input type="checkbox"/> Web Cache		
<input type="checkbox"/> WAN Optimization		
Security Profiles		
<input checked="" type="checkbox"/> AntiVirus	default	
<input type="checkbox"/> Web Filter	default	
<input type="checkbox"/> Application Control	default	
<input checked="" type="checkbox"/> IPS	default	
<input type="checkbox"/> Email Filter	default	
<input type="checkbox"/> DLP Sensor	default	
<input type="checkbox"/> VoIP	default	
<input type="checkbox"/> ICAP	default	
Proxy Options	default	
<input checked="" type="checkbox"/> SSL Inspection	default	

4. Results

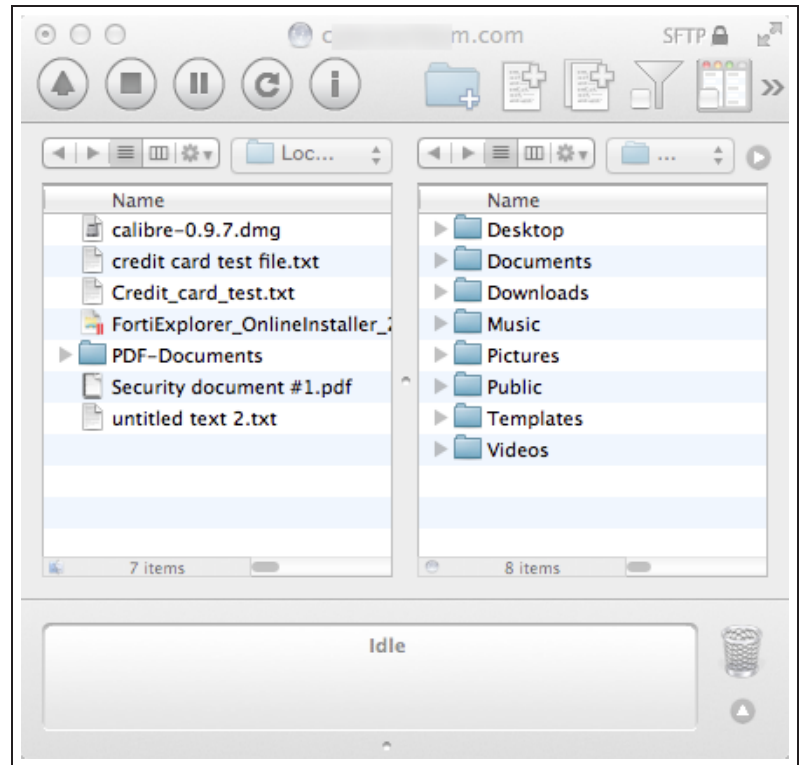
To ensure that TCP port 80 is open, connect to the web server on the other side of the firewall.



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

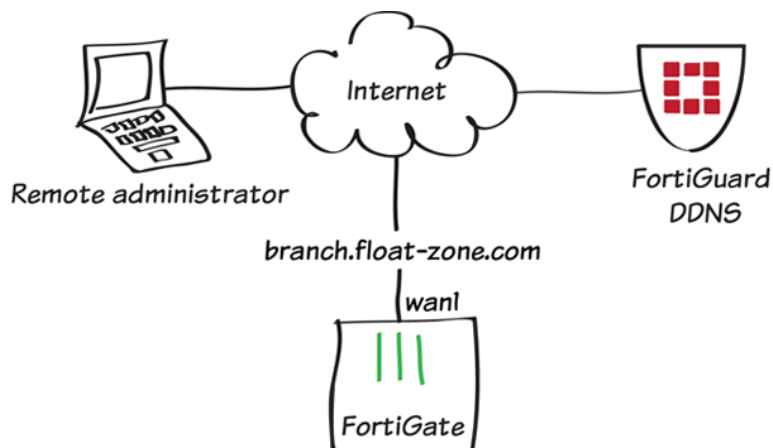


To ensure that TCP port 21 is open, use an FTP client to connect to the FTP server on the other side of the firewall.



For further reading, check out [Virtual IPs](#) in the [FortiOS 5.2 Handbook](#).

FortiGuard DDNS



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

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

1. Limited administrative access to trusted hosts

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

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

The screenshot shows a configuration page with a checked checkbox for "Restrict this Administrator Login from Trusted Hosts Only". Below this are six input fields for trusted hosts:

Trusted Host #1	192.168.200.110/32
Trusted Host #2	172.20.120.100/32
Trusted Host #3	0.0.0.0/0.0.0.0
IPv6 Trusted Host #1	::/0
IPv6 Trusted Host #2	::/0
IPv6 Trusted Host #3	::/0

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

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

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

The screenshot shows the "Administrative Access" section with several checkboxes:

<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input type="checkbox"/> HTTP	<input checked="" type="checkbox"/> FMG-Access	<input type="checkbox"/> CAPWAP
<input type="checkbox"/> SSH	<input type="checkbox"/> SNMP	<input type="checkbox"/> FCT-Access		

2. Setting up FortiGuard DDNS

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

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

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

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

The screenshot shows the "Enable FortiGuard DDNS" configuration page with the following fields:

<input checked="" type="checkbox"/> Enable FortiGuard DDNS	
Interface	wan1
Server	float-zone.com
Unique Location	branch
Domain	branch.float-zone.com (172.20.120.236)

You can also configure FortiGuard

```
config system ddns
```

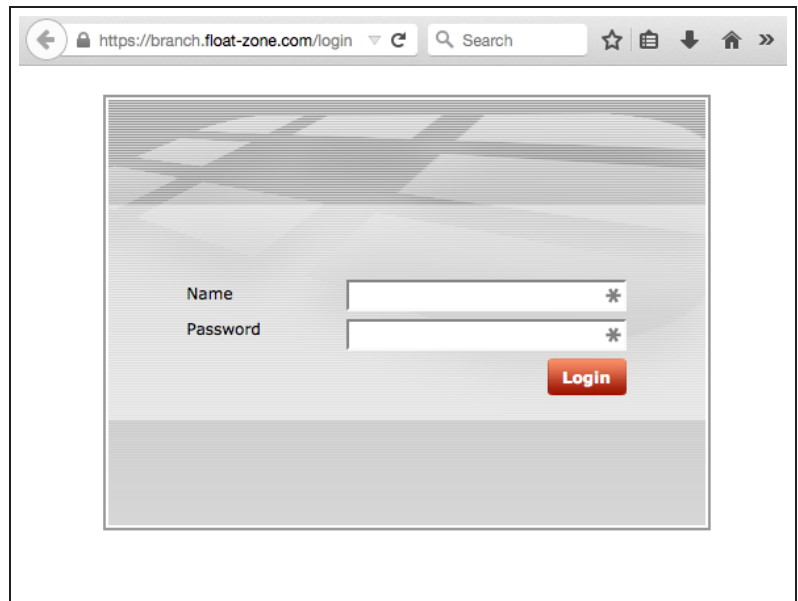

DDNS by using the following CLI commands:

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

3. Results

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

The FortiGate login screen will appear.



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

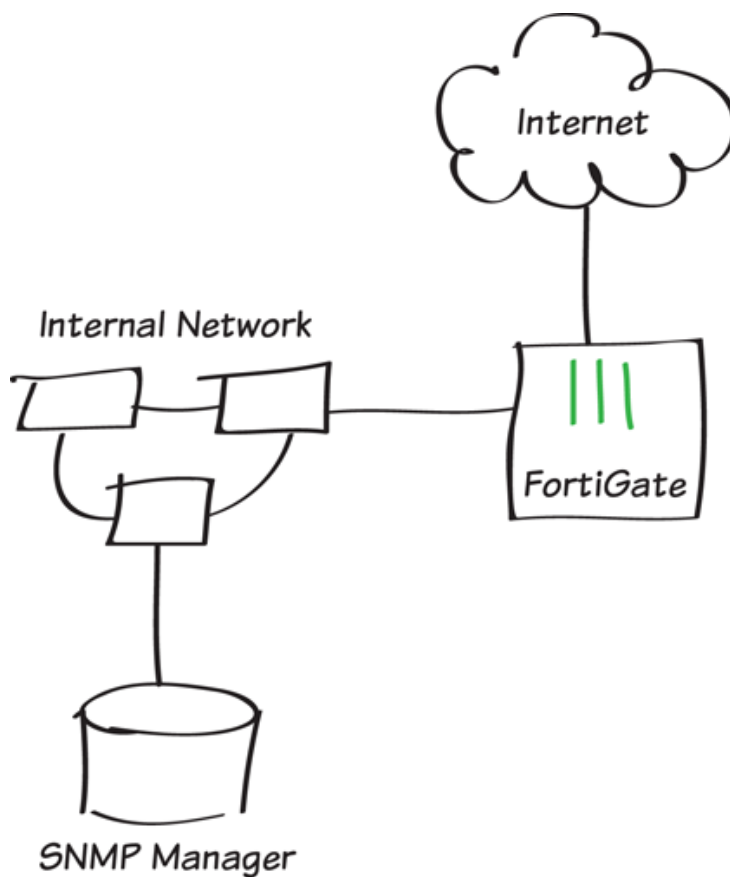
Change the interface's **IP Address/Netmask**.

Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicated to Extension Device
IP/Network Mask	<input type="text" value="172.20.120.237/255.255.255.0"/>

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

For further reading, check out [Dynamic DNS configuration](#) in the [FortiOS 5.2 Handbook](#).

SNMP monitoring



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

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

1. Configuring the FortiGate SNMP agent

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

SNMP Agent Enable

Description

Location

Contact

SNMP v1/v2c

<input type="checkbox"/>	Community Name	Queries	Traps	Enable
<input type="checkbox"/>	FortiGates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

SNMP v3

<input type="checkbox"/>	User Name	Security Level	Notification Host	Queries
--------------------------	-----------	----------------	-------------------	---------

FortiGate SNMP MIB

[Download FortiGate MIB File](#)

[Download Fortinet Core MIB File](#)

Under SNMP v1/v2c, create a new community.

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

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

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

Edit SNMP Community

Community Name FortiGates

Hosts:

IP Address/Netmask	Interface	Delete
<input type="text" value="192.168.1.114/255.255.255.255"/>	<input type="text" value="ANY"/>	

Add

Queries:

Protocol	Port	Enable
v1	<input type="text" value="161"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="161"/>	<input checked="" type="checkbox"/>

Traps:

Protocol	Local	Remote	Enable
v1	<input type="text" value="162"/>	<input type="text" value="162"/>	<input checked="" type="checkbox"/>
v2c	<input type="text" value="162"/>	<input type="text" value="162"/>	<input checked="" type="checkbox"/>

SNMP Events

- CPU usage is high
- Memory is low
- Log disk space is low
- Interface IP is changed
- VPN tunnel up
- VPN tunnel down
- WiFi Controller AP up
- WiFi Controller AP down

- HA cluster status is changed
- HA heartbeat failure
- HA member up
- HA member down

- Virus detected
- Matched file pattern detected
- Fragmented email detected
- Oversized file/email detected
- Oversized file/email blocked
- Oversized file/email passed
- AV bypass happens</

2. Enabling SNMP on a FortiGate interface

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

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

Edit Interface

Interface Name: Internal(00:09:0F:DF:43:48)
Alias:
Link Status: Up
Type: Physical Interface

Addressing mode: Manual DHCP PPPoE Dedicate to Extension Device
IP/Network Mask:

Administrative Access:
 HTTPS PING HTTP FMG-Access CAPWAP
 SSH SNMP FCT-Access
 Auto IPsec Request

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

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

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

SNMP Agent: Enable
Description:
Location:
Contact:

SNMP v1/v2c

	Community Name	Queries	Traps	Enable
<input type="checkbox"/>	FortiGates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

SNMP v3

	User Name	Security Level	Notification Host	Queries
--	-----------	----------------	-------------------	---------

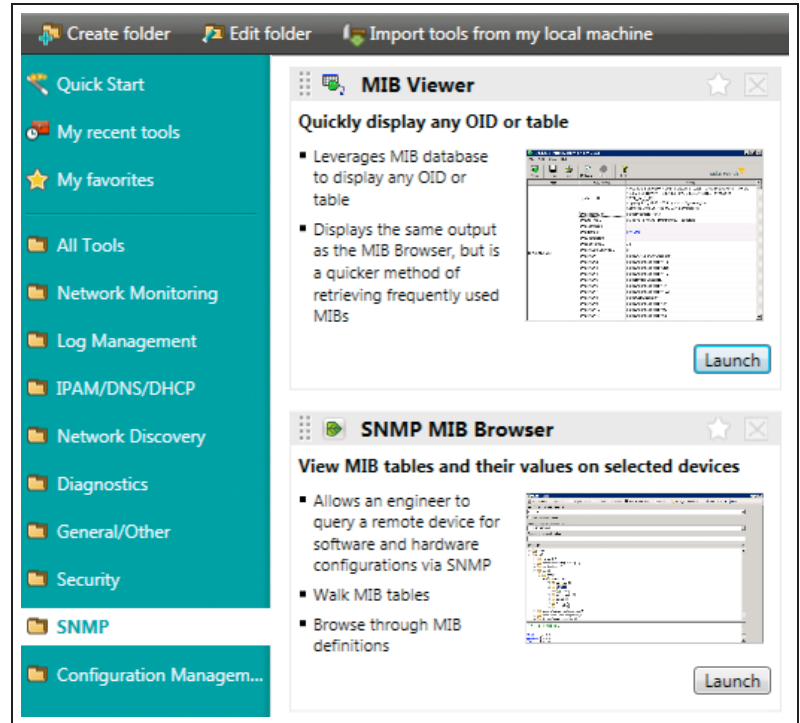
FortiGate SNMP MIB

[Download FortiGate MIB File](#)
[Download Fortinet Core MIB File](#)

4. Results

This example uses the SolarWinds SNMP trap viewer.

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



The screenshot displays the SolarWinds Toolset Launch Pad interface. On the left is a teal sidebar with a navigation menu. The main area on the right shows two tool cards under the 'SNMP' category.

Navigation Menu (Left Sidebar):

- Quick Start
- My recent tools
- My favorites
- All Tools
- Network Monitoring
- Log Management
- IPAM/DNS/DHCP
- Network Discovery
- Diagnostics
- General/Other
- Security
- SNMP**
- Configuration Managem...

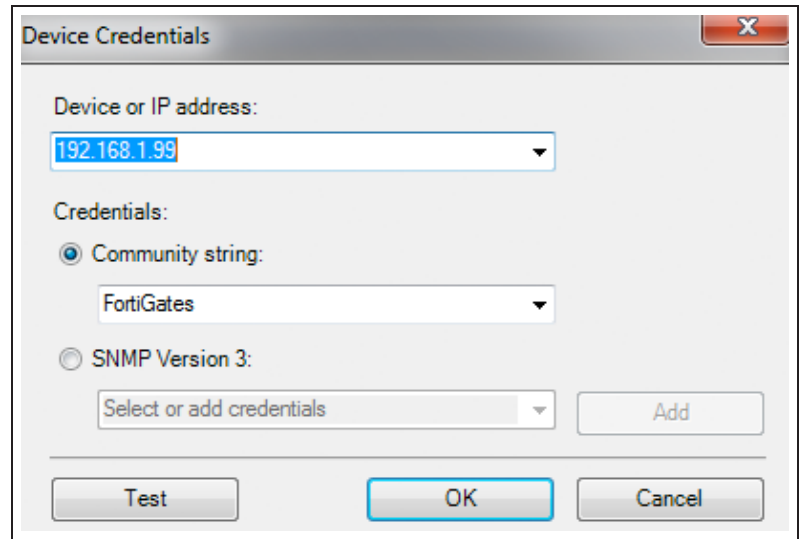
MIB Viewer Card:

- Quickly display any OID or table**
- Leverages MIB database to display any OID or table
- Displays the same output as the MIB Browser, but is a quicker method of retrieving frequently used MIBs
- Launch**

SNMP MIB Browser Card:

- View MIB tables and their values on selected devices**
- Allows an engineer to query a remote device for software and hardware configurations via SNMP
- Walk MIB tables
- Browse through MIB definitions
- Launch**

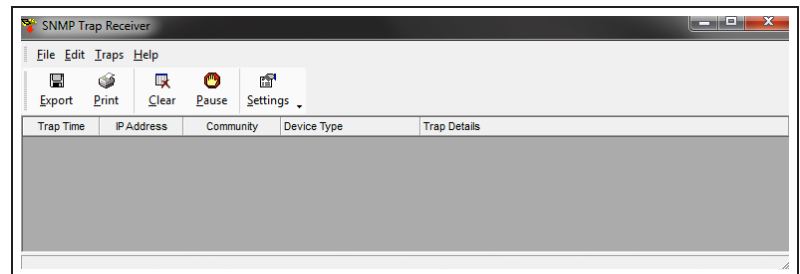
Choose **Select Device**, enter the IP address of the FortiGate unit, and choose the appropriate community string credentials.



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



The SNMP Trap Receiver will appear.



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

Edit Interface

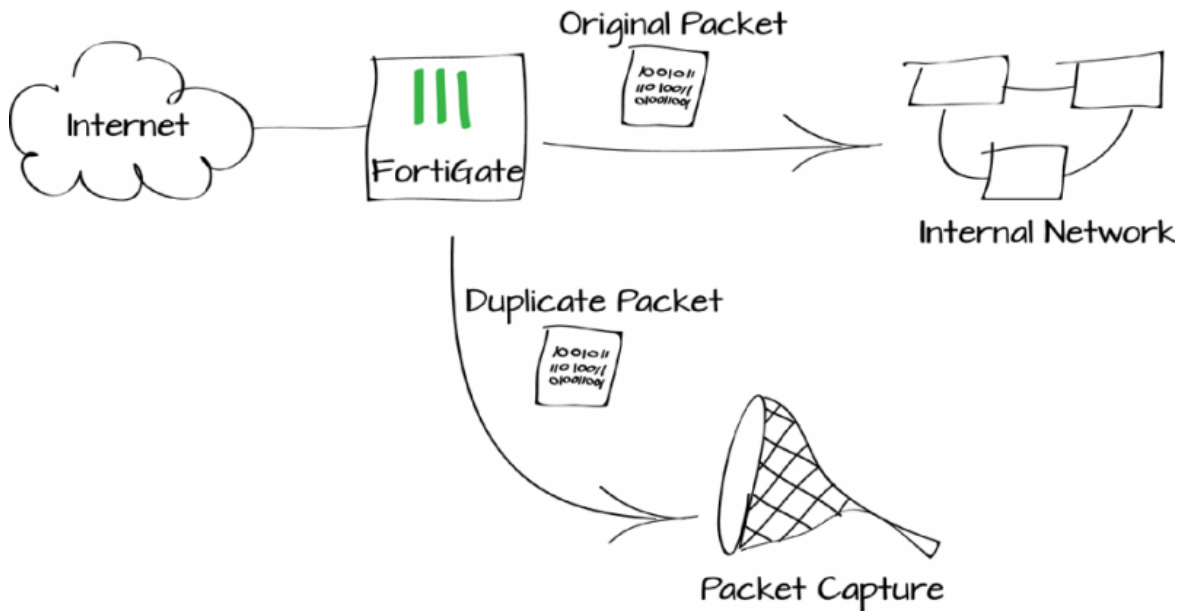
Interface Name	dmz(00:09:0F:DF:43:4B)
Alias	<input type="text"/>
Link Status	Down ●
Type	Physical Interface
Addressing mode	
	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> One-Arm Sniffer <input type="radio"/> Dedicate to Extension Device
IP/Network Mask	<input style="border: 1px solid blue;" type="text" value="10.10.10.10/255.255.255.0"/>

Verify that the SNMP manager receives the trap.

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

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

Packet capture



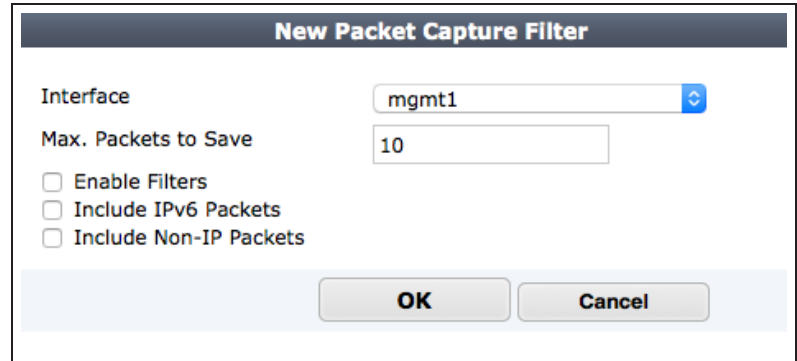
In this example, you will set up and run some basic packet capture filters on your FortiGate and download and view the resulting .pcap file.

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

1. Creating packet capture filters

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

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



New Packet Capture Filter

Interface: mgmt1

Max. Packets to Save: 10

Enable Filters

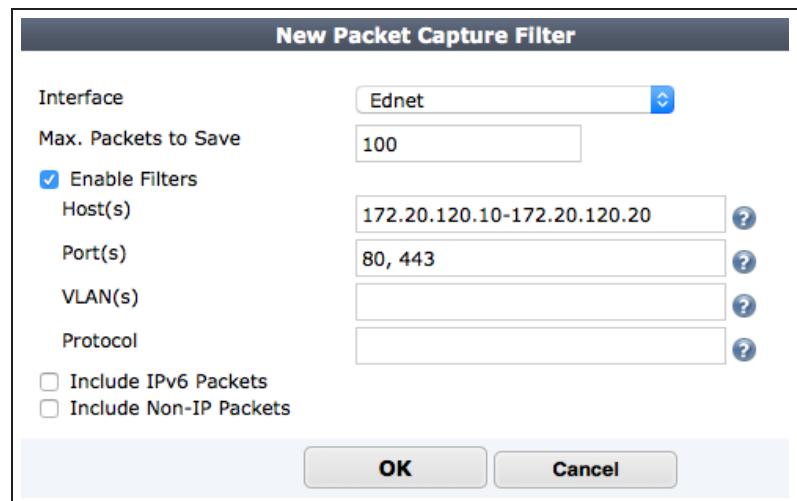
Include IPv6 Packets

Include Non-IP Packets

OK Cancel

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

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



New Packet Capture Filter

Interface: Ednet

Max. Packets to Save: 100

Enable Filters

Host(s): 172.20.120.10-172.20.120.20

Port(s): 80, 443

VLAN(s):

Protocol:

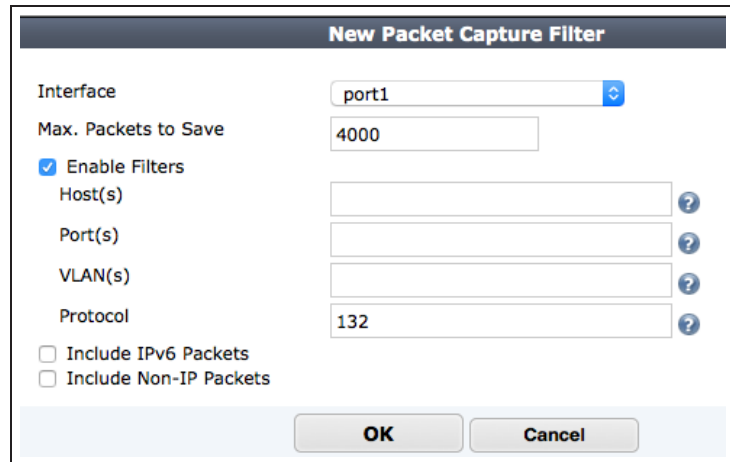
Include IPv6 Packets

Include Non-IP Packets

OK Cancel

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

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

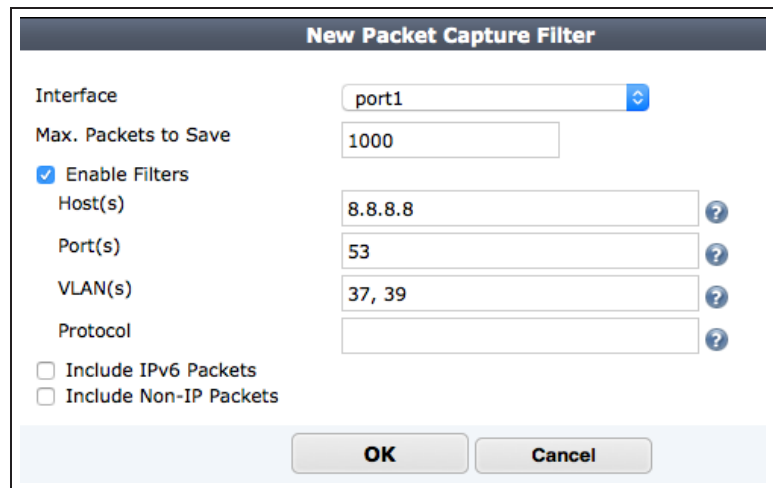


The dialog box is titled "New Packet Capture Filter". It contains the following fields and options:

- Interface: port1
- Max. Packets to Save: 4000
- Enable Filters
- Host(s):
- Port(s):
- VLAN(s):
- Protocol: 132
- Include IPv6 Packets
- Include Non-IP Packets

Buttons: OK, Cancel

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



The dialog box is titled "New Packet Capture Filter". It contains the following fields and options:

- Interface: port1
- Max. Packets to Save: 1000
- Enable Filters
- Host(s): 8.8.8.8
- Port(s): 53
- VLAN(s): 37, 39
- Protocol:
- Include IPv6 Packets
- Include Non-IP Packets

Buttons: OK, Cancel

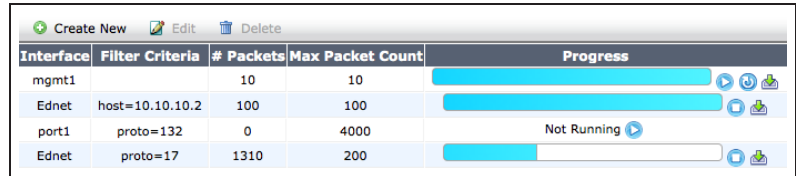
2. Results

Running packet capture filters may affect FortiGate performance.

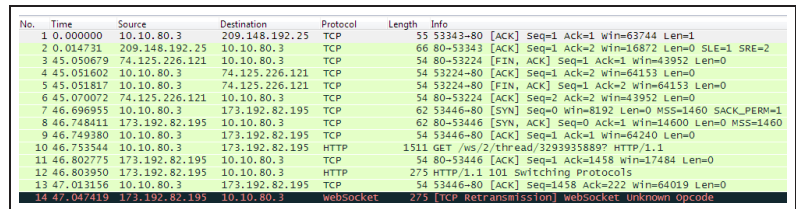
Go to **System > Network > Packet Capture**, choose a filter, and select the **Play** icon. You can watch the filter capture packets. When the number of packets specified in the filter are captured the filter stops.

You can stop and restart multiple filters at any time.

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



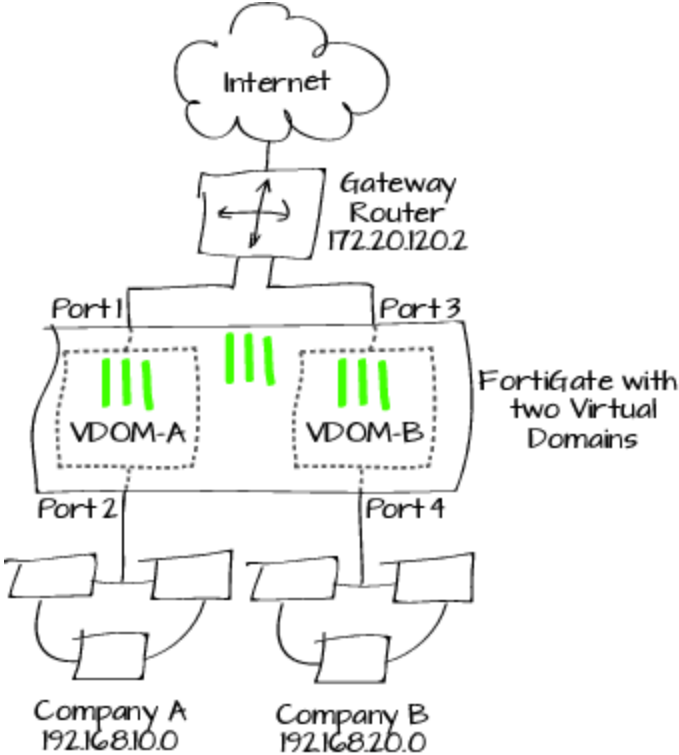
Interface	Filter Criteria	# Packets	Max Packet Count	Progress
mgmt1		10	10	<div style="width: 100%;"></div>
Ednet	host=10.10.10.2	100	100	<div style="width: 100%;"></div>
port1	proto=132	0	4000	Not Running
Ednet	proto=17	1310	200	<div style="width: 65.5%;"></div>



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

For further reading, check out [Monitoring](#) in the [FortiOS 5.2 Handbook](#).

VDOM configuration



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

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

1. Switching to VDOM mode and creating two VDOMS

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

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

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

System Information	
HA Status	Standalone [Configure]
Host Name	FGT60C3G10016011 [Change]
Serial Number	FGT60C3G10016011
System Time	Wed Dec 10 11:39:34 2014 (FortiGuard) [Change]
Firmware Version	v5.2.2,build642 (GA) [Update]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	20 day(s) 1 hour(s) 58 min(s)
Virtual Domain	Enabled [Disable]

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

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

Name	<input type="text" value="VDOM-A"/>
Enable	<input checked="" type="checkbox"/>
Operation Mode	<input type="button" value="NAT"/>
Comments	<input type="text" value="Write a comment..."/> 0/255

Name	<input type="text" value="VDOM-B"/>
Enable	<input checked="" type="checkbox"/>
Operation Mode	<input type="button" value="NAT"/>
Comments	<input type="text" value="Write a comment..."/> 0/255

2. Assigning interfaces to each VDOM

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

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

The screenshot shows the configuration for interface port1 (00:09:0F:B0:EB:F0). The Name is port1(00:09:0F:B0:EB:F0). The Link Status is Down. The Type is Physical Interface. The Virtual Domain is VDOM-A. The Addressing mode is Manual. The IP/Network Mask is 172.20.120.10/255.255.255.0. The IPv6 Address is ::/0.

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

The screenshot shows the configuration for interface port2 (00:09:0F:B0:EB:F1). The Name is port2(00:09:0F:B0:EB:F1). The Link Status is Down. The Type is Physical Interface. The Virtual Domain is VDOM-A. The Addressing mode is Manual. The IP/Network Mask is 192.168.10.1/255.255.255.0. The IPv6 Address is ::/0. Administrative Access is enabled for HTTPS, PING, and SSH. The DHCP Server is enabled. The Address Range is 192.168.10.2 to 192.168.10.254. The Netmask is 255.255.255.0.

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

The screenshot shows the configuration for interface port3 (00:09:0F:B0:EB:F2). The Name is port3(00:09:0F:B0:EB:F2). The Link Status is Down. The Type is Physical Interface. The Virtual Domain is VDOM-B. The Addressing mode is Manual. The IP/Network Mask is 172.20.120.20/255.255.255.0. The IPv6 Address is ::/0.

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

Interface Name	internal4(00:09:0F:DF:43:4D)				
Alias	<input type="text"/>				
Link Status	Down				
Type	Physical Interface				
Virtual Domain	VDOM-B				
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicated to Extension Device				
IP/Network Mask	<input type="text" value="192.168.20.1/255.255.255.0"/>				
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP <input checked="" type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access <input type="checkbox"/> Auto IPsec Request				
DHCP Server	<input checked="" type="checkbox"/> Enable				
Address Range	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> ➤ Create New ✎ Edit 🗑 Delete </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Starting IP</th> <th style="text-align: left;">End IP</th> </tr> </thead> <tbody> <tr> <td>192.168.20.2</td> <td>192.168.20.254</td> </tr> </tbody> </table> </div>	Starting IP	End IP	192.168.20.2	192.168.20.254
Starting IP	End IP				
192.168.20.2	192.168.20.254				
Netmask	<input type="text" value="255.255.255.0"/>				

3. Creating administrators for each VDOM

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

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

Administrator	<input type="text" value="a-admin"/>
Type	<input checked="" type="radio"/> Regular <input type="radio"/> Remote <input type="radio"/> PKI
Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Admin Profile	<input type="text" value="prof_admin"/>
Virtual Domain	<input type="text" value="VDOM-A"/>

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

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

Administrator	<input type="text" value="b-admin"/>
Type	<input checked="" type="radio"/> Regular <input type="radio"/> Remote <input type="radio"/> PKI
Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Admin Profile	<input type="text" value="prof_admin"/>
Virtual Domain	<input type="text" value="VDOM-B"/>

4. Creating a basic configuration for VDOM-A

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

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

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

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

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

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

Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Device	<input type="text" value="internal1 (port1)"/>
Gateway	<input type="text" value="172.20.120.2"/>

Incoming Interface	<input type="text" value="internal2 (port2)"/>
Source Address	<input type="text" value="all"/>
Source User(s)	<input type="text" value="Click to add..."/>
Source Device Type	<input type="text" value="Click to add..."/>
Outgoing Interface	<input type="text" value="internal1 (port1)"/>
Destination Address	<input type="text" value="all"/>
Schedule	<input type="text" value="always"/>
Service	<input type="text" value="ALL"/>
Action	<input type="text" value="ACCEPT"/>
Firewall / Network Options	
<input checked="" type="checkbox"/> NAT	
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	<input type="text" value="Click to add..."/>

5. Creating a basic configuration for VDOM-B

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

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

Go to **System > Network > Routing**

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

Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Device	<input type="text" value="internal3 (port3)"/>
Gateway	<input type="text" value="172.20.120.2"/>

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

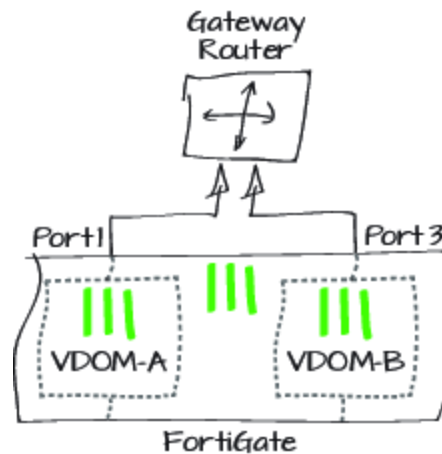
Go to **Policy & Objects > Policy > IPv4**

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

Incoming Interface	internal4 (port4)
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	internal3 (port3)
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
Firewall / Network Options	
<input checked="" type="checkbox"/> ON NAT	
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...

6. Connecting the gateway router

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



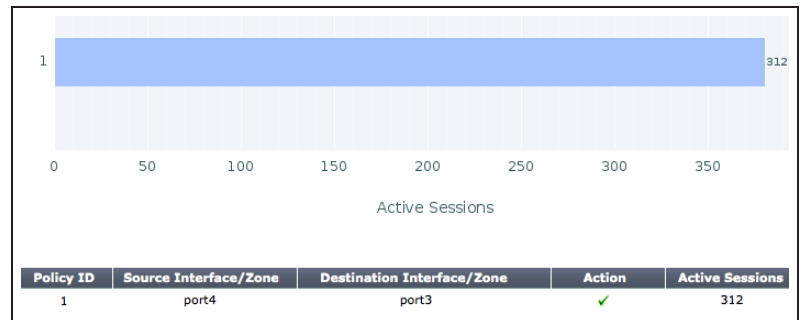
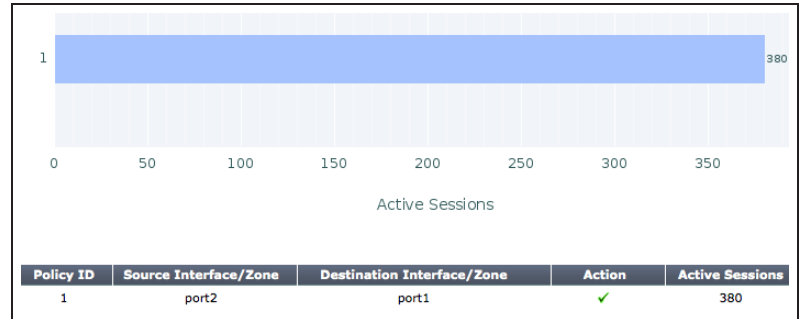
7. Results

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

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

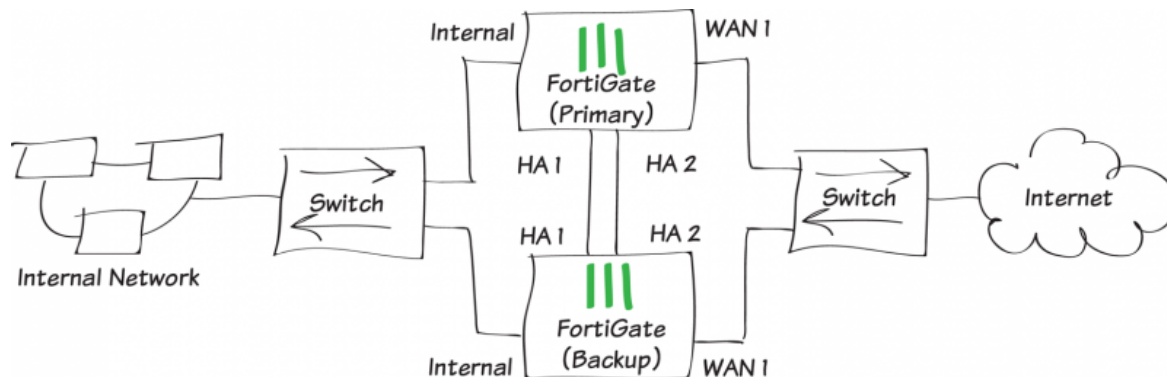
Go to **Policy & Objects > Monitor > Policy Monitor** to view the sessions being processed on VDOM-A.

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



For further reading, check out [Virtual Domains](#) in the [FortiOS 5.2 Handbook](#).

High Availability with two FortiGates



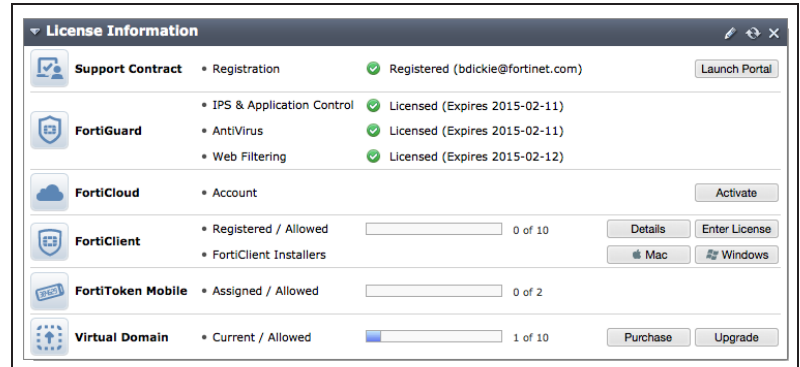
In this recipe, a backup FortiGate unit will be installed and connected to a FortiGate unit that has previously been installed to provide redundancy if the primary FortiGate unit fails. This set up, called High Availability (HA), improves network reliability.

If you have not already installed a FortiGate, see [Installing a FortiGate in NAT/Route mode](#).

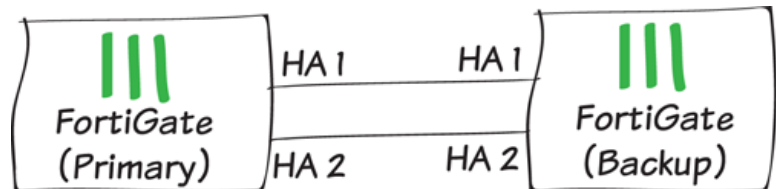
A video of this recipe is available [here](#).

1. Adding the backup FortiGate unit and configuring HA

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

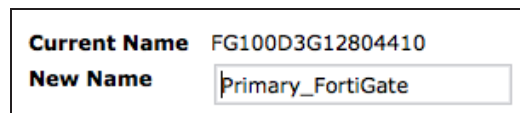


Connect your network as shown in the initial diagram, with Ethernet cables connecting the **HA** heartbeat interfaces of the two FortiGate units. If your FortiGate unit does not have dedicated HA heartbeat interfaces, you can use different interfaces, provided they are not used for any other function.



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

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



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

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

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

Mode Active-Passive

Device Priority

Reserve Management Port for Cluster Member Internal

Cluster Settings

Group Name

Password

Enable Session Pick-up

	Port Monitor	Heartbeat Interface	
		Enable	Priority(0-512)
dmz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
ha1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="50"/>
ha2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="50"/>
mgmt	<input type="checkbox"/>		
port9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
port10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
port11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
port14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
port15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
port16	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
wan1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
wan2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

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

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

Current Name FG100D3G12801361

New Name

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

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

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

Mode

Device Priority

Reserve Management Port for Cluster Member

Cluster Settings

Group Name

Password

Enable Session Pick-up

	Port Monitor	Heartbeat Interface	
		Enable	Priority(0-512)
dmz	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
ha1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="50"/>
ha2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="50"/>
mgmt	<input type="checkbox"/>		
port1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
wan1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
wan2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

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

Cluster Member	Hostname	Serial No.	Role	Priority
	Primary_FortiGate	FG100D3G12804410	MASTER	128
	Backup_FortiGate	FG100D3G12801361	SLAVE	50

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

Unit	Status	Up Time	Monitor			
Primary_FortiGate FG100D3G12804410	✔	0 days	CPU Usage	Active Sessions	Total Packets	Virus Detected
		1 hours	1%	26	81857	0
		44 minutes	Memory Usage	Network Utilization	Total Bytes	Intrusion Detected
		2 seconds	34%	78 Kbps	27300058	0
Backup_FortiGate FG100D3G12801361	✔	2 days	CPU Usage	Active Sessions	Total Packets	Virus Detected
		0 hours	0%	6	8718576	0
		15 minutes	Memory Usage	Network Utilization	Total Bytes	Intrusion Detected
		15 seconds	19%	13 Kbps	2778691497	0

2. Results

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

To test this, ping the IP address 8.8.8.8 using a PC on the internal network. After a moment, power off the primary FortiGate

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

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

```

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

```


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

For information about accessing firmware images, see [Updating your FortiGate's firmware](#).

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

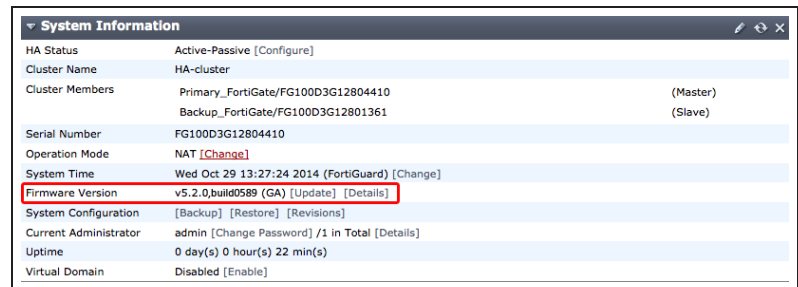
Always review the Release Notes and Supported Upgrade Paths documentation before installing new firmware. These documents can be found at the [Fortinet Document Library](#).

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

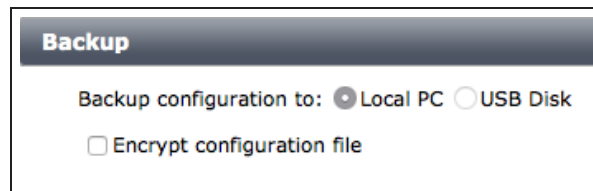
Select **Backup** beside **System Configuration**. Always remember to back up your configuration before doing any firmware upgrades.

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

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



System Information	
HA Status	Active-Passive [Configure]
Cluster Name	HA-cluster
Cluster Members	Primary_FortiGate/FG100D3G12804410 (Master) Backup_FortiGate/FG100D3G12801361 (Slave)
Serial Number	FG100D3G12804410
Operation Mode	NAT [Change]
System Time	Wed Oct 29 13:27:24 2014 (FortiGuard) [Change]
Firmware Version	v5.2.0,build0589 (GA) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	0 day(s) 0 hour(s) 22 min(s)
Virtual Domain	Disabled [Enable]



Backup

Backup configuration to: Local PC USB Disk

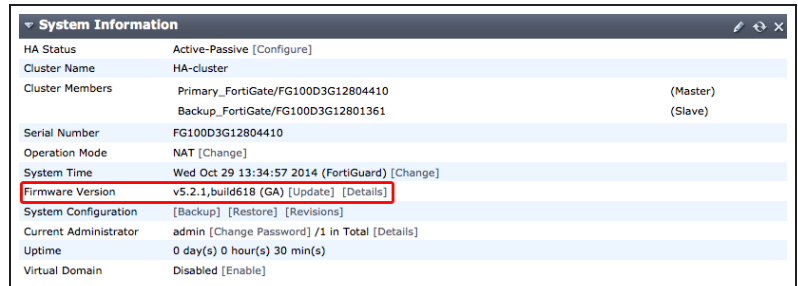
Encrypt configuration file



Upgrade From: Local Hard Disk

Upgrade File: Browse... FGT_100D-v5-build0618-FORTINET.out

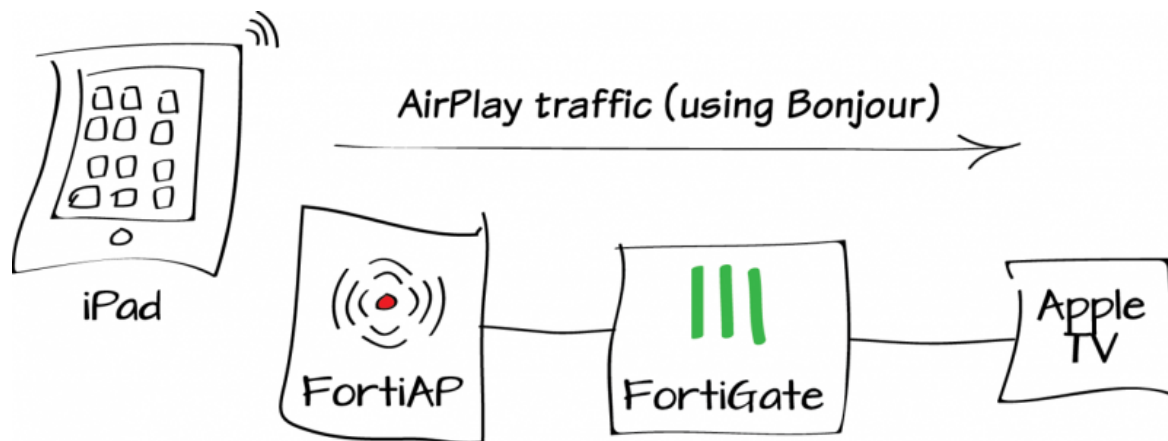
Go to **System > Dashboard > Status** and verify that the **System Information** widget shows the new firmware version.



System Information	
HA Status	Active-Passive [Configure]
Cluster Name	HA-cluster
Cluster Members	Primary_FortiGate/FG100D3G12804410 (Master)
	Backup_FortiGate/FG100D3G12801361 (Slave)
Serial Number	FG100D3G12804410
Operation Mode	NAT [Change]
System Time	Wed Oct 29 13:34:57 2014 (FortiGuard) [Change]
Firmware Version	v5.2.1, build618 (GA) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] / 1 in Total [Details]
Uptime	0 day(s) 0 hour(s) 30 min(s)
Virtual Domain	Disabled [Enable]

For further reading, check out [Configuring and connecting HA clusters in the FortiOS 5.2 Handbook](#).

AirPlay for Apple TV



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

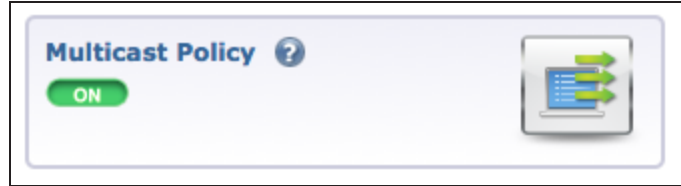
Apple TV can also be connected to the Internet wirelessly. AirPlay will function from any iOS device connected to the same SSID as the Apple TV, without any configuration required on the FortiGate.

This recipe uses a FortiAP in Tunnel mode. For more information, see [Setting up WiFi with FortiAP](#).

1. Enabling multicast policies

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

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



2. Creating AirPlay services

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

Name	AirPlay - Apple TV to iOS		
Comments	<input type="text"/> 0/255		
Show in Service List	<input checked="" type="checkbox"/>		
Category	Uncategorized		
Protocol Type	TCP/UDP/SCTP		
IP/FQDN	<input type="text"/>		
		Destination Port	<input style="float: right;" type="button" value="+"/>
		Low	High
Protocol	<input type="button" value="TCP"/>	<input type="text" value="7000"/>	<input type="text" value=""/> ×
	<input type="button" value="UDP"/>	<input type="text" value="1"/>	<input type="text" value="65535"/> ×
Specify Source Ports	<input type="checkbox"/>		

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

Name	AirPlay - iOS to Apple TV		
Comments			
Show in Service List	<input checked="" type="checkbox"/>		
Category	Uncategorized		
Protocol Type	TCP/UDP/SCTP		
IP/FQDN			
	Destination Port		<input style="color: green;" type="button" value="+"/>
	Low	High	
Protocol	TCP	7000 -	<input type="text"/>
	TCP	7100 -	<input type="text"/>
	TCP	49152 -	50000
	UDP	1 -	65535
Specify Source Ports	<input type="checkbox"/>		

3. Allowing multicast between the wireless and internal networks

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

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

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

Incoming Interface	lan (VLAN ID: 0)
Source Address	all <input style="color: green;" type="button" value="+"/>
Outgoing Interface	wireless (SSID: myWifi)
Destination Address	Bonjour <input style="color: green;" type="button" value="+"/>
<input type="checkbox"/> Enable SNAT	
DNAT	0.0.0.0
Protocol	UDP
Port Range	1-5353
Action	<input checked="" type="checkbox"/> ACCEPT
<input checked="" type="checkbox"/> Log Allowed Traffic	
<input checked="" type="checkbox"/> Enable this policy	

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

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

Incoming Interface	wireless (SSID: myWifi)
Source Address	all
Outgoing Interface	lan (VLAN ID: 0)
Destination Address	Bonjour
<input type="checkbox"/> Enable SNAT	
DNAT	0.0.0.0
Protocol	UDP
Port Range	1-5353
Action	ACCEPT
<input checked="" type="checkbox"/> Log Allowed Traffic	
<input checked="" type="checkbox"/> Enable this policy	

4. Allowing airplay between the wireless and internal networks

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

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

Incoming Interface	lan (VLAN ID: 0)
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wireless (SSID: myWifi)
Destination Address	all
Schedule	always
Service	AirPlay - Apple TV to iOS
Action	ACCEPT
Firewall / Network Options	
<input checked="" type="checkbox"/> NAT	
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...

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

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

Incoming Interface	wireless (SSID: myWifi)
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	lan (VLAN ID: 0)
Destination Address	all
Schedule	always
Service	AirPlay - iOS to Apple TV
Action	ACCEPT
Firewall / Network Options	
<input checked="" type="checkbox"/> NAT	
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...

5. Results

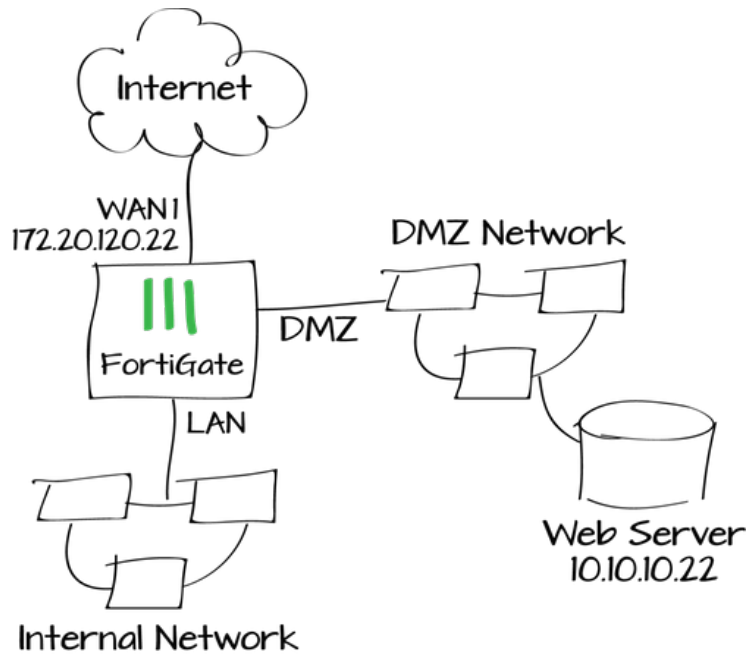
Use AirPlay to stream audio or video from an iOS device to the Apple TV.

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

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

For further reading, check out [Multicast forwarding](#) in the [FortiOS 5.2 Handbook](#).

Protect a web server with DMZ



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

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

1. Configuring the FortiGate's DMZ interface

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

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

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

Interface Name	dmz(00:09:0F:99:4B:E5)
Alias	<input type="text" value="DMZ server network"/>
Link Status	Up
Type	Physical Interface
<hr/>	
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> One-Arm Sniffer <input type="radio"/> Dedicated to Extension Device
IP/Network Mask	<input type="text" value="10.10.10.1/255.255.255.0"/>
<hr/>	
Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access
<hr/>	
DHCP Server	<input type="checkbox"/> Enable
<hr/>	
Security Mode	<input type="text" value="None"/>
<hr/>	
Device Management	<input type="checkbox"/> Detect and Identify Devices
<hr/>	
Listen for RADIUS Accounting Messages	<input type="checkbox"/>
Secondary IP Address	<input type="checkbox"/>
<hr/>	
Comments	<input type="text" value=""/> <small>0/255</small>
Administrative Status	<input checked="" type="radio"/> Up <input type="radio"/> Down

2. Creating virtual IPs (VIPs)

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

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

Name	Web server http access	
Comments	<input type="text"/> 0/255	
Interface	wan1	
Type	Static NAT	
<input type="checkbox"/> Source Address Filter		
External IP Address/Range	172.20.120.22	- 172.20.120.22
Mapped IP Address/Range	10.10.10.22	- 10.10.10.22
<input checked="" type="checkbox"/> Port Forwarding		
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP <input type="radio"/> ICMP	
External Service Port	80	- 80
Map to Port	80	- 80

Name	Web server https access	
Comments	<input type="text"/> 0/255	
Interface	wan1	
Type	Static NAT	
<input type="checkbox"/> Source Address Filter		
External IP Address/Range	172.20.120.22	- 172.20.120.22
Mapped IP Address/Range	10.10.10.22	- 10.10.10.22
<input checked="" type="checkbox"/> Port Forwarding		
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP <input type="radio"/> ICMP	
External Service Port	443	- 443
Map to Port	443	- 443

3. Creating security policies

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

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

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

The screenshot shows the configuration for a security policy. The fields are as follows:

Incoming Interface	wan1
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	dmz (DMZ server network)
Destination Address	Web server http access, Web server https access
Schedule	always
Service	HTTP, HTTPS
Action	ACCEPT

Firewall / Network Options

OFF NAT

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

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

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

The screenshot shows the configuration for a second security policy. The fields are as follows:

Incoming Interface	Internal
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	dmz (DMZ server network)
Destination Address	all
Schedule	always
Service	HTTP, HTTPS
Action	ACCEPT

Firewall / Network Options

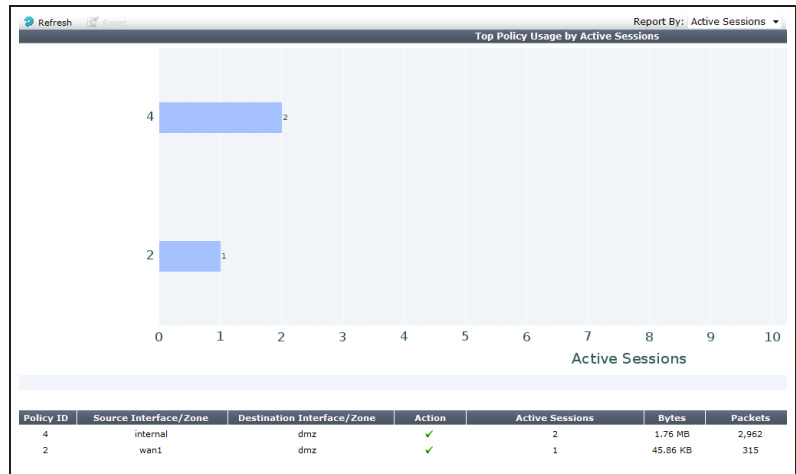
OFF NAT

4. Results

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

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

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



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

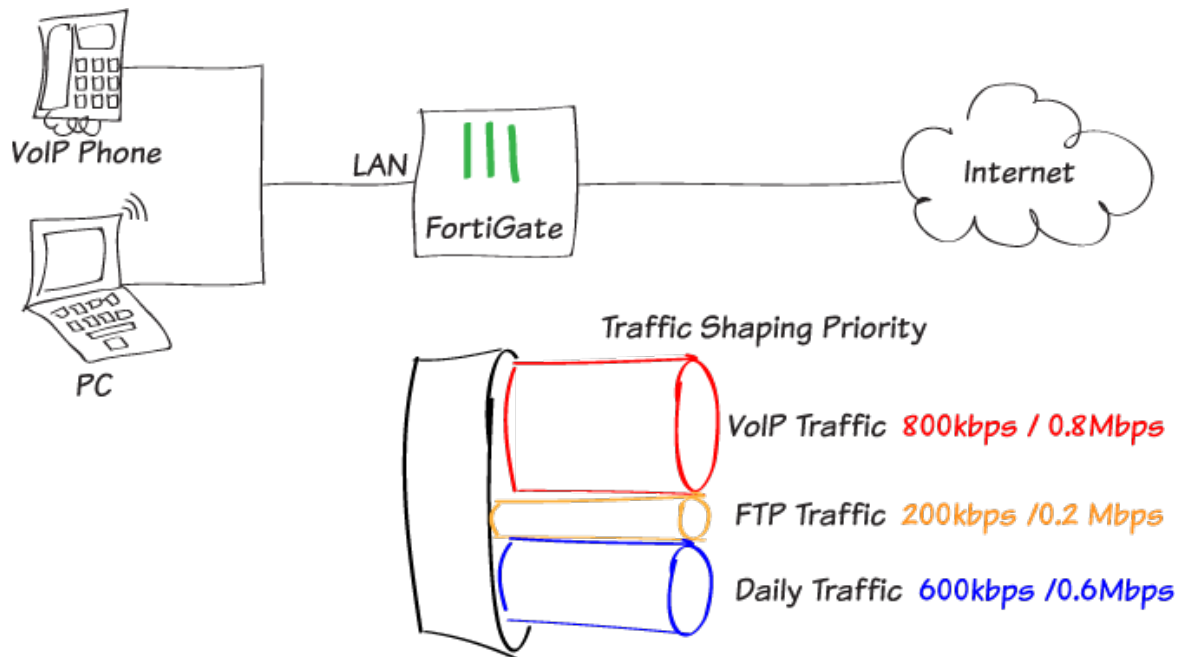
The traffic log shows sessions from the internal network and from the Internet accessing the web server on the DMZ network.

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received	Policy ID	Service
3	3 seconds ago	internal	dmz	192.168.100.110	10.10.10.22	48 B / 40 B	4	HTTP
4	3 seconds ago	internal	dmz	192.168.100.110	10.10.10.22	0 B / 0 B	4	HTTP
5	4 seconds ago	internal	dmz	192.168.100.110	10.10.10.22	0 B / 0 B	4	HTTP
6	31 seconds ago	internal	dmz	192.168.100.110	10.10.10.22	1.21 KB / 1.59 KB	4	HTTPS
7	31 seconds ago	internal	dmz	192.168.100.110	10.10.10.22	1.16 KB / 1.63 KB	4	HTTPS
8	33 seconds ago	internal	dmz	192.168.100.110	10.10.10.22	839 B / 1.40 KB	4	HTTPS

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Dst NAT IP	Policy ID	Service
1	4 seconds ago	wan1	dmz	172.20.120.21	172.20.120.22	10.10.10.22	2	HTTP
2	57 seconds ago	wan1	dmz	172.20.120.123	172.20.120.22	10.10.10.22	2	HTTPS
3	1 minute ago	wan1	dmz	172.20.120.123	172.20.120.22	10.10.10.22	2	HTTPS

For further reading, check out [Firewall](#) in the [FortiOS 5.2 Handbook](#).

Traffic shaping for VoIP



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

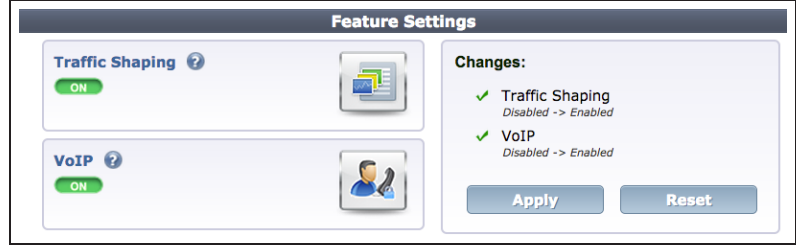
To achieve high quality real-time voice transmissions, VoIP traffic requires priority over other types of traffic, minimal packet loss, and jitter buffers. You will limit bandwidth consuming services, like FTP, while providing a consistent bandwidth for day-to-day email and web-based traffic. First,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

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

1. Enabling Traffic Shaping and VoIP features

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

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



The screenshot shows the 'Feature Settings' interface. On the left, there are two sections: 'Traffic Shaping' and 'VoIP', both with a green 'ON' indicator and a help icon. On the right, a 'Changes:' section lists 'Traffic Shaping' and 'VoIP', both with green checkmarks and the text 'Disabled -> Enabled'. At the bottom right, there are 'Apply' and 'Reset' buttons.

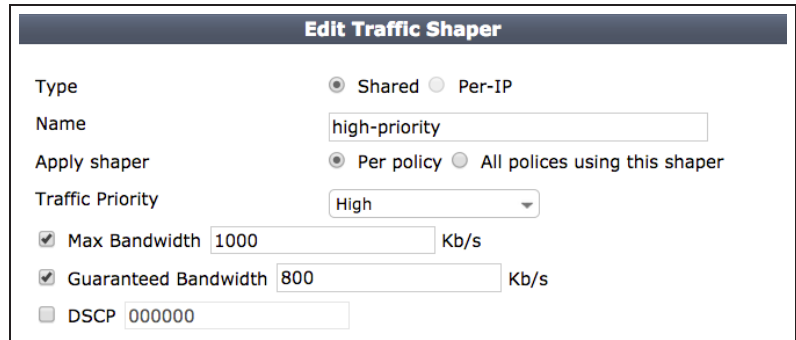
2. Configuring a high priority VoIP traffic shaper

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

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

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

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



The screenshot shows the 'Edit Traffic Shaper' configuration page. The 'Type' is set to 'Shared'. The 'Name' is 'high-priority'. The 'Apply shaper' is set to 'Per policy'. The 'Traffic Priority' is set to 'High'. The 'Max Bandwidth' is 1000 Kb/s, 'Guaranteed Bandwidth' is 800 Kb/s, and 'DSCP' is 000000.

3. Configuring a low priority FTP traffic shaper

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

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

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

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

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

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

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

Edit Traffic Shaper

Type Shared Per-IP

Name

Apply shaper Per policy All policies using this shaper

Traffic Priority

Max Bandwidth Kb/s

Guaranteed Bandwidth Kb/s

DSCP

4. Configuring a medium priority daily traffic shaper

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

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

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

Edit Traffic Shaper

Type Shared Per-IP

Name

Apply shaper Per policy All policies using this shaper

Traffic Priority

Max Bandwidth Kb/s

Guaranteed Bandwidth Kb/s

DSCP

5. Applying each shaper to a device-based policy

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

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

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

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

New Policy	
Incoming Interface	lan (VLAN ID: 0)
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1 (external)
Destination Address	all
Schedule	always
Service	SIP
Action	ACCEPT
Firewall / Network Options	
<input checked="" type="checkbox"/> NAT	
<input type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...
Security Profiles	
<input type="checkbox"/> AntiVirus	default
<input type="checkbox"/> Web Filter	default
<input type="checkbox"/> Application Control	default
<input checked="" type="checkbox"/> VoIP	default
<input checked="" type="checkbox"/> SSL/SSH Inspection	certificate-inspection
Traffic Shaping	
<input checked="" type="checkbox"/> Shared Shaper	high-priority
<input checked="" type="checkbox"/> Reverse Shaper	high-priority
<input type="checkbox"/> Per-IP Shaper	Click to set...
Logging Options	
<input checked="" type="checkbox"/> Log Allowed Traffic	
<input type="checkbox"/> Security Events	
<input checked="" type="checkbox"/> All Sessions	

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

New Policy	
Incoming Interface	lan (VLAN ID: 0)
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1 (external)
Destination Address	all
Schedule	always
Service	FTP
Action	<input checked="" type="checkbox"/> ACCEPT
Firewall / Network Options	
<input checked="" type="checkbox"/> NAT	
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...
Security Profiles	
<input type="checkbox"/> AntiVirus	default
<input type="checkbox"/> Web Filter	default
<input type="checkbox"/> Application Control	default
<input type="checkbox"/> VoIP	default
<input type="checkbox"/> SSL/SSH Inspection	certificate-inspection
Traffic Shaping	
<input checked="" type="checkbox"/> Shared Shaper	low-priority
<input checked="" type="checkbox"/> Reverse Shaper	low-priority
<input type="checkbox"/> Per-IP Shaper	Click to set...
Logging Options	
<input checked="" type="checkbox"/> Log Allowed Traffic	
<input type="checkbox"/> Security Events	
<input checked="" type="checkbox"/> All Sessions	

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

You can also edit your existing general access security policy.

Edit Policy

Incoming Interface	lan (VLAN ID: 0) +
Source Address	all +
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1 (external) +
Destination Address	all +
Schedule	always
Service	ALL +
Action	ACCEPT +

Firewall / Network Options

NAT

Use Outgoing Interface Address Fixed Port

Use Dynamic IP Pool Click to add...

Security Profiles

AntiVirus default

Web Filter default

Application Control default

VoIP default ⚙

SSL/SSH Inspection certificate-inspection ⚙

Traffic Shaping

Shared Shaper medium-priority ⚙

Reverse Shaper medium-priority ⚙

Per-IP Shaper Click to set...

Logging Options

Log Allowed Traffic

Security Events

All Sessions

Arrange your policies in the following order:

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

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

Seq.#	From	To	Source	Destination	Traffic Shaper	Service	Action
1	lan	wan1 (external)	all	all	high-priority high-priority	SIP	ACCEPT
2	lan	wan1 (external)	all	all	low-priority low-priority	FTP	ACCEPT
3	lan	wan1 (external)	all	all	medium-priority medium-priority	ALL	ACCEPT
4	any	any	all	all		ALL	DENY

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

6. Results

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

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

The FTP download or upload should occur slowly.

Finally, generate SIP traffic.

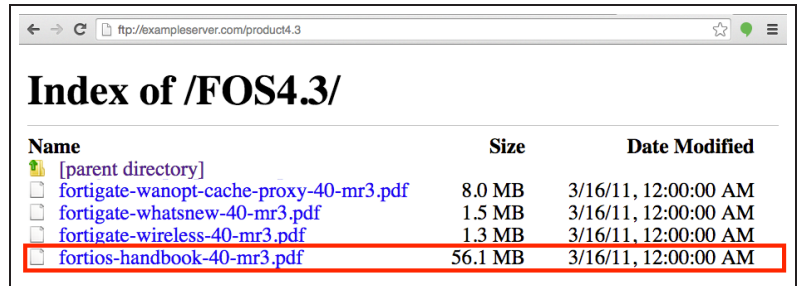
In this example, SIP traffic was generated by placing a call with a VoIP FortiFone connected to the internal interface of the FortiGate.

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

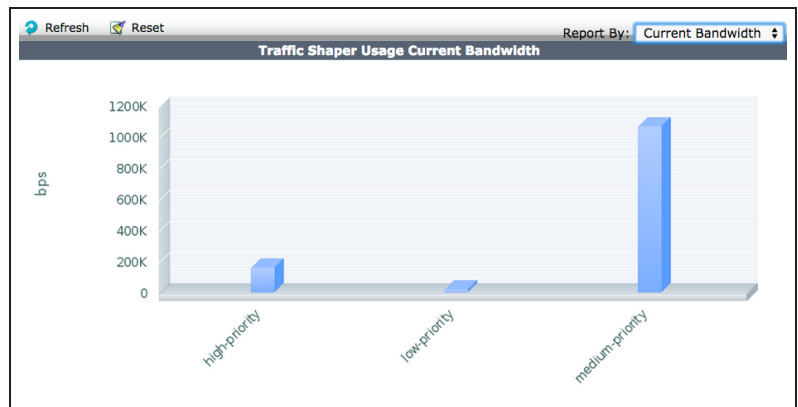
In the screenshot, the SIP traffic is only using a small part of the allocated bandwidth.

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

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



Name	Size	Date Modified
[parent directory]		
fortigate-wanopt-cache-proxy-40-mr3.pdf	8.0 MB	3/16/11, 12:00:00 AM
fortigate-whatsnew-40-mr3.pdf	1.5 MB	3/16/11, 12:00:00 AM
fortigate-wireless-40-mr3.pdf	1.3 MB	3/16/11, 12:00:00 AM
fortios-handbook-40-mr3.pdf	56.1 MB	3/16/11, 12:00:00 AM



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

For further reading, check out [Traffic Shaping](#) in the [FortiOS 5.2 Handbook](#).

Security

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

Application Control

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

Data Leak Prevention

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

Intrusion Protection

- Protecting a web server
- Logging DNS domain lookups

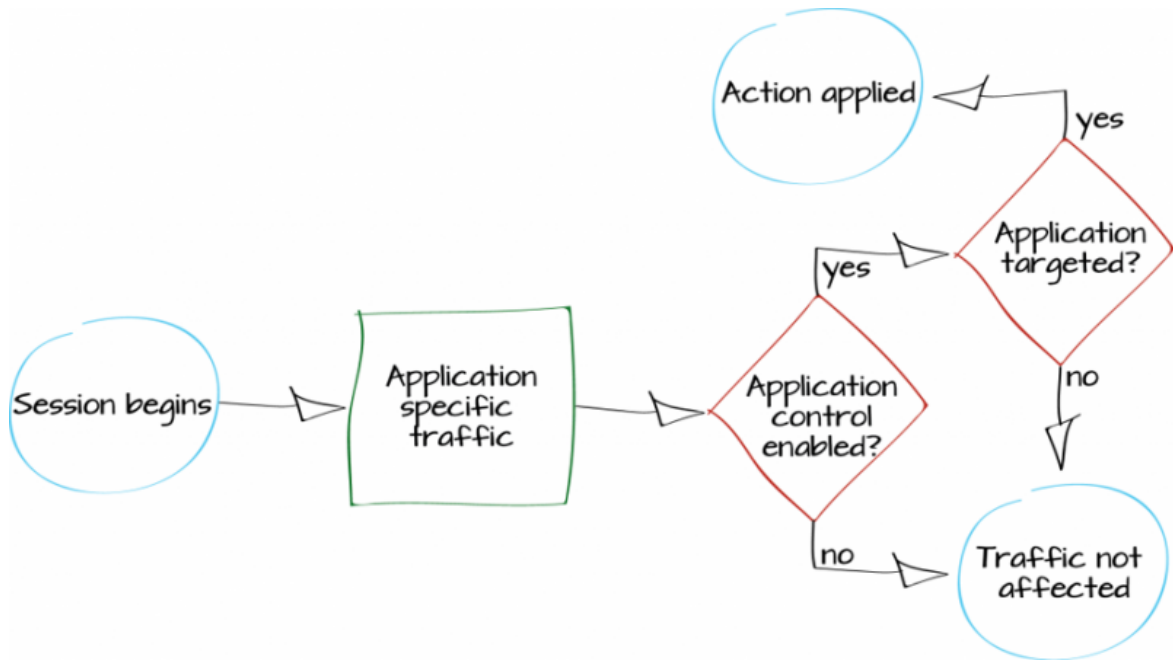
SSL Inspection

- Why you should use SSL inspection
- Preventing certificate warnings

Web Filtering

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

Blocking P2P traffic and YouTube applications

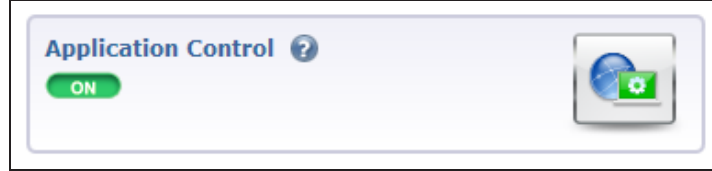


In this example, you will learn how to use Application Control to monitor traffic and determine if there are any applications currently in use that should not have network access. If you discover any applications that you wish to block, application control will then be used to ensure that these applications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

A video of this recipe is available [here](#).

1. Enabling Application Control and multiple security profiles

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



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

Apply the changes.

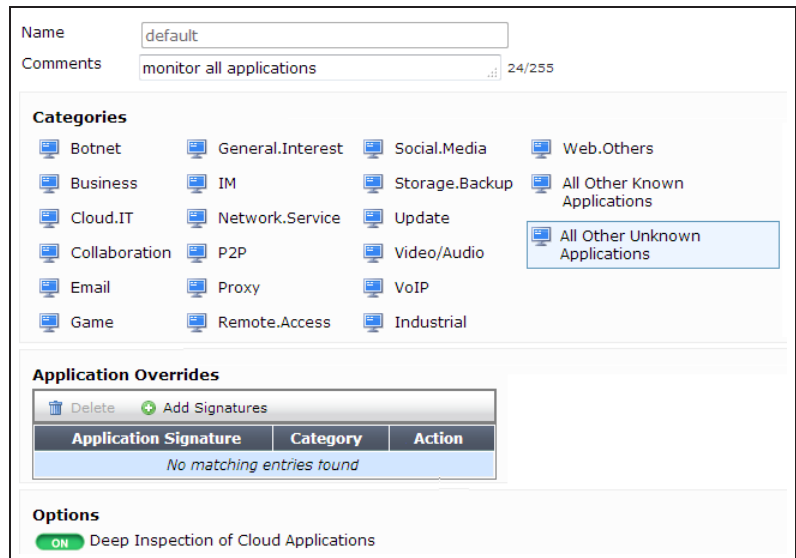


2. Using the default application profile to monitor network traffic

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

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

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



3. Adding the default profile to a security policy

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

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

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

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

The screenshot shows the configuration for a Security Policy. The 'Security Profiles' section is expanded, showing the following settings:

- AntiVirus: OFF
- Web Filter: OFF
- Application Control: ON (Profile: default)
- IPS: OFF
- SSL Inspection: ON (Profile: deep-inspection)

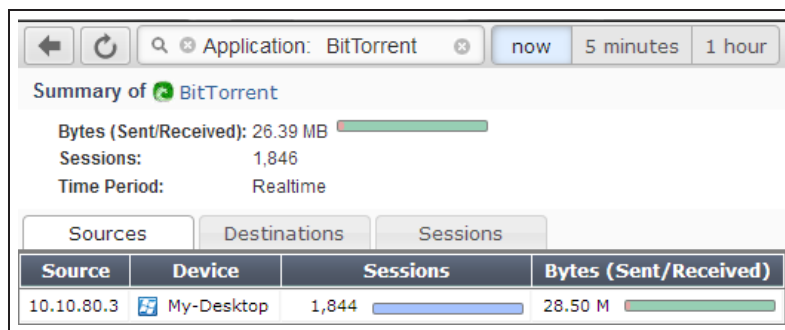
3. Reviewing the FortiView dashboards

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

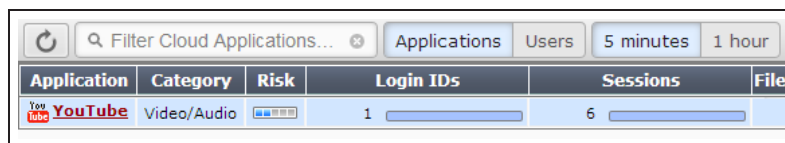
This dashboard shows the traffic that is currently flowing through your FortiGate, arranged by application (excluding Cloud Applications).

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

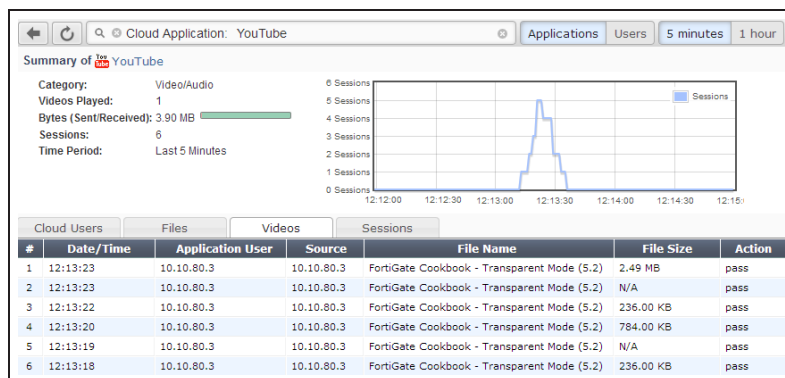
If you wish to know more about an application's traffic, double-click on its entry to view drilldown information, including traffic sources, traffic destinations, and information about individual sessions.



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



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



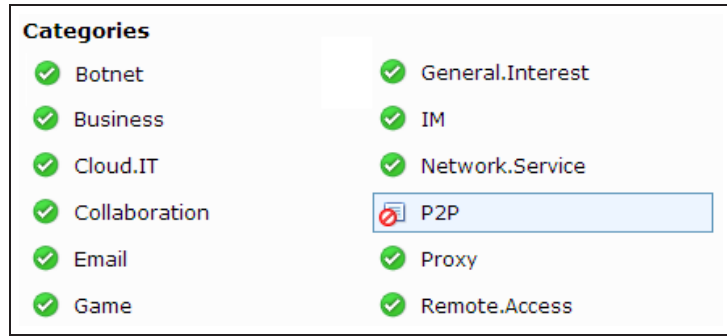
5. Creating an application profile to block applications

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

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

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

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



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

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

Select **Use Selected Signatures**.

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

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

Enable **Deep Inspection of Cloud Applications**.

Application Overrides

Delete
 Add Signatures

Application Signature	Category	Action
YouTube	Video/Audio	Block
YouTube.App	Video/Audio	Block
Youtube.Downloader.YTD	Video/Audio	Block
YouTube_Comment.Posting	Video/Audio	Block
YouTube_HD.Streaming	Video/Audio	Block
YouTube_Search.Safety.Mode.Off	Video/Audio	Block
YouTube_Search.Video	Video/Audio	Block
YouTube_Video.Access	Video/Audio	Block
YouTube_Video.Embedded	Video/Audio	Block
YouTube_Video.Play	Video/Audio	Block
YouTube_Video.Upload	Video/Audio	Block
Youtubeproxyfree	Proxy	Block

Options

ON Deep Inspection of Cloud Applications

6. Adding the blocking profile to a security policy

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

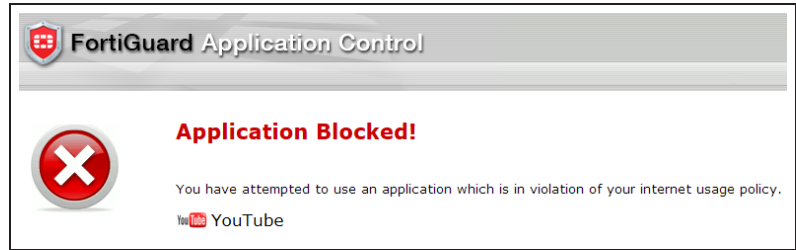
Set **Application Control** to use the new profile.

Security Profiles

<input checked="" type="checkbox"/> ON Antivirus	<input type="text" value="default"/>	
<input type="checkbox"/> OFF Web Filter	<input type="text" value="default"/>	
<input checked="" type="checkbox"/> ON Application Control	<input type="text" value="block-applications"/>	

7. Results

Attempt to browse to [YouTube](#). A warning message will appear, stating that the application was blocked.



Traffic from BitTorrent applications will also be blocked.

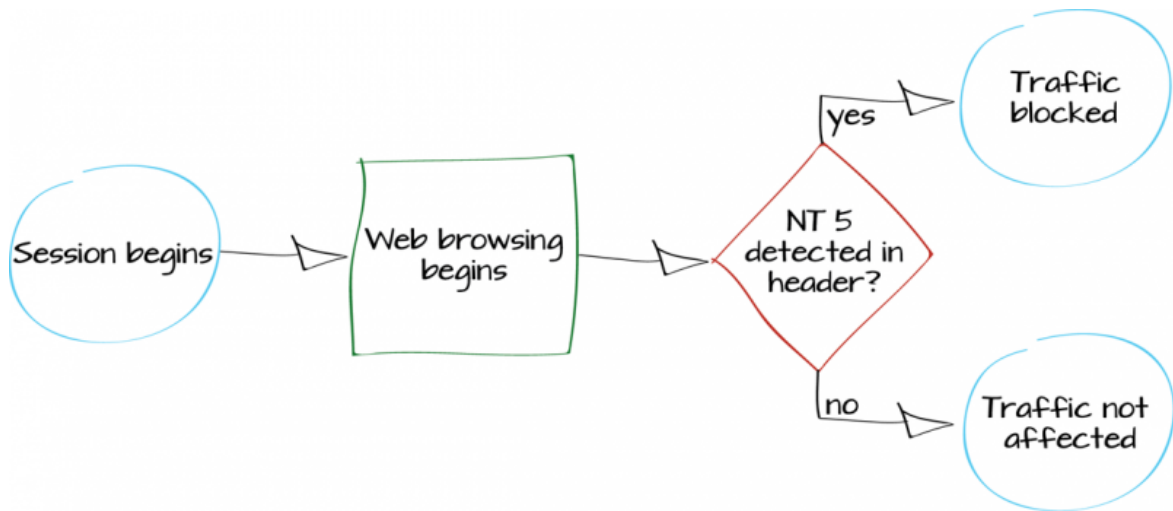
To see information about this blocked traffic, go to **System > FortiView > All Sessions**, select the **5 minutes** view, and filter the traffic by application.

The screenshot shows the FortiView traffic log interface. At the top, there is a search bar with "Application: BitTorrent" and filter buttons for "now", "5 minutes", and "1 hour". Below the search bar is a table with the following columns: #, Date/Time, Source, Device, Application Name, Security Action, and Security Events. The table contains 11 rows of data, all showing BitTorrent traffic blocked from My-Desktop.

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

For further reading, check out [Application control](#) in the [FortiOS 5.2 Handbook](#).

Blocking Windows XP traffic



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

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

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

1. Enabling Application Control

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



2. Creating a custom application control signature

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

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

Name	<input type="text" value="Block-Windows-NT5"/>
Comments	<input type="text" value=""/> 0/255
Signature	<pre>F-SBID(--attack_id 8151; --vuln_id 8151; --name "Windows.NT.5.Web.Surfing"; --default_action drop_session; --service HTTP; --protocol tcp; --app_cat 25; --flow from_client; --pattern "Windows NT 5."; --no_case; --context header;)</pre> Submit Signature

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

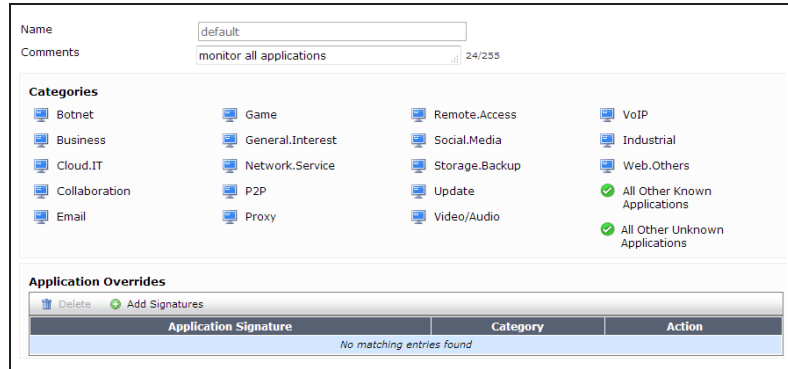
The signature will appear at the top of the application list and be listed in the **Web.Others** category.

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

3. Adding the signature to the default Application Control profile

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

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



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

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



4. Adding the default profile to a security policy

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

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

Incoming Interface	internal	+
Source Address	all	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	wan1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	
Firewall / Network Options		
<input checked="" type="checkbox"/> NAT		
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	Click to add...	
Security Profiles		
<input type="checkbox"/> AntiVirus	default	
<input type="checkbox"/> Web Filter	default	
<input checked="" type="checkbox"/> Application Control	default	

5. Results

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

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

Application Blocked!

You have attempted to use an application which is in violation of your internet usage policy.

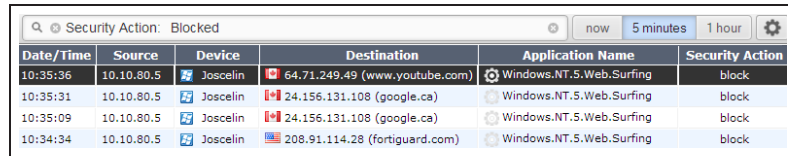
Windows.NT.5.Web.Surfing

Category: Web.Others
URL: http://google.ca/
Client IP: 10.10.80.5
Server IP: 24.156.131.108
User name:
Group name:
Policy: e4769b60-bc02-51e3-73cd-93f99281538d
FortiGate Hostname: FWF90D3Z13002661

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

Filter the results to show sessions that were blocked.

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

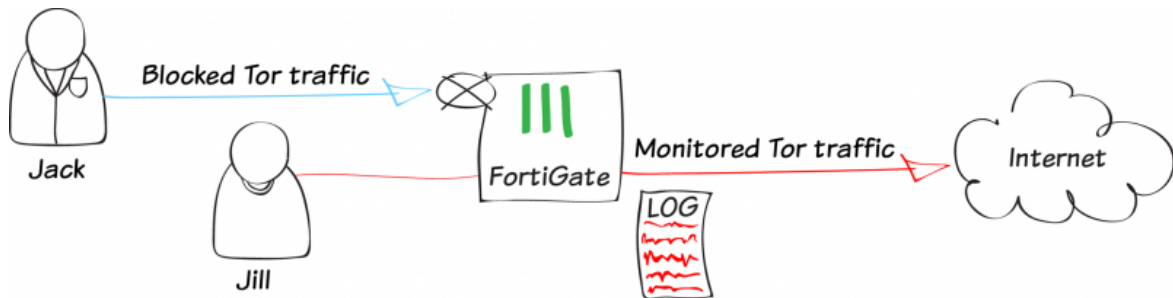


The screenshot shows a table titled "Security Action: Blocked" with a search bar and filter options (now, 5 minutes, 1 hour). The table has six columns: Date/Time, Source, Device, Destination, Application Name, and Security Action. It contains three rows of blocked sessions.

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

For further reading, check out [Custom Application & IPS Signatures](#) in the [FortiOS 5.2 Handbook](#).

Blocking and monitoring Tor traffic



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

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

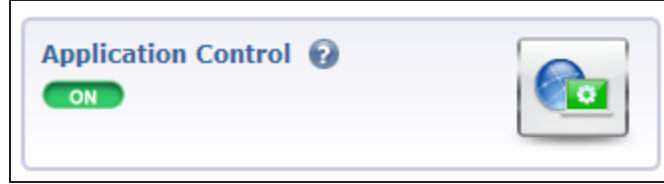
This recipe uses the default application control signatures for the Tor client and web-based Tor. These signatures will only match unmodified versions of the Tor application. Also, if a Tor session has already been established prior to connecting to the network, it may take up to 10 minutes before the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

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

A video of this recipe is available [here](#).

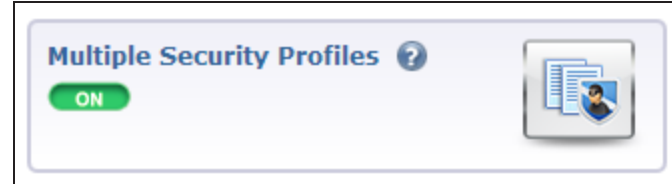
1. Enabling Application Control and multiple security profiles

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



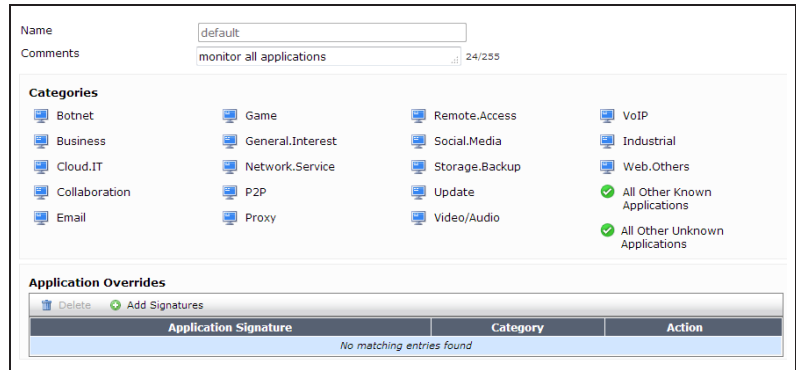
Select **Show More** and enable **Multiple Security Profiles**.

Apply the changes.



2. Blocking Tor traffic using the default profile

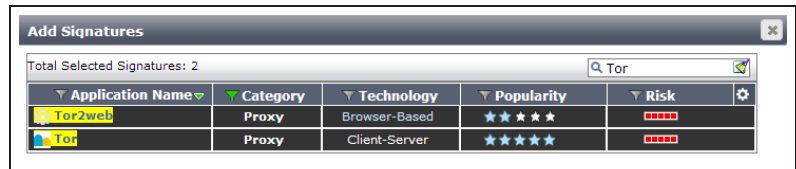
Go to **Security Profiles > Application Control** and edit the default profile.



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

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

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



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

Application Overrides		
Application Signature	Category	Action
Tor	Proxy	Block
Tor2web	Proxy	Block

3. Creating a profile that monitors Tor traffic

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

Application Overrides		
Application Signature	Category	Action
Tor	Proxy	Monitor
Tor2web	Proxy	Monitor

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

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

4. Adding the application control profiles to your security policies

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

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

Incoming Interface	lan	+
Source Address	all	+
Source User(s)	jack	+
Source Device Type	Click to add...	
Outgoing Interface	wan1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	
Firewall / Network Options		
<input checked="" type="checkbox"/> NAT		
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	Click to add...	
Security Profiles		
<input type="checkbox"/> AntiVirus	default	
<input type="checkbox"/> Web Filter	default	
<input checked="" type="checkbox"/> Application Control	default	

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

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

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

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

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

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

5. Results

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

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

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

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

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

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

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



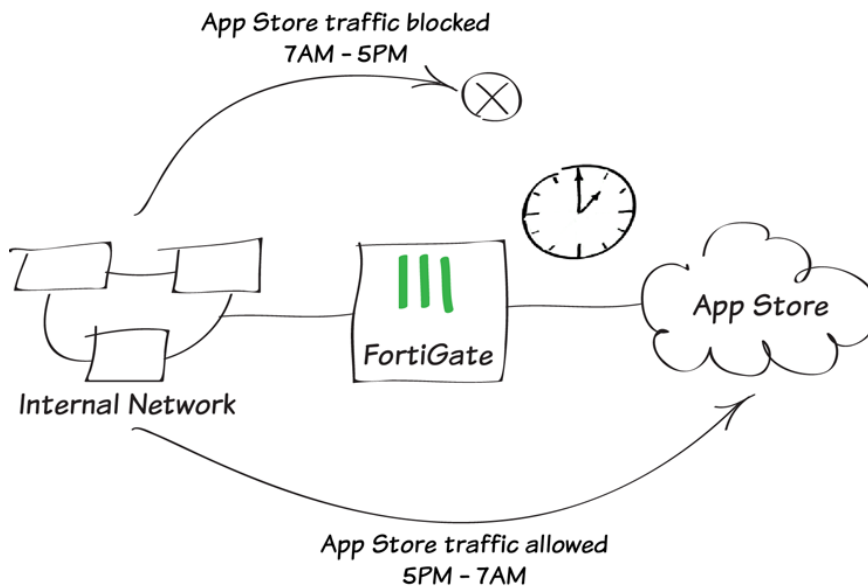
Authenticate using *jack*'s credentials. The **Tor** browser will be blocked.

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

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

For further reading, check out [Application control](#) in the [FortiOS 5.2 Handbook](#).

Controlling access to Apple's App Store

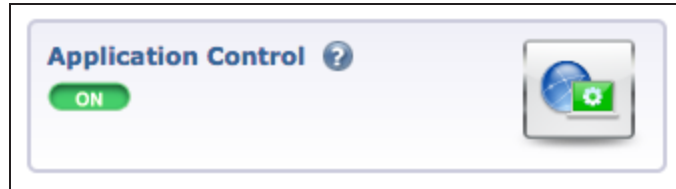


In this recipe, access to Apple's App Store is blocked between 7AM and 5PM. During the rest of the day, access is allowed.

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

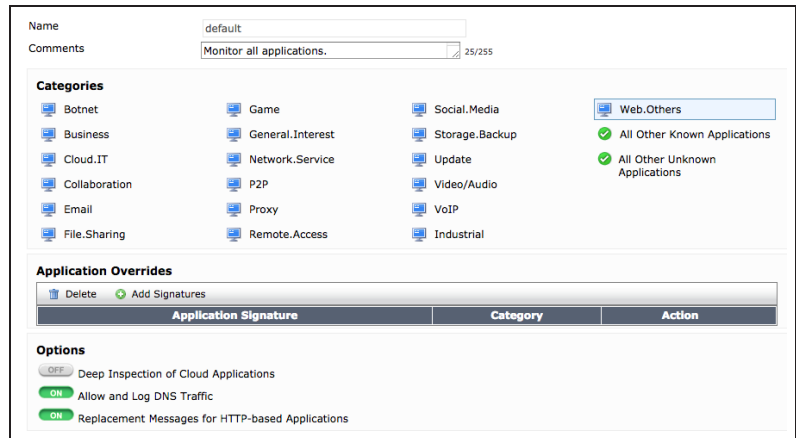
1. Enabling Application Control

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



2. Blocking the App Store

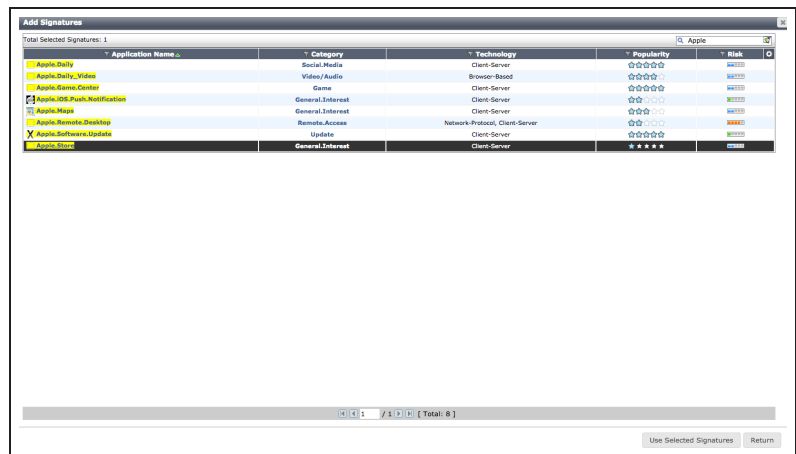
Go to **Security Profiles > Application Control** and edit the default profile.



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

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

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



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

Application Overrides		
Application Signature	Category	Action
Apple.Store	General.Interest	Block

3. Creating a schedule

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

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

Type: Recurring One-time

Name:

Days: Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Start Time: Hour Minute

Stop Time: Hour Minute

4. Creating a security policy to block the App Store

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

Set **Schedule** to the new schedule.

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

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

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

Incoming Interface:

Source Address:

Source User(s):

Source Device Type:

Outgoing Interface:

Destination Address:

Schedule:

Service:

Action:

Firewall / Network Options

NAT

Use Outgoing Interface Address Fixed Port

Use Dynamic IP Pool

Security Profiles

AntiVirus

Web Filter

Application Control

IPS

DLP Sensor

SSL/SSH Inspection

5. Ordering the security policies

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

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

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

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

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

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

6. Enforcing the schedule

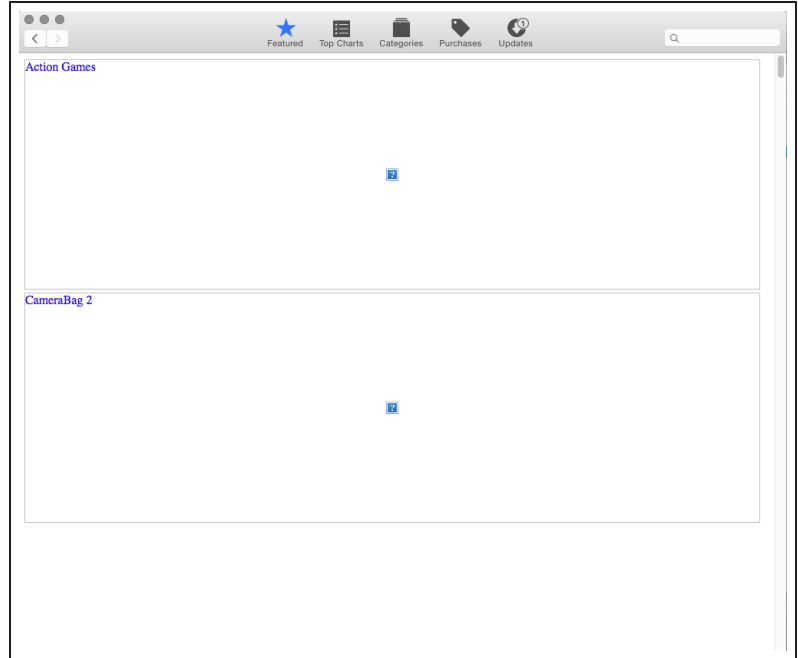
Go to **System > Dashboard > Status** and enter the following into the **CLI Console**, substituting the correct Policy ID for the new policy.

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

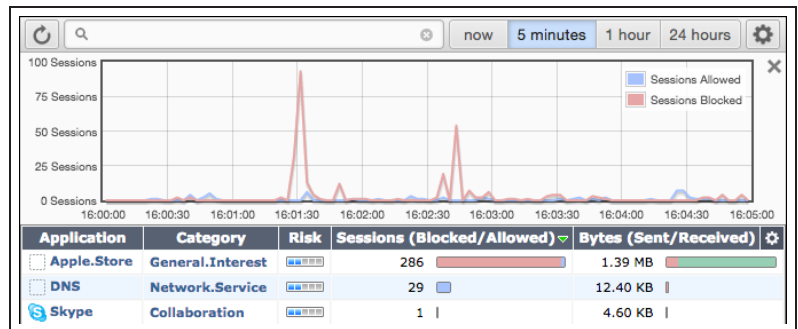
```
config firewall policy
  edit <policy-id>
    set schedule-timeout enable
  end
end
```

7. Results

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



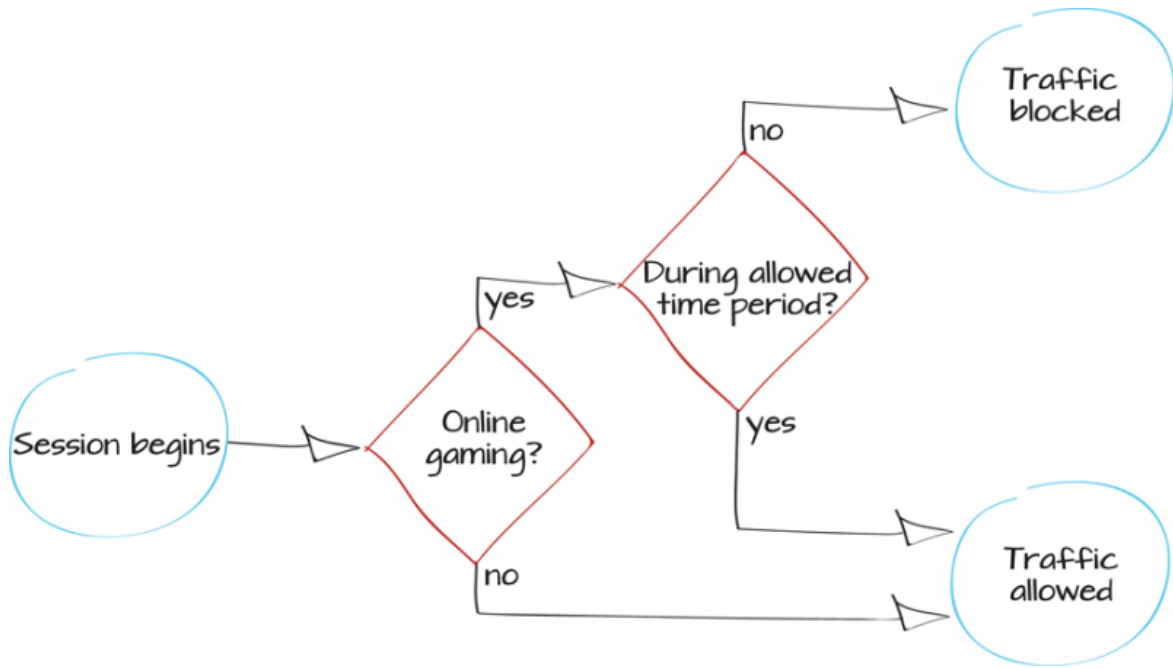
You can find information about the blocked traffic by going to **System > FortiView > Applications** and selecting the **5 minutes** view.



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

For further reading, check out [Application control](#) in the [FortiOS 5.2 Handbook](#).

Restricting online gaming to evenings



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

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

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

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



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



2. Configuring application control and web filtering

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

Under **Categories**, select **Game**, and set the category to **Block**.

Under **Options**, enable **Deep Inspection of Cloud Applications**.

Name: default
Comments: Monitor all applications. 25/255

Categories

- Botnet
- Business
- Cloud.IT
- Collaboration
- Email
- Game (selected)
- General.Interest
- Network.Service
- P2P
- Proxy
- Remote.Access
- Social.Media
- Storage.Backup
- Update
- Video/Audio
- VoIP
- Industrial
- Web.Others
- All Other Known Applications
- All Other Unknown Applications

Application Overrides

Application Signature	Category	Action
No matching entries found		

Options

- ON Deep Inspection of Cloud Applications
- ON Allow and Log DNS Traffic
- ON Replacement Messages for HTTP-based Applications

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

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

The screenshot shows the configuration page for the 'default' web filter profile. The 'Name' field is set to 'default' and the 'Comments' field contains 'Default web filtering.' with a character count of 22/255. The 'Inspection Mode' is set to 'Proxy'. The 'FortiGuard Categories' checkbox is checked. A dropdown menu is set to 'Show All'. The 'General Interest - Personal' category is expanded, showing a list of sub-categories: Advertising, Arts and Culture, Brokerage and Trading, Child Education, Content Servers, Digital Postcards, Domain Parking, Dynamic Content, Education, Entertainment, Folklore, Games, Global Religion, Health and Wellness, and Instant Messaging. The 'Games' sub-category is marked with a red 'X' icon, indicating it is blocked. A note at the bottom states: 'Quota on Categories with Monitor, Warning and Authenticate Actions'.

3. Editing your general policy to block gaming

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

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

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

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

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

The screenshot shows the configuration for a Firewall Policy. The Incoming Interface is 'lan (VLAN ID: 0)' and the Outgoing Interface is 'wan1'. The Source Address is 'all' and the Destination Address is 'all'. The Schedule is 'always' and the Service is 'ALL'. The Action is 'ACCEPT'. Under Firewall / Network Options, NAT is turned ON, and 'Use Dynamic IP Pool' is selected. Under Security Profiles, Web Filter and Application Control are turned ON and set to 'default', while AntiVirus and DLP Sensor are turned OFF. Proxy Options are set to 'default', and SSL/SSH Inspection is turned ON and set to 'deep-inspection'.

3. Creating a schedule for when gaming is allowed

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

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

The screenshot shows the configuration for a recurring schedule named 'gaming-allowed'. The Type is 'Recurring'. The Days are selected for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. The Start Time is set to Hour 19 and Minute 0. The Stop Time is set to Hour 23 and Minute 0.

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

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

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

Incoming Interface	lan (VLAN ID: 0)
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	all
Schedule	gaming-allowed
Service	ALL
Action	ACCEPT

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

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

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

6. Ordering the policies

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

Seq.#	Source	Destination	Schedule	Service	Action	NAT	Web Filter	Application Control	SSL Inspection
1	all	all	gaming-allowed	ALL	ACCEPT	Enable			
2	all Android Phone Mac iPad Windows PC	all	always	ALL	ACCEPT	Enable	default	default	deep-inspection

7. Results


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

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

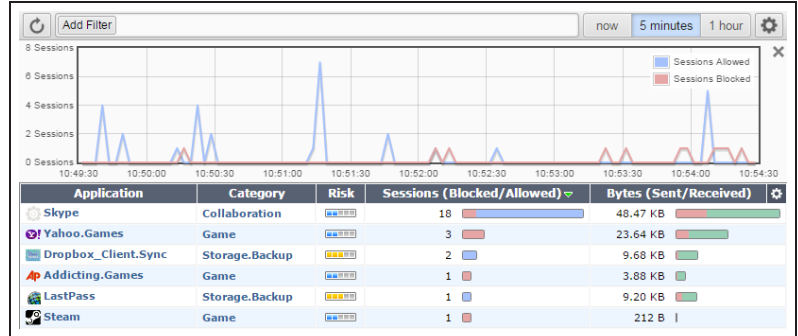
To view information about this blocked traffic, go to **System > FortiView > Applications**.

Application Blocked!

You have attempted to use an application which is in violation of your internet usage policy.

 **Yahoo.Games**

Category: Game
URL: spdy://
Client IP: 10.10.80.4
Server IP: 98.139.199.204
User name:
Group name:
Policy: e4769b60-bc02-51e3-73cd-93f99281538d
FortiGate Hostname: FWF90D3Z13002661

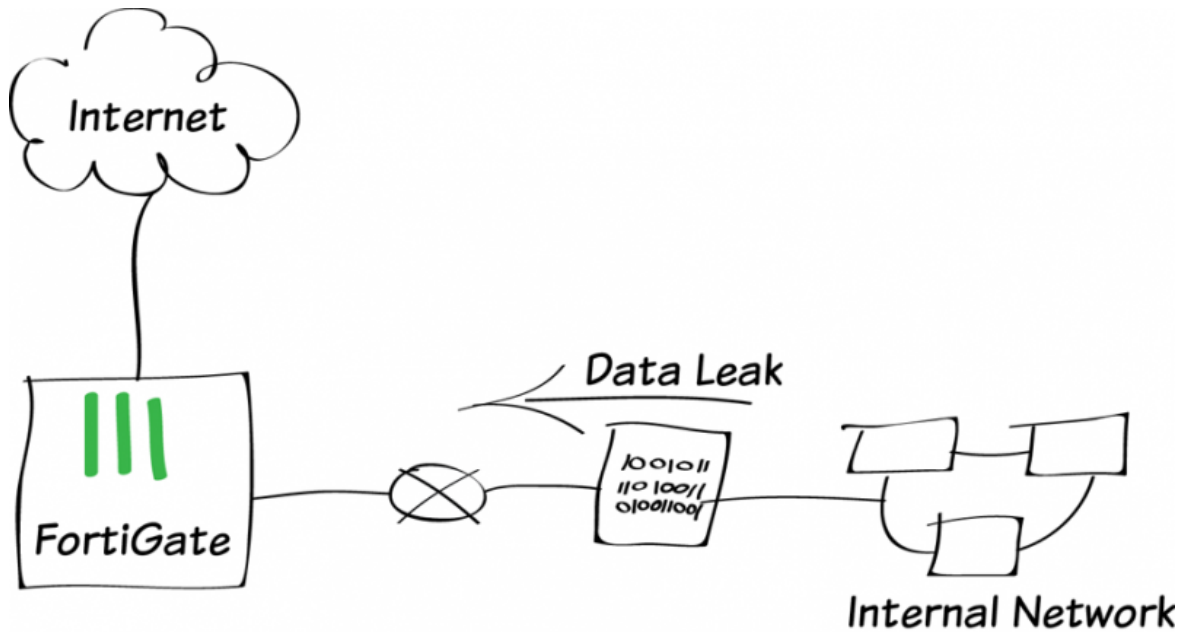


Attempt to connect to the Internet using a gaming console. The console will be unable to connect to the Internet.

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

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

Preventing data leaks



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

1. Enabling DLP and multiple security profiles

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



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

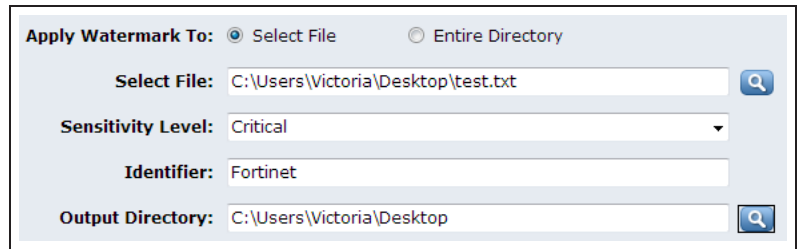


2. Applying a DLP watermark to a file

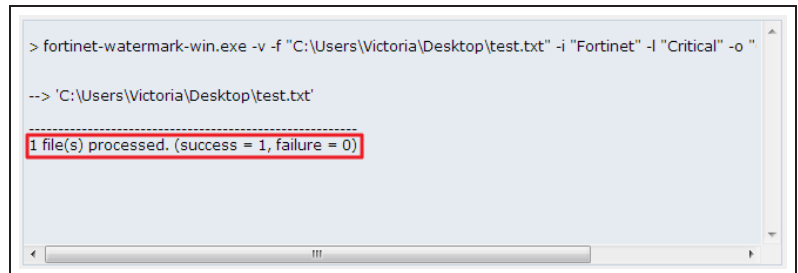
The DLP watermarking client is available as part of FortiExplorer. This feature is currently only available using FortiExplorer for Microsoft Windows.

If you do not already have FortiExplorer on your computer, click [here](#) to download it.

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



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



3. Creating a DLP profile

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

Seq #	Type	Action	Services	Archive
No matching entries found				

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

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

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

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

Filter

Messages Files

Containing KB

File Size >= KB

Specify File Types

File Finger Print

Watermark Sensitivity: Corporate Identifier:

Regular Expression

Encrypted

Examine the Following Services

Web Access HTTP-POST HTTP-GET

Email SMTP POP3 IMAP MAPI

Others FTP NNTP

Action

Create a second filter.

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

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

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

Filter

Messages Files

Containing KB

File Size >= KB

Specify File Types

File Types:

File Name Patterns:

File Finger Print

Watermark Sensitivity: Corporate Identifier:

Regular Expression

Encrypted

Examine the Following Services

Web Access HTTP-POST HTTP-GET

Email SMTP POP3 IMAP MAPI

Others FTP NNTP

Action

Both filters now appear in the Filters list.

Name:	block-sensitive-information			
Comment:	Comment 0/255			
Create New Edit Filter Delete				
Seq #	Type	Action	Services	Archive
1	Watermark Sensitivity: Critical, Corporate Identifier: Fortinet	Block	SMTP, POP3, IMAP, HTTP-GET, HTTP-POST, FTP	Disable
2	Specified File Types	Block	SMTP, POP3, IMAP, HTTP-GET, HTTP-POST, FTP	Disable

4. Adding the profile to a security policy

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

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

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

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

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

Security Profiles

- OFF Antivirus default
- OFF Web Filter default
- OFF Application Control default
- OFF IPS default
- ON DLP Sensor default
- Proxy Options default
- ON SSL Inspection deep-inspection

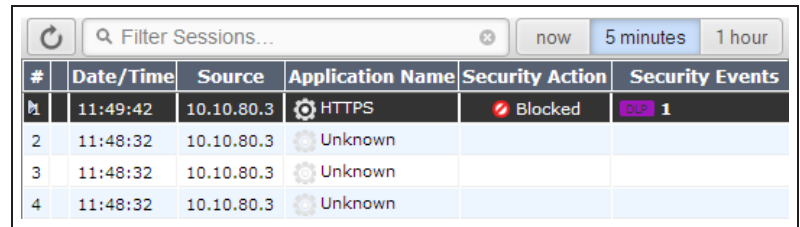
Logging Options

- ON Log Allowed Traffic
- Security Events
- All Sessions

5. Results

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

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

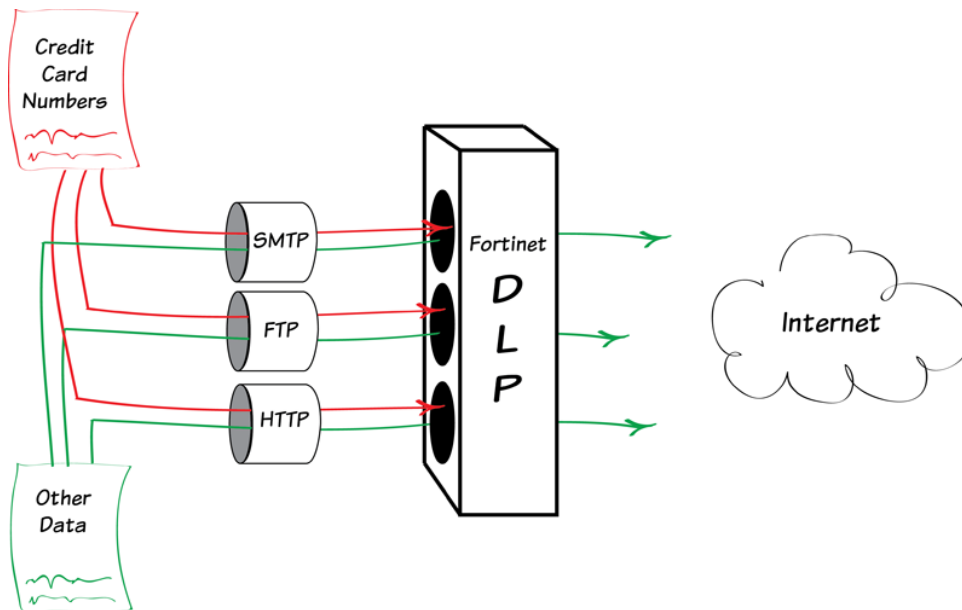


The screenshot shows a table with columns: #, Date/Time, Source, Application Name, Security Action, and Security Events. The first row is selected and highlighted in black. The Security Action for this row is 'Blocked' with a red prohibition icon. The Security Events column shows a purple icon and the number '1'. The other rows show 'Unknown' application names and no security actions or events.

#	Date/Time	Source	Application Name	Security Action	Security Events
1	11:49:42	10.10.80.3	HTTPS	Blocked	1
2	11:48:32	10.10.80.3	Unknown		
3	11:48:32	10.10.80.3	Unknown		
4	11:48:32	10.10.80.3	Unknown		

For further reading, check out [Data leak prevention](#) in the [FortiOS 5.2 Handbook](#).

Prevent credit card numbers from being leaked



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

1. Enabling DLP

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



2. Adding two filters to the default DLP sensor

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

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

A screenshot of a 'New Filter' dialog box. The title bar says 'New Filter'. Under the 'Filter' section, 'Messages' is selected with a radio button. The 'Containing' option is chosen, with a dropdown menu showing 'Credit Card #'. Below this, there are checkboxes for 'Regular Expression' and an empty text input field. The 'Examine the Following Services' section has checkboxes for 'Web Access' (HTTP-POST), 'Email' (SMTP, POP3, IMAP, MAPI), and 'Others' (NNTP). The 'Action' section has a dropdown menu set to 'Block'. 'OK' and 'Cancel' buttons are at the bottom right.

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

A screenshot of a 'New Filter' dialog box. The title bar says 'New Filter'. Under the 'Filter' section, 'Files' is selected with a radio button. The 'Containing' option is chosen, with a dropdown menu showing 'Credit Card #'. Below this, there are several options: 'File Size >= [input] KB', 'Specify File Types', 'File Finger Print [Critical]', 'Watermark Sensitivity: [Critical] Corporate Identifier: [input]', 'Regular Expression [input]', and 'Encrypted'. The 'Examine the Following Services' section has checkboxes for 'Web Access' (HTTP-POST, HTTP-GET), 'Email' (SMTP, POP3, IMAP, MAPI), and 'Others' (FTP, NNTP). The 'Action' section has a dropdown menu set to 'Block'. 'OK' and 'Cancel' buttons are at the bottom right.

Both filters appear in the default sensor.

Seq #	Type	Action	Services	Archive
1	Containing Credit Card	Block	SMTP, POP3, IMAP, HTTP-POST	Disable
2	Containing Credit Card	Block	SMTP, POP3, IMAP, HTTP-GET, HTTP-POST, FTP	Disable

3. Adding the new DLP sensor to a security policy

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

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

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

Incoming Interface: lan (VLAN ID: 0) +

Source Address: all +

Source User(s): Click to add...

Source Device Type: Click to add...

Outgoing Interface: wan1 +

Destination Address: all +

Schedule: always

Service: ALL +

Action: ACCEPT

Firewall / Network Options

NAT

Use Outgoing Interface Address Fixed Port

Use Dynamic IP Pool

Security Profiles

AntiVirus: default

Web Filter: default

Application Control: default

DLP Sensor: default

Proxy Options: default

SSL/SSH Inspection: deep-inspection

4. Results

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

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

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

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

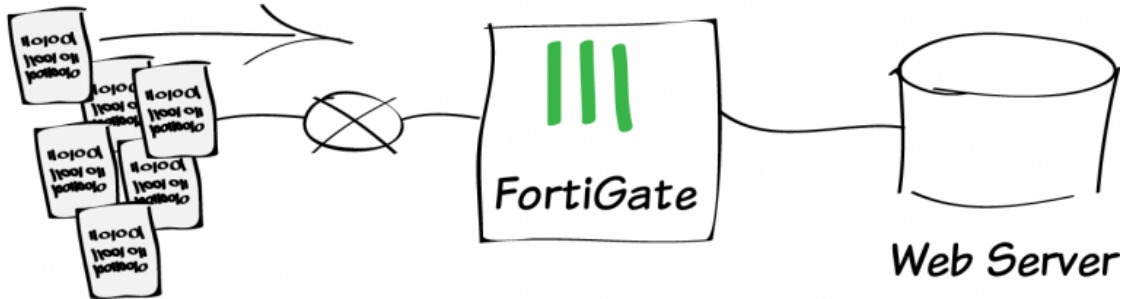
To view more information about the blocked traffic, go to **Log & Report > Traffic Log > Forward Traffic** and filter for **Security Actions: Blocked**.

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

For further reading, check out [Data leak prevention](#) in the [FortiOS 5.2 Handbook](#).

Protecting a web server

External Attacks



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

A video of this recipe is available [here](#).

1. Enabling Intrusion Protection

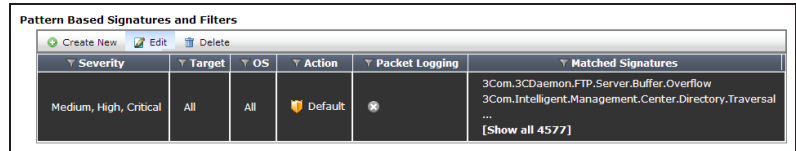
Go to **System > Config > Features** and ensure that **Intrusion Protection** is turned **ON**. Apply your changes if necessary.



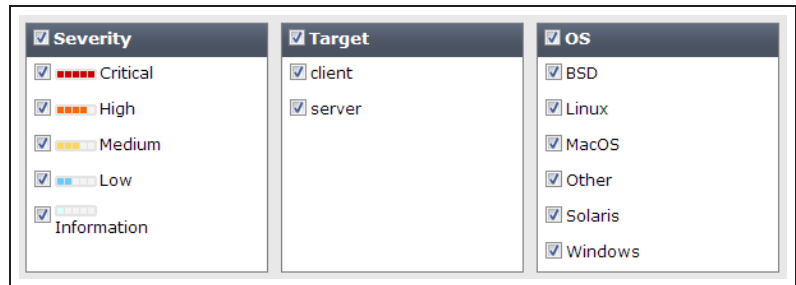
2. Configuring the default IPS profile to block common attacks

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

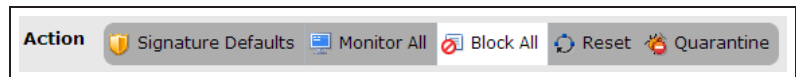
In the **Pattern Based Signatures and Filters** list, highlight the default entry and select **Edit**.



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



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



Enable all the listed Rate Based Signatures.

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

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

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

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

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

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

Incoming Interface: wan1

Source Address: all

Source User(s): Click to add...

Source Device Type: Click to add...

Outgoing Interface: internal

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

Firewall / Network Options

NAT

Use Destination Interface Address Fixed Port

Use Dynamic IP Pool

Security Profiles

AntiVirus: default

Web Filter: default

Application Control: default

IPS: default

DLP Sensor: default

SSL/SSH Inspection: deep-inspection

4. Creating a DoS policy

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

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

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

Incoming Interface

Source Address

Destination Address

Service

Anomalies

Name	<input checked="" type="checkbox"/> Status	<input checked="" type="checkbox"/> Logging	Action	Threshold
tcp_syn_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	2000
tcp_port_scan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	1000
tcp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	5000
tcp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	5000
udp_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	2000
udp_scan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	2000
udp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	5000
udp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	5000
icmp_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	250
icmp_sweep	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	100
icmp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	300
ip_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	5000
sctp_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	2000
sctp_scan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	1000
sctp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	5000
sctp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block ▾	5000

ON Enable this policy

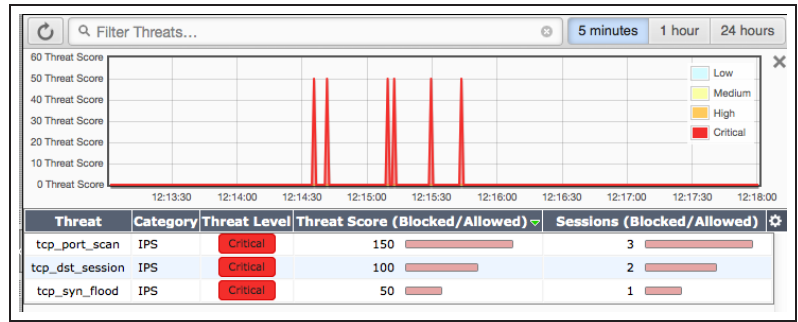
5. Results

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

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

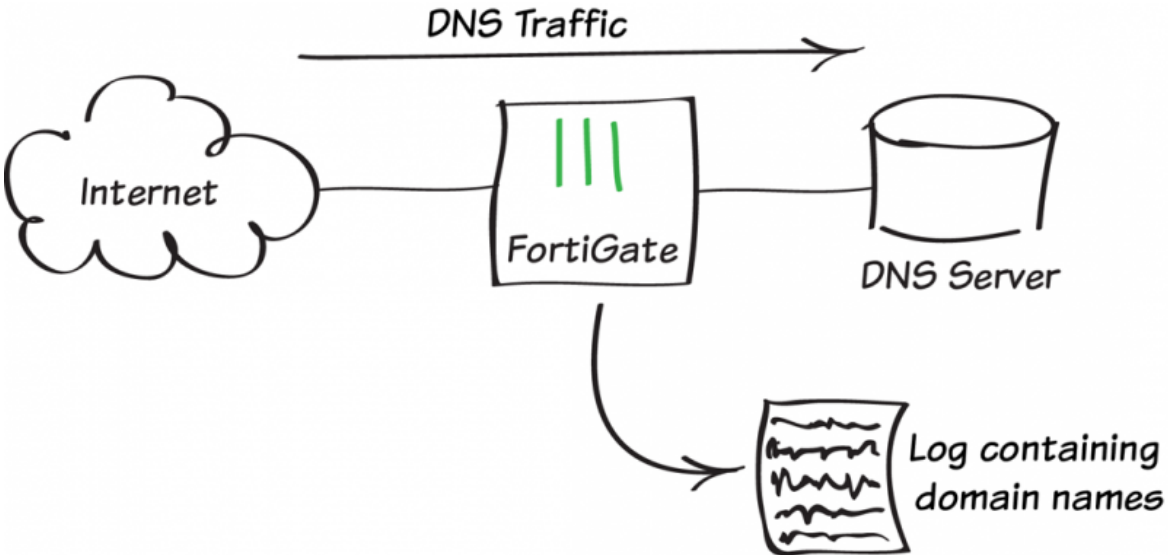
Go to **System > FortiView > Threats** and select the **5 Minutes** view.

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



For further reading, check out [Intrusion Protection](#) in the [FortiOS 5.2 Handbook](#).

Logging DNS domain lookups



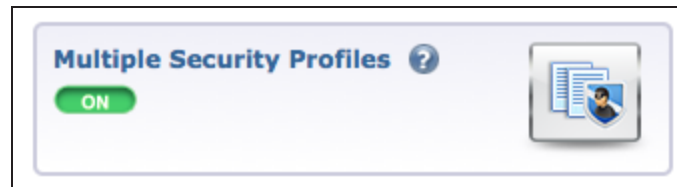
In this recipe, you will add a custom Intrusion Protection (IPS) signature to a security policy to record all domain lookups accepted by the policy. The signature records an IPS log message containing the domain name every time a DNS lookup occurs.

1. Enabling Intrusion Protection and multiple security profiles

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

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

Apply the changes.



2. Creating a custom IPS signature

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

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

Name	<input type="text" value="log-DNS_QUERY"/>
Signature	<input type="text" value="F-SBID(--name DOM-ALL; --protocol udp; -"/>

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

3. Adding the signature to an IPS profile

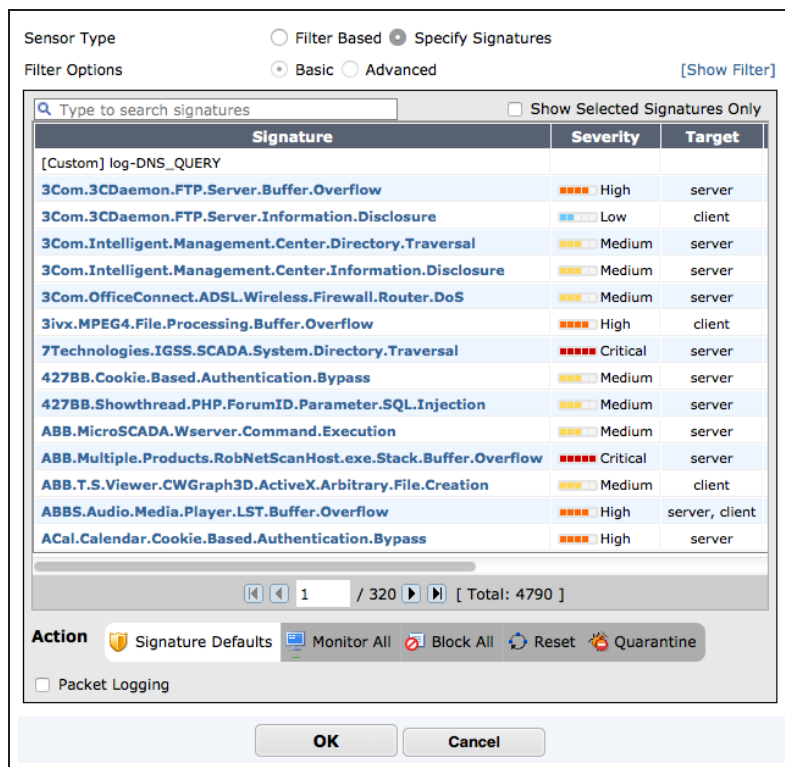
Go to **Security Profiles > Intrusion Protection** and create a new profile.

Name	<input type="text" value="DNS-logging"/>
Comments	<input type="text" value=""/> 0/255

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

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

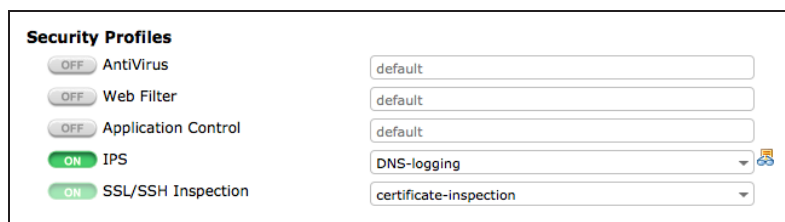
Select the signature, then select **OK**.



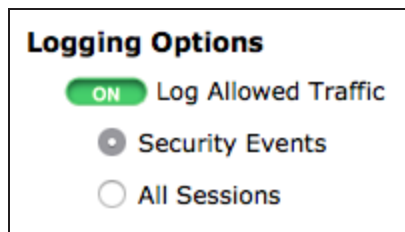
4. Adding the profile to the DNS server's security policy

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

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



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



5. Results

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

This log only appears when an IPS event has occurred.

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

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

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


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

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

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

Name	DNS-Query
Log Type	Attack
Query	<pre>select msg, sum(totalnum) as totalnum from ###(select srcip, msg, count(*) as totalnum from \$log where \$filter-exclude-var group by srcip, msg order by totalnum desc)### t where \$filter- var-only and msg is not null group by msg order by totalnum desc</pre>

This dataset can then be used in a custom report.

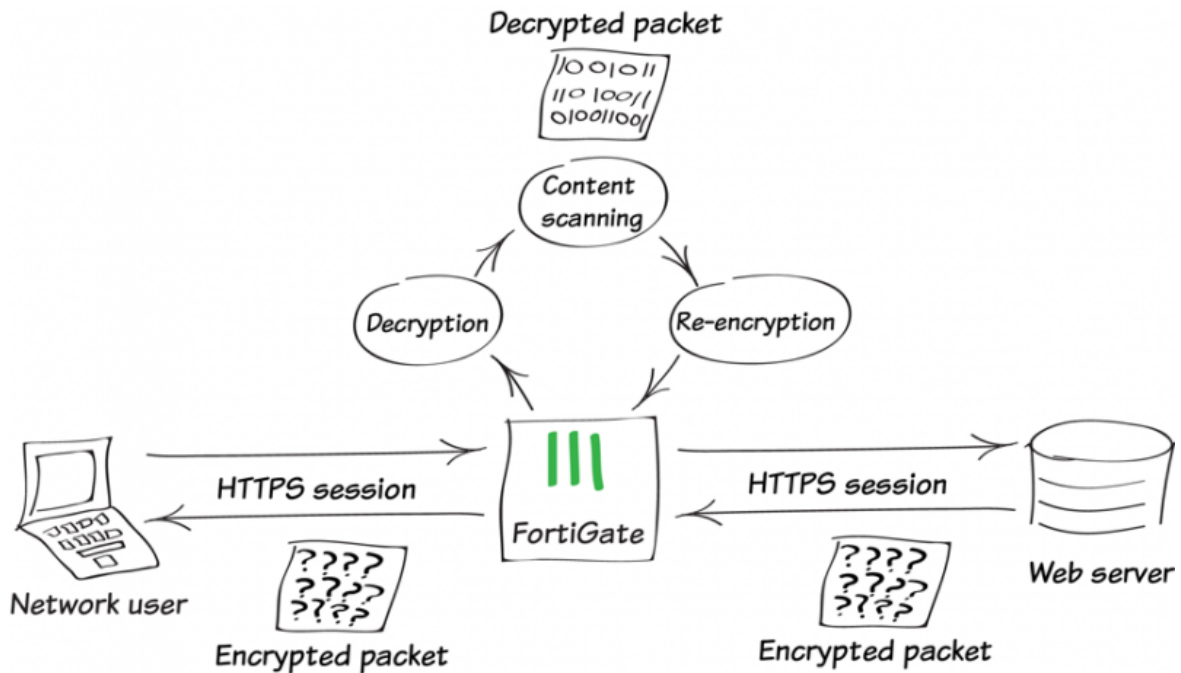


TOP 10 requested DNS Domains

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

For further reading, check out [DNS Service](#) in the [FortiOS 5.2 Handbook](#).

Why you should use SSL inspection



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

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

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

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

Full SSL inspection

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

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

There are two deployment methods for full SSL inspection:

Multiple Clients Connecting to Multiple Servers:

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

Protecting SSL Server

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

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

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

SSL certificate inspection

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

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

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

Troubleshooting

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

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

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

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

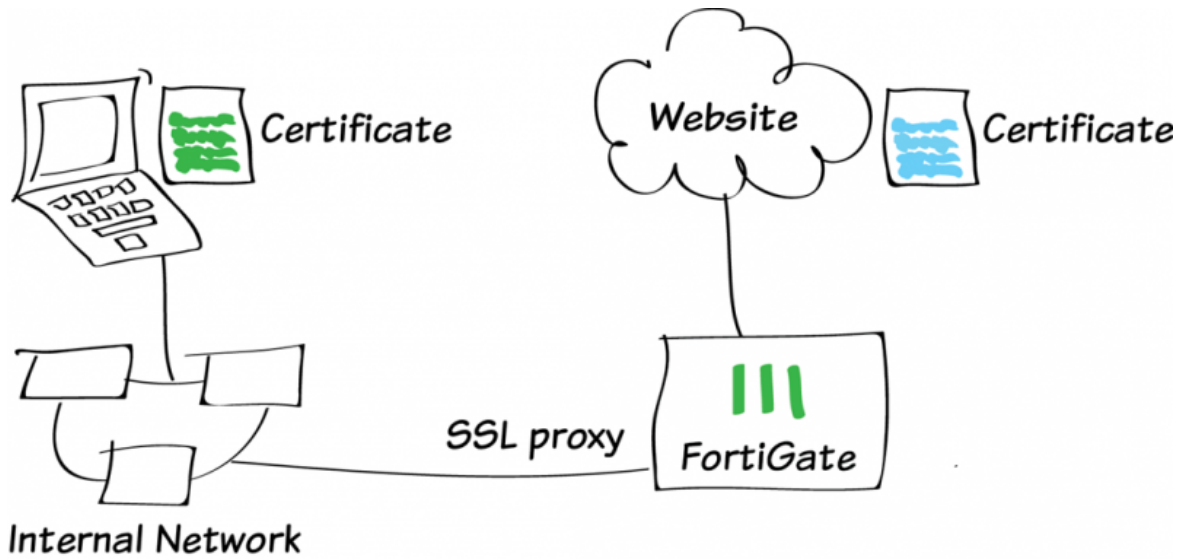
For corporate-owned mobile devices, MDM solutions like AirWatch, MobileIron, or Fiberlink, use Simple Certificate Enrollment Protocol (SCEP) to ease certificate enrollment.

Best practices

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

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

Preventing certificate warnings



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

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

For more information about SSL inspection, see [Why you should use SSL inspection](#).

Using the default FortiGate certificate

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

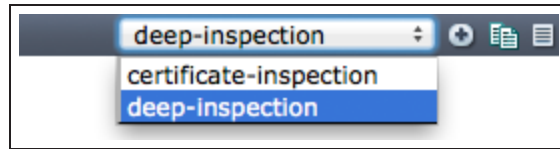
To prevent your users from seeing certificate warnings you can distribute this certificate to your user's devices.

A video of this example can be found [here](#).

1. Viewing the deep-inspection SSL profile

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

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




In this policy, the web categories **Health and Wellness**, **Personal Privacy**, and **Finance and Banking** are excluded from SSL inspection by default. Applications that require unique certificates, such as iTunes and Dropbox, have also been excluded.

Name	<input type="text" value="deep-inspection"/>
Comments	<input type="text" value="Deep inspection."/> 16/255
SSL Inspection Options	
Enable SSL Inspection of	<input checked="" type="radio"/> Multiple Clients Connecting to Multiple Servers <input type="radio"/> Protecting SSL Server
CA Certificate	<input type="text" value="Fortinet_CA_SSLProxy"/>
Inspection Method	<input type="radio"/> SSL Certificate Inspection <input checked="" type="radio"/> Full SSL Inspection
<input type="checkbox"/> Inspect All Ports	
<input checked="" type="checkbox"/> ON HTTPS	<input type="text" value="443"/>
<input checked="" type="checkbox"/> ON SMTPS	<input type="text" value="465"/>
<input checked="" type="checkbox"/> ON POP3S	<input type="text" value="995"/>
<input checked="" type="checkbox"/> ON IMAPS	<input type="text" value="993"/>
<input checked="" type="checkbox"/> ON FTPS	<input type="text" value="990"/>
Exempt from SSL Inspection	
Web Categories	<input type="text" value="Health and Wellness"/> X + <input type="text" value="Personal Privacy"/> X <input type="text" value="Finance and Banking"/> X
Addresses	<input type="text" value="android"/> X + <input type="text" value="apple"/> X <input type="text" value="appstore.com"/> X <input type="text" value="citrixonline"/> X <input type="text" value="dropbox.com"/> X <input type="text" value="Gotomeeting"/> X <input type="text" value="icloud"/> X <input type="text" value="itunes"/> X <input type="text" value="skype"/> X <input type="text" value="swscan.apple.com"/> X <input type="text" value="update.microsoft.com"/> X

2. Enabling certificate configuration in the web-based manager

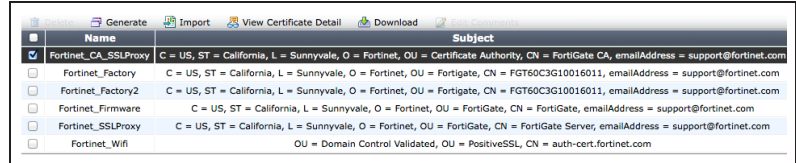
Go to **System > Config > Features**. Click **Show More**, enable **Certificates**, and **Apply** the changes.

Certificates ? <input checked="" type="checkbox"/> ON		Changes: No changes <input type="button" value="Apply"/> <input type="button" value="Reset"/>
---	--	--

3. Downloading the Fortinet_CA_SSLProxy certificate

Go to **System > Certificates > Local Certificates** to download the **Fortinet_CA_SSLProxy** certificate.

Make the CA certificate file available to your users by checkmarking the box next to the certificate name.



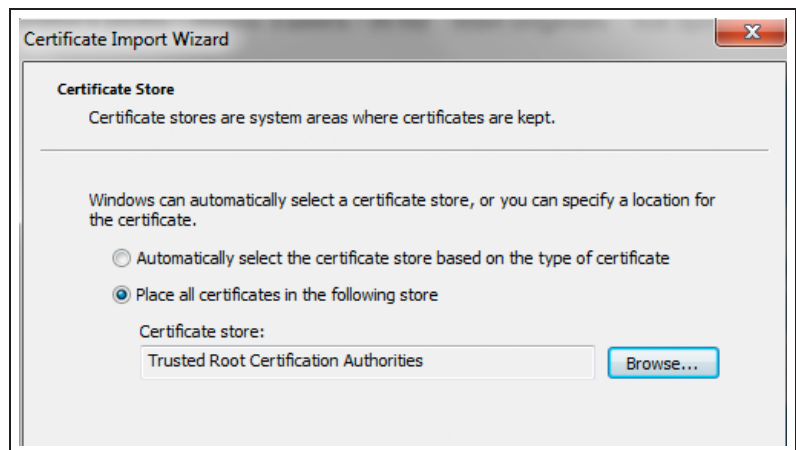
4. Importing the CA certificate into the web browser

For Internet Explorer:

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

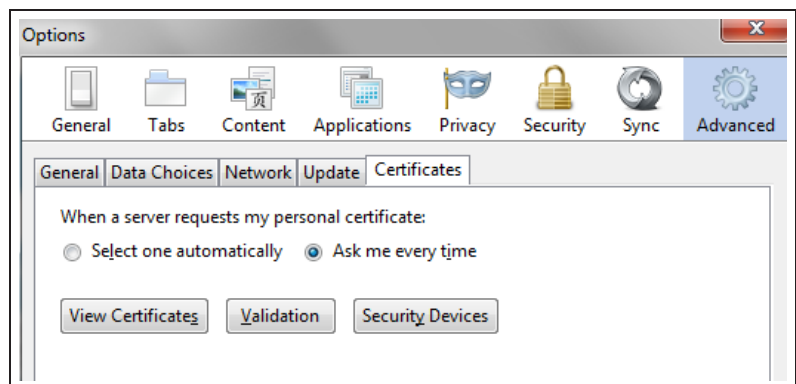
Import the certificate using the Import Wizard. Make sure that the certificate is imported into **Trusted Root Certification Authorities**.

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

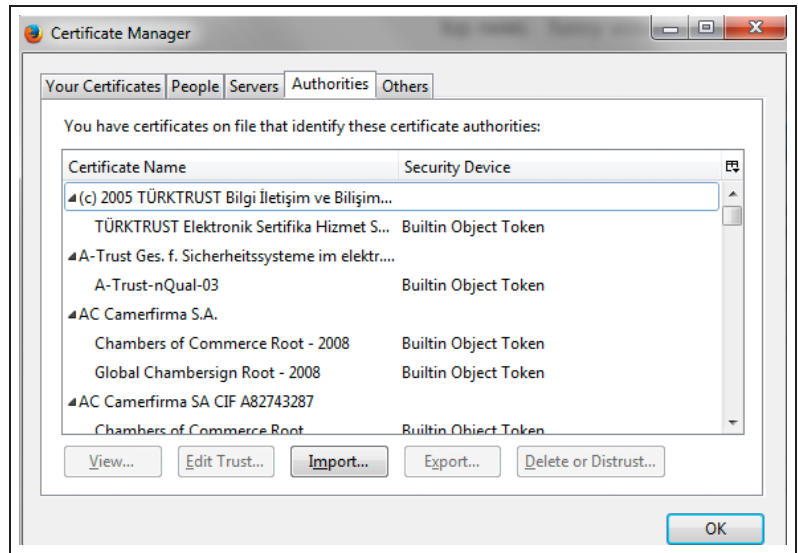


For Firefox:

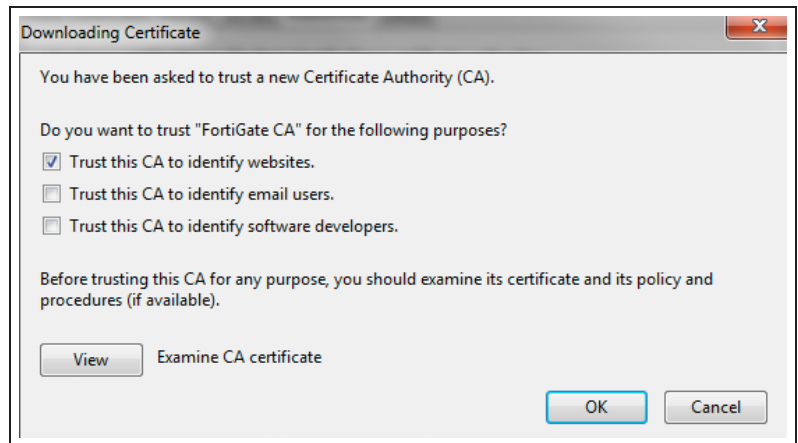
Depending on the platform, go to **Menu > Options** or **Preferences > Advanced** and find the **Certificates** tab.



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

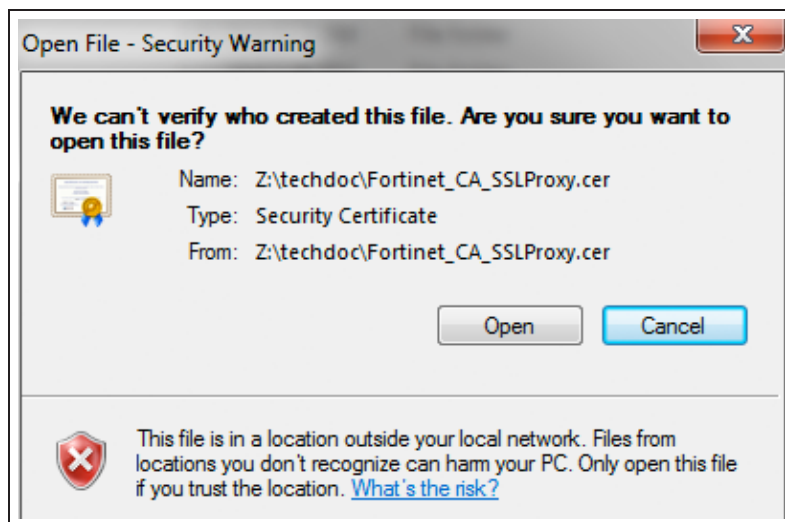


Click **Import** and select the **Fortinet_CA_SSLProxy** certificate file.



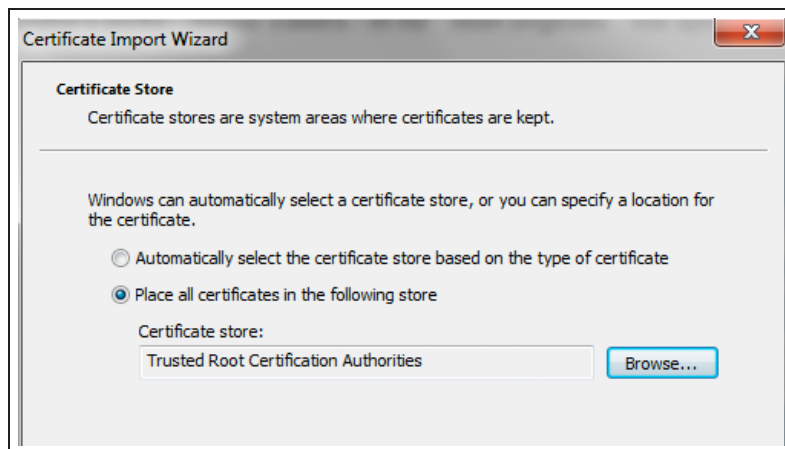
For Google Chrome and Safari:

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



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

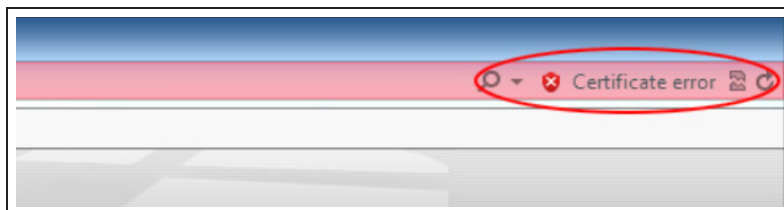
You will see a warning because the FortiGate unit's certificate is self-signed. It is safe to select **Yes** to install the certificate.



5. Results

Before installing the FortiGate SSL CA certificate, even if you bypass the error message by selecting **Continue to this website**, the browser may still show an error in the toolbar.

After you install the FortiGate SSL CA certificate, you should not experience a certificate security issue when you browse to sites on which the FortiGate



unit performs SSL content inspection.

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

For further reading, check out [SSL/SSH Inspection](#) in the [FortiOS 5.2 Handbook](#).

Using a custom certificate

In this method, a custom certificate is first signed by a recognized third-party CA and then installed on the FortiGate. This results in a chain of trust that does not exist when the FortiGate's default certificate is used. This example allows network users to trust the FortiGate as a CA in its own right. Once the FortiGate is trusted you users should no longer see certificate warnings without having to distribute certificates to your users.

1. Generating a certificate signing request (CSR)

Go to **System > Certificates > Local Certificates** and select **Generate**.

In the **Generate Certificate Signing Request** page, fill out the required fields. You can enter a maximum of five **Organizational Units**.

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

To ensure PKCS12 compatibility, do not include spaces in the certificate name.

Generate Certificate Signing Request

Certificate Name

Subject Information

ID Type

IP

Optional Information

Organization Unit

Organization

Locality(City)

State/Province

Country/Region

E-mail

Subject Alternative Name

Key Type

Key Size

Enrollment Method File Based Online SCEP

Go to **System > Certificates > Local Certificates** to view the certificate list. The status of the CSR created will be listed as **Pending**. Select the certificate and click **Download**.

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

	Delete	Generate	Import	View Certificate Detail	Download			
						Name	Status	Ref.
<input type="checkbox"/>						Fortinet_CA_SSLProxy	OK	2
<input type="checkbox"/>						Fortinet_Factory	OK	0
<input type="checkbox"/>						Fortinet_Factory2	OK	0
<input type="checkbox"/>						Fortinet_Firmware	OK	1
<input type="checkbox"/>						Fortinet_SSLProxy	OK	4
<input type="checkbox"/>						Fortinet_Wifi	OK	1
<input checked="" type="checkbox"/>						MyCert	PENDING	0

Subordinate Certificate Authority is used.


2. Importing a signed server certificate from an enterprise root CA


Once the CSR is signed by an enterprise root CA, you can import it into the FortiGate Unit.

Go to **System > Certificates > Local Certificates** and click **Import**.

From the **Type** drop down menu select **Local Certificate** and click **Choose File**.

Locate the certificate you wish to import, select it, and click **Open**. The CA signed certificate will now appear on the **Local Certificates** list.

Generate Certificate Signing Request	
Certificate Name	<input type="text" value="MyCert"/>
<hr/>	
Subject Information	
ID Type	<input type="text" value="Host IP"/>
IP	<input type="text" value="192.168.1.99"/>
<hr/>	
Optional Information	
Organization Unit	<input type="text" value="Tech"/> 

Name	Date Modified
 MyCert.cer	Jun 19, 2014, 9:56 AM

3. Creating an SSL inspection profile

To use your certificate in an SSL inspection profile go to **Policy & Objects > Policy > SSL/SSH Inspection**. Create a new **SSL Inspection Profile**.

In the **CA Certificate** drop down menu, select the certificate you imported.

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

Set the **Inspection Method** to **Full SSL Inspection** and **Inspect All Ports**.

You may also need to select web categories and addresses to be exempt from SSL inspection. For more information on exemptions, see [Using the default FortiGate certificate](#).

New SSL Inspection Profile

Name: My Inspection

Comments: Write a comment... 0/255

SSL Inspection Options

Enable SSL Inspection of: Multiple Clients Connecting to Multiple Servers Protecting SSL Server

CA Certificate: MyCert

Inspection Method: SSL Certificate Inspection Full SSL Inspection

Inspect All Ports

- ON HTTPS
- ON SMTPS
- ON POP3S
- ON IMAPS
- ON FTPS

Exempt from SSL Inspection

Web Categories: Click to add...

Addresses: Click to add...

4. Editing your Internet policy to use the new SSL inspection profile

Go to **Policy & Objects > Policy > IPv4** and edit the policy controlling Internet traffic. Under **Security Profiles**, ensure that **SSL Inspection** dropdown menu, select your new profile.

The **Web Filter** can remain as **default**.

Security Profiles

- OFF AntiVirus: default
- ON Web Filter: default
- OFF Application Control: default
- OFF Email Filter: default
- OFF DLP Sensor: default
- Proxy Options: default
- ON SSL Inspection: My Inspection

5. Results

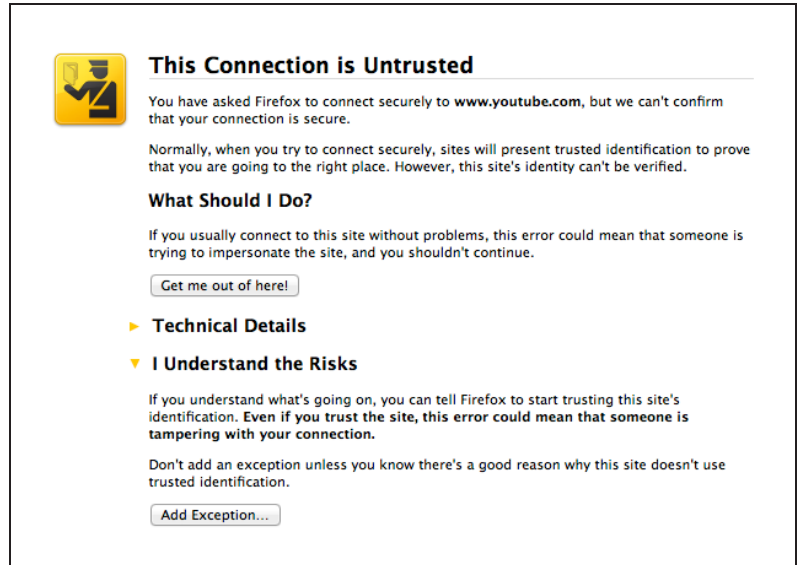
When visiting an HTTPS website such as <https://www.youtube.com/> a warning would normally appear if you are using a self-signed certificate.

If you have the correct type of certificate, signed by a recognized CA, warnings should no longer appear.

If you view the website's certificate information the **Issued By** section should contain the information of your custom certificate, indicating that the traffic is subject to deep inspection.

Network users can now manually import the certificate into their trusted root CA certificate into their trusted root CA certificate store (IE and Chrome) and/or into their browsers (Firefox).

Alternately, if the users are members of a Windows domain, the domain administrator can use a group policy to force them to trust the self-signed certificate the FortiGate is presenting.



This Connection is Untrusted

You have asked Firefox to connect securely to www.youtube.com, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

► **Technical Details**

▼ **I Understand the Risks**

If you understand what's going on, you can tell Firefox to start trusting this site's identification. Even if you trust the site, this error could mean that someone is tampering with your connection.

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

[Add Exception...](#)



General Details

Could not verify this certificate because the issuer is not trusted.

Issued To

Common Name (CN)	*.google.com
Organization (O)	Google Inc
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	34:10:F9:22:E2:0D:BF:E0:12:F6:54:53:CD:0D:BF:E0

Issued By

Common Name (CN)	fortinet.com
Organization (O)	Fortinet
Organizational Unit (OU)	Tech

Validity

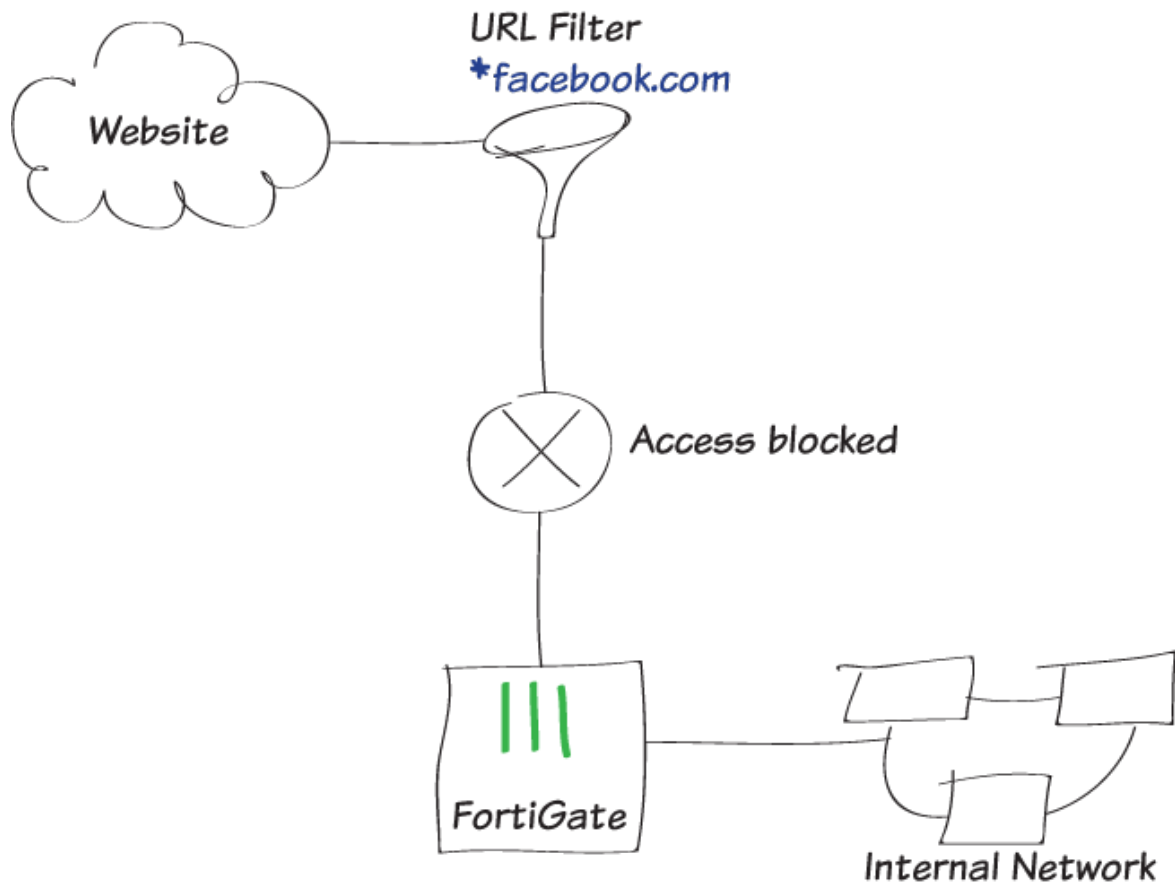
Issued On	2014-06-04
Expires On	2014-09-01

Fingerprints

SHA1 Fingerprint	AE:7D:23:3D:73:69:F3:5B:20:6E:C6:DB:7B:48:73:64:2E:52:B4:38
MD5 Fingerprint	80:12:18:86:B8:E7:F0:0B:2F:DC:15:93:45:81:A0:62

For further reading, check out [SSL/SSH Inspection](#) in the [FortiOS 5.2 Handbook](#).

Blocking Facebook



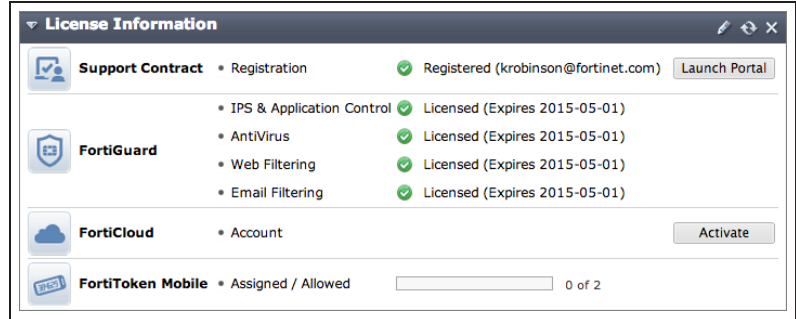
In this example, you will learn how to configure a FortiGate to prevent access to a specific social networking website, including its subdomains, by means of a static URL filter.

When you allow access to a particular type of content, such as the FortiGuard Social Networking category, there may still be certain websites in that category that you wish to prohibit. And by using SSL inspection, you ensure that this website is also blocked when accessed through HTTPS protocol.

A video of this recipe is available [here](#).

1. Verifying FortiGuard Services subscription

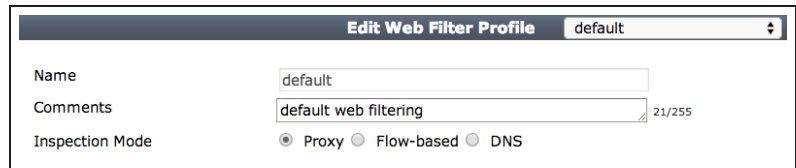
Go to **System > Dashboard > Status**. In the **License Information** widget, verify that you have an active subscription to FortiGuard Web Filtering. If you have a subscription, the service will have a green checkmark beside it.



2. Editing the Web Filter profile

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

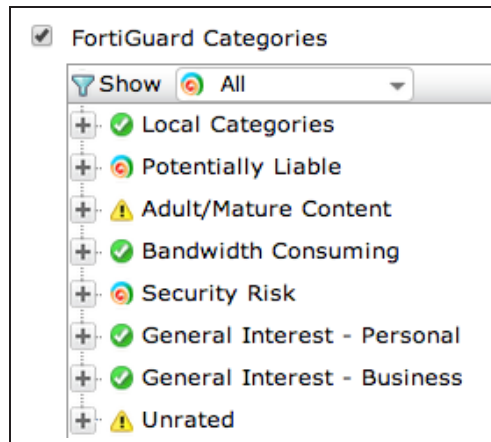
Set **Inspection Mode** to **Proxy**.



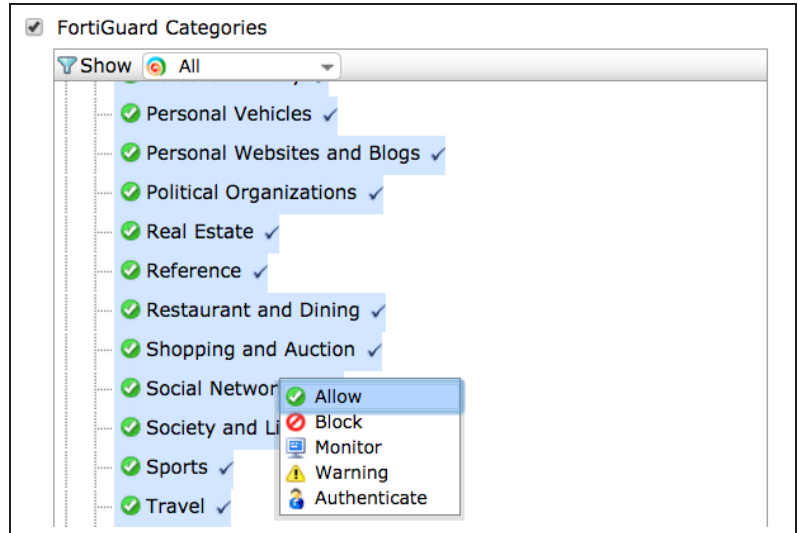
Enable the FortiGuard Categories that allow, block, monitor, warn or authenticate depending on the type of content.

Learn more about FortiGuard Categories at the FortiGuard Center web filtering rating page:

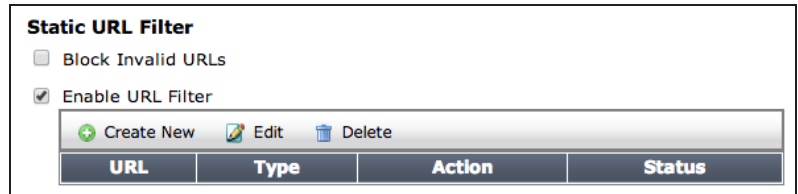
www.fortiguard.com/static/webfiltering.html



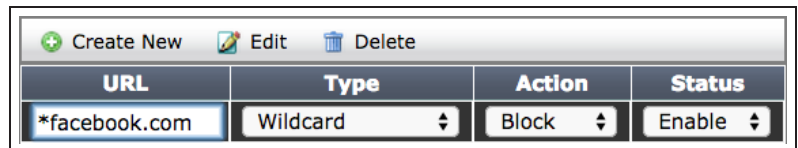
Under FortiGuard Categories, go to **General Interest - Personal**. Right-click on the **Social Networking** subcategory and ensure it is set to **Allow**.



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



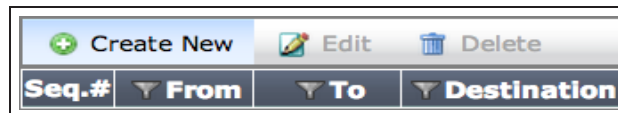
For your new web filter, enter the URL of the website you are attempting to block. If you want to block all of the subdomains for that website, omit the protocol in the URL and enter an asterisk (*). For this example, enter: **facebook.com*



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

3. Creating a security policy

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



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

Enable **NAT**.

Incoming Interface: lan

Source Address: all

Source User(s): Click to add...

Source Device Type: Click to add...

Outgoing Interface: wan1

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

Firewall / Network Options

NAT

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

Security Profiles

AntiVirus

Web Filter

default

default

This automatically enables **SSL/SSH Inspection**. Select **certificate-inspection** from the dropdown menu. This profile allows the FortiGate to inspect and apply web filtering to HTTPS traffic.

Proxy Options: default

SSL/SSH Inspection: certificate-inspection

After you have created your new policy, ensure that it is at the top of the policy list. To move your policy up or down, click and drag the far left column of the policy.

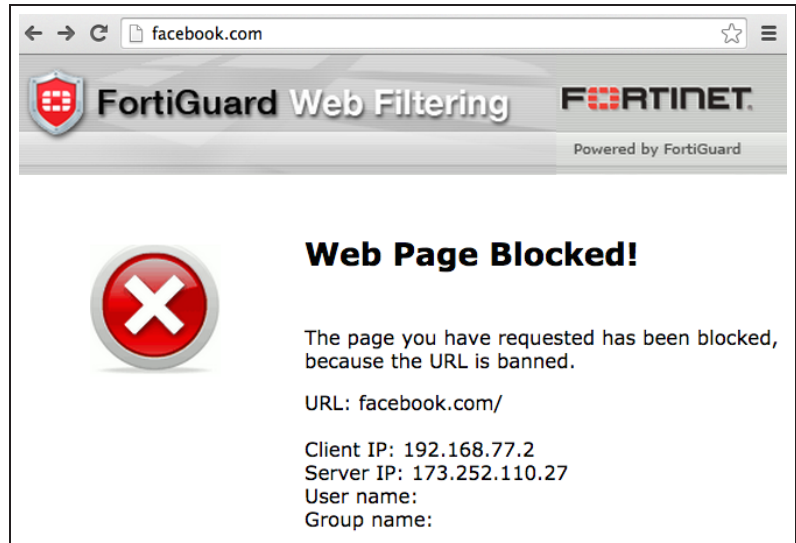
Seq.#	Source	Destination	ID	Schedule	Service	AV
lan - wan1 (1 - 2)						
1	all	all	2	always	ALL	None
2	all	all	1	always	ALL	AV default
Implicit (3 - 3)						

4. Results

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

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

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



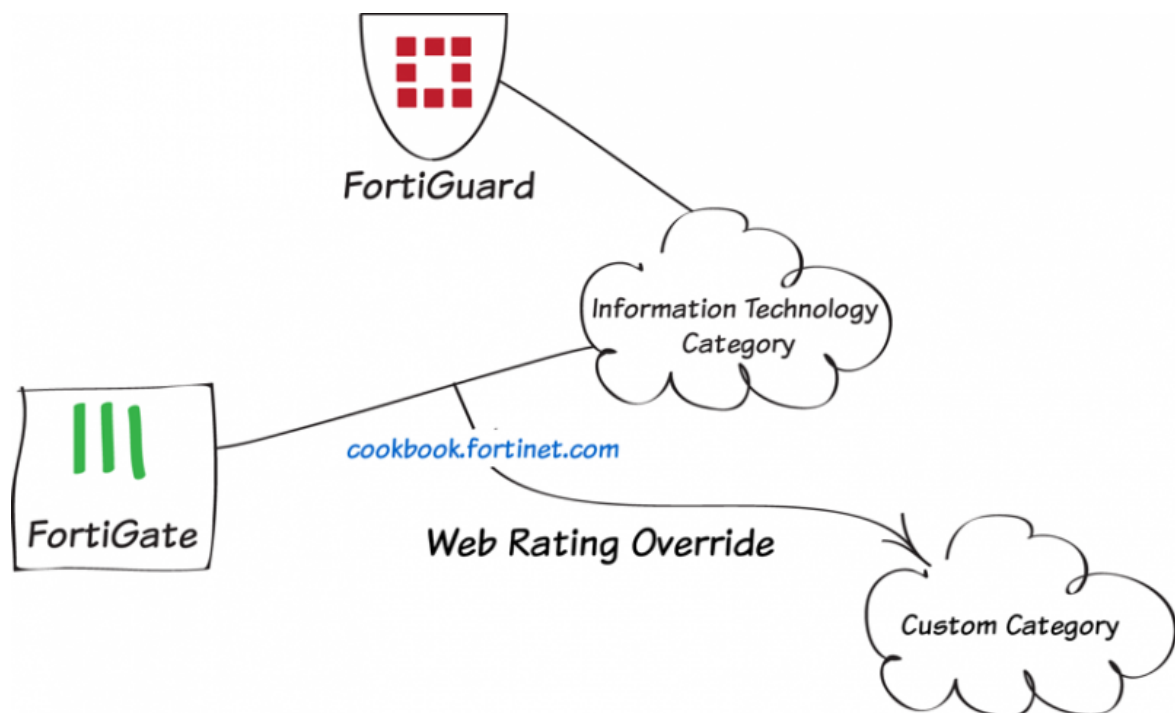
Visit <https://www.facebook.com> to verify that HTTPS protocol is blocked.

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



For further reading, check out [Static URL Filter](#) in the [FortiOS 5.2 Handbook](#).

Web rating overrides



In this recipe, you will change a website's FortiGuard web rating

An active license for FortiGuard Web Filtering Services is required to use web ratings.

For testing purposes, the Cookbook website (cookbook.fortinet.com) will be changed from the category **Information Technology** to a custom category named **Allowed Sites**.

By changing the web rating for a website, you can control access to the site without affecting the rest of the sites in its original category.

This recipe only changes the website's rating on your FortiGate. To request that the rating is changed for all of FortiGuard, go [here](#).

1. Enabling web filtering

Go to **System > Config > Features** and make sure that **Web Filter** is **ON**. If necessary, **Apply** your changes.



2. Creating a custom category and web rating override

Go to **Security Profiles > Advanced > Web Rating Overrides** and select **Custom Categories**.

Create a new category named *Allowed Sites*.

+ Create New Edit Delete		
Name	Number of Override URLs	Number of Web Filter Profile References
custom1	0	0
custom2	0	0
Allowed Sites	0	0

Go to **Security Profiles > Advanced > Web Rating Overrides** and create a new override.

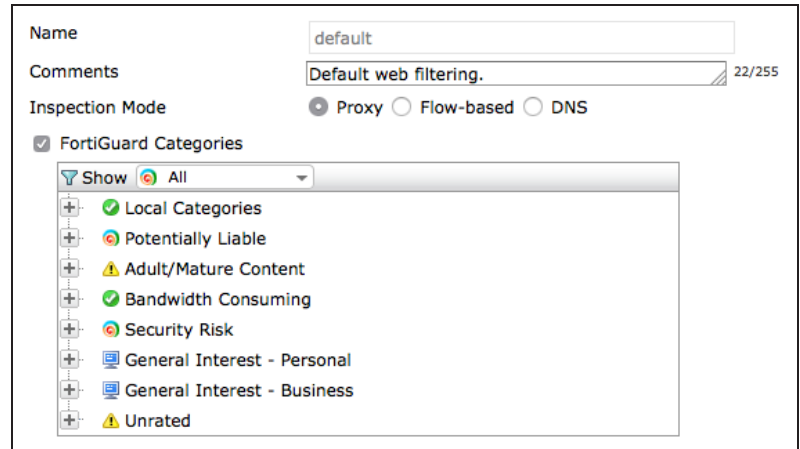
Enter the website's **URL** and select **Lookup Rating** to see the current rating.

In the **Override to** section, set **Category** to **Custom Categories** and **Sub-category** to **Allowed Sites**.

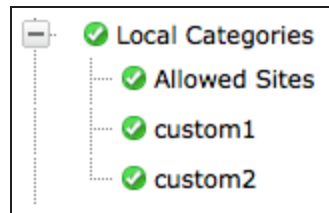
URL	<input type="text" value="cookbook.fortinet.com"/>	Lookup Rating
FortiGuard Rating		
Category: General Interest - Business		
Sub-Category: Information Technology		
Override to		
Category	<input type="text" value="Custom Categories"/>	
Sub-Category	<input type="text" value="Allowed Sites"/>	

3. Adding FortiGuard blocking to the default web filter profile

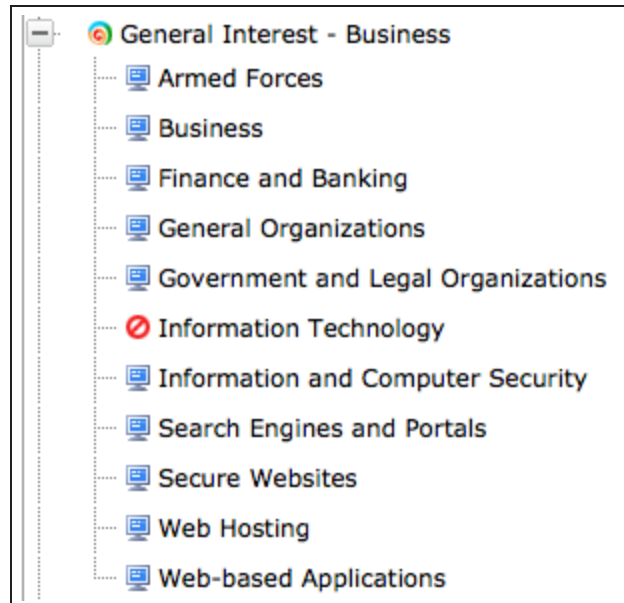
Go to **Security Profiles > Web Filter** and edit the default profile. Enable **FortiGuard Categories**.



Expand **Local Categories** to make sure that the **Allowed Sites** category is set to **Allow**.



Expand **General Interest - Business**. Right-click on **Information Technology** to set it to **Block**.



4. Adding the default web filter profile to a security policy

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

Under **Security Profiles**, turn on **Web Filter** and use the **default** profile.

Incoming Interface	lan
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	always
Action	ACCEPT
Firewall / Network Options	
<input checked="" type="checkbox"/> NAT	
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...
Security Profiles	
<input type="checkbox"/> AntiVirus	default
<input checked="" type="checkbox"/> Web Filter	default
<input type="checkbox"/> Application Control	default
<input type="checkbox"/> IPS	default
<input type="checkbox"/> DLP Sensor	default
Proxy Options	default
<input checked="" type="checkbox"/> SSL/SSH Inspection	certificate-inspection

5. Results

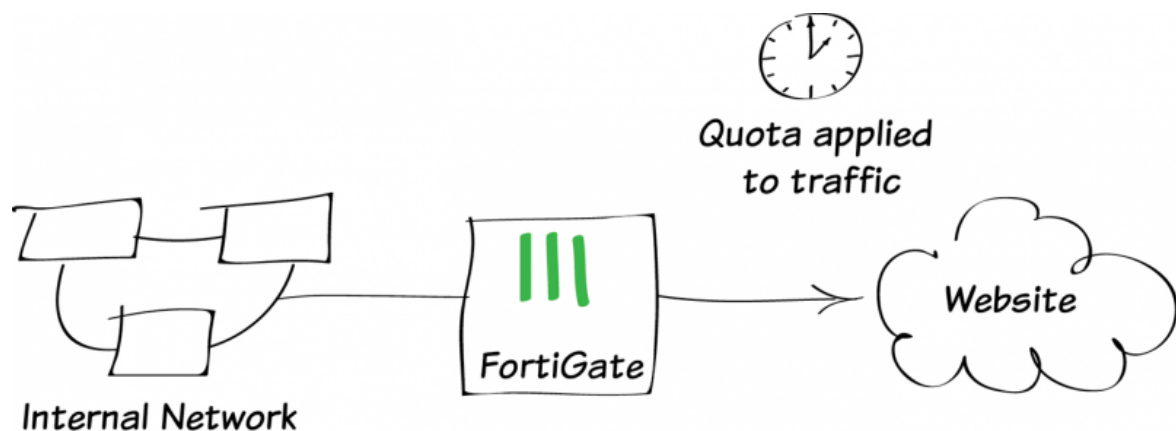
Browse to www.fortinet.com, which is part of the **Information Technology** category. A message will appear from FortiGuard, stating that access to this website is blocked.



If you browse to cookbook.fortinet.com, you will still be able to access the site.

For further reading, check out [FortiGuard Web Filtering Service](#) in the [FortiOS 5.2 Handbook](#).

Web filtering using quotas



In this example, you will create a web filter profile that allows access to websites that are categorized as "Personal Interest" at any point during the day, but limits access for a total of 5 minutes for each user.

An active license for FortiGuard Web Filtering Services is required to use web filtering with quotas.

Quotas are the most efficient way of allowing limited access to websites, as they do not require set schedules. To apply web filtering using quotas, you must use a security policy with either user or device authentication. In this recipe, a user account, *alstair*, has already been configured. For more information about creating user accounts, see [User and device authentication](#).

1. Enabling web filtering

Go to **System > Config > Features** and make sure that **Web Filter** is **ON**. If necessary, **Apply** your changes.

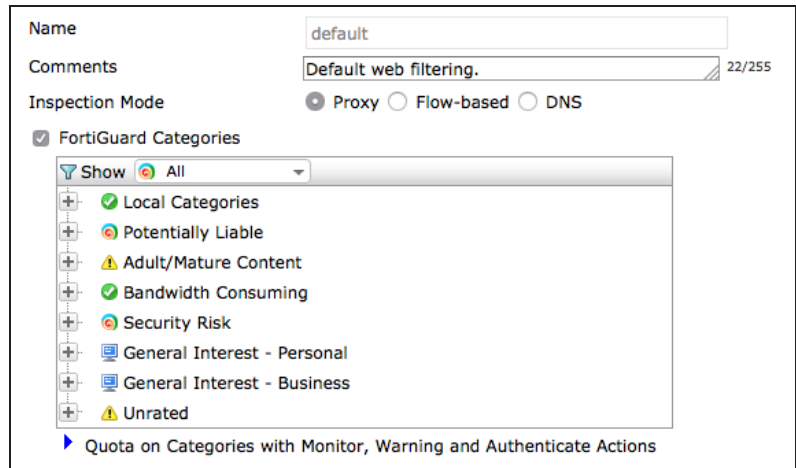


2. Creating a web filter profile that uses quotas

Go to **Security Profiles > Web Filter > Profiles**. Edit the **default** profile and enable **FortiGuard Categories**.

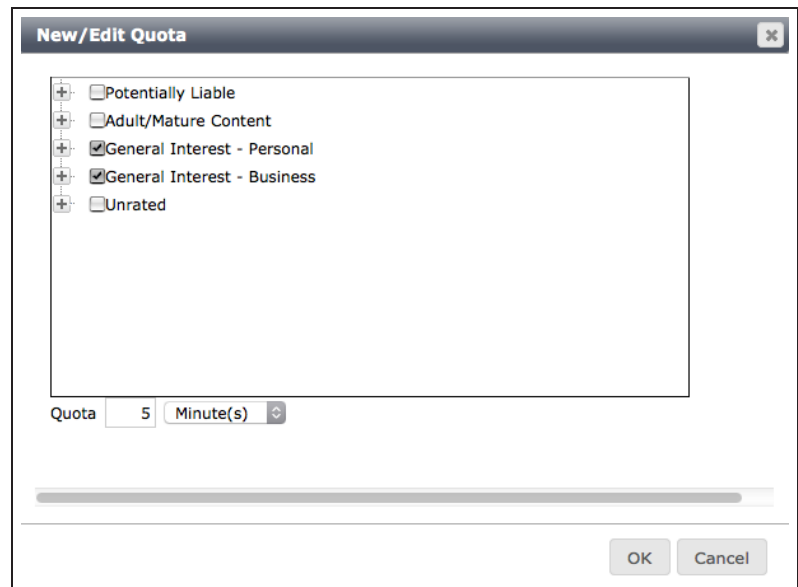
Right-click on the category **General Interest - Personal** and select **Monitor**. Do the same for the category **General Interest - Business**.

These categories include a variety of sites that are commonly blocked in the workplace, such as games, instant messaging, and social media.

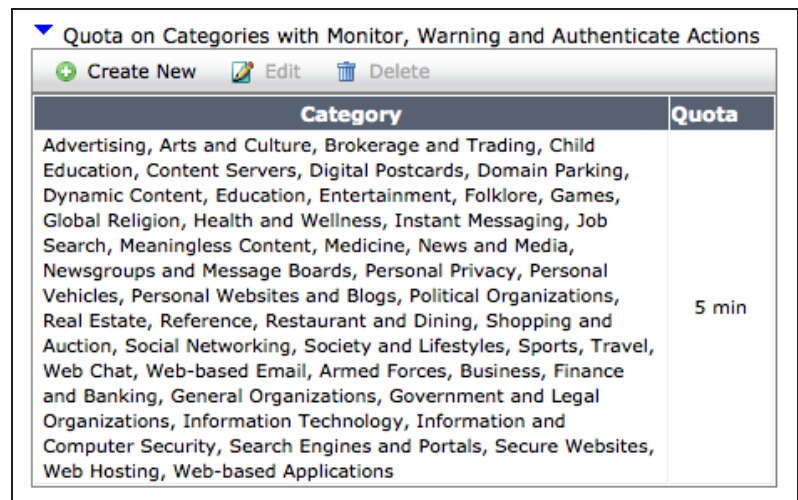


Expand **Quota on Categories with Monitor, Warning and Authenticate Actions** and select **Create New**.

Select both **General Interest - Personal** and **General Interest - Business**. For testing purposes, set the **Quota** amount to **5 Minutes**.



The web filter will now list all the sub-categories listed in the two categories and the applied quota.



3. Adding web filtering to a security policy with user authentication

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

Under **Security Profiles**, turn on **Web Filter** and use the **default** profile.

Incoming Interface	lan	+
Source Address	all	+
Source User(s)	alistair	X +
Source Device Type	Click to add...	
Outgoing Interface	wan1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	
Firewall / Network Options		
<input checked="" type="checkbox"/> NAT		
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	Click to add...	
Security Profiles		
<input type="checkbox"/> AntiVirus	default	
<input checked="" type="checkbox"/> Web Filter	default	+
<input type="checkbox"/> Application Control	default	
<input type="checkbox"/> IPS	default	
<input type="checkbox"/> DLP Sensor	default	
Proxy Options	default	+
<input checked="" type="checkbox"/> SSL/SSH Inspection	certificate-inspection	+

4. Results

Browse to www.ebay.com, a website that is found within the General Interest - Personal category.

Access to the website is allowed for 5 minutes, after which a block message appears. The message will persist for all General Interest - Personal sites until the quota is reset, which occurs every 24 hours at midnight.

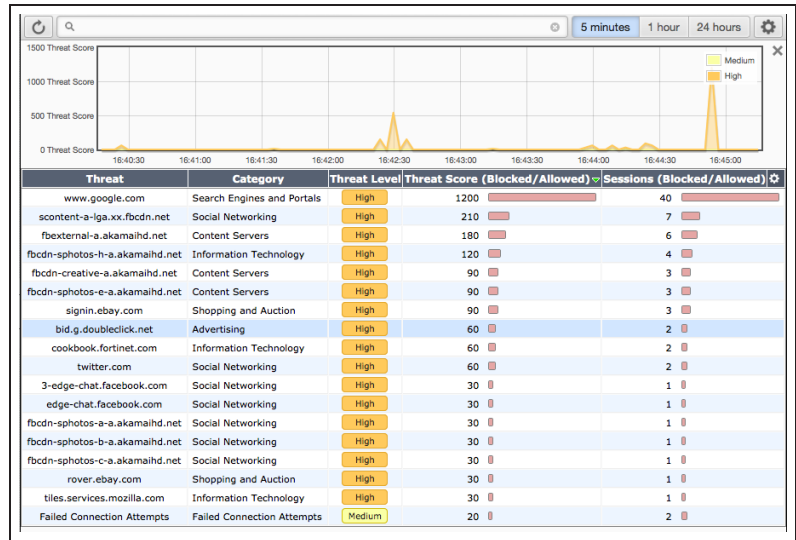
Web Page Blocked

Your daily quota for this category of webpage has expired, in accordance with your internet usage policy.

URL: signin.ebay.com/
Category: Shopping and Auction

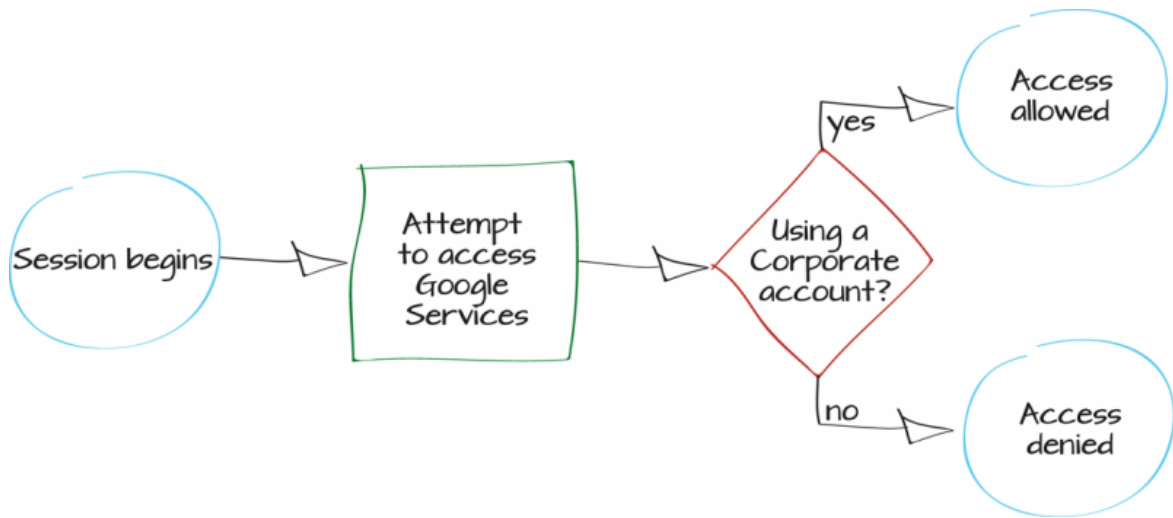
To have the rating of this web page re-evaluated [please click here](#).

Go to **System > FortiView > Threats** and select the **5 minutes** view. You will be able to see the blocked traffic.



For further reading, check out **FortiGuard Web Filtering Service** in the **FortiOS 5.2 Handbook**.

Blocking Google access for consumer accounts



In this recipe, you will block access to Google services for consumer accounts, while allowing access for corporate accounts.

If your organization has set up a Google corporate account to be able to use Google services, such as Gmail and Google Docs, this recipe can be used to block users from accessing those services with their own personal accounts. In this example, a corporate account has been created that uses the domain *fortidocs.com*.

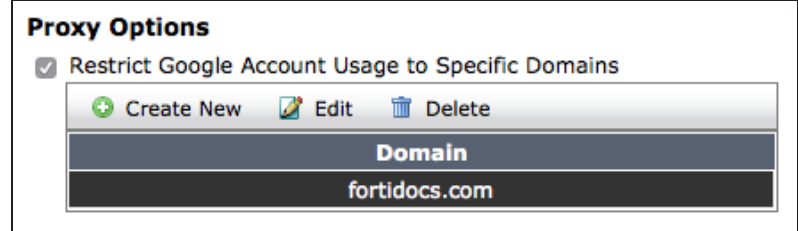
A video of this recipe is available [here](#).

1. Editing the default web filter profile to restrict Google access

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

Make sure that **Inspection Mode** is set to **Proxy**. Under **Proxy Options**, select **Restrict Google Account Usage to Specific Domains**.

Select **Create New** in the list that appears and add an entry for the domains for your Corporate Google accounts (in the example, *fortidocs.com*).

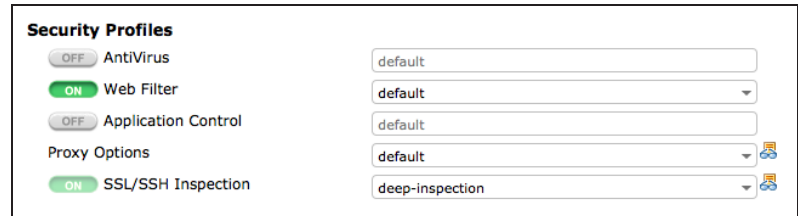


2. Adding the profile to your Internet-access policy

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

Enable **Web Filter** and set it to use the **default** profile. Doing this will automatically enable **SSL/SSH Inspection**. Set this to use the **deep-inspection** profile.

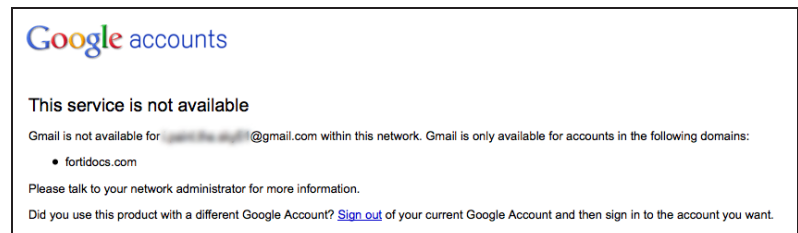
Using the **deep-inspection** profile may cause certificate errors. For information about avoiding this, see [Preventing certificate warnings](#).



3. Results

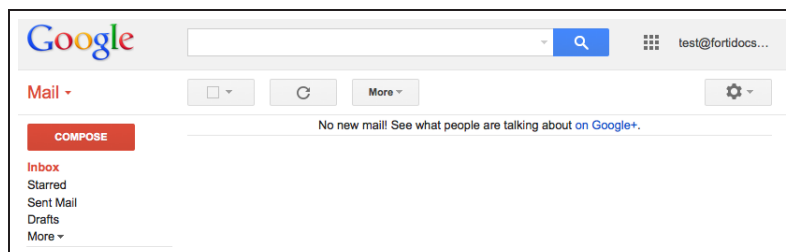
Log in to Google using a personal account. After you are authenticated, attempt to access a Google service, such as **Gmail** or **Google Drive**.

A message appears from Google stating that the service is not available.



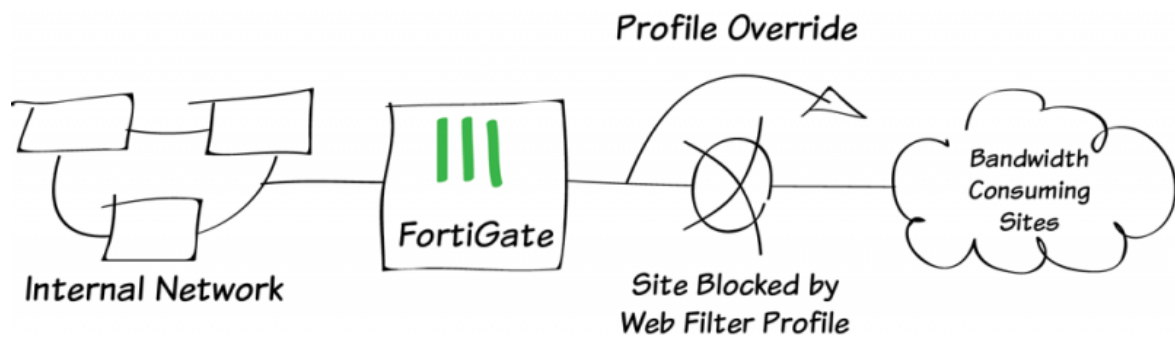
Sign out of the personal account and instead use your corporate account (in the example, *test@fortidocs.com*).

You can now access the Google service.



For further reading, check out [Web filter](#) in the [FortiOS 5.2 Handbook](#).

Overriding a web filter profile



In this example, one user is temporarily allowed to override a web filter profile to be able to access sites that would otherwise be blocked.

In this example, web filtering blocks the **Bandwidth Consuming** category for all users, except those who can override the filter.

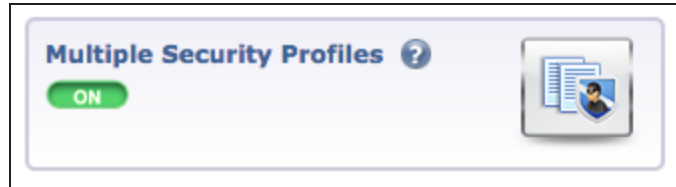
1. Enabling web filtering and multiple profiles

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



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

Apply the changes.



2. Creating a user group and two users

Go to **User & Device > User > User Groups**. Create a new group for users who can override web filtering (in the example, *web-filter-override*).

Name	<input type="text" value="web-filter-override"/>
Type	<input checked="" type="radio"/> Firewall <input type="radio"/> Fortinet Single Sign-On (FSSO) <input type="radio"/> Guest <input type="radio"/> RADIUS Single Sign-On (RSSO)
Members	<input type="text" value="Click to add..."/>
Remote groups	

Go to **User & Device > User > User Definition** and create two users (in the example, *ckent* and *bwayne*).

1 User Type	2 Login Credentials	3 Contact Info	4 Extra Info
<input checked="" type="radio"/> Local User			
<input type="radio"/> Remote RADIUS User			
<input type="radio"/> Remote TACACS+ User			
<input type="radio"/> Remote LDAP User			
<input type="button" value=" < Back"/>		<input type="button" value=" Next >"/>	<input type="button" value=" Cancel"/>

Progress: 1 User Type | 2 Login Credentials | 3 Contact Info | 4 Extra Info

User Name:

Password:

< Back Next > Cancel

Progress: 1 User Type | 2 Login Credentials | 3 Contact Info | 4 Extra Info

Email Address:

SMS

< Back Next > Cancel

Assign *ckent* to the *web-filter-override* group, but not *bwayne*.

Progress: 1 User Type | 2 Login Credentials | 3 Contact Info | 4 Extra Info

Enable

Two-factor Authentication

User Group: +

< Back Create Cancel

3. Creating a web filter profile and override

Go to **Security Profiles > Web Filter** and create a new profile (in the example, *block-bandwidth-consuming*).

Enable FortiGuard Categories, then right-click **Bandwidth Consuming** and select **Block**.

The screenshot shows the configuration for a web filter profile named "block-bandwidth-consuming". The "Inspection Mode" is set to "Proxy". The "FortiGuard Categories" section is expanded, showing a list of categories with their status:

- Local Categories:
- Potentially Liabile:
- Adult/Mature Content:
- Bandwidth Consuming: (with a red 'X' icon)
- Security Risk:
- General Interest - Personal:
- General Interest - Business:
- Unrated:

A blue arrow points to the text: "Quota on Categories with Monitor, Warning and Authenticate Actions".

Go to **Security Profiles > Advanced > Web Profile Overrides** and create a new override.

Set **Scope Range** to **User Group**, **User Group** to the *web-filter-override* group, **Original Profile** to the *block-bandwidth-consuming* profile, and **New Profile** to the **default** profile.

The screenshot shows the configuration for a web profile override. The "Scope Range" is set to "User Group". The "User Group" is "web-filter-override". The "Original Profile" is "block-bandwidth-consuming" and the "New Profile" is "default". The "Expires" time is set to 100 Days, 0 Hours, and 0 Minutes. The expiration date and time are shown as "(Expires: 7/18/2015, 2:57:00 PM)".

Set an appropriate **Expires** time to control how long the override can be used (in the example, *100 hours* after the override is created).

4. Adding the new web filter profile to a security policy

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

Set **Source User(s)** to allow both the *web-filter-override* group and user *bwayne*.

Under **Security Profiles**, turn on **Web Filter** and use the new profile.

Incoming Interface	lan (VLAN ID: 0)	+
Source Address	all	+
Source User(s)	web-filter-override bwayne	X X
Source Device Type	Click to add...	
Outgoing Interface	wan1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	
Firewall / Network Options		
<input checked="" type="checkbox"/> NAT		
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	Click to add...	
Security Profiles		
<input type="checkbox"/> AntiVirus	default	🔧
<input checked="" type="checkbox"/> Web Filter	block-bandwidth-consuming	🔧
<input type="checkbox"/> Application Control	default	🔧
Proxy Options	default	🔧
<input checked="" type="checkbox"/> SSL/SSH Inspection	certificate-inspection	🔧

5. Results

Browse to blip.tv, a website that is part of the **Bandwidth Consuming** category.

Authenticate using the *bwayne* account. The website is blocked.

**FortiGuard Web Filtering**



Web Page Blocked!

You have tried to access a web page which is in violation of your internet usage policy.

URL: blip.tv/
Category: Streaming Media and Download
Client IP: 192.168.150.100
Server IP: 74.122.172.235
User name: bwayne
Group name: bwayne

To have the rating of this web page re-evaluated [please click here](#).

Go to **User & Device > Monitor > Firewall** and **De-authenticate** *bwayne*.

Browse to blip.tv again, this time authenticating using the *ckent* account. You can access the website until the override expires.

For further reading, check out [Web Filter](#) in the [FortiOS 5.2 Handbook](#).

Troubleshooting web filtering

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

The Web Filter option does not appear in the GUI.

Go to **Config > System > Features** and enable **Web Filter**.

New Web Filter profiles cannot be created.

Go to **Config > System > Features** and select **Show More**. Enable **Multiple Security Profiles**.

Web Filtering has been configured but is not working.

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

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

First, ensure that web filtering is enabled in one of your security policies. The FortiGuard service will sometimes show as expired when it is not being used, to save CPU cycles.

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

WiFi

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

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

Getting started with WiFi

- [Setting up WiFi with FortiAP](#)
- [Setting up a WiFi bridge with a FortiAP](#)
- [Combining WiFi and wired networks with a software switch](#)
- [WiFi network with external DHCP service](#)
- [Providing remote access to the office and Internet](#)
- [Extending WiFi range with mesh topology](#)

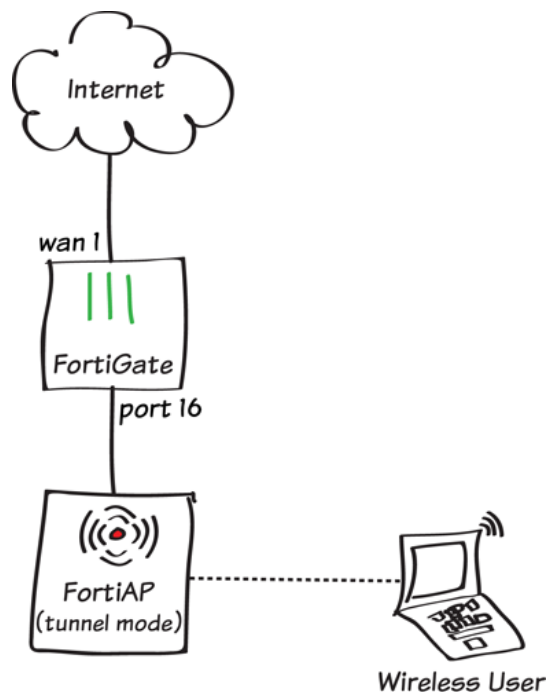
WiFi access control

- [Guest WiFi accounts](#)
- [Captive portal WiFi access control](#)
- [WPA2 WiFi access control](#)
- [WiFi with external RADIUS authentication](#)
- [MAC access control](#)
- [BYOD scheduling](#)
- [BYOD for a user with multiple wireless devices](#)

WiFi with other technologies

- [Explicit proxy with web caching](#)
- [AirPlay for Apple TV](#)

Setting up WiFi with FortiAP



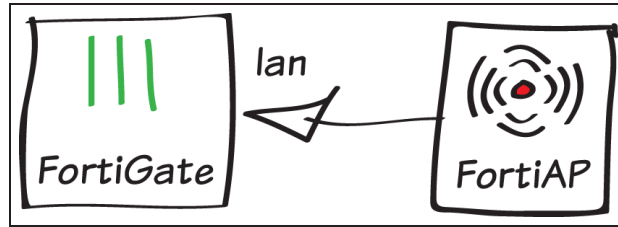
In this example, a FortiAP unit is connected to and managed by a FortiGate unit in Tunnel mode, allowing wireless access to the network.

You can configure a FortiAP unit in either Tunnel mode or Bridge mode. When a FortiAP is in Tunnel mode, a wireless-only subnet is used for wireless traffic. When a FortiAP is in Bridge mode, the Ethernet and WiFi interfaces are connected (or bridged), allowing wired and wireless networks to be on the same subnet. Tunnel mode is the default mode for a FortiAP.

For information about using a FortiAP in Bridge mode, see [Setting up a WiFi bridge with a FortiAP](#).

1. Connecting and authorizing the FortiAP unit

Connect the FortiAP unit to the the lan interface.



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

Mesh	Access Point	State	Connected Via
▣	FAP11C3X13000412	?	192.168.10.2

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

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

Mesh	Access Point	State	Connected Via
▣	FAP11C3X13000412	✓	192.168.10.2

2. Creating an SSID

Go to **WiFi Controller > WiFi Network > SSID** and create a new SSID.

Set **Traffic Mode** to **Tunnel to Wireless Controller**.

Select an **IP/Network Mask** for the wireless interface and enable **DHCP Server**.

Set the **WiFi Settings** as required, including a secure **Pre-shared Key**.

Interface Name	<input type="text" value="wireless"/>						
Type	<input type="text" value="WiFi SSID"/>						
Traffic Mode	<input type="text" value="Tunnel to Wireless Controller"/>						
IP/Network Mask	<input type="text" value="10.10.10.10/255.255.255.0"/>						
Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access						
DHCP Server	<input checked="" type="checkbox"/> Enable						
Address Range	<table border="1"><tr><td colspan="2">+ Create New Edit Delete</td></tr><tr><td>Starting IP</td><td>End IP</td></tr><tr><td>10.10.10.11</td><td>10.10.10.254</td></tr></table>	+ Create New Edit Delete		Starting IP	End IP	10.10.10.11	10.10.10.254
+ Create New Edit Delete							
Starting IP	End IP						
10.10.10.11	10.10.10.254						
Netmask	<input type="text" value="255.255.255.0"/>						
Default Gateway	<input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify						
DNS Server	<input checked="" type="radio"/> Same as System DNS <input type="radio"/> Specify						
	▶ Advanced...						
WiFi Settings							
SSID	<input type="text" value="myWiFi"/>						
Security Mode	<input type="text" value="WPA2 Personal"/>						
Pre-shared Key	<input type="text" value="....."/> (8 - 63 characters)						

3. Creating a custom FortiAP profile

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

Set **Platform** to the correct FortiAP model you are using (FAP11C in the example).

Set **SSID** to use the new SSID.

Name: myprofile
Comments: Write a comment... 0/255
Platform: FAP11C

Radio 1
Mode: Disable Access Point
Spectrum Analysis:
WIDS Profile: Click to set...
Radio Resource Provision:
Client Load Balancing: Frequency Handoff AP Handoff
Band: 2.4GHz 802.11n/g/b
Channel: 1 2 3 4 5 6 7 8 9 10 11
Auto TX Power Control: Disable Enable
TX Power: 100 %
SSID: wireless (SSID: myWiFi)

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and edit the FortiAP. Set **FortiAP Profile** to use the new profile.

Wireless Settings
FortiAP Profile: myprofile Override Settings

Radio Settings Summary

Radio	Settings	Channels	SSIDs
Radio 1	AP (2.4 GHz Band)	1, 6, 11	wireless (SSID: myWiFi)

4. Allowing wireless access to the Internet

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the SSID and **Outgoing Interface** to your Internet-facing interface. Ensure that **NAT** is turned **ON**.

Incoming Interface	wireless (SSID: myWiFi)	+
Source Address	all	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	wan1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	
Firewall / Network Options		
<input checked="" type="checkbox"/> NAT		
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	Click to add...	

5. Results

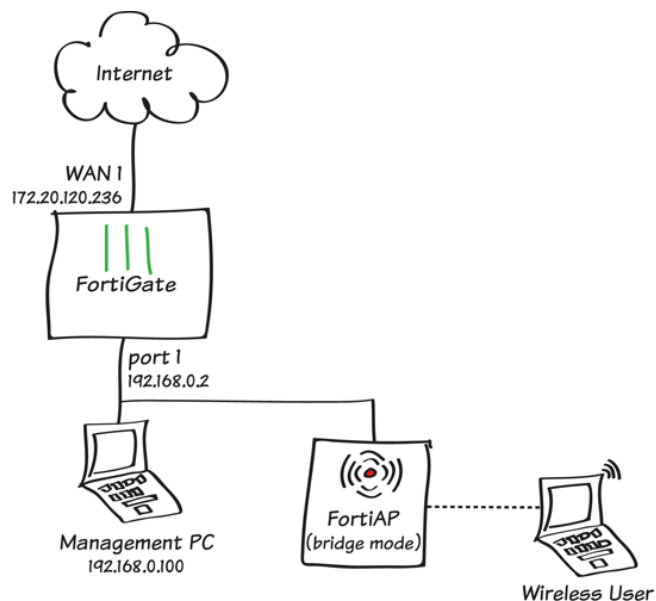
Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. A green checkmark now appears beside the FortiAP, showing that the unit is authorized and online.

Mesh	Access Point	State	Connected Via
■	FAP11C3X13000412	✓	🖨️ 192.168.10.2

Connect to the SSID with a wireless device. After a connection is established, you are able to browse the Internet.

For further reading, check out [Configuring a WiFi LAN](#) in the [FortiOS 5.2 Handbook](#).

Setting up a WiFi bridge with a FortiAP



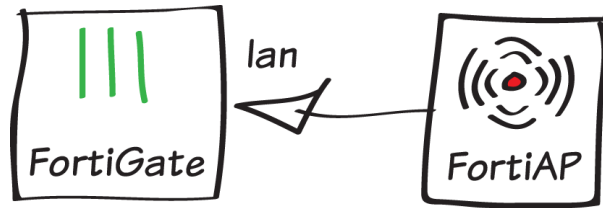
In this example, a FortiAP unit is connected to and managed by a FortiGate unit in Bridge mode.

You can configure a FortiAP unit in either Tunnel mode or Bridge mode. When a FortiAP is in Tunnel mode, a wireless-only subnet is used for wireless traffic. When a FortiAP is in Bridge mode, the Ethernet and WiFi interfaces are connected (or bridged), allowing wired and wireless networks to be on the same subnet. Tunnel mode is the default mode for a FortiAP.

For information about using a FortiAP in Tunnel mode, see [Setting up WiFi with FortiAP](#).

1. Connecting and authorizing the FortiAP unit

Connect the FortiAP unit to the the lan interface.



Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. The FortiAP is listed, with a yellow question mark beside it because the device is not authorized.

Mesh	Access Point	State	Connected Via
■	FAP11C3X13000412	?	192.168.10.2

The FortiAP may not appear until a few minutes have passed.

Highlight the FortiAP unit on the list and select **Authorize**. A grey checkmark is now shown beside the FortiAP, showing that it is authorized but not yet online.

Mesh	Access Point	State	Connected Via
■	FAP11C3X13000412	✓	192.168.10.2

2. Creating an SSID

Go to **WiFi Controller > WiFi Network > SSID** and create a new SSID.

Set **Traffic Mode** to **Local bridge with FortiAP's Interface**.

Set the **WiFi Settings** as required, including a secure **Pre-shared Key**.

Interface Name	wireless
Type	WiFi SSID
Traffic Mode	Local bridge with FortiAP's Interf...
WiFi Settings	
SSID	myWiFi
Security Mode	WPA2 Personal
Pre-shared Key (8 - 63 characters)
Allow New WiFi Client Connections When Controller Is Down	<input type="checkbox"/>
Maximum Clients	<input type="checkbox"/>
Optional VLAN ID	0

3. Creating a custom FortiAP profile

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and create a new profile.

Set **Platform** to the correct FortiAP model you are using (FAP11C in the example).

Set **SSID** to use the new SSID.

Name: myprofile
Comments: Write a comment... 0/255
Platform: FAP11C

Radio 1
Mode: Disable Access Point
Spectrum Analysis:
WIDS Profile: Click to set...
Radio Resource Provision:
Client Load Balancing: Frequency Handoff AP Handoff
Band: 2.4GHz 802.11n/g/b
Channel: 1 2 3 4 5 6 7 8 9 10 11
Auto TX Power Control: Disable Enable
TX Power: 100 %
SSID: wireless (SSID: myWiFi)

Go to **WiFi Controller > Managed Access Points > Managed FortiAPs** and edit the FortiAP. Set **FortiAP Profile** to use the new profile.

Wireless Settings
FortiAP Profile: myprofile Override Settings

Radio Settings Summary

Radio	Settings	Channels	SSIDs
Radio 1	AP (2.4 GHz Band)	1, 6, 11	wireless (SSID: myWiFi)

4. Results

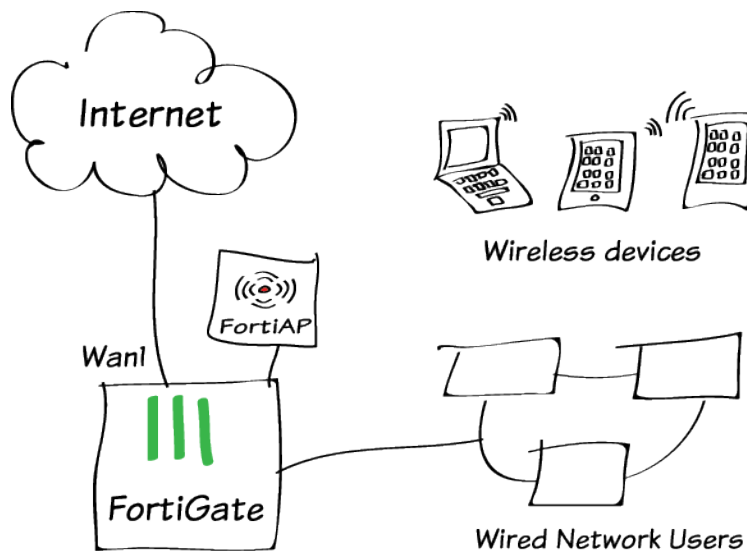
Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**. A green checkmark now appears beside the FortiAP, showing that the unit is authorized and online.

Mesh	Access Point	State	Connected Via
<input type="checkbox"/>	FAP11C3X13000412	<input checked="" type="checkbox"/>	192.168.10.2

Connect to the SSID with a wireless device. After a connection is established, you are able to browse the Internet.

For further reading, check out [Bridge SSID to FortiGate wired network](#) in the [FortiOS 5.2 Handbook](#).

Combining WiFi and wired networks with a software switch



Including mobile (WiFi) users on your office LAN can be more convenient than putting them on a separate wireless network. The Software Switch feature of your FortiGate is a simple way to do this.

Software Switches are only available if your FortiGate is in Interface mode. For more information, see [Choosing your FortiGate's switch mode](#).

1. Create the SSID

Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network.

Leave the IP address empty. This is allowed.

You can use any type of security/authentication. In this example, your users must be members of the *employees* group to access the network.

Interface Name	example-wifi
Type	WiFi SSID
Traffic Mode	Tunnel to Wireless Controller
IP/Network Mask	<input type="text"/>
WiFi Settings	
SSID	<input type="text" value="example-staff"/>
Security Mode	WPA2 Enterprise
Authentication	<input checked="" type="radio"/> Local <input type="radio"/> RADIUS Server
	<input type="text" value="employees"/> +
Broadcast SSID	<input checked="" type="checkbox"/>
Block Intra-SSID Traffic	<input type="checkbox"/>
Maximum Clients	<input type="checkbox"/>
Optional VLAN ID	<input type="text" value="0"/>

2. Combine the WiFi and wired interfaces

Go to **System > Network > Interface**. Edit the existing **lan** software switch interface or create a new one.

Make sure your wired and WiFi interfaces are both included.

Make sure there is a **DHCP Server** configured. It will provide IP addresses to both WiFi and wired users.

Interface Name	lan									
Type	Software Switch									
Physical Interface Members	<input type="text" value="port1"/> X + <input type="text" value="example-wifi (SSID: exa..."/> X									
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE									
IP/Network Mask	<input type="text" value="192.168.65.1/255.255.255.0"/>									
Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP <input checked="" type="checkbox"/> SSH <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> FCT-Access									
DHCP Server	<input checked="" type="checkbox"/> Enable									
Address Range	<table border="1"><tr><td>+ Create New</td><td>✎ Edit</td><td>🗑 Delete</td></tr><tr><th>Starting IP</th><th>End IP</th><td></td></tr><tr><td>192.168.65.2</td><td>192.168.65.254</td><td></td></tr></table>	+ Create New	✎ Edit	🗑 Delete	Starting IP	End IP		192.168.65.2	192.168.65.254	
+ Create New	✎ Edit	🗑 Delete								
Starting IP	End IP									
192.168.65.2	192.168.65.254									
Netmask	<input type="text" value="255.255.255.0"/>									
Default Gateway	<input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify									
DNS Server	<input checked="" type="radio"/> Same as System DNS <input type="radio"/> Same as Interface IP <input type="radio"/> Specify									

3. Create the security policy

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing all users on the software switch interface to connect to the Internet.

The screenshot shows the configuration for a Firewall Policy. The 'Incoming Interface' is set to 'lan', 'Source Address' to 'all', 'Outgoing Interface' to 'wan1', 'Destination Address' to 'all', 'Schedule' to 'always', and 'Service' to 'ALL'. The 'Action' is set to 'ACCEPT'. Under 'Firewall / Network Options', 'NAT' is turned ON, and 'Use Outgoing Interface Address' is selected.

Incoming Interface	lan
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

Firewall / Network Options

ON NAT

Use Outgoing Interface Address Fixed Port

Use Dynamic IP Pool

4. Connect and authorize the FortiAP unit

Go to **System > Network > Interface**. Configure a network interface that is dedicated to extension devices.

The screenshot shows the configuration for a Network Interface. The 'Addressing mode' is set to 'Dedicated to Extension Device'. The 'IP/Network Mask' is '10.11.12.1/255.255.255.0' and 'Connected Devices' is 'None'.

Addressing mode	<input type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input checked="" type="radio"/> Dedicated to Extension Device
IP/Network Mask	10.11.12.1/255.255.255.0
Connected Devices	None

Connect the FortiAP unit and wait for it to be listed in **WiFi Controller > Managed Access Points > Managed FortiAPs**.

The screenshot shows a table of Managed FortiAPs. The table has columns for Mesh, Access Point, State, Connected Via, SSIDs, Channel, Clients, OS Version, and FortiAP Profile. One FortiAP is listed with ID FP221C3X14019926, connected via 10.11.12.2.

Mesh	Access Point	State	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile
	FP221C3X14019926		10.11.12.2	Radio 1: Radio 2:	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0		FAP221C-default

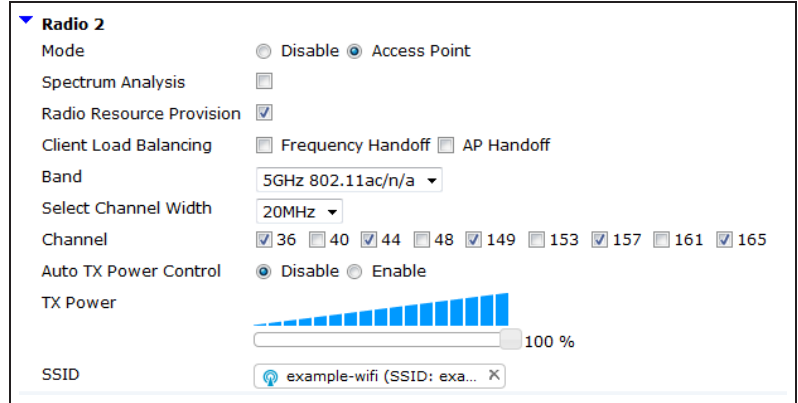
Highlight the FortiAP unit on the list and select **Authorize**.

5. Add the SSID to the FortiAP profile

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the profile for your FortiAP model.

For each radio:

- Enable **Radio Resource Provision**.
- Select your SSID.



Radio 2

Mode Disable Access Point

Spectrum Analysis

Radio Resource Provision

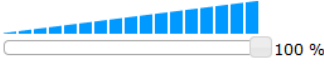
Client Load Balancing Frequency Handoff AP Handoff

Band 5GHz 802.11ac/n/a

Select Channel Width 20MHz

Channel 36 40 44 48 149 153 157 161 165

Auto TX Power Control Disable Enable

TX Power  100 %

SSID

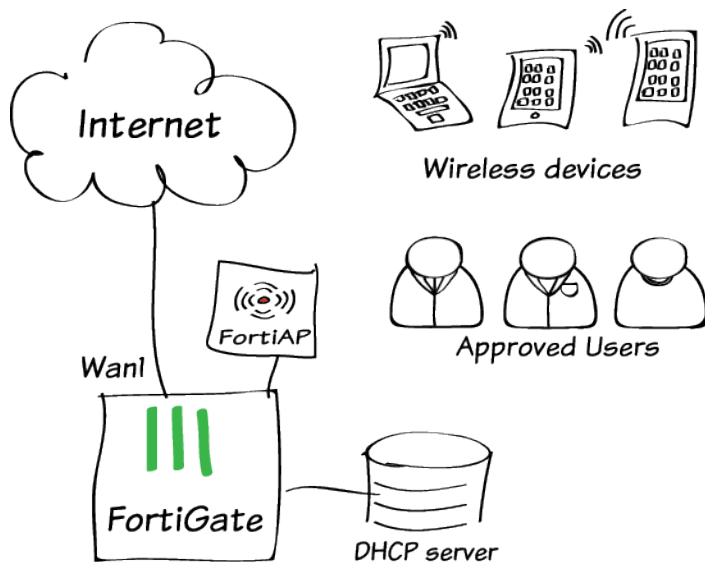
Results

Go to **WiFi Controller > Monitor > Client Monitor** to see connected users.

SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength
example-staff	FP221C3X14019926 (1)	rgreen	192.168.65.2	08:fd:0e:ff:0c:56	1	906 bps	30 dB

For further reading, check out [Software switch](#) in the [FortiOS 5.2 Handbook](#).

WiFi network with external DHCP service



In this example, you use an external DHCP server to assign IP addresses to your WiFi clients.

The DHCP server assigns IP addresses in the range of 10.10.12.100 to 10.10.12.200. The server is attached to Port 13 of the FortiGate and has an IP address of 10.10.13.254.

1. Configure the FortiGate network interface for the DHCP server

Go to **System > Network > Interfaces** and edit Port13.

The external DHCP server is on the 10.10.13.0 network, so put the interface on that network.

Interface Name	port13(08:5B:0E:1A:8A:FF)
Alias	<input type="text"/>
Link Status	Up
Type	Physical Interface
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input type="radio"/> Dedicated to Extension Device
IP/Network Mask	<input type="text" value="10.10.13.1/255.255.255.0"/>

2. Create the SSID

Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network.

The DHCP server assigns IP addresses on the 10.10.12.0 network, so configure the SSID address on this network.

Interface Name	<input type="text" value="example-wifi"/>
Type	WiFi SSID
Traffic Mode	Tunnel to Wireless Controller
IP/Network Mask	<input type="text" value="10.10.12.1/255.255.255.0"/>
IPv6 Address/Prefix	<input type="text" value="::/0"/>

Enable **DHCP Server**, then expand **Advanced** and change the mode to **Relay**. Enter the external **DHCP server IP** address.

DHCP Server	<input checked="" type="checkbox"/> Enable
Advanced...	
Mode	<input type="radio"/> Server <input checked="" type="radio"/> Relay
DHCP Server IP	<input type="text" value="10.10.13.254"/>
Type	<input checked="" type="radio"/> Regular <input type="radio"/> IPsec

Set up security and authentication for your SSID.

In this case, WPA2 Enterprise authentication allows access only to members of the *employees* user group.

WiFi Settings	
SSID	<input type="text" value="example-staff"/>
Security Mode	WPA2 Enterprise
Authentication	<input checked="" type="radio"/> Local <input type="radio"/> RADIUS Server
	<input type="text" value="employees"/>
Broadcast SSID	<input checked="" type="checkbox"/>
Block Intra-SSID Traffic	<input checked="" type="checkbox"/>
Maximum Clients	<input type="checkbox"/>
Optional VLAN ID	<input type="text" value="0"/>

3. Create the security policies

Create a policy to allow the WiFi network to communicate with the DHCP Server on Port 13.

The source and destination networks are directly visible to each other, so NAT is not required.

The screenshot shows a Firewall Policy configuration. The Incoming Interface is 'example-wifi (SSID: example-staff)'. The Source Address is 'all'. The Source User(s) is 'Click to add...'. The Source Device Type is 'Click to add...'. The Outgoing Interface is 'port13'. The Destination Address is 'all'. The Schedule is 'always'. The Service is 'DHCP'. The Action is 'ACCEPT'. Under 'Firewall / Network Options', the NAT toggle is 'OFF'.

Create a policy to allow WiFi clients to connect to the Internet on wan1.

The screenshot shows a Firewall Policy configuration. The Incoming Interface is 'example-wifi (SSID: example-staff)'. The Source Address is 'all'. The Source User(s) is 'Click to add...'. The Source Device Type is 'Click to add...'. The Outgoing Interface is 'wan1'. The Destination Address is 'all'. The Schedule is 'always'. The Service is 'ALL'. The Action is 'ACCEPT'. Under 'Firewall / Network Options', the NAT toggle is 'ON'.

4. Connect and authorize the FortiAP unit

Configure the network interface where the FortiAP will be connected.

The screenshot shows the configuration for a network interface. The Addressing mode is 'Dedicated to Extension Device'. The IP/Network Mask is '10.11.12.1/255.255.255.0'. The Connected Devices are 'None'.

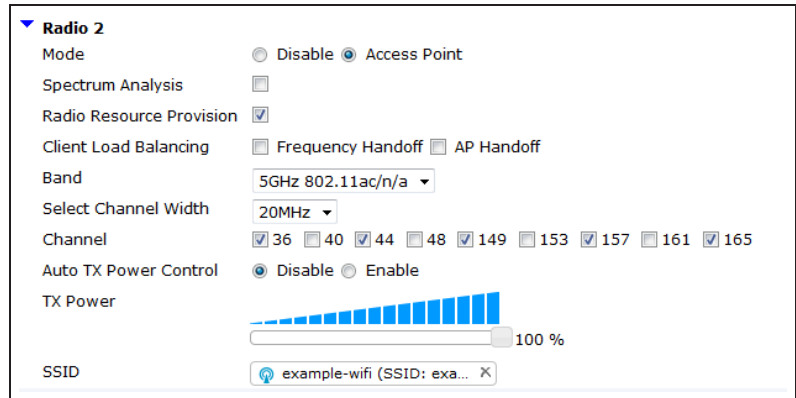
Go to WiFi Controller > Managed Access Points > Managed FortiAPs. The FortiAP is listed, with a yellow question mark beside it because the device is not authorized.

Mesh	Access Point	State	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile
	FP221C3X14019926	?	10.11.12.2	Radio 1: Radio 2:	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0		FAP221C-default

The FortiAP may not appear until a few minutes have passed.

Highlight the FortiAP unit on the list and select **Authorize**. A grey checkmark is now shown beside the FortiAP, showing that it is authorized but not yet online.

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the profile, adding your SSID to each radio.



Radio 2

Mode Disable Access Point

Spectrum Analysis

Radio Resource Provision


Client Load Balancing Frequency Handoff AP Handoff

Band 5GHz 802.11ac/n/a

Select Channel Width 20MHz

Channel 36 40 44 48 149 153 157 161 165

Auto TX Power Control Disable Enable

TX Power 

SSID

Results

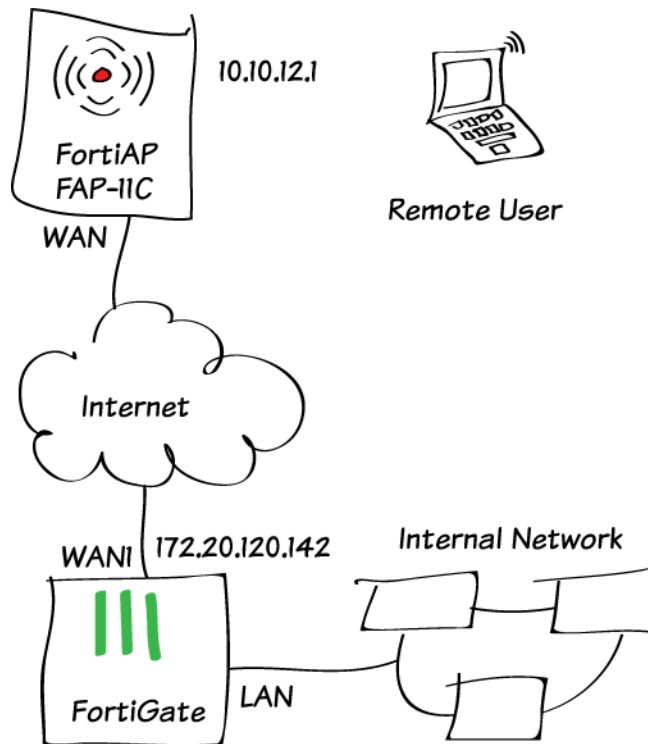
WiFi devices can connect to the Internet. You can see them in the client monitor (**WiFi Controller > Monitor > Client Monitor**). Note the IP addresses assigned by the external DHCP server.



SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx	Signal
example-staff	FP221C3X14019926 (2)	rgreen	10.10.12.100	08:fd:0e:ff:0c:56	165	6.52 Mbps	50

For further reading, check out the [Deploying Wireless Networks](#) in the [FortiOS 5.2 Handbook](#).

Providing remote access to the office and Internet



In this example, you pre-configure a FortiAP to provide access to the office network from any remote location simply by connecting the FortiAP to the Internet. This FortiAP could be given to an employee to use at home or when traveling.

The FortiAP's configuration also supports Internet browsing from behind the corporate firewall. The remote user's local network remains accessible by defining it as a split tunnel destination that is not routed through the FortiGate unit.

1. Enable the split tunneling feature

By default, split tunneling options are not visible in the FortiGate GUI. You can make these options visible using the CLI.

Go to **System > Dashboard > Status** and use the CLI Console.

```
config system global
  set gui-fortiap-split-tunneling enable
end
```

2. Create the WiFi network

Go to **WiFi Controller > WiFi Network > SSID** and create a new SSID. The SSID will accept logons from the *employees* user group.

The screenshot shows the 'WiFi Settings' configuration page. The SSID is 'example-staff', Security Mode is 'WPA2 Enterprise', and Authentication is set to 'Local'. The user group is 'employees'. Other settings include 'Broadcast SSID' (checked), 'Block Intra-SSID Traffic' (checked), 'Maximum Clients' (disabled), 'Split Tunneling' (checked), and 'Optional VLAN ID' (0).

Enable the DHCP Server and make note of the IP range.

The screenshot shows the 'DHCP Server' configuration page. The 'Enable' checkbox is checked. The 'Address Range' table shows a range from 10.10.12.2 to 10.10.12.254. The 'Netmask' is 255.255.255.0. The 'Default Gateway' is set to 'Same as Interface IP'. The 'DNS Server' is set to 'Same as System DNS'. There is an 'Advanced...' link at the bottom.

Starting IP	End IP
10.10.12.2	10.10.12.254

3. Create the security policy

Go to **Policy & Objects > Objects > Addresses** and create an address representing the range of remote user addresses that the DHCP server can assign.

Name	remote_users
Type	IP Range
Subnet / IP Range	10.10.12.2-10.10.12.254
Interface	example-wifi (SSID: example-staff)
Visibility	<input checked="" type="checkbox"/>
Comments	<input type="text"/> 0/255

Go to **Policy & Objects > Policy > IPv4** and create a policy that allows remote wireless users to access the Internet and the corporate network.

Incoming Interface	example-wifi (SSID: example-staff) +
Source Address	remote_users +
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1 X + lan X
Destination Address	all +
Schedule	always
Service	ALL +
Action	ACCEPT
Firewall / Network Options	
<input checked="" type="checkbox"/> NAT	
<input checked="" type="radio"/> Use Outgoing Interface Address <input type="checkbox"/> Fixed Port	

4. Create the FortiAP Profile

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and create a new profile for the FortiAP model you are using.

The **Split Tunneling Subnet(s)** entry exempts a typical home network subnet from being routed through the FortiGate.

Select the **SSID** that the remote FortiAP will broadcast.

Name: FAP11C-remote
Comments: 0/255
Platform: FAP11C
Split Tunneling Subnets(s): 192.168.1.0/24

Radio 1
Mode: Disable Access Point
WIDS Profile: default X
Radio Resource Provision:
Client Load Balancing: Frequency Handoff AP Handoff
Band: 2.4GHz 802.11n/g/b
Channel: 1 2 3 4 5 6 7 8 9 10 11
Auto TX Power Control: Disable Enable
TX Power:
SSID: example-wifi (SSID: exa... X)
LAN Port
Mode: None Bridge to WAN Port

5. Enable CAPWAP on the Internet interface

Go to **System > Network > Interfaces** and edit the Internet-facing interface. In **Administrative Access**, enable CAPWAP.

Administrative Access

<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> PING	<input type="checkbox"/> HTTP	<input checked="" type="checkbox"/> FMG-Access	<input checked="" type="checkbox"/> CAPWAP
<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP	<input type="checkbox"/> FCT-Access		

6. Pre-authorize the FortiAP unit

Go to **WiFi Controller > Managed Devices > Managed FortiAPs** and create a new entry.

Enter your FortiAP's **Serial Number** and a **Name** to identify whose device it is.

Choose the **FortiAP Profile** that you created.

Serial Number	<input type="text" value="FAP11C3X13000412"/>
Name	<input type="text" value="rgreen-ap"/>
Comments	<input type="text" value=""/> 0/35
State	Authorized
Wireless Settings	
FortiAP Profile	<input type="text" value="FAP11C-remote"/> <input type="checkbox"/> Override Settings

7. Configure the FortiAP unit

Use FortiExplorer to access the FortiAP CLI through the USB MGMT port.

Enter these commands to specify the IP address of the FortiGate WiFi controller, which will be the Internet-facing interface IP address. Enter *exit* to end.

```
FAP11C3X13000412 # login: admin
FAP11C3X13000412 # cfg -a AC_IPADDR_1=172.20.120.142
FAP11C3X13000412 # cfg -c
FAP11C3X13000412 # exit
```

The remote user can now take this device to a remote location to connect securely to the corporate FortiGate unit.

Results

At the remote location, connect the FortiAP to the Internet using an Ethernet cable. Next, connect the FortiAP to power. The network must provide DHCP service and allow the FortiAP to access the internet.

Once connected, the FortiAP requests an IP address and locates the FortiGate wireless controller.



The remote WiFi user can now access the corporate network and browse the Internet securely from behind the corporate firewall.

Connections to destinations on the "split tunneling" network are possible, but will not be visible in the FortiGate logs as the traffic remains local to the FortiAP.

Go to **WiFi Controller > Monitor > Client Monitor** to see remote wireless users connected to the FortiAP unit.

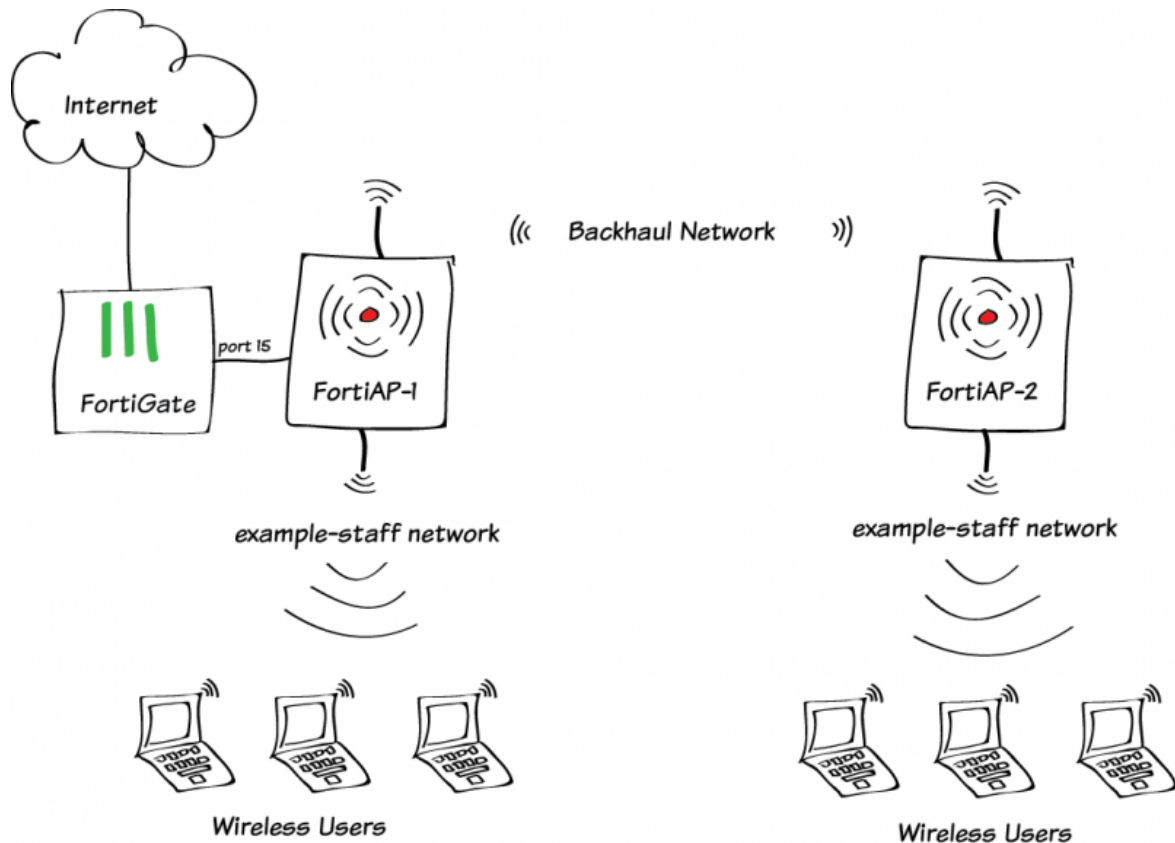
SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal
example-staff	rgreen-ap (1)	rgreen	10.10.12.4	08:fd:De:ff:0c:56	6	328.97 Kbps	44 dB	████████

Go to **Log & Report > Traffic Log > Forward Traffic** to see remote wireless users appear in the logs. Select an entry to view more information about remote traffic to the corporate network and to the Internet.

#	1	Action	ip-conn
Date/Time	11:46:46	Destination	208.91.112.52
Dst Interface	wan1	Dst Port	53
Group	employees	Level	██████
Log ID	11	Policy ID	8
Policy UUID	450ac232-ce5c-51e4-c482-a35b764918e	Sequence Number	4011
Source	 rgreen (10.10.12.4)	Source SSID	example-staff
Src Interface	example-wifi	Src Name	android-1b1c4f3382fb4b0
Src Port	35023	Sub Type	forward
Threat	262144	Threat Level	medium
Threat Score	10	Timestamp	4/30/2015, 11:46:46 AM
User	 rgreen	Virtual Domain	root

For further reading, check out [Deploying Wireless Networks](#) in the [FortiOS 5.2 Handbook](#).

Extending WiFi range with mesh topology



In this example, two FortiAPs are used to extend the range of a single WiFi network. The second FortiAP is connected to the FortiGate WiFi controller through a dedicated WiFi backhaul network.

In this example, both FortiAPs provide the example-staff network to clients that are in range.

More mesh-connected FortiAPs could be added to further expand the coverage range of the network. Each AP must be within range of at least one other FortiAP. Mesh operation requires FortiAP models with two radios, such as the FortiAP-221C units used here.

1. Create the backhaul SSID

Go to **WiFi Controller > WiFi Network > SSID**.

Create a new SSID. Set **Traffic Mode** to **Mesh Downlink**.

You will need the pre-shared key when configuring the mesh-connected FortiAP.

Interface Name	Backhaul_mesh
Type	WiFi SSID
Traffic Mode	Mesh Downlink
WiFi Settings	
SSID	backhaul-ssid
Security Mode	WPA2 Personal
Pre-shared Key (8 - 63 characters)
Comments	<input type="text"/> 0/255
Administrative Status	<input checked="" type="radio"/> Up <input type="radio"/> Down

2. Create the client SSID

Go to **WiFi Controller > WiFi Network > SSID**. Create the WiFi network (SSID) that clients will use.

WiFi Settings	
SSID	example-staff
Security Mode	WPA2 Enterprise
Authentication	<input checked="" type="radio"/> Local <input type="radio"/> RADIUS Server
	employees <input type="button" value="+"/>
Broadcast SSID	<input checked="" type="checkbox"/>
Block Intra-SSID Traffic	<input checked="" type="checkbox"/>
Maximum Clients	<input type="checkbox"/>
Optional VLAN ID	0

Configure DHCP for your clients.

DHCP Server	<input checked="" type="checkbox"/> Enable				
Address Range	<input type="button" value="Create New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				
	<table border="1"><thead><tr><th>Starting IP</th><th>End IP</th></tr></thead><tbody><tr><td>10.10.12.2</td><td>10.10.12.254</td></tr></tbody></table>	Starting IP	End IP	10.10.12.2	10.10.12.254
Starting IP	End IP				
10.10.12.2	10.10.12.254				
Netmask	255.255.255.0				
Default Gateway	<input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify				
DNS Server	<input checked="" type="radio"/> Same as System DNS <input type="radio"/> Same as Interface IP <input type="radio"/> Specify				
	Advanced...				

3. Create the FortiAP Profile

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and create a profile for the Platform (FortiAP model) that you are using.

Configure Radio 1 for the client channel on the 2.4GHz 802.11n/g Band.

Configure Radio 2 for the backhaul channel on the 5GHz 802.11ac/n Band.

The screenshot shows the configuration for two radio profiles. **Radio 1** is configured for the 2.4GHz 802.11n/g band. Its mode is set to 'Access Point', and it has 11 channels selected (1-11). The TX Power is set to 100%. The SSID is 'example-wifi'. **Radio 2** is configured for the 5GHz 802.11ac/n band. Its mode is also 'Access Point', and it has 8 channels selected (36, 40, 44, 48, 149, 153, 157, 161, 165). The TX Power is set to 100%. The SSID is 'Backhaul_mesh'.

4. Configure the security policy

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

The screenshot shows the configuration of a new IPv4 Firewall Policy. The Incoming Interface is 'example-wifi (SSID: example-staff)', Source Address is 'all', Source User(s) is 'Click to add...', Source Device Type is 'Click to add...', Outgoing Interface is 'wan1', Destination Address is 'all', Schedule is 'always', Service is 'ALL', and Action is 'ACCEPT'. The Firewall / Network Options are set to 'ON' and 'NAT'.

5. Configure an interface dedicated to FortiAP

Go to **System > Network > Interfaces** and edit an available interface (in this example, port 15). Set **Addressing mode** to **Dedicate to Extension Device**.

Addressing mode	<input type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input checked="" type="radio"/> Dedicated to Extension Device
IP/Network Mask	<input type="text" value="192.168.1.1/255.255.255.0"/>
Connected Devices	1 FortiAP(s)

6. Preauthorize FortiAP-1

Go to **WiFi Controller > Managed Devices > Managed FortiAPs** and create a new entry.

Enter the serial number of the FortiAP unit and give it a name. Select the FortiAP profile that you created earlier.

Serial Number	<input type="text" value="FP221C3X14019926"/>
Name	<input type="text" value="FortiAP-1"/>
Comments	<input type="text" value=""/> 0/35
State	Authorized
Wireless Settings	
FortiAP Profile	<input type="text" value="FAP221C-mesh"/> <input type="checkbox"/> Override Settings

7. Configure FortiAP-2 for mesh operation

Connect FortiAP-2 to Port 15.

Go to **WiFi Controller > Managed Devices > Managed FortiAPs**. FortiAP-2, identified by serial number, will be listed within two minutes. Note the **Connected Via** IP address.

Mesh	Access Point	State	Connected Via	SSIDs
<input type="checkbox"/>	FP221C3X14023979	?	192.168.1.4	Radio 1: Radio 2:
<input type="checkbox"/>	FortiAP-1	✓	-	Radio 1: example-staff Radio 2: backhaul-ssid

Go to **System > Dashboard > Status**.

In the CLI Console, enter `exec telnet 192.168.1.4` (your address might be different) to log in to the FortiAP as *admin*. Enter the commands to change the AP to mesh uplink on the *backhaul-ssid* network. Enter `exit` to end.

Disconnect FortiAP-2 from the FortiGate. Install it in its planned location and apply power.

```
FP221C3X14019926 login: admin
```

```
FP221C3X14019926 # cfg -a MESH_AP_TYPE=1
FP221C3X14019926 # cfg -a MESH_AP_SSID=backhaul-ssid
FP221C3X14019926 # cfg -a MESH_AP_PASSWD=backhaul-ssid-passwd
FP221C3X14019926 # cfg -c
FP221C3X14019926 # exit
```

Connect FortiAP-1 to Port 15 and apply power.

Go to **WiFi Controller > Managed Devices > Managed FortiAPs**. Select the FortiAP-2 entry (identified by serial number) and edit the new entry. Enter the **Name**, FortiAP-2. Select the **FortiAP Profile** that you created earlier. Click **Authorize**. Click **OK**.

Radio	Settings	Channels	SSIDs
Radio 1	AP (2.4 GHz Band)	11	example-wifi (SSID: example-staff)
Radio 2	AP (5 GHz Band)	153	Backhaul_mesh (SSID: backhaul-ssid)

8. Connect and authorize the FortiAPs

Go to **WiFi Controller > Managed Devices > Managed FortiAPs**. The FortiAPs will be listed as online within about two minutes. (Click **Refresh** to update the display.)

Mesh	Access Point	State	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile
	FortiAP-1	✓	192.168.1.3	Radio 1: example-staff Radio 2: backhaul-ssid	Radio1: 11 Radio2: 153	Radio 1: 0 Radio 2: 1	v5.2-build0237	FAP221C-mesh
	FortiAP-2	✓	192.168.1.2	Radio 1: example-staff Radio 2: backhaul-ssid	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0	v5.2-build0237	FAP221C-mesh

9. Results

Go to **WiFi Controller > Monitor > Client Monitor**. Click **Refresh** to see updated information.

SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal
example-staff	FortiAP-2 (1)	rgreen	10.10.12.2	08:fd:0e:ff:0e:56	11	3.14 Mbps	44 dB	Strong
backhaul-ssid	FortiAP-1 (2)		192.168.1.4	7a:5b:0e:89:1b:75	153	0 bps	44 dB	Strong

Use a mobile device near FortiAP-2 to connect to the *example-staff* network. The monitor shows the mobile user *rgreen* as a client of FortiAP-2.

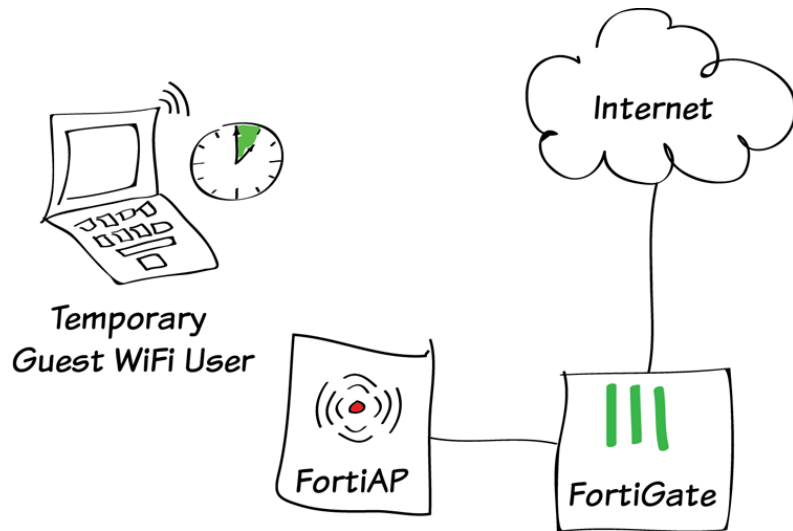
Disconnect from the *example-staff* network and then reconnect near FortiAP-1. The monitor shows the mobile user *rgreen* as a client of FortiAP-1.

SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength/Noise	Signal
example-staff	FortiAP-1 (1)	rgreen	10.10.12.2	08:fd:0e:ff:0e:56	11	3.14 Mbps	0 dB	Strong
backhaul-ssid	FortiAP-1 (2)		192.168.1.4	7a:5b:0e:89:1b:75	153	0 bps	44 dB	Strong

Notice that in both cases FortiAP-2 is listed on *backhaul-ssid* as a client of FortiAP-1.

For further reading, check out [Wireless Mesh](#) in the [FortiOS 5.2 Handbook](#).

Guest WiFi accounts



In this example, a guest user account will be created to allow temporary wireless access to the Internet. Access will only be allowed using HTTP, HTTPS, and DNS protocols.

In this example, a FortiAP in Tunnel mode is used to provide wireless access to guests.

If you have not already set up a wireless network, see [Setting up WiFi with FortiAP](#).

A video of this recipe is available [here](#).

1. Creating a WiFi guest user group

Go to **User & Device > User > User Groups** and create a new group.

Set **Type** to **Guest**. Set **User ID** to **Email**, ensure that **Password** is set to **Auto-Generate**, and set **Expire Type** to **After first login**. Leave **Default Expiry Time** set to **4 Hours**.

The screenshot shows the configuration for a new user group named 'WiFi_guests'. The 'Type' is set to 'Guest'. The 'User ID' is 'Email', 'Password' is 'Auto-Generate', and 'Expire Type' is 'After first login'. The 'Default Expiry Time' is '4 Hours'. There are several checkboxes for enabling features like 'Enable Batch Guest Account Creation', 'Enable Name', 'Enable Sponsor', 'Enable Company', 'Enable Email', and 'Enable SMS'. The 'Required' checkboxes for 'Sponsor' and 'Company' are also visible.

2. Creating a guest SSID that uses Captive Portal

Go to **Wireless Controller > WiFi Network > SSID** and create a new SSID.

Set **Traffic Mode** to **Tunnel to Wireless Controller**. Assign an **IP/Network Mask** to the interface and enable **DHCP server**. Under **WiFi Settings**, set **Security Mode** to **Captive Portal** and **User Group(s)** to the WiFi guest user group.

The screenshot shows the configuration for a new WiFi SSID named 'WiFi_guests'. The 'Type' is 'WiFi SSID' and the 'Traffic Mode' is 'Tunnel to Wireless Controller'. The 'IP/Network Mask' is '10.10.80.1/255.255.255.0'. Under 'Administrative Access', 'HTTPS', 'PING', 'HTTP', and 'FMG-Access' are checked. The 'DHCP Server' is enabled, and the 'Address Range' is '10.10.80.2' to '10.10.80.254' with a 'Netmask' of '255.255.255.0'. Under 'WiFi Settings', the 'SSID' is 'guest', 'Security Mode' is 'Captive Portal', 'Portal Type' is 'Authentication', and 'User Groups' is 'WiFi_guests'.

Go to **Wireless Controller > WiFi Network > FortiAP Profiles** and edit the profile for your FortiAP model (in the example, FortiAP-11C).

Set the FortiAP to broadcast the new SSID.

The screenshot shows the configuration for a FortiAP profile. The 'SSID' is 'WiFi_guests (SSID: guest)'. There are icons for 'Create New', 'Edit', and 'Delete'.

3. Creating a security policy for WiFi guests

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the guest SSID, **Source User(s)** to the WiFi guest user group, the **Outgoing Interface** to your Internet-facing interface, and **Service** to HTTP, HTTPS, and DNS.

Incoming Interface	WiFi_guests (SSID: guest)
Source Address	all
Source User(s)	WiFi_guests
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	HTTP HTTPS DNS
Action	ACCEPT
Firewall / Network Options	
<input checked="" type="checkbox"/> NAT	
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...

4. Creating a guest user account

Go to **User & Device > User > Guest Management** and create a new account.

Set **Email** to the user's email address (in the example, *ballen@example.com*). To test the account, set **Expiration** to **5 Minutes**.

User ID	Use Email Address
Password	Auto Generated
Sponsor	<input type="text"/> Optional
Company	<input type="text"/> Optional
Email	ballen@example.com
Expiration	5 <input type="text"/> Minutes

After you select **OK**, a **User Created Successfully** notice will appear, listing the generated Password. This password can then be printed or emailed to the guest user.

User Created Successfully	
User ID	ballen@example.com
Password	qa3q3z
Email	ballen@example.com
Expiration	0:05:00
Send	

(Optional) 5. Creating a restricted admin account for guest user management

To make it easier for guest accounts to be created, an admin account can be made that is only used for guest user management. In this example, the account is made for use by the receptionist.

Go to **System > Admin > Administrators** and create a new account.

Set **Type** to **Regular** and set a **Password**. Select **Restrict to Provision Guest Accounts** and set **Guest Groups** to the WiFi guest user group.

The screenshot shows the configuration page for a new administrator account. The fields are as follows:

- Administrator:** Reception
- Type:** Regular (selected), Remote, PKI
- Password:** [Redacted]
- Confirm Password:** [Redacted]
- Comments:** Write a comment... (0/255)
- Contact Info:**
 - Email Address
 - SMS
 - FortiGuard Messaging Service
 - Custom
 - Country/Region: Click to add...
 - Phone Number: [Redacted]
- Enable Two-factor Authentication
- Restrict this Administrator Login from Trusted Hosts Only
- Restrict to Provision Guest Accounts
 - Guest Groups: WiFi_guests

Sign in to the FortiGate using this account. You will only be able to see the menu for **Guest User Management**.

The screenshot shows the FortiGate Guest User Management interface. The top bar displays "Guest Groups: WiFi_guests" and "Guest User Management" with a "Logout" link. Below the top bar is a navigation menu with "Create New", "Edit", "Delete", "Purge", "Print", "Send", and "Refresh". The main content area shows a table with two columns: "User ID" and "expires". The first row contains "ballen@example.com" and "5 Minutes after first login".

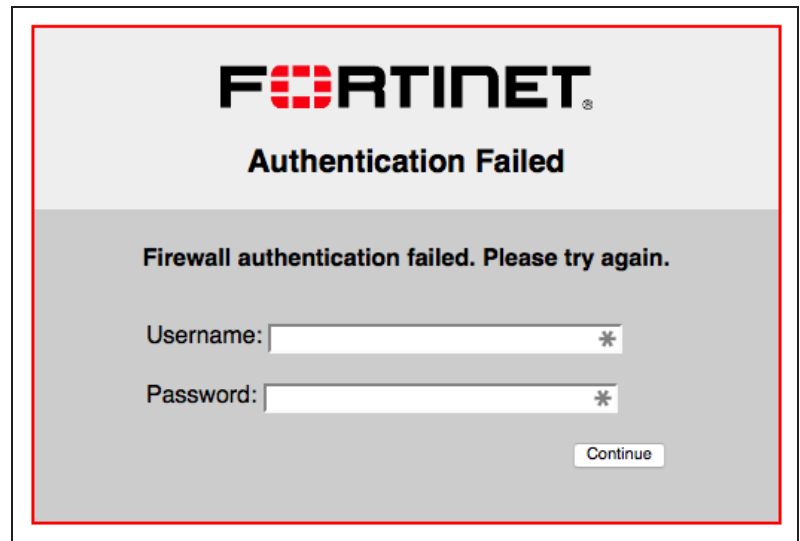
6. Results

On a PC, connect to the guest SSID. When the authentication screen appears, log in using the guest user's credentials. You will be able to connect to the Internet.



The screenshot shows the Fortinet Authentication Required screen. At the top, the Fortinet logo is displayed in black with a red grid pattern in the 'O'. Below the logo, the text "Authentication Required" is centered. Underneath, a message reads "Please enter your username and password to continue." There are two input fields: "Username:" with the value "ballen@example.com" and "Password:" with masked characters ".....". A "Continue" button is located at the bottom right of the form area.

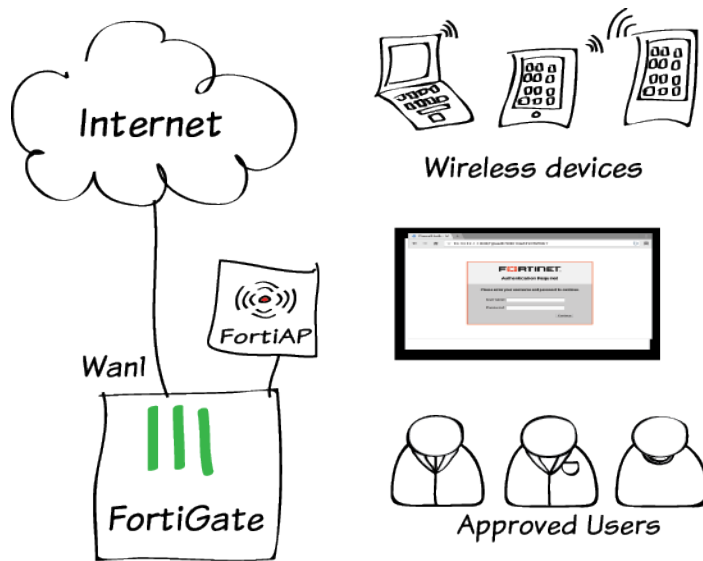
Five minutes after the initial login, the user account will expire and you will no longer be able to log in using those credentials.



The screenshot shows the Fortinet Authentication Failed screen. At the top, the Fortinet logo is displayed in black with a red grid pattern in the 'O'. Below the logo, the text "Authentication Failed" is centered. Underneath, a message reads "Firewall authentication failed. Please try again." There are two input fields: "Username:" and "Password:", both with asterisks at the end of the input boxes. A "Continue" button is located at the bottom right of the form area.

For further reading, check out [Managing Guest Access](#) in the [FortiOS 5.2 Handbook](#).

Captive portal WiFi access control



In this example, your employees can log on to your Wi-Fi network through a captive portal.

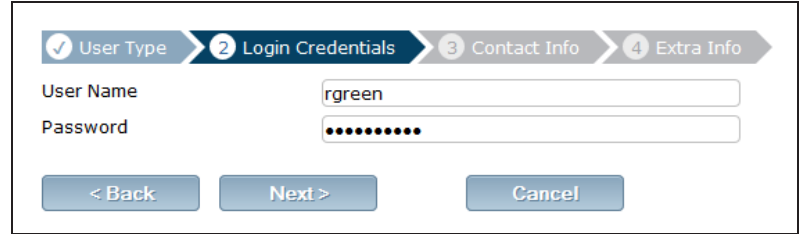
Captive portals are often used for public Wi-Fi networks where you want Wi-Fi users to respond to a disclaimer. Captive portals can also be used to provide unlimited access to open Wi-Fi networks.

As shown in this example, captive portals can also be used as the authentication method for restricting access to a wireless network. Some users may find it more intuitive to add their account information to a captive portal web page instead of entering their user name and password into a wireless network configuration.

1. Create user accounts

Go to **User & Device > User > User Definition** and create a Local user.

Create additional users as needed. You can use any authentication method.




The screenshot shows the 'Login Credentials' step of the user creation process. At the top, there are four steps: 1. User Type (checked), 2. Login Credentials (active), 3. Contact Info, and 4. Extra Info. Below the steps, there are two input fields: 'User Name' with the value 'rgreen' and 'Password' with a masked password of ten dots. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

2. Create a user group

Go to **User & Device > User > User Groups**.

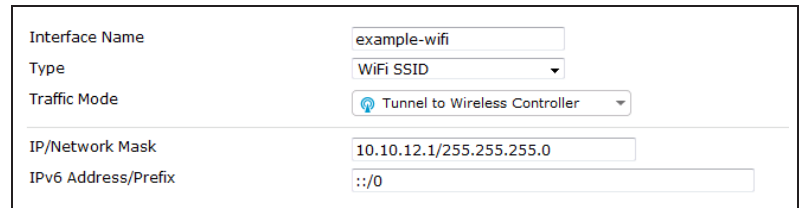
Create a user group for employees and add the new user(s) to the group.



The screenshot shows the 'User Group' configuration form. The 'Name' field is 'employees'. The 'Type' field has three radio buttons: 'Firewall' (selected), 'Fortinet Single Sign-On (FSSO)', and 'Guest'. The 'Members' field contains a list of users: 'gbrown' and 'rgreen', each with a delete icon (X) and a plus icon (+) to the right.

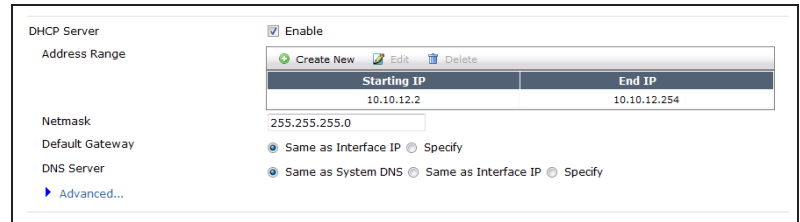
3. Create the SSID

Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network.



The screenshot shows the 'WiFi SSID' configuration form. The 'Interface Name' is 'example-wifi'. The 'Type' is 'WiFi SSID'. The 'Traffic Mode' is 'Tunnel to Wireless Controller'. The 'IP/Network Mask' is '10.10.12.1/255.255.255.0'. The 'IPv6 Address/Prefix' is ':::0'.

Configure DHCP addressing for clients.



The screenshot shows the 'DHCP Server' configuration form. The 'Enable' checkbox is checked. The 'Address Range' section has a table with columns 'Starting IP' and 'End IP'. The 'Netmask' is '255.255.255.0'. The 'Default Gateway' has radio buttons for 'Same as Interface IP' (selected) and 'Specify'. The 'DNS Server' has radio buttons for 'Same as System DNS' (selected), 'Same as Interface IP', and 'Specify'. There is an 'Advanced...' link at the bottom.

Starting IP	End IP
10.10.12.2	10.10.12.254

Configure Captive Portal authentication using the *employees* user group.

The screenshot shows the 'WiFi Settings' configuration page. The SSID is 'example-staff'. Security Mode is 'Captive Portal'. Portal Type is 'Authentication'. Authentication Portal is 'Local'. User Groups is 'employees'. Exempt List is 'Click to add...'. Customize Portal Messages is 'Login Page'. Redirect after Captive Portal is 'Original Request'. Broadcast SSID, Block Intra-SSID Traffic, and Maximum Clients are all checked. Optional VLAN ID is '0'.

4. Create the security policy

Create an address for your SSID, using the same IP range that was set on the DHCP server.

The screenshot shows the 'New Address' dialog box. Category is 'Address'. Name is 'example-wifi-net'. Type is 'Subnet'. Subnet / IP Range is '10.10.12.0/24'. Interface is 'example-wifi (SSID: example-staff)'. Visibility is checked. Comments is empty. OK and Cancel buttons are at the bottom right.

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing WiFi users to connect to the Internet. Select the *employees* user group as permitted **Source Users**.

The screenshot shows the Policy configuration page. Incoming Interface is 'example-wifi (SSID: example-staff)'. Source Address is 'example-wifi-net'. Source User(s) is 'employees'. Source Device Type is 'Click to add...'. Outgoing Interface is 'wan1'. Destination Address is 'all'. Schedule is 'always'. Service is 'ALL'. Action is 'ACCEPT'.

5. Connect and authorize the FortiAP unit

Go to **System > Network > Interface**. Configure an interface dedicated to extension devices and assign it an IP address.

Addressing mode Manual DHCP PPPoE Dedicated to Extension Device

IP/Network Mask

Connected Devices

Connect the FortiAP unit to the interface and go to **WiFi Controller > Managed Access Points > Managed FortiAPs**.

Mesh	Access Point	State	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile
	FP221C3X14019926	?	10.11.12.2	Radio 1: Radio 2:	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0		FAP221C-default

The FortiAP is listed, with a yellow question mark beside it because the device is not authorized.

The FortiAP may not appear for a minute or two.

Highlight the FortiAP unit on the list and select **Authorize**.

Mesh	Access Point	State	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile
	FP221C3X14019926	✓	10.11.12.2	Radio 1: Radio 2:	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0		FAP221C-default

A grey check mark is now shown beside the FortiAP, showing that it is authorized but not yet online.

Mesh	Access Point	State	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile
	FP221C3X14019926	✓	10.11.12.2	Radio 1: Radio 2:	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0		FAP221C-default

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the profile. For each radio:

Enable **Radio Resource Provision**.

Select your SSID.

Radio 2

Mode Disable Access Point

Spectrum Analysis

Radio Resource Provision

Client Load Balancing Frequency Handoff AP Handoff

Band

Select Channel Width

Channel 36 40 44 48 149 153 157 161 165

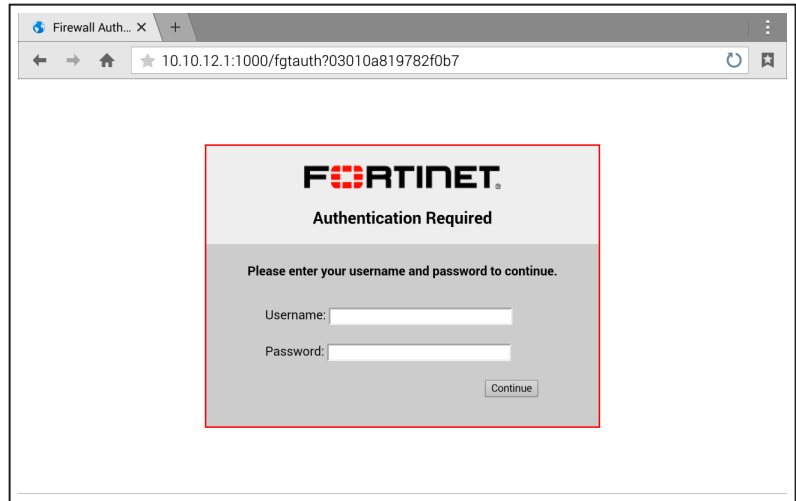
Auto TX Power Control Disable Enable

TX Power

SSID

6. Results

The user's device shows the WiFi network as "open" and associates with it without requesting credentials. The first time that a wireless user attempts to use a web browser, the captive portal login screen is displayed. Users who are members of the *employees* group can log on using their username and password and proceed to access the wireless network.

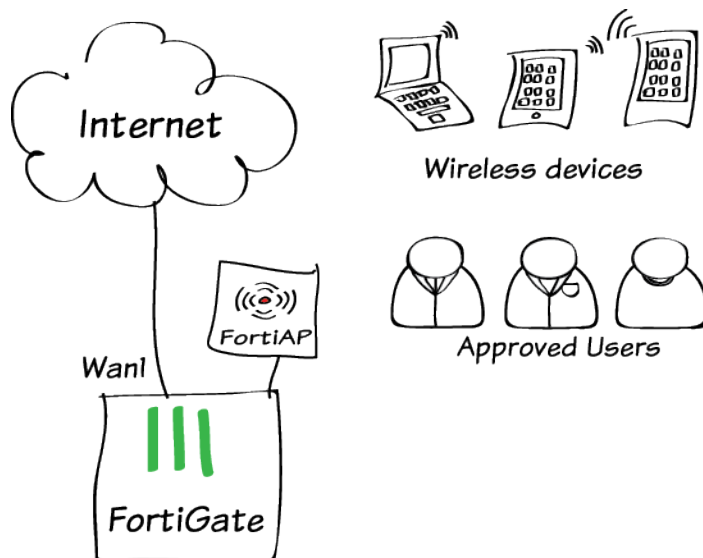


Go to **WiFi Controller > Monitor > Client Monitor** to see connected users.

SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength
example-staff	FP221C3X14019926 (2)	rgreen	10.10.12.2	08:fd:0e:ff:0c:56	165	76.02 Kbps	50 dB

For further reading, check out [Captive portals](#) in the [FortiOS 5.2 Handbook](#).

WPA2 WiFi access control



In this example, you will improve your WiFi security with WPA2 enterprise authentication.

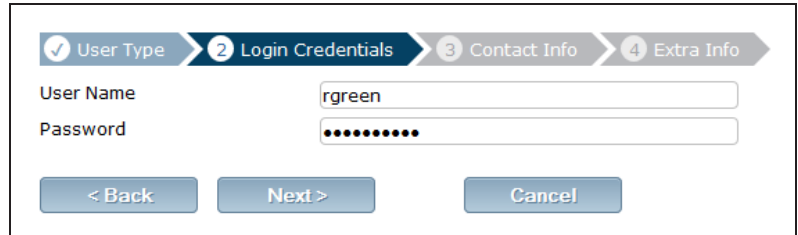
In the [Setting up WiFi with FortiAP](#) recipe, you set up a WiFi network with a single pre-shared key. In this example, there is no longer a pre-shared key that could fall into the wrong hands, or that needs to be changed if someone leaves the company. Each user has an individual user account and password, and accounts can be added or removed later as needed.

This example shows how to authenticate local FortiGate users. You can also integrate WPA2 security with most 3rd party authentication solutions including RADIUS.

1. Create user accounts

Go to **User & Device > User > User Definition** and create a Local user.

Create additional users as needed. You can use any authentication method.

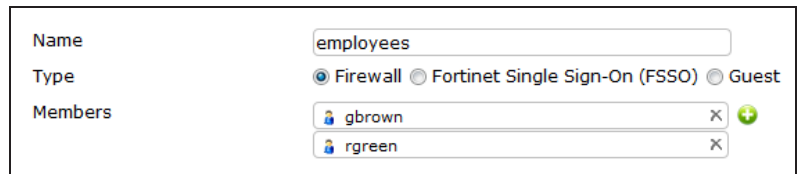


The screenshot shows the 'Login Credentials' step of the user creation process. At the top, there are four steps: 1. User Type (checked), 2. Login Credentials (active), 3. Contact Info, and 4. Extra Info. Below the steps, there are two input fields: 'User Name' with the value 'rgreen' and 'Password' with a masked password of ten dots. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

2. Create a user group

Go to **User & Device > User > User Groups**.

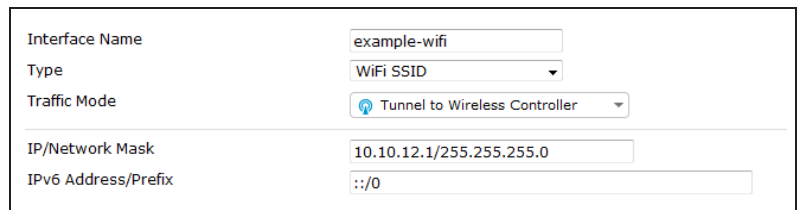
Create a user group for employees and add the new user(s) to the group.



The screenshot shows the 'User Group' configuration form. The 'Name' field is 'employees'. The 'Type' field has three radio buttons: 'Firewall' (selected), 'Fortinet Single Sign-On (FSSO)', and 'Guest'. The 'Members' field contains a list of users: 'gbrown' and 'rgreen', each with a delete icon (X) and a plus icon (+) to the right.

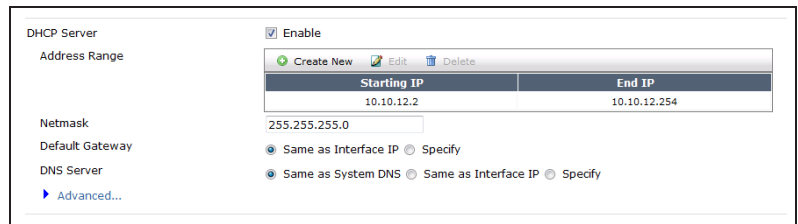
3. Create the SSID and enable the WiFi radio

Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network.



The screenshot shows the 'WiFi SSID' configuration form. The 'Interface Name' is 'example-wifi'. The 'Type' is 'WiFi SSID'. The 'Traffic Mode' is 'Tunnel to Wireless Controller'. The 'IP/Network Mask' is '10.10.12.1/255.255.255.0'. The 'IPv6 Address/Prefix' is ':::0'.

Configure DHCP addressing for clients.



The screenshot shows the 'DHCP Server' configuration form. The 'Enable' checkbox is checked. The 'Address Range' table has one entry with 'Starting IP' 10.10.12.2 and 'End IP' 10.10.12.254. The 'Netmask' is 255.255.255.0. The 'Default Gateway' is 'Same as Interface IP'. The 'DNS Server' is 'Same as System DNS'. There is an 'Advanced...' link at the bottom.

Starting IP	End IP
10.10.12.2	10.10.12.254

Configure WPA2-Enterprise authentication using the *employees* user group.

The screenshot shows the 'WiFi Settings' configuration page. The SSID is set to 'example-staff'. The Security Mode is 'WPA2 Enterprise'. The Authentication method is 'Local', and the user group is 'employees'. The 'Broadcast SSID' and 'Block Intra-SSID Traffic' checkboxes are checked. 'Maximum Clients' is disabled. 'Optional VLAN ID' is set to 0.

WiFi Settings	
SSID	example-staff
Security Mode	WPA2 Enterprise
Authentication	Local (selected) RADIUS Server
	employees
Broadcast SSID	<input checked="" type="checkbox"/>
Block Intra-SSID Traffic	<input checked="" type="checkbox"/>
Maximum Clients	<input type="checkbox"/>
Optional VLAN ID	0

4. Create the security policy

Create an address for your SSID, using the same IP range that was set on the DHCP server.

The screenshot shows the 'New Address' dialog box. The Category is 'Address'. The Name is 'example-wifi-net'. The Type is 'Subnet'. The Subnet / IP Range is '10.10.12.0/24'. The Interface is 'example-wifi (SSID: example-staff)'. The Visibility checkbox is checked. The Comments field is empty. The dialog has 'OK' and 'Cancel' buttons.

Category	Address (selected) IPv6 Address Multicast Address
Name	example-wifi-net
Type	Subnet
Subnet / IP Range	10.10.12.0/24
Interface	example-wifi (SSID: example-staff)
Visibility	<input checked="" type="checkbox"/>
Comments	

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing WiFi users to connect to the Internet.

The screenshot shows the 'Policy' configuration page. The Incoming Interface is 'example-wifi (SSID: example-staff)'. The Source Address is 'example-wifi-net'. The Source User(s) is 'employees'. The Source Device Type is 'Click to add...'. The Outgoing Interface is 'wan1'. The Destination Address is 'all'. The Schedule is 'always'. The Service is 'ALL'. The Action is 'ACCEPT'.

Incoming Interface	example-wifi (SSID: example-staff)
Source Address	example-wifi-net
Source User(s)	employees
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

Results

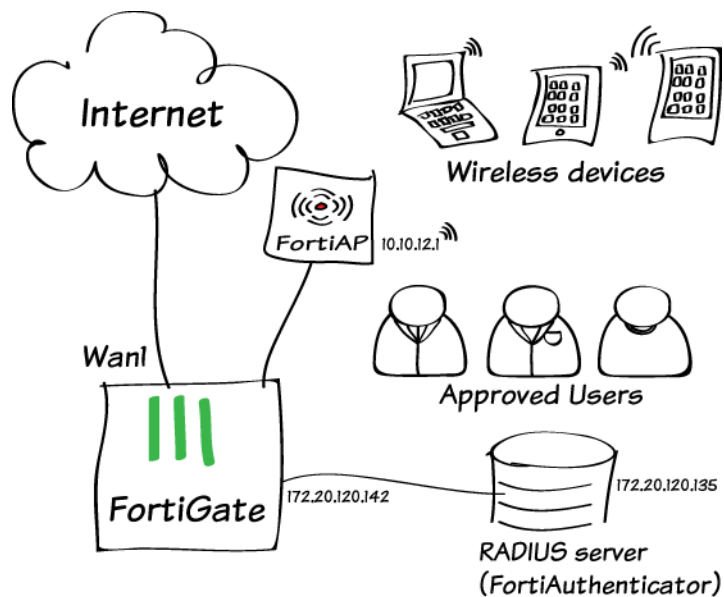
Users who are members of the *employees* group can log on to the WiFi network using their username and password.

Go to **WiFi Controller > Monitor > Client Monitor** to see connected users.

SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx	Signal Strength
example-staff	FP221C3X14019926 (2)	rgreen	10.10.12.2	08:fd:0e:ff:0c:56	165	76.02 Kbps	50 dB

For further reading, check out [Deploying Wireless Networks](#) in the [FortiOS 5.2 Handbook](#).

WiFi with external RADIUS authentication



In this example, you use an external RADIUS server to authenticate your WiFi clients.

In the example, a FortiAuthenticator (v3.00-build0176) is used as a RADIUS server to authenticate users who belong to the employees user group.

1. Create the user accounts and user group on the FortiAuthenticator

Go to **Authentication > User Management > Local Users** and create a user account.

User Role settings are available after you click **OK**.

Create additional user accounts as needed, one for each employee.

Go to **Authentication > User Management > User Groups** and create the local user group "employees" on the FortiAuthenticator.

Add users who are allowed to use the WiFi network.

The screenshot shows the configuration page for a user named 'rgreen'. The 'Username' field is filled with 'rgreen'. There are several checkboxes: 'Disabled' (unchecked), 'Password-based authentication' (checked), 'Token-based authentication' (unchecked), and 'Enable account expiration' (unchecked). A 'Change Password' link is next to the password-based authentication checkbox. Below this is the 'User Role' section, where 'User' is selected with a radio button, and 'Administrator' is unselected. At the bottom, there are two more checkboxes: 'Allow RADIUS authentication' (checked) and 'Allow LDAP browsing' (unchecked).

The screenshot shows the configuration page for a user group named 'employees'. The 'Name' field is filled with 'employees'. The 'Type' is set to 'Local'. The 'Users' section contains two lists: 'Available users' and 'Selected users'. The 'Available users' list includes: admin, gbrown, hsimpson, jsmith, miburns, twittle, and wfoman. The 'Selected users' list contains 'rgreen'. There are 'Choose all visible' and 'Remove all' buttons at the bottom.

2. Register the FortiGate as a RADIUS client on the FortiAuthenticator

Go to **Authentication > RADIUS Service > Clients** and create a user account.

Enable all of the EAP types.

The screenshot shows the configuration page for a RADIUS client named 'FortiGate-1'. The 'Name' field is filled with 'FortiGate-1'. The 'Client name/IP' field is filled with '172.20.120.142'. The 'Secret' field is filled with a masked password. The 'Description' field is filled with '200D'. The 'Authentication method' section has four radio buttons: 'Enforce two-factor authentication' (unselected), 'Apply two-factor authentication if available (authenticate any user)' (unselected), 'Password-only authentication (exclude users without a password)' (selected), and 'FortiToken-only authentication (exclude users without a FortiToken)' (unselected). The 'Username input format' section has three radio buttons: 'username@realm' (selected), 'realmusername' (unselected), and 'realmusername' (unselected). The 'Realms' section is a table with columns: Default, Realm, Allow local users to override remote users, Use Windows AD domain authentication, Groups, and Delete. The table has one row with 'local | Local users' in the Realm column, 'Filter: employees [edit]' in the Groups column, and 'Filter local users: [edit]' in the Delete column. There is an 'Add a realm' button below the table. At the bottom, there are two checkboxes: 'Allow MAC-based authentication' (unchecked) and 'Check machine authentication' (unchecked). The 'EAP types' section has five checkboxes: 'EAP-GTC' (checked), 'EAP-TLS' (checked), 'PEAP' (checked), and 'EAP-TTLS' (checked).

3. Configure FortiGate to use the RADIUS server

Go to **User & Device > Authentication > RADIUS Servers** and add the FortiAuthenticator unit as a RADIUS server.

Name	<input type="text" value="facRADIUS"/>	
Primary Server IP/Name	<input type="text" value="172.20.120.135"/>	
Primary Server Secret	<input type="password" value="....."/>	<input type="button" value="Test"/>
Secondary Server IP/Name	<input type="text"/>	
Secondary Server Secret	<input type="password"/>	<input type="button" value="Test"/>
Authentication Method	<input checked="" type="radio"/> Default <input type="radio"/> Specify	
NAS IP / Called Station ID	<input type="text"/>	
Include in every User Group	<input type="checkbox"/>	

4. Create the SSID and set up authentication

Go to **WiFi Controller > WiFi Network > SSID** and define your wireless network.

Interface Name	example-wifi
Type	WiFi SSID
Traffic Mode	Tunnel to Wireless Controller
IP/Network Mask	<input type="text" value="10.10.12.1/255.255.255.0"/>

Set up DHCP for your clients.

DHCP Server	<input checked="" type="checkbox"/> Enable				
Address Range	<input type="button" value="Create New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				
	<table><thead><tr><th>Starting IP</th><th>End IP</th></tr></thead><tbody><tr><td>10.10.12.2</td><td>10.10.12.100</td></tr></tbody></table>	Starting IP	End IP	10.10.12.2	10.10.12.100
Starting IP	End IP				
10.10.12.2	10.10.12.100				
Netmask	<input type="text" value="255.255.255.0"/>				
Default Gateway	<input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify				
DNS Server	<input checked="" type="radio"/> Same as System DNS <input type="radio"/> Same as Interface IP <input type="radio"/> Specify				

Configure WPA2 Enterprise security that uses the external RADIUS server.

WiFi Settings	
SSID	<input type="text" value="example-staff"/>
Security Mode	<input type="text" value="WPA2 Enterprise"/>
Authentication	<input type="radio"/> Local <input checked="" type="radio"/> RADIUS Server
	<input type="text" value="facRADIUS"/>
Broadcast SSID	<input checked="" type="checkbox"/>
Block Intra-SSID Traffic	<input checked="" type="checkbox"/>
Maximum Clients	<input type="checkbox"/>

5. Connect and authorize the FortiAP

Go to **System > Network > Interfaces** and configure a dedicated interface for the FortiAP.

Addressing mode	<input type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input checked="" type="radio"/> Dedicated to Extension Device
IP/Network Mask	10.11.12.1/255.255.255.0
Connected Devices	None

Connect the FortiAP unit. Go to **WiFi Controller > Managed Access Points > Managed FortiAPs**.

Mesh	Access Point	State	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile
	FP221C3X14019926		10.11.12.2	Radio 1: Radio 2:	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0		FAP221C-default

When the FortiAP is listed, select and authorize it.

Mesh	Access Point	State	Connected Via	SSIDs	Channel	Clients	OS Version	FortiAP Profile
	FP221C3X14019926		10.11.12.2	Radio 1: Radio 2:	Radio1: 0 Radio2: 0	Radio 1: 0 Radio 2: 0		FAP221C-default

Go to **WiFi Controller > WiFi Network > FortiAP Profiles** and edit the profile. For each radio:

- Enable **Radio Resource Provision**.
- Select your SSID.

Radio 2

Mode: Disable Access Point

Spectrum Analysis:

Radio Resource Provision:

Client Load Balancing: Frequency Handoff AP Handoff

Band: 5GHz 802.11ac/n/a

Select Channel Width: 20MHz

Channel: 36 40 44 48 149 153 157 161 165

Auto TX Power Control: Disable Enable

TX Power:

SSID: example-wifi (SSID: exa... X)

5. Create the security policy

Go to **Policy & Objects > Policy > IPv4** and add a policy that allows WiFi users to access the Internet.

Incoming Interface	example-wifi (SSID: example-staff)
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

Firewall / Network Options

NAT

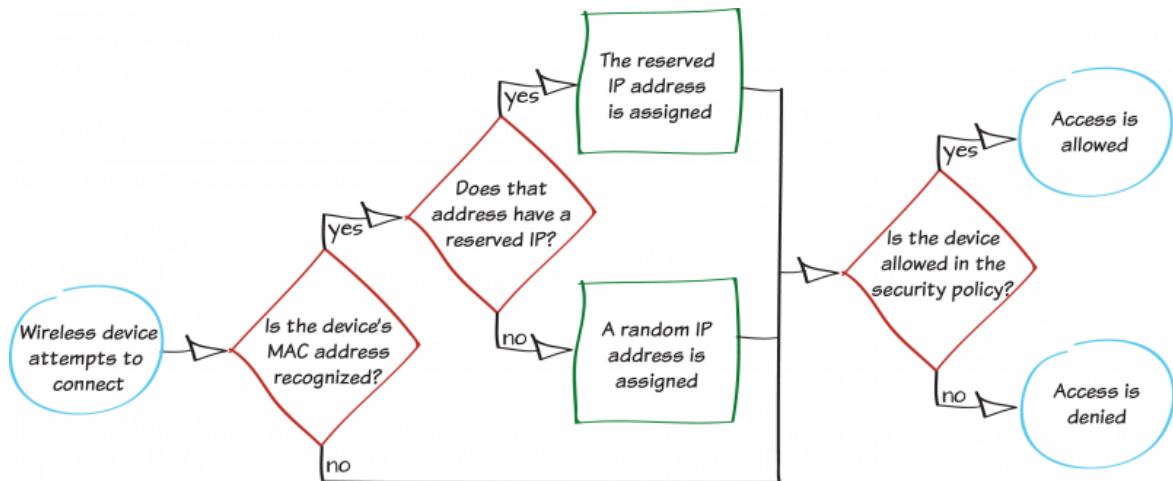
Results

Go to **WiFi Controller > Monitor > Client Monitor** to see that clients connect and authenticate.

SSID	FortiAP	User	IP	Device	Channel	Bandwidth Tx/Rx
example-staff	FP221C3X14019926 (2)	rgreen	10.10.12.2	08:fd:0e:ff:0c:56	165	10.18 Kbps

For further reading, check out the [Deploying Wireless Networks in the FortiOS 5.2 Handbook](#).

MAC access control



In this example, you will add device definitions to your FortiGate using Media Access Control (MAC) addresses. These definitions are then used to determine which devices can access the wireless network.

By using a MAC address for identification, you will also be able to assign a reserved IP for exclusive use by the device when it connects to the wireless network.

Warning: Since MAC addresses can be easily spoofed, using MAC access control should not be considered a security measure.

1. Finding the MAC address of a device

The instructions below were written for the most recent OS versions. Older versions may use different methods.

For Windows devices:

Open the command prompt and type
`ipconfig /all`

This output displays configuration information for all of your network connections. Look for the information about the wireless adapter and take note of the **Physical Address**.

```
Wireless LAN adapter Wireless Network Connection 3:  
Connection-specific DNS Suffix . :  
Description . . . . . : 802.11n USB Wireless LAN Card  
Physical Address. . . . . : C8-3A-35-C4-2F-B7  
DHCP Enabled. . . . . : Yes
```

For Mac OS X devices:

Open **Terminal** and type `ifconfig en1 | grep ether`

Take note of the displayed MAC address.

```
drs:~ % ifconfig en1 | grep ether  
ether c8:bc:c8:de:26:3c
```

For iOS devices:

Open **Settings > General** and take note of the **Wi-Fi Address**.

Version	
Model	
Serial Number	
Wi-Fi Address	B0:34:95:C2:EF:D8

For Android devices:

Open **Settings > More > About Device > Status** and take note of the **Wi-Fi MAC** address.



2. Defining a device using its MAC address

Go to **User & Device > Device > Device Definitions** and create a new device definition.

Set MAC Address to the address of the device and set the other fields as required. In the example, a device definition is created for an iPhone with the MAC Address B0:34:95:C2:EF:D8.

Alias	<input type="text" value="iPhone"/>
MAC Address	<input type="text" value="B0:34:95:C2:EF:D8"/>
Additional MACs	<input type="text" value="Click to add..."/>
Device Type	<input type="text" value="iPhone"/>
Custom Groups	<input type="text" value="None"/>
Comments	<input type="text" value="Write a comment..."/> 0/255

The new definition will now appear in your device list.

If you have enabled device identification on the wireless interface, device definitions will be created automatically. You can then use MAC addresses to identify which device a definition refers to.

Status	Device	OS	IP Address
Online	My-Desktop	Windows	10.10.80.3
Offline	My-Android	Android / 2.2.2	10.10.80.4
Offline	My-iPhone	iPod / iOS	10.10.80.7
Offline	My-Netbook	Windows	10.10.80.5
Offline	My-Printer	Linux	10.10.80.6

3. Creating a device group

Go to **User & Device > Device > Device Groups** and create a new group.

Add the new device to the **Members** list.

Name	<input type="text" value="wifi-access"/>
Members	<input type="text" value="My-iPhone"/> X +
Comments	<input type="text" value="Write a comment..."/> 0/255

4. Reserving an IP address for the device

Go to **System > Network > Interfaces** and edit the wireless interface.

If the FortiAP is in bridge mode, you will need to edit the internal interface.

Under **DHCP Server**, expand **Advanced**. Create a new entry in the **MAC Reservation + Access Control** list that reserves an IP address within the DHCP range for the device's MAC address.

Name	<input type="text" value="wifi-access"/>
Members	<input type="text" value="My-iPhone"/> X +
Comments	<input type="text" value="Write a comment..."/> 0/255

5. Creating a security policy for wireless traffic

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to your wireless interface, **Source Device Type** to the device group, and **Outgoing Interface** to the Internet-facing interface.

Ensure that **NAT** is turned on.

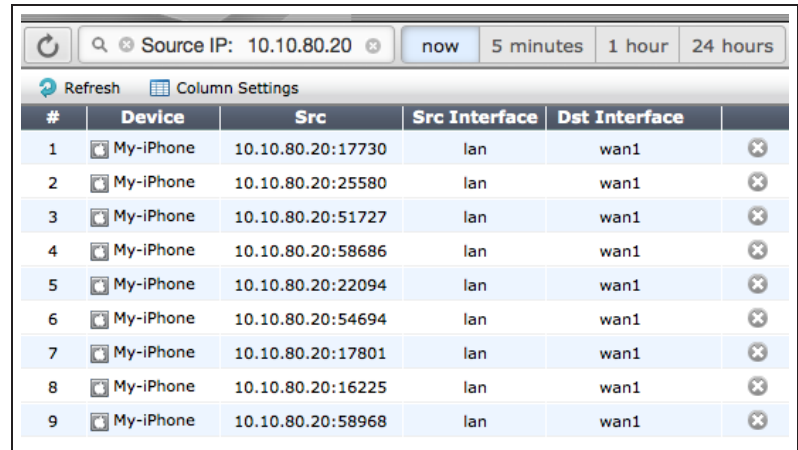
Incoming Interface	<input type="text" value="wifi (SSID: NAMA AH)"/> +
Source Address	<input type="text" value="all"/> +
Source User(s)	<input type="text" value="Click to add..."/>
Source Device Type	<input type="text" value="wifi-access"/> X +
Outgoing Interface	<input type="text" value="any"/> +
Destination Address	<input type="text" value="all"/> +
Schedule	<input type="text" value="always"/> +
Service	<input type="text" value="ALL"/> +
Action	<input type="text" value="ACCEPT"/>
Firewall / Network Options	
<input checked="" type="checkbox"/> ON NAT	
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	<input type="text" value="Click to add..."/>

6. Results

Connect to the wireless network with a device that is a member of the device group. The device should be able to connect and allow Internet access.

Connection attempts from a device that is not a group member will fail.

Go to **System > FortiView > All Sessions** and view the results for now. Filter the results using the reserved **Source IP** (in the example, 10.10.80.20), to see that it is being used exclusively by the wireless device.

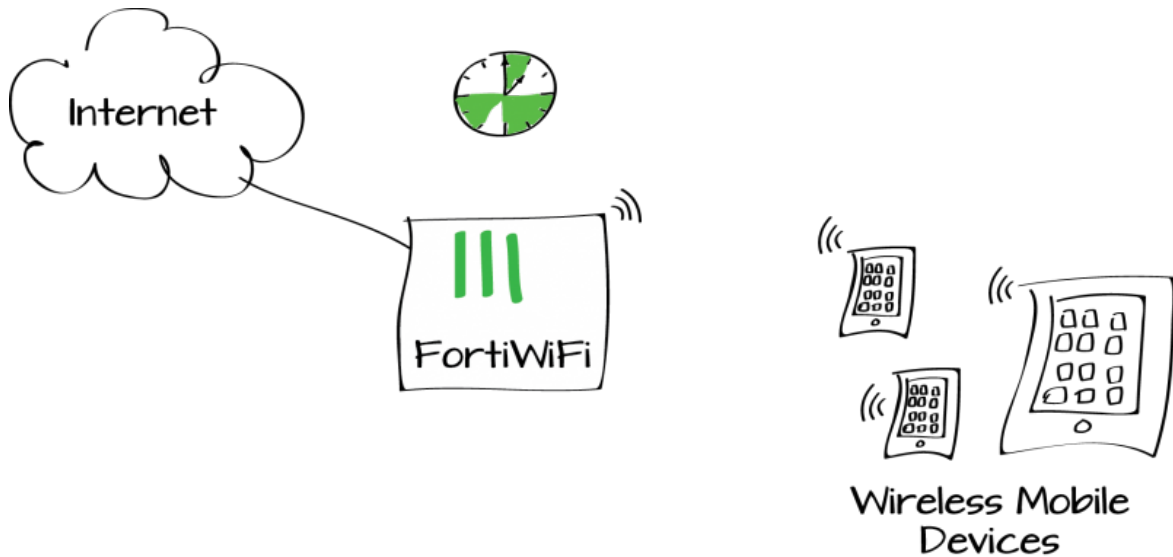


The screenshot shows the FortiView interface with a search filter for Source IP: 10.10.80.20. The table below displays the resulting sessions, all originating from the 'lan' interface and terminating at the 'wan1' interface.

#	Device	Src	Src Interface	Dst Interface	
1	My-iPhone	10.10.80.20:17730	lan	wan1	✕
2	My-iPhone	10.10.80.20:25580	lan	wan1	✕
3	My-iPhone	10.10.80.20:51727	lan	wan1	✕
4	My-iPhone	10.10.80.20:58686	lan	wan1	✕
5	My-iPhone	10.10.80.20:22094	lan	wan1	✕
6	My-iPhone	10.10.80.20:54694	lan	wan1	✕
7	My-iPhone	10.10.80.20:17801	lan	wan1	✕
8	My-iPhone	10.10.80.20:16225	lan	wan1	✕
9	My-iPhone	10.10.80.20:58968	lan	wan1	✕

For further reading, check out [Managing "bring your own device"](#) in the [FortiOS 5.2 Handbook](#).

BYOD scheduling



In this example, a school blocks Internet access to mobile devices during class time (9am - 12pm and 1pm - 3pm).

This recipe shows how to use a schedule group and a BYOD device policy to permit mobile device Internet access before and after class time and during lunch. The school is open from 7am to 6pm.

In this example a FortiWiFi unit provides the wireless network. The steps are the same if the wireless network is provided by FortiAP with a FortiGate as a wireless controller.

1. Creating schedules and a schedule group

Go to **Policy & Objects > Objects > Schedules**. Create recurring schedules for the before class (7-9 am), lunch (12-1 pm), and after class (3-6 pm) periods.

New Schedule

Type: Recurring One-time

Name: before class

Days: Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Start Time: Hour 7 Minute 0

Stop Time: Hour 9 Minute 0

OK Cancel

New Schedule

Type: Recurring One-time

Name: lunch

Days: Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Start Time: Hour 12 Minute 0

Stop Time: Hour 13 Minute 0

OK Cancel

New Schedule

Type: Recurring One-time

Name: after class

Days: Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Start Time: Hour 15 Minute 0

Stop Time: Hour 18 Minute 0

OK Cancel

Select **Create New > Schedule Group** and add create the schedule group by adding the outside of class time schedules to a schedule group.

New Schedule Group

Name: non-class time

Members:

- after class
- before class
- lunch

OK Cancel

2. Creating a policy to block mobile devices outside of class time

Go to **Policy & Objects > Policy > IPv4** and create a policy that allows Internet access for mobile devices on the Student-net wireless network according to the schedule.

Set **Incoming Interface** to the wireless interface, **Source Device Type** to **Mobile Devices** (a default device group that includes tablets and mobile phones), **Outgoing Interface** to the Internet-facing interface, and set **Schedule** to the new schedule group.

Using a device group will automatically enable device identification on the wireless interface.

New Policy

Incoming Interface	Ednet (SSID: Student-net)
Source Address	all
Source User(s)	Click to add...
Source Device Type	Mobile Devices
Outgoing Interface	port1
Destination Address	all
Schedule	non-class time
Service	ALL
Action	ACCEPT

Firewall / Network Options

NAT

Use Outgoing Interface Address Fixed Port

3. Results

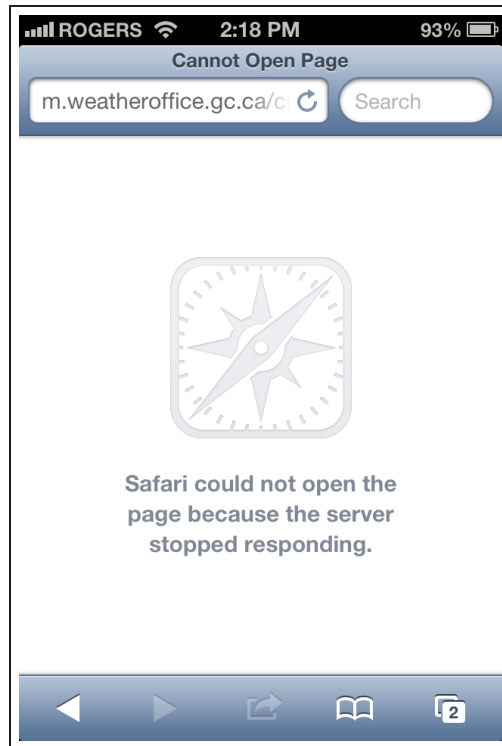
Verify that mobile devices can connect to the Internet outside of class time, when the schedule group is valid.

Go to **Log & Report > Traffic Log > Forward Traffic** to view mobile device traffic.

#	Date/Time	Src	Device	Dst
161	17:00:48	20.10.10.40	Android Phone	8.8.8.8
162	15:00:28	20.10.10.40	Android Phone	216.250.166.65
163	12:58:38	20.10.10.40	Android Phone	65.55.172.252
164	12:48:26	20.10.10.41	iPad	17.172.208.30
165	7:44:46	20.10.10.41	iPad	8.8.8.8

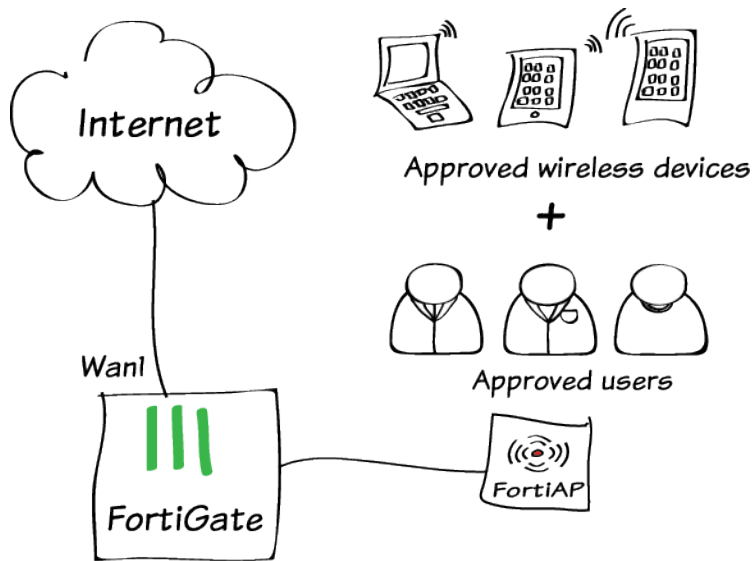
When the time in the schedule is reached, further surfing cannot continue.

This traffic does not appear in the logs, as only allowed traffic is logged.



For further reading, check out [Managing "bring your own device"](#) in the [FortiOS 5.2 Handbook](#).

BYOD for a user with multiple wireless devices



In this example, you will make a FortiOS security policy that requires both user and device authentication, so that known users can only access the network when they are using known devices.

Using a combination of user and device authentication improves security in BYOD environments. Any authenticated user can connect through wireless, using any wireless device that is included in the device group specified in the policy. Thus, the BYOD policy can even support a user with multiple devices.

1. Create users and a user group

Go to **User & Device > User > User Definition** and create a Local user.

Create additional users as needed. You can use any authentication method.

The screenshot shows the 'Login Credentials' step of the user definition process. At the top, there are four steps: 1. User Type (checked), 2. Login Credentials (active), 3. Contact Info, and 4. Extra Info. Below the steps, there are two input fields: 'User Name' with the value 'rgreen' and 'Password' with a masked password of ten dots. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Go to **User & Device > User > User Groups**.

Create a user group for employees and add the new user(s) to the group.

The screenshot shows the 'User Groups' form. The 'Name' field contains 'employees'. The 'Type' field has three radio buttons: 'Firewall' (selected), 'Fortinet Single Sign-On (FSSO)', and 'Guest'. The 'Members' field contains two entries: 'gbrown' and 'rgreen', each with a user icon, an 'X' to remove, and a '+' to add. At the bottom right, there is a '0/255' character count.

2. Create devices and a device group

Go to **User & Device > Device > Device Definitions** and enter the user's device information.

The screenshot shows the 'Device Definitions' form. The 'Alias' field contains 'rgreen tablet'. The 'MAC Address' field contains '08:fd:0e:ff:0c:56'. The 'Additional MACs' field has a dropdown menu with 'Click to add...'. The 'Device Type' field has a dropdown menu with 'Android Tablet'. The 'Custom Groups' field has a dropdown menu with 'None'. The 'Comments' field is empty, with a '0/255' character count at the bottom right.

Go to **User & Device > Device > Device Groups**. Create a device group and add user's devices to it.

The screenshot shows the 'Device Groups' form. The 'Name' field contains 'staff devices'. The 'Members' field contains one entry: 'rgreen tablet', with a device icon, an 'X' to remove, and a '+' to add. At the bottom right, there is a '0/255' character count.

3. Configure WiFi security

Go to **WiFi Controller > WiFi Network > SSID** and configure your wireless network for WPA-Enterprise authentication using the employees user group.

WiFi Settings

SSID: example-staff

Security Mode: WPA2 Enterprise

Authentication: Local RADIUS Server

Broadcast SSID:

Block Intra-SSID Traffic:

Maximum Clients: 0

Optional VLAN ID: 0

4. Create the security policy

Go to **Policy & Objects > Policy > IPv4** and create a policy to enable traffic from the WiFi interface to the Internet (in the example, *wan1*) and office LAN (in the example, *Internal*) interfaces.

Restrict the policy to allow only the employees user group and device group.

Incoming Interface: example-wifi (SSID: example-staff)

Source Address: example-wifi-net

Source User(s): employees

Source Device Type: staff devices

Outgoing Interface: wan1, Internal

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

5. Results

User **rgreen** can connect to the Internet using the **rgreen tablet** that belongs to the **staff devices** group.

Go to **Policy & Objects > Monitor > Policy Monitor** to see the security policy in use.

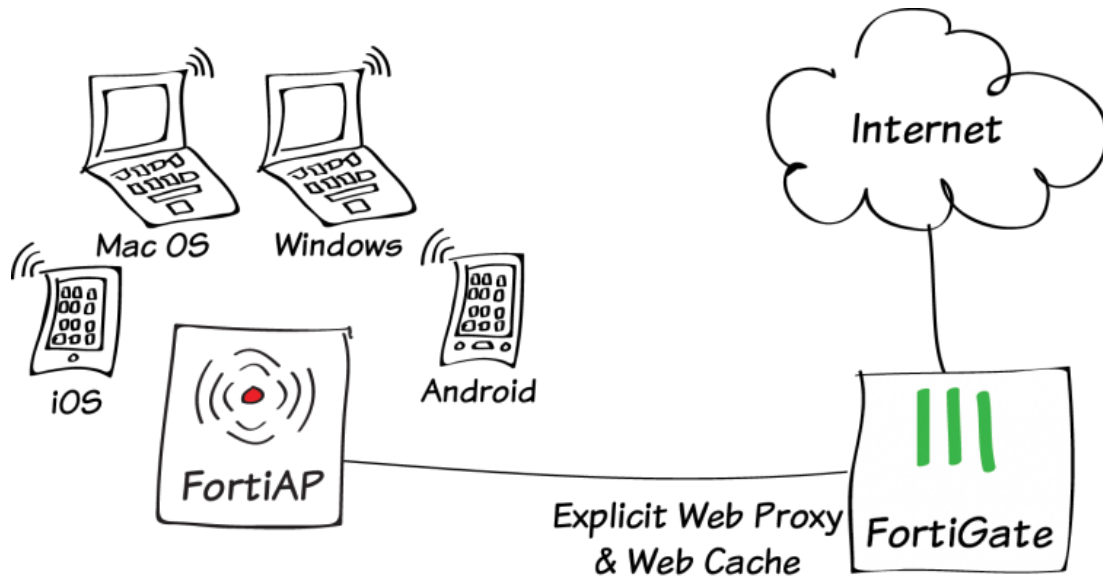
Policy ID	Source Interface/Zone	Destination Interface/Zone	Action	Active Sessions	Bytes	Packets
4	example-wifi	wan1, Internal	✓	30	79,12 MB	124,095

Attempts to access the Internet fail if any of the following are true:

- the user does not belong to the employees user group
- the device does not belong to the staff devices group

For further reading, check out [Deploying Wireless Networks](#) in the [FortiOS 5.2 Handbook](#).

Explicit proxy with web caching



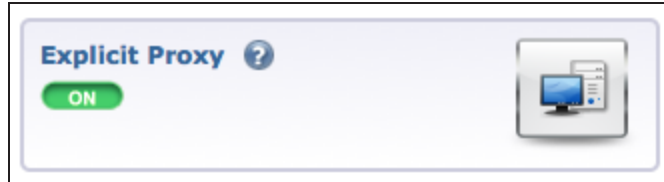
In this example, you will add explicit proxy with web caching to your wireless network.

All devices on the wireless network will be required to connect to the proxy at port 8080 before they can browse web pages on the Internet. WAN Optimization web caching is added to reduce the amount of Internet bandwidth used and improve web browsing performance.

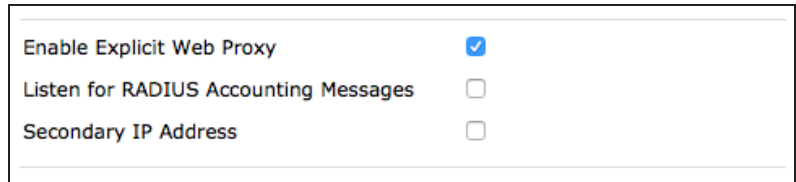
A video of this recipe is available [here](#).

1. Enabling WAN Optimization and configuring the explicit web proxy for the wireless interface

Go to **System > Config > Features**. Ensure that **Explicit Proxy** and **WAN Opt & Cache** are enabled.



Go to **System > Network > Interfaces**, edit the wireless interface and select **Enable Explicit Web Proxy**.



Go to **System > Network > Explicit Proxy**. Select **Enable Explicit Web Proxy** for HTTP/HTTPS. Make sure that **Default Firewall Policy Action** is set to **Deny**.

▼ Explicit Web Proxy Options

Enable Explicit Web Proxy HTTP / HTTPS FTP PAC

Enable IPv6 Explicit Proxy

Listen on Interfaces

HTTP Port

HTTPS Port (0 to use HTTP port)

FTP Port (0 to use HTTP port)

PAC Port (0 to use HTTP port)

PAC File Content

Proxy FQDN

Max HTTP request length Kb

Max HTTP message length Kb

Unknown HTTP version

Realm

Default Firewall Policy Action Accept Deny

2. Adding an explicit web proxy policy

Go to **Policy & Objects > Policy > Explicit Proxy** and create a new policy. Set **Explicit Proxy Type** to **Web** and the **Outgoing Interface** to the Internet-facing interface.

Explicit Proxy Type Web FTP

Enabled On

Source Address

Outgoing Interface

Destination Address

Schedule

Action

Turn on **Web Cache**.

ON

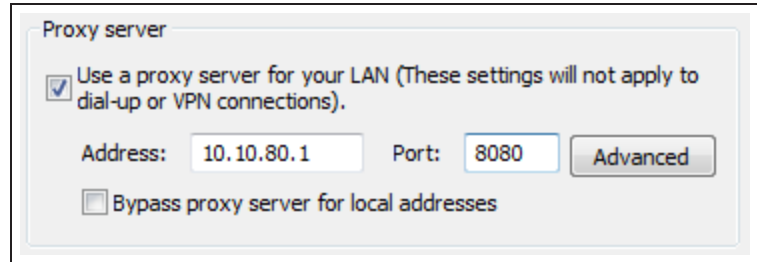
Web Cache

3. Configuring devices on the wireless network to use the web proxy

To use the web proxy, all devices on the wireless network must be configured to use the explicit proxy server. The IP address of the server is the IP address of the FortiGate's wireless interface (in the example, *10.10.80.1*) and the port is 8080. Some browsers may have to be configured to use the device's proxy settings.

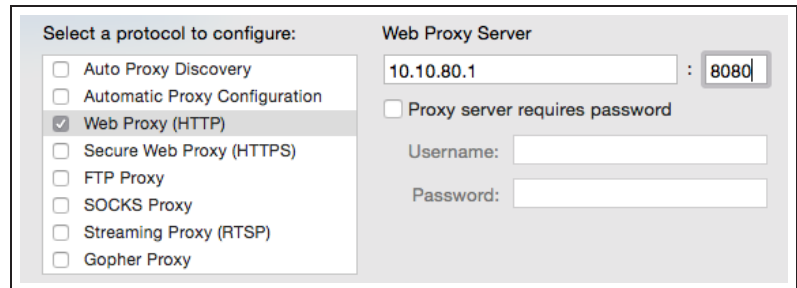
Windows Vista/7/8:

Open **Internet Properties**. Go to **Connections > LAN Settings** and enable and configure the **Proxy Server**.



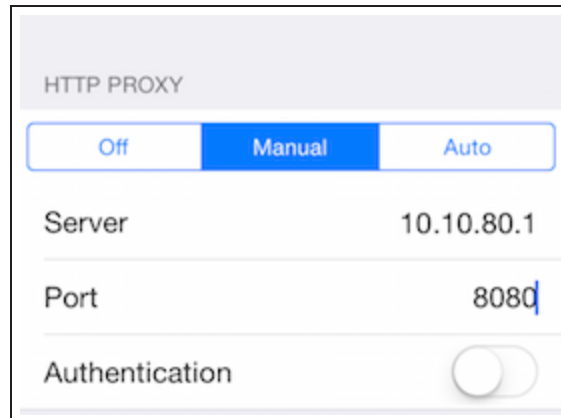
Mac OS X:

Open **Network Preferences > Wi-Fi > Advanced > Proxies**. Select **Web Proxy (HTTP)** and configure the proxy settings.



iOS:

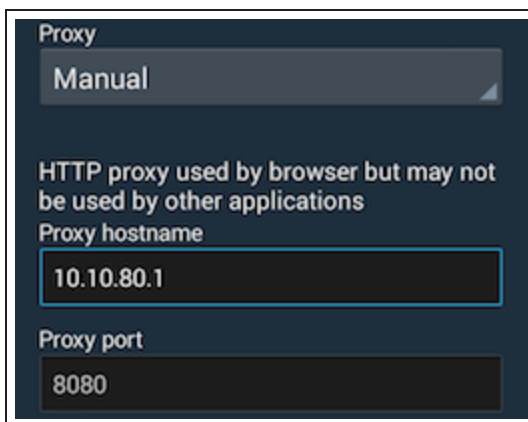
Go to **Settings > Wi-Fi**. Edit the wireless network. Scroll down to **HTTP PROXY** select **Manual** and configure the proxy settings.



Android:

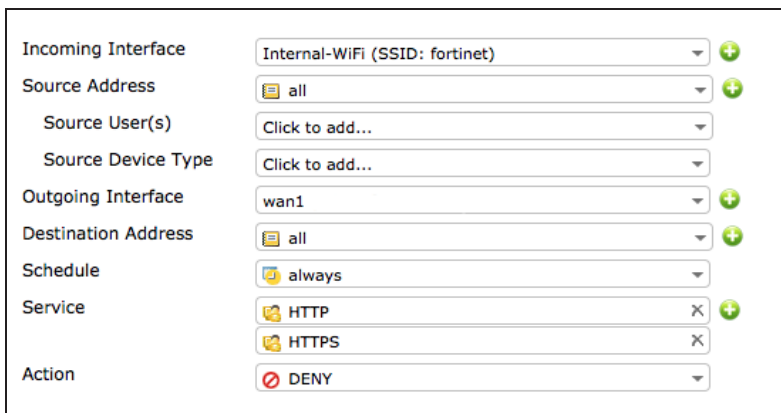
In WiFi network connection settings, edit the wireless network. Select **Show advanced options**, configure a **Manual** proxy and enter the proxy settings.

s



4. Force HTTP and HTTPS traffic to use the Web Proxy

Block HTTP and Replace...HTTPS access to the Internet from the wireless network so that the only path to the Internet is through the explicit proxy. You can edit or delete policies that allow HTTP or HTTPS access. You can also add a policy to the top of the list that **Denies** HTTP and HTTPS traffic.

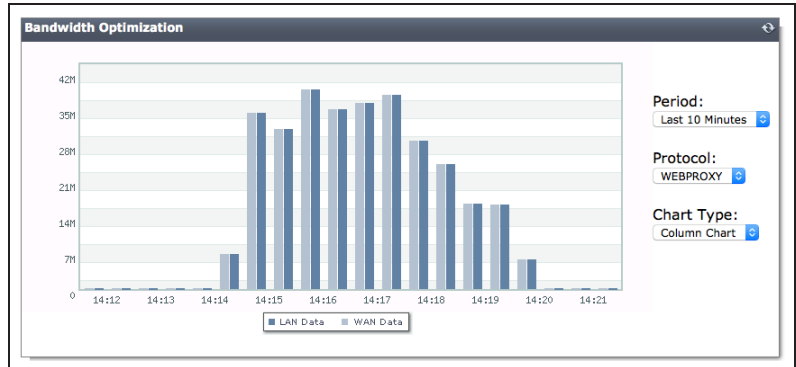
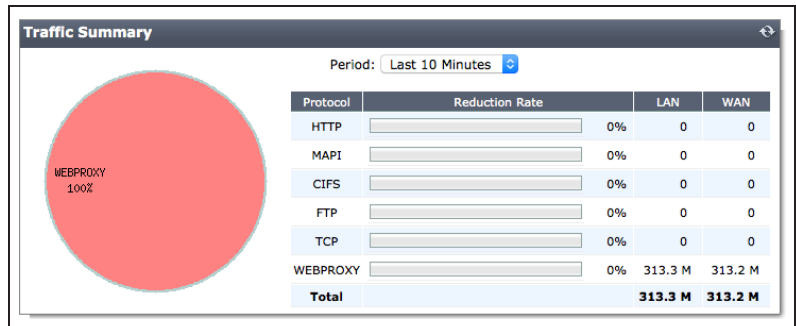


5. Results

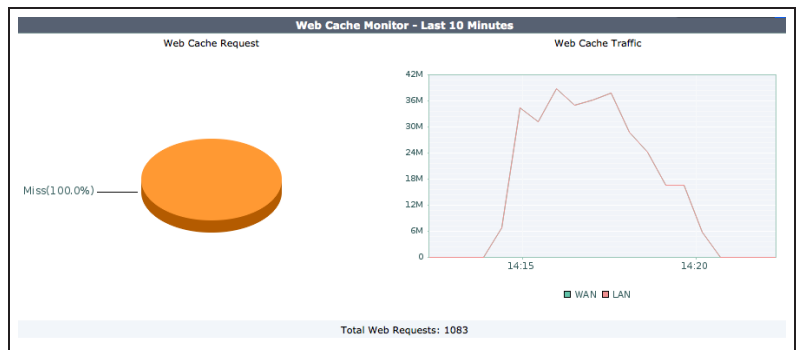
To confirm that the proxy is processing traffic, attempt to connect to the Internet from the Wireless network using a device that has not been configured to connect to the proxy. Access should be blocked.

Configure the device to use the proxy.
You should now be able to connect to the Internet.

Go to **WAN Opt. & Cache > Monitor > WAN Opt. Monitor** to view **WEBPROXY** traffic in the **Traffic Summary**. Check the **Bandwidth Optimization** graph for **WEBPROXY** traffic.



Go to **WAN Opt. & Cache > Monitor > Cache Monitor** to view web caching activity.



For further reading, check out [The FortiGate explicit web proxy in the FortiOS 5.2 Handbook](#).

Authentication

This section contains information about authenticating users and devices.

Authentication, the act of confirming the identity of a person or device, is a key part of network security. When authentication is used, the identities of users or host computers must be established to ensure that only authorized parties can access the network.

User accounts and device definitions

- User and device authentication
- Excluding users from security scanning
- MAC access control
- BYOD scheduling
- BYOD for a user with multiple wireless devices
- FSSO in Polling mode

Authentication and security

- Web filtering using quotas
- Blocking and monitoring Tor traffic

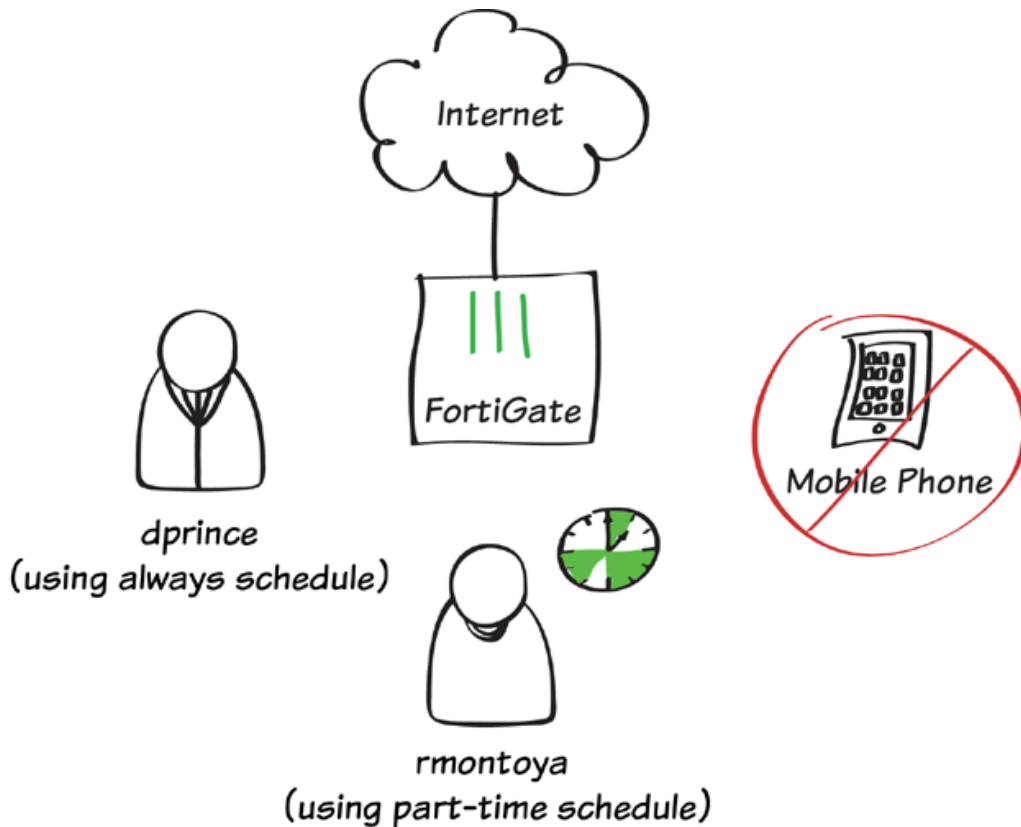
WiFi authentication

- Captive portal WiFi access control
- WP2A WiFi access control
- WiFi with external RADIUS authentication

Authentication with other technologies

- Two-factor authentication with FortiToken Mobile

User and device authentication



In this example, user authentication and device authentication provide different access for staff members based on whether they are full-time or part-time employees, while denying all traffic from mobile phones.

In this example, a wireless network has already been configured that is in the same subnet as the wired LAN. For information about this configuration, see [Setting up a WiFi bridge with a FortiAP](#).

A video of this recipe can be found [here](#).

1. Defining two users and two user groups

Go to **User & Device > User > User Definitions**.

Create two new users (in the example, *dprince* and *montoya*).

1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info
4 Provide Extra Info

Local User
 Remote RADIUS User
 Remote TACACS+ User
 Remote LDAP User

< Back Next > Cancel

1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info
4 Provide Extra Info

User Name
Password

< Back Next > Cancel

1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info
4 Provide Extra Info

Email Address
 SMS

< Back Next > Cancel

1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info
4 Provide Extra Info

Enable
 Two-factor Authentication
 User Group

< Back Create Cancel

Both user definitions now appear in the user list.

User Name	Type	Two-factor Authentication	Ref.
dprince	LOCAL	X	0
guest	LOCAL	X	1
rmontoya	LOCAL	X	0

Go to **User & Device > User > User Groups**.

Create the user group *full-time* and add user *dprince*.

Name:

Type: Firewall Fortinet Single Sign-On (FSSO) Guest RADIUS Single Sign-On (RSSO)

Members: X +

Create a second user group, *part-time*, and add user *rmontoya*.

Name:

Type: Firewall Fortinet Single Sign-On (FSSO) Guest RADIUS Single Sign-On (RSSO)

Members: X +

2. Creating a schedule for part-time staff

Go to **Policy & Objects > Objects > Schedules** and create a new recurring schedule.

Set an appropriate schedule. In order to get results later, do not select the current day of the week.

Type: Recurring One-time

Name:

Days: Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Start Time: Hour Minute

Stop Time: Hour Minute

3. Defining a device group for mobile phones

Go to **User & Device > Device > Device Groups** and create a new group.

Add the various types of mobile phones as **Members**.

Name:

Members: X +
 X
 X
 X

Comments: 0/255

4. Creating a policy for full-time staff

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source User(s)** to the full-time group, **Outgoing Interface** to your Internet-facing interface, and ensure that **Schedule** is set to **always**.

Turn on **NAT**.

Incoming Interface	lan
Source Address	all
Source User(s)	full-time
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

Firewall / Network Options

NAT

Use Destination Interface Address Fixed Port

Use Dynamic IP Pool

Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

Logging Options

Log Allowed Traffic

Security Events

All Sessions

Capture Packets

5. Creating a policy for part-time staff that enforces the schedule

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source User(s)** to the part-time group, **Outgoing Interface** to your Internet-facing interface, and set **Schedule** to use the part-time schedule.

Turn on **NAT**.

Incoming Interface	lan
Source Address	all
Source User(s)	part-time
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	all
Schedule	part-time
Service	ALL
Action	ACCEPT

Firewall / Network Options

NAT

Use Destination Interface Address Fixed Port

Use Dynamic IP Pool

Scroll down to view the **Logging Options**. In order to view the results later, enable **Log Allowed Traffic** and select **All Sessions**.

Logging Options

Log Allowed Traffic

Security Events

All Sessions

Capture Packets

View the policy list. Click on the title row and select **ID** from the dropdown menu, then select **Apply**. Take note of the ID number that has been given to the part-time policy.

Seq.#	From	To	Schedule	Source	Destination	ID
1	lan	wan1	always	all full-time	all	1
2	lan	wan1	part-time	all part-time	all	2
3	any	any	always	all	all	

Go to **System > Dashboard > Status** and enter the following command into the **CLI Console**, using the ID number of the part-time policy.

```
config firewall policy
edit 2
set schedule-timeout enable
end
end
```

This will ensure that part-time users will have their access revoked during days they are not scheduled, even if their current session began when access was allowed.

6. Creating a policy that denies mobile traffic

Go to **Policy & Objects > Policy > IPv4** and create a new policy.

Set **Incoming Interface** to the local network interface, **Source Device** to **Mobile Devices** (a default device group that includes tablets and mobile phones), **Outgoing Interface** to your Internet-facing interface, and set **Action** to **DENY**.

Using a device group will automatically enable device identification on the local

Incoming Interface	lan +
Source Address	all +
Source User(s)	Click to add...
Source Device Type	mobile-phones x +
Outgoing Interface	wan1 +
Destination Address	all +
Schedule	always +
Service	ALL +
Action	DENY +

Logging Options

Log Violation Traffic

network interface.

Leave **Log Violation Traffic** turned on.

In order for this policy to be used, it must be located at the top of the policy list. Select any area in the far-left column of the policy and drag it to the top of the list.

Seq.#	From	To	Devices	Groups	Action
3	lan	wan1	Mobile Devices		DENY
1	lan	wan1		full-time	ACCEPT
2	lan	wan1		part-time	ACCEPT
4	any	any			DENY

7. Results

Browse the Internet using a computer. You will be prompted to enter authentication credentials.


Log in using the *dprince* account. You will be able to access the Internet at any time.



The image shows a Fortinet Authentication Required dialog box. At the top, the Fortinet logo is displayed. Below it, the text "Authentication Required" is centered. Underneath, a message says "Please enter your username and password to continue." There are two input fields: "Username:" and "Password:", both with asterisks indicating they are required. A "Continue" button is located at the bottom right of the dialog box.

Go to **User & Device > Monitor > Firewall**. Highlight *dprince* and select **De-authenticate**.

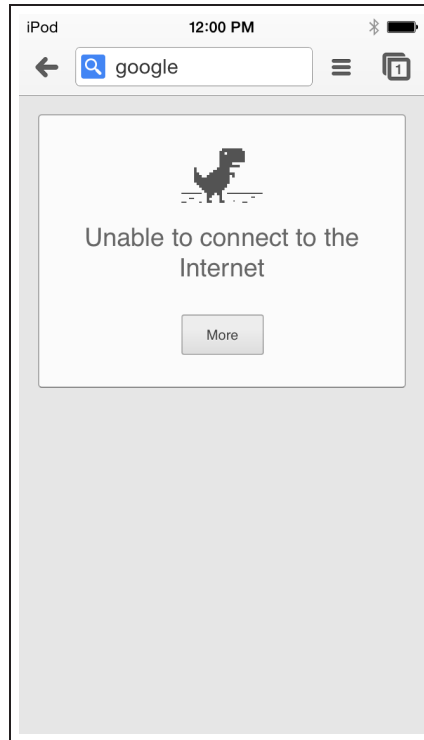
Attempt to browse the Internet again. This time, log in using the *montoya* account. After authentication occurs, you will not be able to access the Internet.



The image shows a table from the Fortinet User & Device Monitor Firewall section. At the top, there are two buttons: "Refresh" and "De-authenticate". Below the buttons, there are two columns: "User Name" and "User Group". The table contains one row with the user name "dprince" and the user group "full-time".

User Name	User Group
dprince	full-time

Attempts to connect to the Internet using any mobile phone will also be denied.



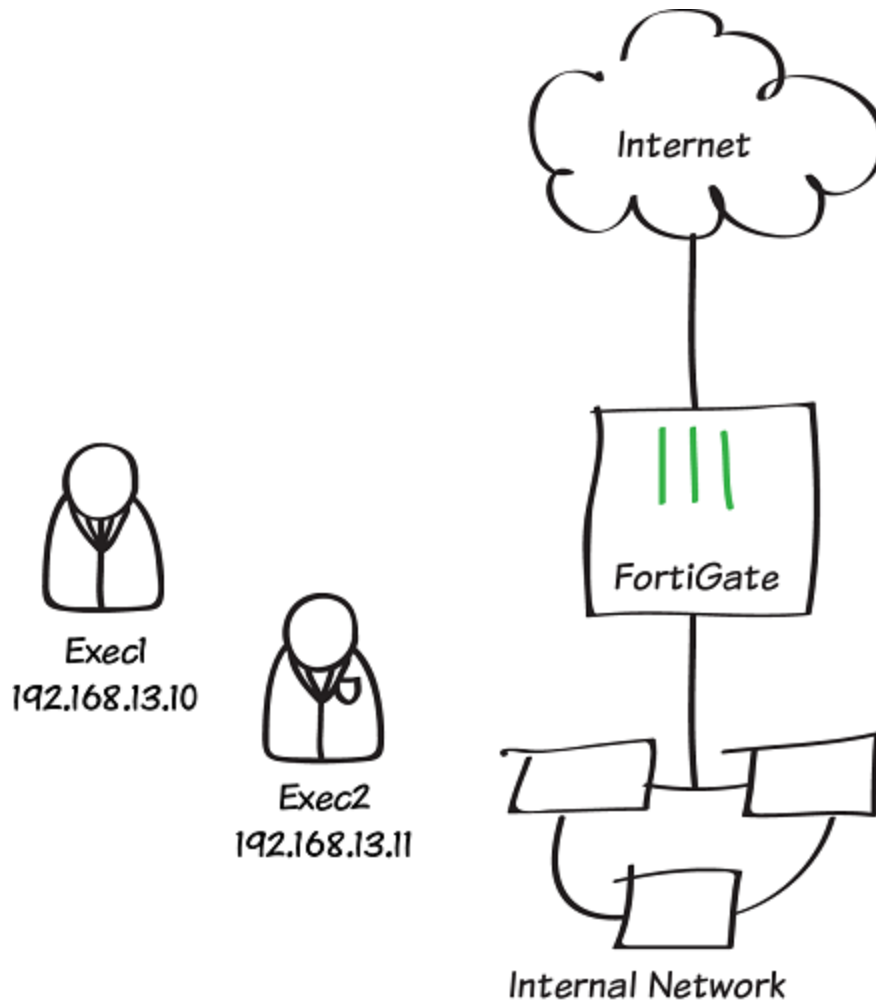
You can view more information about the blocked and allowed sessions by going to **System > FortiView > All Sessions**.

*Sessions that were blocked when you attempted to sign in using the **rmontoya** account will not have a user account shown in the **User** column.*

Date/Time	User	Device	Destination	Action
09:10:21		iPhone	208.91.112.53	deny
09:10:21		Mac Mini	157.55.56.159	deny
09:10:21		Mac Mini	111.221.74.30	deny
09:10:21		Mac Mini	111.221.77.159	deny
09:10:21		iPhone	208.91.112.52	deny
09:10:20		iPhone	208.91.112.53	deny
09:10:20		iPhone	208.91.112.53	deny
09:10:19		Mac Mini	157.55.56.159	deny
09:10:19		Mac Mini	157.56.52.30	deny
09:10:17		iPhone	208.91.112.52	deny
09:10:17	dprince	Mac Mini	54.231.0.33 (s3-1-w.amazonaws.com)	accept
09:10:16	dprince	Mac Mini	54.231.0.33 (s3-1-w.amazonaws.com)	accept
09:10:16	dprince	Mac Mini	54.231.0.33 (s3-1-w.amazonaws.com)	accept
09:10:15	dprince	Mac Mini	64.94.107.34 (map-pb.quantserve.com.akadns.net)	accept
09:10:15	dprince	Mac Mini	174.36.240.82 (api.mixpanel.com)	accept

For further reading, check out **Users and user groups** in the **FortiOS 5.2 Handbook**.

Excluding users from security scanning



In this example, two company executives are excluded from the security scanning that a FortiGate applies to all other staff Internet traffic.

The executives in this example connect to the Internet using PCs with static IP addresses, so these addresses can be used to identify their traffic. If identifying users with a static IP address will not work for your network you can set up authentication or device identification (BYOD).

1. Applying security profiles to the staff policy

Go to **Policy & Objects > Policy > IPv4** and edit the general policy that allows staff to access the Internet.

Under **Security Profiles**, enable **Web Filter** and **Application Control**. Set them to use the default profiles. Also set **SSL/SSH Insection** to the **deep-inspection** profile.

To be able to see results enable logging all sessions.

Incoming Interface	internal	+	
Source Address	Internal-net	+	
Source User(s)	Click to add...		
Source Device Type	Click to add...		
Outgoing Interface	wan1	+	
Destination Address	all	+	
Schedule	always		
Service	ALL	+	
Action	ACCEPT		
Firewall / Network Options			
<input checked="" type="checkbox"/> NAT			
<input checked="" type="radio"/> Use Outgoing Interface Address		<input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool		Click to add...	
Security Profiles			
<input type="checkbox"/> AntiVirus		default	+
<input checked="" type="checkbox"/> Web Filter		default	+
<input checked="" type="checkbox"/> Application Control		default	+
Proxy Options		default	+
<input checked="" type="checkbox"/> SSL/SSH Inspection		certificate-inspection	+
Logging Options			
<input checked="" type="checkbox"/> Log Allowed Traffic			
<input type="checkbox"/> Security Events			
<input checked="" type="checkbox"/> All Sessions			

2. Creating firewall addresses for the executives

Go to **Policy & Objects > Objects > Addresses**. Create an address for each executive. Use /32 as the Netmask to ensure that the firewall address applies only to the specified IP.

Name	Exec1
Type	IP/Netmask
Subnet / IP Range	192.168.13.10
Interface	internal
Show in Address List	<input checked="" type="checkbox"/>
Comments	<input type="text"/> 0/255

Name	Exec2
Type	IP/Netmask
Subnet / IP Range	192.168.13.11
Interface	internal
Show in Address List	<input checked="" type="checkbox"/>
Comments	<input type="text"/> 0/255

Select **Create New > Address Group** and create an address group for the executive addresses.

Group Name	Executives						
Show in Address List	<input checked="" type="checkbox"/>						
Members	<table border="1"> <tr> <td>Exec1</td> <td>X</td> <td>+</td> </tr> <tr> <td>Exec2</td> <td>X</td> <td></td> </tr> </table>	Exec1	X	+	Exec2	X	
Exec1	X	+					
Exec2	X						

3. Creating a security policy for the executives

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing the executives to access the Internet. Set **Source Address** to **Executives**. Enable logging and select Log all Sessions to be able to view results.

Leave all Security Profiles disabled.

Incoming Interface	internal	+
Source Address	Executives	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	wan1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	
Firewall / Network Options		
<input checked="" type="checkbox"/> NAT		
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	<input type="text"/> Click to add...	
Security Profiles		
<input type="checkbox"/> AntiVirus	default	+
<input type="checkbox"/> Web Filter	default	+
<input type="checkbox"/> Application Control	default	+
<input type="checkbox"/> SSL/SSH Inspection	certificate-inspection	+
Logging Options		
<input checked="" type="checkbox"/> Log Allowed Traffic		
<input type="radio"/> Security Events		
<input checked="" type="radio"/> All Sessions		

In the policy list, the policy for executives (in this example ID=3) must be above the policy for staff (in this example ID=2).

ID	Source	Destination	Schedule	Service	Action	NAT	AV	Web Filter	Application Control
internal - wan1 (2)									
3	Executives	all	always	ALL	ACCEPT	Enable			
2	Internal-net	all	always	ALL	ACCEPT	Enable	url default	app default	

You can re-order policies by hovering your mouse cursor over the borders of the left-most cell of a policy until the cursor changes into crossed arrows and then clicking and dragging that policy up or down into the required order.

Note that in this screen shot the policy ID (ID) is shown for each policy and the sequence number (Seq.#) is hidden.

4. Results

Connect to the Internet from two computers on the internal network: one from an executive address and one from a staff address.

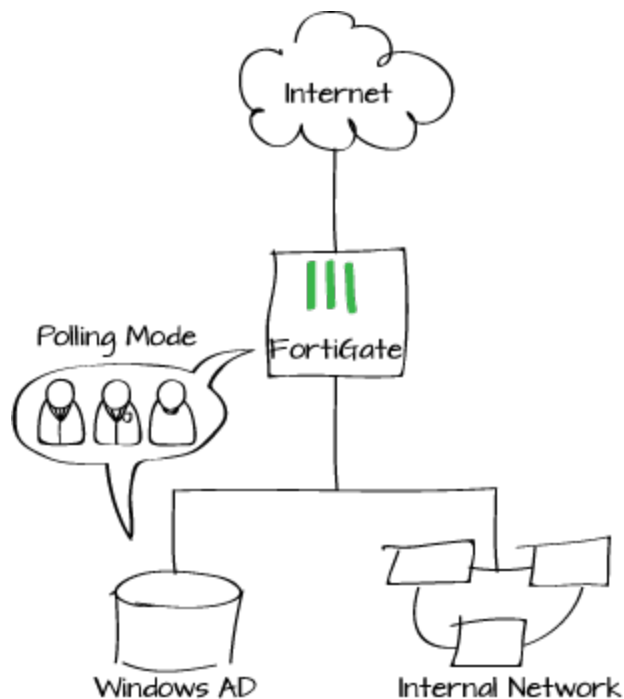
Go to **Log & Report > Traffic Log > Forward Traffic**. Right-click the column headings and make sure that the **Policy ID** column is visible.

In this example output, connections from 192.168.13.10 (an executive address) use policy ID 3 and connections from 192.168.13.144 (a staff address) use policy ID 2.

#	Policy ID	Date/Time	Source	Sent / Received
1	3	07:46:28	192.168.13.10	1.11 KB / 10.99 KB
2	3	07:46:28	192.168.13.10	1.10 KB / 9.13 KB
3	3	07:46:28	192.168.13.10	1.07 KB / 9.51 KB
4	3	07:46:28	192.168.13.10	1.16 KB / 12.48 KB
5	3	07:46:28	192.168.13.10	1.12 KB / 11.14 KB
6	2	07:45:48	192.168.13.144	8.41 KB / 10.79 KB
7	2	07:45:24	192.168.13.144	653 B / 4.99 KB
8	2	07:44:57	192.168.13.144	48 B / 0 B
9	2	07:44:47	192.168.13.144	2.51 KB / 1.28 KB
10	2	07:44:47	192.168.13.144	3.49 KB / 5.99 KB

For further reading, check out [Security Profiles](#) in the [FortiOS 5.2 Handbook](#).

FSSO in Polling mode



In this example, you will configure Fortinet Single Sign-On (FSSO) directly in the security policy using the new FSSO wizard introduced in FortiOS 5.2.2.

This recipe requires that your FortiGate's DNS point to a DNS server that can resolve the IP addresses or fully qualified domain names of the users' PCs.

This example uses Active Directory polling to establish FSSO for a Windows AD Domain Controller, without requiring a FortiAuthenticator or a collector agent to act as an intermediary between the FortiGate and the domain. An LDAP server is also used for authentication.

A video of this recipe is available [here](#).

1. Adding the LDAP Server to the FortiGate

In the FortiGate web interface, go to **User & Device > Authentication > LDAP Servers**.

For the **Server IP/Name** enter the LDAP Server's fully qualified domain name or the IP address.

Set the **Bind Type** to **Regular** and enter a **User DN** and **Password**.

Click **Fetch DN** to retrieve your **Distinguished Name**.

Edit LDAP Server

Name: FAC_LDAP

Server IP/Name: 172.20.120.132

Server Port: 389

Common Name Identifier: cn

Distinguished Name: dc=fortidocs,dc=com

Bind Type: Simple Anonymous Regular

User DN: example_admin

Password:

Secure Connection

Test

OK Cancel

Click **Test** and verify that your connection is successful.



2. Configuring the FortiGate unit to poll the Active Directory

Next, go to **User & Device > Authentication > Single Sign-On** and add a new Single Sign-On Server.

For the **Type**, select **Poll Active Directory Server**. Enter the **Server IP/Name**, **User**, and **Password**, then select the **LDAP Server** you added previously. Make sure **Enable Polling** is checked. Add a test user group of your choice.

You must add at least one user group to create your SSO server.

New Single Sign-On Server

Type: Poll Active Directory Server Fortinet Single-Sign-On Agent RADIUS Single-Sign-On Agent

Server IP/Name: 172.20.120.132

User: example_admin

Password:

LDAP Server: FAC_LDAP

Enable Polling:

Users/Groups

LDAP Tree: Recursive ON

Users: Groups: Selected (0)

ID	Name	
Account Operators	Account Operators	CN=Ac
Administrators	Administrators	CN=Ad
Allowed RODC Password Replication Group	Allowed RODC Password Replication Group	CN=All
Backup Operators	Backup Operators	CN=Ba
Cert Publishers	Cert Publishers	CN=Ce

1 / 2 [Total: 54]

3. Adding a firewall address for the Internal network

Go to **Policy & Objects > Objects > Addresses** and create an internal network address to be used by your security policy.

The 'Edit Address' window shows the following configuration:

- Category: Address Multicast Address
- Name: Local_LAN
- Type: Subnet
- Subnet / IP Range: 172.20.120.0/255.255.255.0
- Interface: any
- Visibility:
- Comments: Internal Network Resources 26/255

Buttons: OK, Cancel

4. One-step FSSO configuration in the security policy

Go to **Policy & Objects > Policy > IPv4** and edit a security policy with access to the Internet. Set the **Source Address** to the **Local_LAN** address created in **Step 3**.

The 'Edit Policy' window shows the following configuration:

- Incoming Interface: lan (VLAN ID: 0)
- Source Address: Local_LAN (highlighted with a red box)
- Source User(s): Click to add...
- Source Device Type: Click to add...
- Outgoing Interface: wan1
- Destination Address: all
- Schedule: always
- Service: ALL
- Action: ACCEPT

Firewall / Network Options

- NAT
- Use Outgoing Interface Address Fixed Port

Under **Source User(s)** scroll down past the dropdown menu, and select **Create Users/Groups** wizard.

Source Address: Local_LAN

Source User(s):

Source Device Type:

Outgoing Interface:

Destination Address:

Schedule:

Service:

Action:

Firewall / Network Options

Please Select

Groups

- Guest-group
- My_Group
- SSO_Guest_Users
- test2
- WIFI_guests
- Local Users
- guest
- twhite

Create Users/Groups

For the **User/Group Type**, select **FSSO** and then click **Next**.

1 User/Group Type 2 Remote Groups 3 Local Group

Local User

Remote RADIUS User

Remote TACACS+ User

Remote LDAP User

FSSO

< Back Next > Cancel

For the **Remote Group**, select the appropriate **FSSO Agent** from the dropdown menu.

Select the **Groups** tab and right-click on the user groups you would like to add.

To add multiple groups, hold the Shift key and click.

User/Group Type 2 Remote Groups 3 Local Group

FSSO Agent: 172.20.120.132

LDAP Server: FAC_LDAP

LDAP Users/Groups

LDAP Tree Recursive ON

dc=fortidocs,dc=com

Users Groups Selected (0)

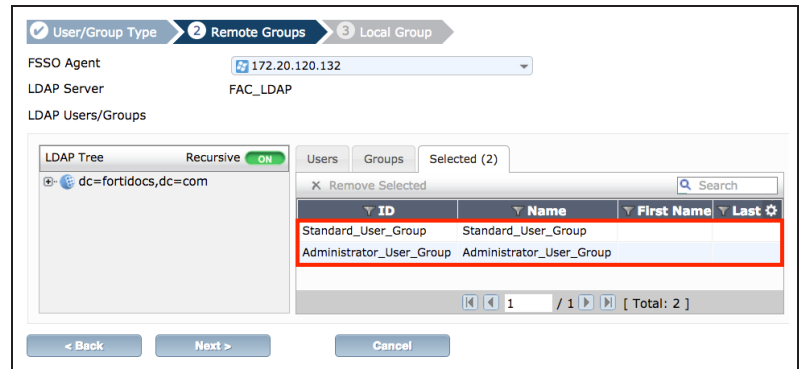
Add Selected

ID	Name	
Session Directory Computers	Session Directory Computers	CN=Ses
Standard_User_Group	Standard_User_Group	CN=Star
TechDoc	TechDoc	CN=Tech
Terminal Server Computers	Terminal Server Computers	CN=Terr

< Back Next > Cancel

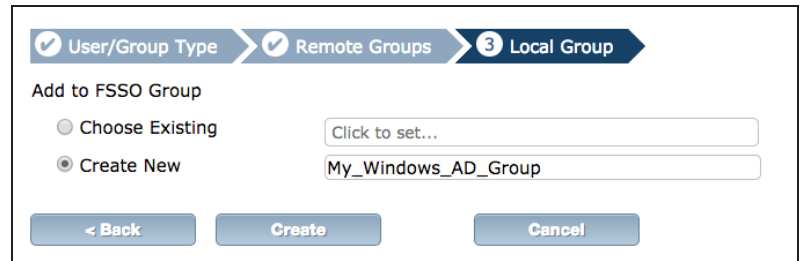
Go to the **Selected** tab. In this example, **Standard_User_Group** and **Admin_User_Group** are shown.

Click **Next**.



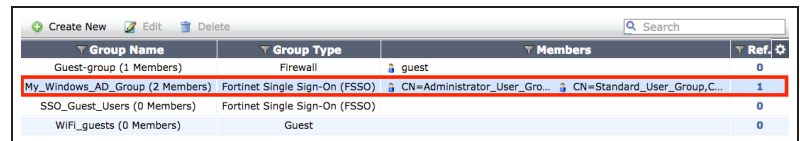
Select **Create New** and name your new FSSO user group.

Click **Create**.

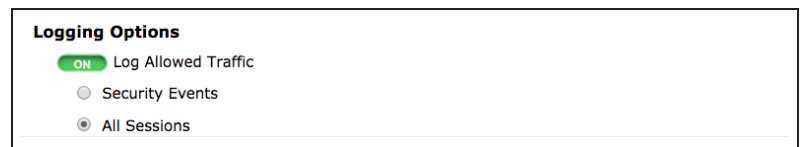


The groups selected have been added to the new FSSO group, **My_Windows_AD_Group**.

*To see these groups go to **User & Device > User > User Groups**.*



Ensure you enable logging and select **All Sessions**.



In the **Global View** your completed policy should look similar to the screenshot shown on the right.

Seq.#	From	To	Source	Action	Destination	Schedule	NAT	Servi
1	lan	wan1	Local_LAN My_Windows_AD_Group	ACCEPT	all	always	Enable	ALL
2	any	any	all	DENY	all	always		ALL

If necessary, select the policy by clicking on the far left column, and move it as close as possible to the top of the list.

All other policies must deny Internet access in order for the user to be forced to authenticate.

5. Results

Go to **Log & Report > Traffic Log > Forward Traffic**.

When users log into the Windows AD network, the FortiGate will automatically poll the domain for their account information, and record their traffic.

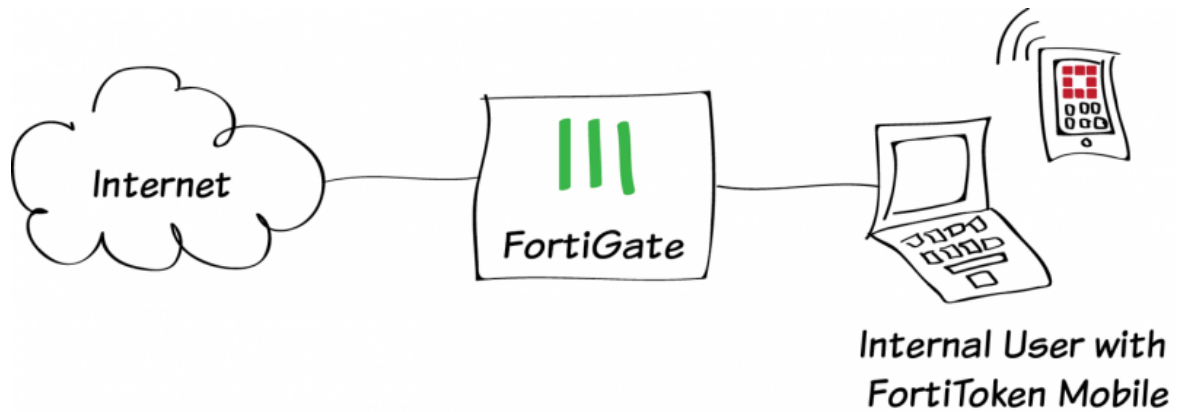
#	Date/Time	Source	Destination	Sent / Received	Application Name	Device
1	16:21:26	twwhite (172.20.120.68)	192.168.27.100	3.04 KB / 33.74 KB	HTTP	BDAVIS-NB
2	16:21:26	twwhite (172.20.120.68)	192.168.27.100	1.00 KB / 2.34 KB	HTTP	BDAVIS-NB
3	16:21:26	twwhite (172.20.120.68)	192.168.27.100	1.53 KB / 19.79 KB	HTTP	BDAVIS-NB
4	16:21:26	twwhite (172.20.120.68)	192.168.27.100	1.06 KB / 6.99 KB	HTTP	BDAVIS-NB
5	16:21:26	twwhite (172.20.120.68)	192.168.27.100	585 B / 950 B	HTTP	BDAVIS-NB
6	16:21:26	twwhite (172.20.120.68)	192.168.27.100	595 B / 735 B	HTTP	BDAVIS-NB

Select an entry for more information.

#	1	Action	deny
Date/Time	17:52:19	Destination	192.168.27.100
Destination Country	Reserved	Device	BDAVIS-NB
Device Type	Windows PC	Dst Interface	wan1
Duration	5526	Group	test2
Level		Log ID	13
Master Src MAC	f0:4d:a2:c5:7c:f4	OS Name	Windows 7 / Windows
Policy ID	0	Policy UUID	d5e34b16-80ba-51e4-4f4a-5dc0ab93d7e0
Protocol	icmp	Protocol Number	1
Received	328140	Sent	328800
Sent Packets	5480	Sequence Number	974328
Service	PING	Source	twwhite (172.20.120.68)
Source Country	Reserved	Src Interface	lan
Src NAT IP	192.168.27.1	Src NAT Port	0
Src Name	BDAVIS-NB	Sub Type	forward
Threat	131072	Threat Level	high
Threat Score	30	Timestamp	12/15/2014, 5:52:19 PM
Tran Display	snat	User	twwhite
Virtual Domain	root		

For further reading, check out [Single Sign-On to Windows AD](#) in the [FortiOS 5.2 Handbook](#).

Two-factor authentication with FortiToken Mobile



In this recipe, two-factor authentication is added to a user account to provide extra security to the authentication process.

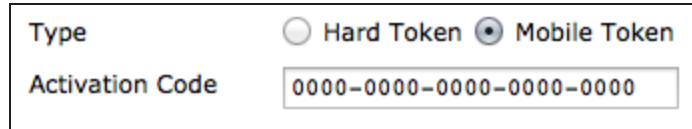
Two-factor authentication requires a user to provide further means of authentication in addition to their credentials. In this recipe, FortiToken Mobile app for Android will be used to generate a token, also known as a one-time password (OTP), to use in the authentication process.

A video of this recipe is available [here](#).

1. Activating your FortiTokens

Ensure that your FortiGate is connected to the Internet. Go to **User & Device > FortiTokens**. Your FortiGate may have two FortiToken Mobile entries listed by default. If so, you may use these tokens and go to step 2.

To add new FortiTokens, select **Create New**. Set **Type** to **Mobile Token** and enter your **Activation Code**.













Type Hard Token Mobile Token
Activation Code

An error stating that the serial number is invalid will appear if you mistyped the code or if it duplicates one you have already entered.

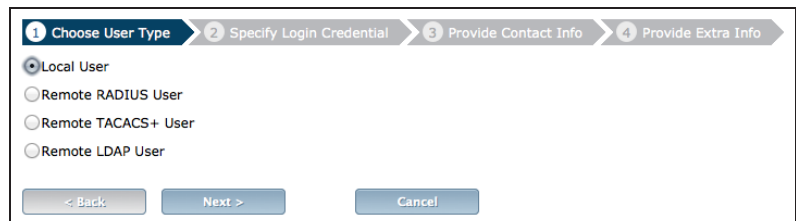
After FortiGuard validates the code, your FortiTokens will appear on the list, with **Status** set to **Available**

*If the FortiToken has already been registered to another FortiGate, the **Status** will be **Error**.*

Type	Serial Number	Status
	FTKMOB4A [blurred]	 Available
	FTKMOB4A [blurred]	 Available
	FTKMOB4A [blurred]	 Available
	FTKMOB4A [blurred]	 Available
	FTKMOB4A [blurred]	 Available

2. Creating a user account with two-factor authentication

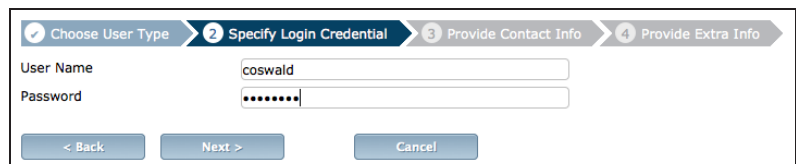
Go to **User & Device > User > User Definition** and create a new local user.



1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info 4 Provide Extra Info

Local User
 Remote RADIUS User
 Remote TACACS+ User
 Remote LDAP User

< Back Next > Cancel



1 Choose User Type 2 Specify Login Credential 3 Provide Contact Info 4 Provide Extra Info

User Name
Password

< Back Next > Cancel

In order to use the FortiToken Mobile, you must enter a mobile number in the third step, **Provide Contact Info**. Select the appropriate **Country/Region** and enter the **Phone Number** without dashes or spaces. Do *not* add an email address.

In the fourth step of the User Creation Wizard, **Provide Extra Info**, enable **Two-Factor Authentication** and select an available token.

The user list shows the FortiToken in the **Two-factor Authentication** column for the new user account.

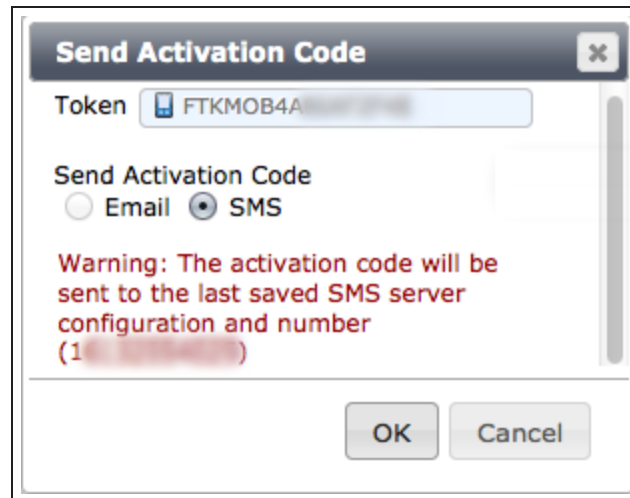
User Name	Type	Two-factor Authentication
coswald	LOCAL	FTKMOB4A86AF2F4B

Go to **User & Device > FortiTokens**. The FortiToken assigned to the user is now listed as **Pending**, until the user activates the FortiToken.

Type	Serial Number	Status	User
	FTKMOB4A86AF2F4B	Pending	coswald

3. Sending the activation code to the user

If your FortiGate can send SMS messages, go to **User & Device > User > User Definition** and edit the new user account. Select **Send Activation Code** and send the code by **SMS**.



If your FortiGate cannot send SMS messages, go to **System > Dashboard > Status** and enter the following into the **CLI Console**, substituting the correct serial number:

```
config user fortitoken
edit serial number
show
```

The activation code will be shown in the output. This code must be given to the user.

```
FG100D3G12812324 (FG100D3G12812324) # show
config user fortitoken
edit "FG100D3G12812324"
set seed "FG100D3G12812324"
set license "FG100D3G12812324"
set activation-code "DEIBYDCK55GZLUCZ"
set activation-expire 1413656099
next
end
```


4. Adding user authentication to your Internet access policy

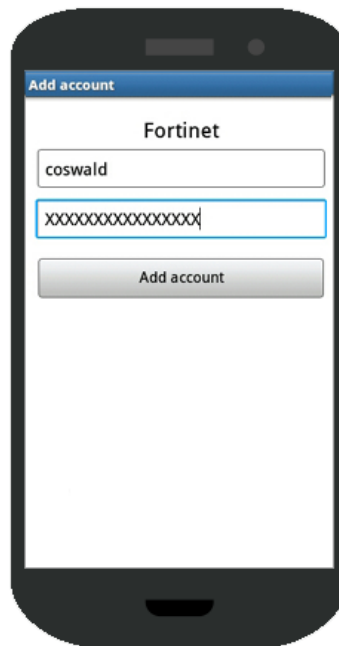
Go to **Policy & Objects > Policy > IPv4** and edit the policy that allows connections from the internal network to the Internet. Set **Source User(s)** to the new user account.

Incoming Interface	port3
Source Address	all
Source User(s)	coswald
Source Device Type	Click to add...
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
Firewall / Network Options	
<input checked="" type="checkbox"/> NAT	
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...

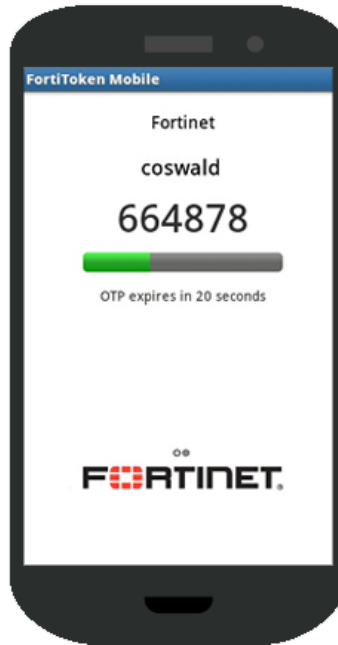
5. Setting up FortiToken Mobile on an Android device

Using your Android device, download and install **FortiToken Mobile**.

Open the app and add a new account. Select **Enter Manually**. Enter the activation code into FortiToken Mobile.



FortiToken Mobile can now generate a token for use with the FortiGate.



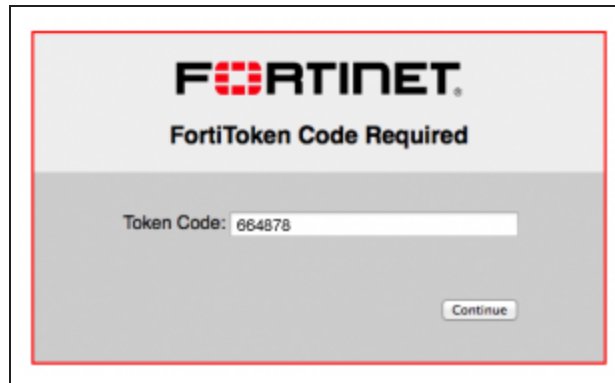
(Optional) For additional security, set a PIN for FortiToken Mobile using the app's **Settings** options.

6. Results

Attempt to browse the Internet. An authentication page will appear, requesting a **Username** and **Password**.



After the correct username and password are entered, a FortiToken code will be requested. Enter the code currently shown in the FortiToken Mobile app. Once the token is authenticated, you can connect to the Internet.



FORTINET
FortiToken Code Required

Token Code:

[Continue](#)

For further reading, check out [FortiToken](#) in the [FortiOS 5.2 Handbook](#).

VPNs

This section contains information about configuring a variety of different Virtual Private Networks (VPNs), as well as different methods of authenticating VPN users. FortiGates support two types of VPNs: IPsec and SSL.

IPsec VPNs use Internet Protocol Security (IPsec) to create a VPN that extends a private network across a public network, typically the Internet. In order to connect to an IPsec VPN, users must install and configure an IPsec VPN client (such as FortiClient) on their PCs or mobile devices.

SSL VPNs use Secure Sockets Layer (SSL) to create a VPN that extends a private network across a public network, typically the Internet. Connections to an SSL VPN are done through a web browser and do not require any additional applications.

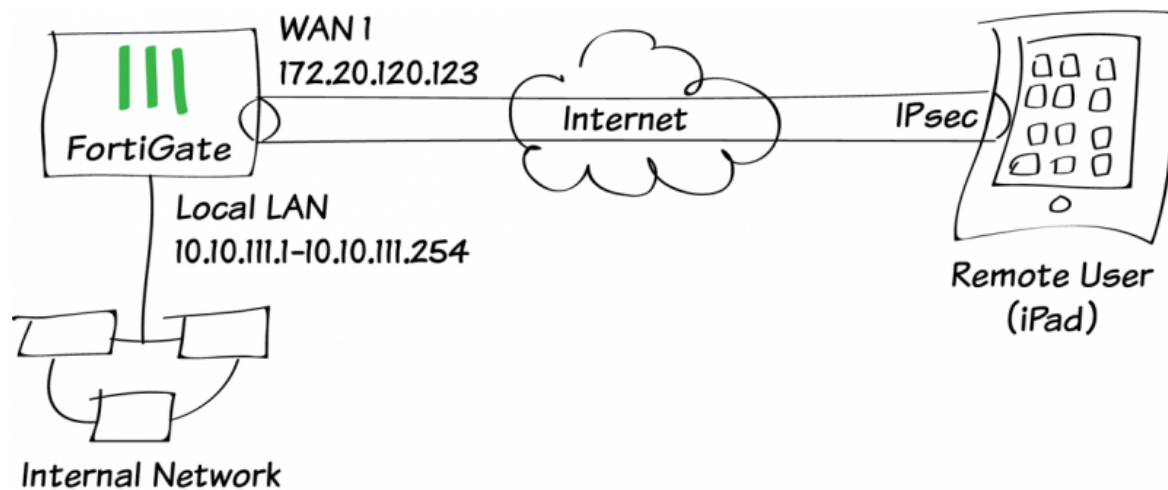
IPsec

- [IPsec VPN for iOS devices](#)
- [IPsec VPN with FortiClient](#)
- [IPsec VPN with the native Mac OS client](#)
- [Site-to-site IPsec VPN with two FortiGates](#)
- [IPsec VPN to Microsoft Azure](#)
- [Remote Internet browsing using a VPN](#)
- [Remote browsing using site-to-site IPsec VPN](#)
- [IPsec troubleshooting](#)

SSL

- [SSL VPN for remote users](#)
- [SSL VPN for Windows Phone 8.1](#)
- [SSL VPN using FortiClient for iOS](#)
- [Remote Internet browsing using a VPN](#)
- [SSL VPN troubleshooting](#)

IPsec VPN for iOS devices



This recipe uses the IPsec VPN Wizard to provide a group of remote iOS users with secure, encrypted access to the corporate network. The tunnel provides group members with access to the internal network, but forces them through the FortiGate unit when accessing the Internet.

This recipe was tested using an iPad 2 running iOS version 7.1.

A video of this recipe can be found [here](#).

1. Creating a user group for iOS users

Go to **User & Device > User > User Definition**.

Create a new user.

The screenshot shows the 'User Definition' dialog box. The 'User Name' field contains 'twhite'. There is a 'Disable' checkbox which is unchecked. Under the 'Password' section, the 'Password' radio button is selected, and the password field contains six dots. Below this, there are three radio buttons for matching user information: 'Match user on LDAP server', 'Match user on RADIUS server', and 'Match user on TACACS+ server'. Each of these has a '[Please Select]' dropdown menu. The 'Contact Info' section has 'Email Address' and 'SMS' checkboxes, both unchecked. There is also an 'Enable Two-factor Authentication' checkbox (unchecked) and an 'Add this user to groups' checkbox (unchecked). At the bottom right, there are 'OK' and 'Cancel' buttons.

Go to **User & Device > User > User Groups**.

Create a user group for iOS users and add the user you created.

The screenshot shows the 'User Groups' dialog box. The 'Name' field contains 'iOS_group'. The 'Type' section has four radio buttons: 'Firewall' (selected), 'Fortinet Single Sign-On (FSSO)', 'Guest', and 'RADIUS Single Sign-On (RSSO)'. The 'Members' field contains 'twhite' with a search icon and a plus sign. Below this is a 'Remote groups' section with 'Add', 'Edit', and 'Delete' icons. A table with columns 'Remote Server' and 'Group Name' is shown, with the message 'No matching entries found' in the center. At the bottom right, there are 'OK' and 'Cancel' buttons.

2. Adding a firewall address for the local network

Go to **Policy & Objects > Objects > Addresses**.

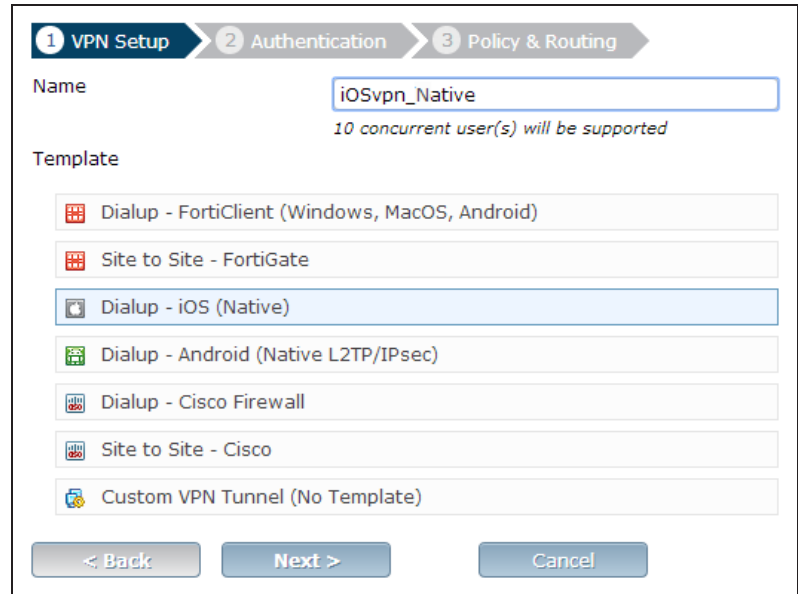
Add a firewall address for the Local LAN, including the subnet and local interface.

The screenshot shows the 'Address' dialog box. The 'Category' section has three radio buttons: 'Address' (selected), 'IPv6 Address', and 'Multicast Address'. The 'Name' field contains 'Local LAN'. The 'Type' field contains 'Subnet'. The 'Subnet / IP Range' field contains '192.168.1.0/255.255.255.0'. The 'Interface' dropdown menu is set to 'port1'. The 'Visibility' checkbox is checked. The 'Comments' field contains 'Write a comment...' and '0/255'. At the bottom right, there are 'OK' and 'Cancel' buttons.

3. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to VPN > IPsec > Wizard.

Name the VPN connection and select **Dial Up - iOS (Native)** and click **Next**.



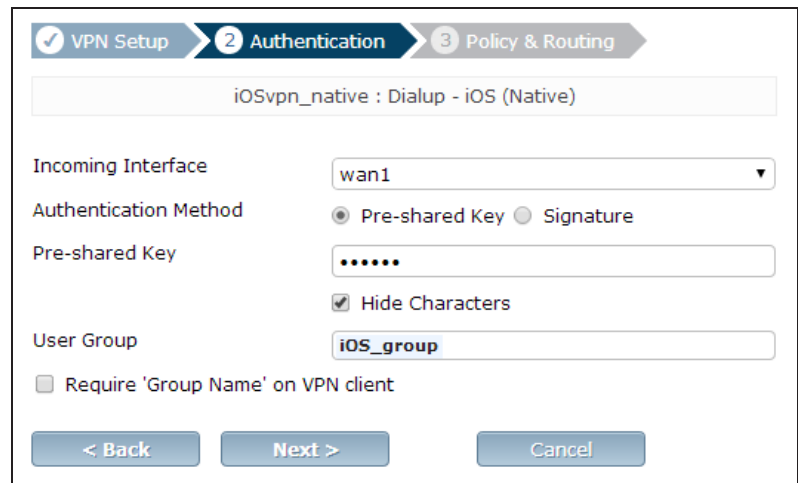
The screenshot shows the first step of the IPsec VPN Wizard, 'VPN Setup'. At the top, there are three progress indicators: '1 VPN Setup' (active), '2 Authentication', and '3 Policy & Routing'. Below this, the 'Name' field contains 'iOSvpn_Native' with a note below it stating '10 concurrent user(s) will be supported'. Under the 'Template' section, a list of templates is shown: 'Dialup - FortiClient (Windows, MacOS, Android)', 'Site to Site - FortiGate', 'Dialup - iOS (Native)' (highlighted in blue), 'Dialup - Android (Native L2TP/IPsec)', 'Dialup - Cisco Firewall', 'Site to Site - Cisco', and 'Custom VPN Tunnel (No Template)'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Set the **Incoming Interface** to the internet-facing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key and select the iOS user group, then click **Next**.

The pre-shared key is a credential for the VPN and should differ from the user's password.



The screenshot shows the second step of the IPsec VPN Wizard, 'Authentication'. The progress indicators at the top are: '1 VPN Setup' (completed), '2 Authentication' (active), and '3 Policy & Routing'. The main area shows the configuration for the selected template: 'iOSvpn_native : Dialup - iOS (Native)'. The 'Incoming Interface' is set to 'wan1'. The 'Authentication Method' is set to 'Pre-shared Key' (selected with a radio button), with 'Signature' as an alternative. The 'Pre-shared Key' field contains six dots, and the 'Hide Characters' checkbox is checked. The 'User Group' is set to 'iOS_group'. There is an unchecked checkbox for 'Require 'Group Name' on VPN client'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Set **Local Interface** to an internal interface (in the example, port 1) and set **Local Address** to the iOS users address.

Enter an IP range for VPN users in the **Client Address Range** field.

*The IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the **_range** suffix (in this case, **iOSvpn_Native_range**).*

In addition, FortiOS automatically creates a security policy to allow remote users to access the internal network.

The screenshot shows the 'Policy & Routing' configuration page for an iOSIPsecVPN. The breadcrumb trail is 'VPN Setup > Authentication > 3 Policy & Routing'. The title is 'iOSIPsecVPN : Dialup - iOS (Native)'. The configuration fields are: Local Interface (port1), Local Address (Local LAN), Client Address Range (10.10.111.1-10.10.111.254), Subnet Mask (255.255.255.255), and DNS Server (Use System DNS selected). There are also checkboxes for 'Specify' and 'Enable IPv4 Split Tunnel'. At the bottom are buttons for '< Back', 'Create', and 'Cancel'.

4. Creating a security policy for access to the Internet

Go to **Policy & Objects > Policy > IPv4**.

Create a security policy allowing remote iOS users to access the Internet securely through the FortiGate unit.

Set **Incoming Interface** to the tunnel interface and set **Source Address** to all.

Set **Outgoing Interface** to wan1 and **Destination Address** to all.

Set **Service** to all and ensure that you enable NAT.

The screenshot shows the Security Policy configuration page. The fields are: Incoming Interface (iOSvpn_Native), Source Address (all), Source User(s) (Click to add...), Source Device Type (Click to add...), Outgoing Interface (wan1), Destination Address (all), Schedule (always), Service (ALL), and Action (ACCEPT). Under 'Firewall / Network Options', NAT is turned ON, and 'Use Destination Interface Address' is selected.

5. Configuring VPN on the iOS device

On the iPad, go to **Settings > General > VPN** and select **Add VPN Configuration**.

Enter the VPN address, user account, and password in their relevant fields. Enter the pre-shared key in the **Secret** field.

The screenshot shows the 'IPsec VPN 5.2' configuration screen on an iPad. At the top, there are 'Cancel' and 'Save' buttons. Below them are three tabs: 'L2TP', 'PPTP', and 'IPSec', with 'IPSec' being the active tab. The Cisco logo is displayed in the center. The configuration fields are as follows:

Field	Value
Description	IPsec VPN 5.2
Server	172.20.120.123
Account	twhite
Password	••••••
Use Certificate	<input type="checkbox"/>
Group Name	
Secret	••••••

At the bottom, there is a 'PROXY' section with three buttons: 'Off', 'Manual', and 'Auto', with 'Off' being the selected option.

6. Results

On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and view the status of the tunnel.

Name	Type	Remote Gatew...	Userna...	Stat...	Incoming D...	Outgoing Data	Phase 2 Proposal
iOSvpn_Native_0	Dialup	172.20.120.16		Up	9.22 K	3.48 K	iOSvpn_Native

Users on the internal network will be accessible using the iOS device.

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

Select an entry to view more information.

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received
1	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	59 B / 221 B
2	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	60 B / 292 B
3	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	56 B / 288 B
4	11:21:42	port1		192.168.1.117	208.91.113.70	304 B / 304 B



Dst	192.168.1.114	Virtual Domain	root
Received	72	Source Country	Reserved
Sent / Received	72 B / 72 B	Duration	63
Sent	72	Application Details	
Service	PING	Protocol	1
Destination Country	Reserved	roll	65428
Status	✓	Timestamp	Thu Feb 21 11:20:44 2014
Tran Display	noop	Sequence Number	220067
Policy ID	6	Src Interface	iOSvpn
Src	10.10.111.16	VPN	iOSvpn_Native
Sent Packets	2	Level	notice
VPN Type	ipsec-dynamic	logid	13
Sub Type	forward	Threat	
Received Packets	2	Date/Time	11:20:44 (Thu Feb 21 11:20:44 2014)
Dst Interface	port1		

Remote iOS users can also access the Internet securely via the FortiGate unit.

Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received
1	11:28:43	ios_P1	wan1	10.10.111.16	74.121.50.17	1023 B / 579 B
2	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	59 B / 221 B
3	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	60 B / 292 B
4	11:22:41	iOSvpn_Native	wan1	10.10.111.16	208.91.112.53	56 B / 288 B
5	11:20:42	iOSvpn_Native	wan1	10.10.111.16	173.194.73.105	812 B / 642 B
6	11:20:42	iOSvpn_Native	wan1	10.10.111.16	74.125.134.102	808 B / 712 B
7	11:20:42	iOSvpn_Native	wan1	10.10.111.16	173.194.73.94	2.96 KB / 23.07 KB
8	11:20:35	iOSvpn_Native	wan1	10.10.111.16	17.149.36.134	104 B / 60 B
9	11:19:15	iOSvpn_Native	wan1	10.10.111.16	204.93.33.67	813 B / 365 B

Select an entry to view more information.

Dst	 74.121.50.17	Virtual Domain	root
Received	579	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	1023 B / 579 B
Duration	2	Sent	1023
Src NAT Port	50189	Application Details	
Service	HTTP	Protocol	6
Destination Country	United States	Dst Port	80
roll	65428	Status	close
Timestamp	Thu Feb 21 11:28:43 2014	Tran Display	snat
Sequence Number	221594	Policy ID	7
Src Interface	iOSvpn_Native	Src	10.10.111.16
VPN	iOSvpn	Sent Packets	6
Level	notice 	VPN Type	ipsec-dynamic
Src Port	50189	logid	13
Sub Type	forward	Threat	
Received Packets	4	Date/Time	11:28:43 (Thu Feb 21 11:28:43 2014)
Dst Interface	wan1		

You can also view the status of the tunnel on the iOS device itself.

On the device, go to **Settings > VPN > Status** and view the status of the connection.

Server	172.20.120.123
Connect Time	9:48
Connected to	172.20.120.82
IP Address	10.10.111.1

Lastly, using a Ping tool, you can send a ping packet from the iOS device directly to an IP address on the LAN behind the FortiGate unit to verify the connection through the VPN tunnel.

IP Address to ping: Start Clear

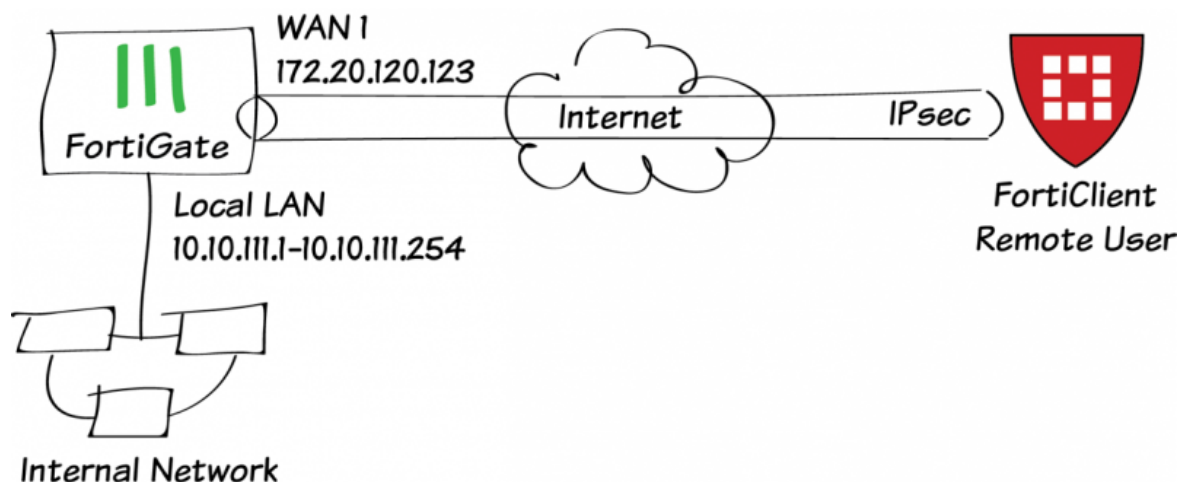
Delay: 2000 ms

Result:

```
PING 172.20.120.123 (172.20.120.123)
36 bytes from 172.20.120.123: icmp_seq=0 ttl=254 time=12 ms
36 bytes from 172.20.120.123: icmp_seq=1 ttl=254 time=5 ms
36 bytes from 172.20.120.123: icmp_seq=2 ttl=254 time=10 ms
36 bytes from 172.20.120.123: icmp_seq=3 ttl=254 time=10 ms
--- 172.20.120.123 ping statistics ---
4 packets transmitted, 4 packets received, lost 0.0 %
```

For further reading, check out [FortiGate dialup-client configurations](#) in the [FortiOS 5.2 Handbook](#).

IPsec VPN with FortiClient



This recipe uses the IPsec VPN Wizard to provide a group of remote users with secure, encrypted access to the corporate network.

The tunnel provides group members with access to the internal network, but forces them through the FortiGate unit when accessing the Internet. When the tunnel is configured, you will connect using the FortiClient application.

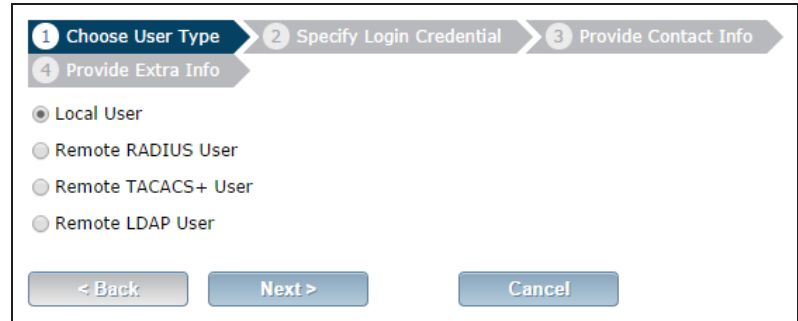
A video of this recipe is available [here](#).

1. Creating a user group for remote users

Go to **User & Device > User > User Definition**.

Create a new **Local User** with the **User Creation Wizard**.

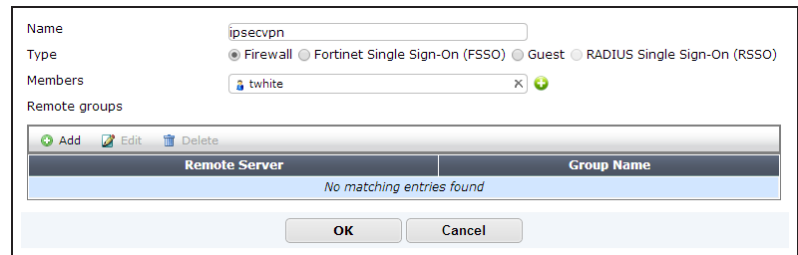
Proceed through each step of the wizard, carefully entering the appropriate information.



The screenshot shows the first step of the User Creation Wizard, titled "Choose User Type". It features a progress bar at the top with four steps: "1 Choose User Type" (highlighted), "2 Specify Login Credential", "3 Provide Contact Info", and "4 Provide Extra Info". Below the progress bar, there are four radio button options: "Local User" (selected), "Remote RADIUS User", "Remote TACACS+ User", and "Remote LDAP User". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

Go to **User & Device > User > User Groups**.

Create a user group for remote users and add the user you created.

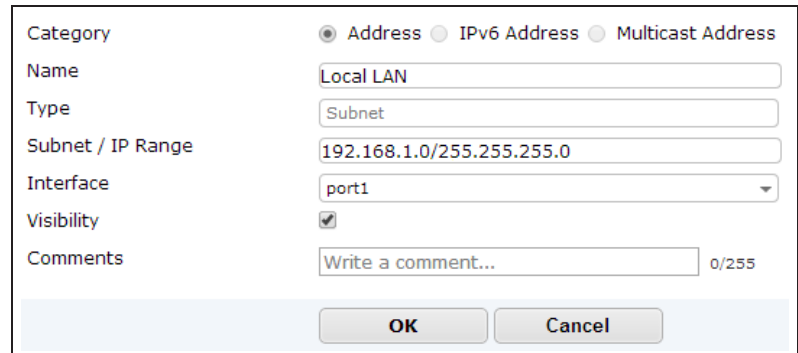


The screenshot shows the "User Group Configuration" dialog box. The "Name" field is set to "ipsecpvn". The "Type" field has radio buttons for "Firewall" (selected), "Fortinet Single Sign-On (FSSO)", "Guest", and "RADIUS Single Sign-On (RSSO)". The "Members" field contains "twhite" with a search icon and a plus sign. Below this is a "Remote groups" section with "Add", "Edit", and "Delete" icons. A table with columns "Remote Server" and "Group Name" is shown, with the message "No matching entries found" below it. At the bottom, there are "OK" and "Cancel" buttons.

2. Adding a firewall address for the local network

Go to **Policy & Objects > Objects > Addresses**.

Add a firewall address for the Local LAN, including the subnet and local interface.



The screenshot shows the "Address Configuration" dialog box. The "Category" field has radio buttons for "Address" (selected), "IPv6 Address", and "Multicast Address". The "Name" field is set to "Local LAN". The "Type" field is set to "Subnet". The "Subnet / IP Range" field is set to "192.168.1.0/255.255.255.0". The "Interface" field is set to "port1". The "Visibility" field has a checked checkbox. The "Comments" field is empty, with a character count of "0/255". At the bottom, there are "OK" and "Cancel" buttons.

3. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to VPN > IPsec > Wizard.

Name the VPN connection and select **Dial Up - FortiClient (Windows, Mac OS, Android)** and click Next.

The tunnel name may not have any spaces in it.

1 VPN Setup 2 Authentication 3 Policy & Routing 4 Client Options

Name: ipsecvpn

Template:

- Dialup - FortiClient (Windows, Mac OS, Android)
- Site to Site - FortiGate
- Dialup - iOS (Native)
- Dialup - Android (Native L2TP/IPsec)
- Dialup - Cisco Firewall
- Site to Site - Cisco
- Custom VPN Tunnel (No Template)

< Back Next > Cancel

Set the **Incoming Interface** to the internet-facing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key and select the new user group, then click **Next**.

The pre-shared key is a credential for the VPN and should differ from the user's password.

1 VPN Setup 2 Authentication 3 Policy & Routing 4 Client Options

FortiClient VPN : Dialup - FortiClient (Windows, Mac OS, Android)

Incoming Interface: wan1

Authentication Method: Pre-shared Key Signature

Pre-shared Key:

Hide Characters

User Group: ipsecvpn

< Back Next > Cancel

Set **Local Interface** to an internal interface (in the example, port 1) and set **Local Address** to the local LAN address.

Enter an IP range for VPN users in the **Client Address Range** field.

The IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the _range suffix (in this case, ipsecvpn_range).

In addition, FortiOS automatically creates a security policy to allow remote users to access the internal network.

Click **Next** and select **Client Options** as desired.

The screenshot shows the 'Policy & Routing' configuration page for a FortiClient VPN. The breadcrumb trail at the top indicates the steps: VPN Setup (checked), Authentication (checked), Policy & Routing (active), and Client Options. The configuration fields are as follows:

- Local Interface: port1
- Local Address: Local LAN
- Client Address Range: 10.10.112.1-10.10.112.254
- Subnet Mask: 255.255.255.255
- DNS Server: Use System DNS, Specify
- Enable IPv4 Split Tunnel:
- Allow Endpoint Registration:

Buttons at the bottom include '< Back', 'Next >', and 'Cancel'.

The screenshot shows the 'Client Options' configuration page for a FortiClient VPN. The breadcrumb trail at the top indicates the steps: VPN Setup (checked), Authentication (checked), Policy & Routing (checked), and Client Options (active). The configuration fields are as follows:

- Save Password:
- Auto Connect:
- Always Up (Keep Alive):

Buttons at the bottom include '< Back', 'Create', and 'Cancel'.

4. Creating a security policy for access to the Internet

Go to **Policy & Objects > Policy > IPv4**.

Create a security policy allowing remote users to access the Internet securely through the FortiGate unit.

Set **Incoming Interface** to the tunnel interface and set **Source Address** to **all**. Set **Outgoing Interface** to **wan1** and **Destination Address** to **all**.

Set **Service** to **ALL** and ensure that you enable **NAT**.

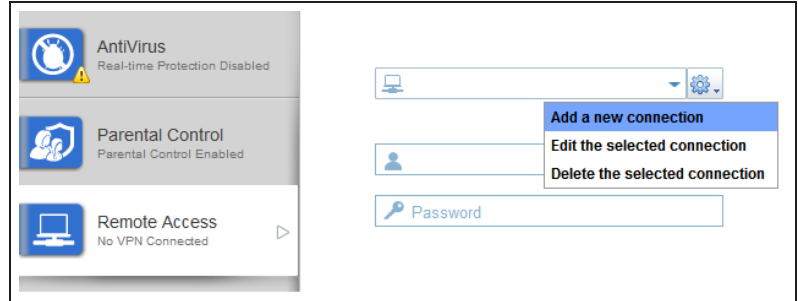
The screenshot shows the 'Policy' configuration page for an IPv4 policy. The configuration fields are as follows:

- Incoming Interface: ipsecvpn
- Source Address: FortiClient VPN_range
- Source User(s): Click to add...
- Source Device Type: Click to add...
- Outgoing Interface: port1
- Destination Address: Local LAN
- Schedule: always
- Service: ALL
- Action: ACCEPT

Under 'Firewall / Network Options', the 'ON' checkbox for NAT is checked.

5. Configuring FortiClient

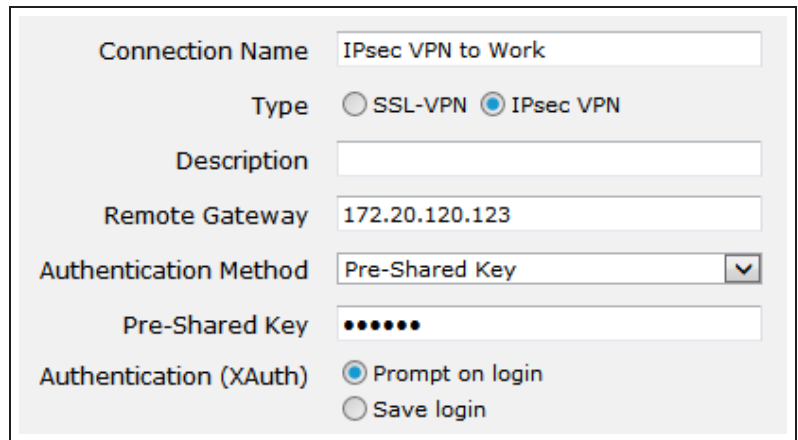
Open FortiClient, go to **Remote Access** and **Add a new connection**.



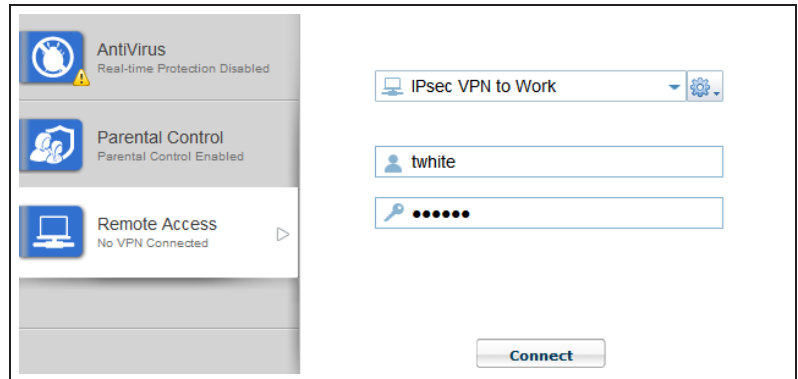
Provide a **Connection Name** and set the **Type** to IPsec VPN.

Set **Remote Gateway** to the FortiGate IP address.

Set **Authentication Method** to **Pre-Shared Key** and enter the key below.

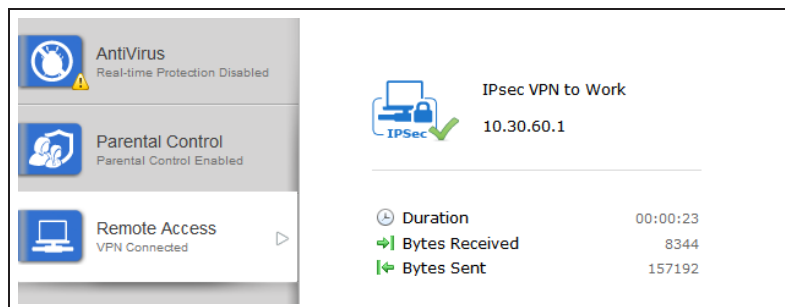


Select the new connection, enter the username and password, and click **Connect**.



6. Results

Once the connection is established, the FortiGate assigns the user an IP address and FortiClient displays the status of the connection, including the IP address, connection duration, and bytes sent and received.



The screenshot shows the FortiClient interface with three status cards on the left: 'AntiVirus' (Real-time Protection Disabled), 'Parental Control' (Parental Control Enabled), and 'Remote Access' (VPN Connected). On the right, the 'IPsec VPN to Work' connection is shown with the IP address 10.30.60.1. Below this, connection statistics are displayed: Duration (00:00:23), Bytes Received (8344), and Bytes Sent (157192).

On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and verify that the tunnel **Status** is **Up**.

Name	Type	Remote Gateway	Status	Incoming Data	Outgoing Data
ipsec_0	Dialup	172.20.120.16	Up	9.22 K	3.48 K

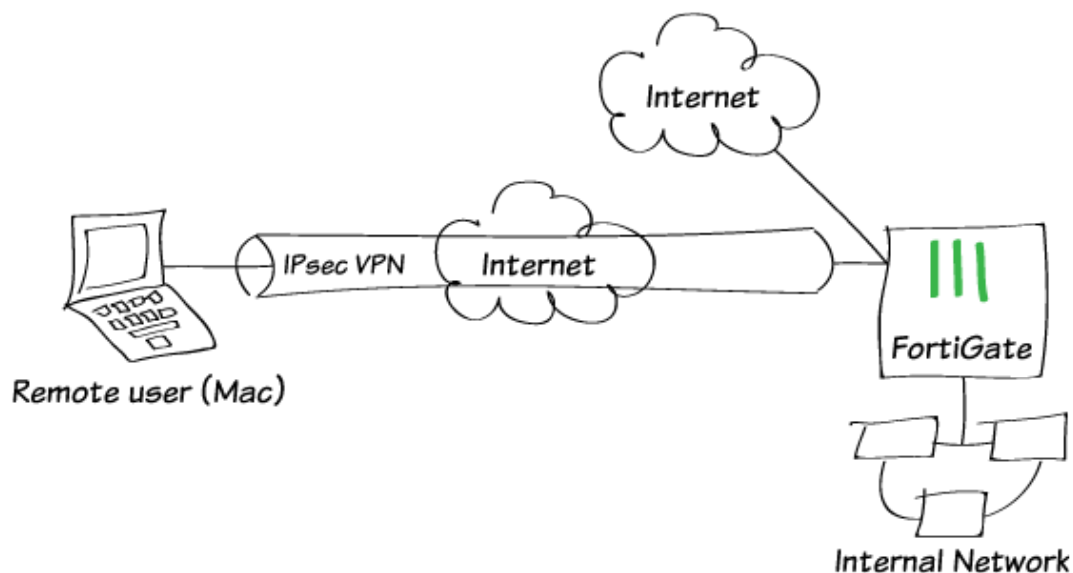
Go to **Log & Report > Traffic Log > Forward Traffic** to view the traffic.

#	Date/Time	Src Interface	Dst Interface	Src	Dst	Sent / Received
1	11:22:41	ipsecvpn	wan1	10.10.111.16	208.91.112.53	59 B / 221 B
2	11:22:41	ipsecvpn	wan1	10.10.111.16	208.91.112.53	60 B / 292 B
3	11:22:41	ipsecvpn	wan1	10.10.111.16	208.91.112.53	56 B / 288 B

Verify that the **Sent/Received** column displays traffic successfully flowing through the tunnel.

For further reading, check out [IPsec VPN in the web-based manager](#) in the [FortiOS 5.2 Handbook](#).

IPsec VPN with the native Mac OS client



In this recipe, you will learn how to create an IPsec VPN on a FortiGate, and connect to it using the default client built into the Mac OS.

This VPN configuration allows Mac users to securely access an internal network as well as browse the Internet through the VPN tunnel.

The recipe assumes that a "mac_users" user group and a Local LAN firewall address have been created.

This recipe was tested using Mac OS 10.10.2 (Yosemite).

1. Configuring the IPsec VPN using the IPsec VPN Wizard

Go to **VPN > IPsec > Wizard**.

Name the VPN connection and select **Dial Up - Cisco Firewall** and click **Next**.

The native Mac OS client is a Cisco client, which is why you select Dialup - Cisco Firewall in the VPN Wizard.

The screenshot shows the first step of the IPsec VPN Wizard, 'VPN Setup'. At the top, there are three progress indicators: '1 VPN Setup' (active), '2 Authentication', and '3 Policy & Routing'. Below this, the 'Name' field contains 'NativeMac'. Under the 'Template' section, a list of options is shown: 'Dialup - FortiClient (Windows, Mac OS, Android)', 'Site to Site - FortiGate', 'Dialup - iOS (Native)', 'Dialup - Android (Native L2TP/IPsec)', 'Dialup - Cisco Firewall' (highlighted in blue), 'Site to Site - Cisco', and 'Custom VPN Tunnel (No Template)'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Set the **Incoming Interface** to the internet-facing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key, select the appropriate **User Group**, then click **Next**.

The screenshot shows the second step of the IPsec VPN Wizard, 'Authentication'. The progress indicators at the top are: '1 VPN Setup' (checked), '2 Authentication' (active), and '3 Policy & Routing'. Below this, the title 'NativeMac : Dialup - Cisco Firewall' is displayed. The 'Incoming Interface' dropdown is set to 'wan1'. The 'Authentication Method' section has 'Pre-shared Key' selected with a radio button, and 'Signature' is unselected. The 'Pre-shared Key' field contains six dots, and the 'Hide Characters' checkbox is checked. The 'User Group' dropdown is set to 'mac_users'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Set **Local Interface** to an internal interface and set **Local Address** to the local LAN address.

Enter an IP address range for VPN users in the **Client Address Range** field then click **Next**.

The IPsec VPN Wizard finishes with a summary of created objects.

Go to **Policy & Objects > Objects > Addresses** and confirm that the wizard has created the IPsec VPN firewall address range.

Name	Type	Details	Interface	Visibility	Ref.	⚙
Address (16)						
Gotomeeting	FQDN	*.gotomeeting.com	Any	✓	1	
Internal	Subnet	192.168.1.0/24	internal1	✓	1	
NativeMac_range	IP Range	10.10.10.1 - 10.10.10.100	Any	✓	1	
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	Any	✓	2	
all	Subnet	0.0.0.0/0	Any	✓	2	

Go to **Policy & Objects > Policy > IPv4** and confirm that the wizard has created the policy from the VPN tunnel interface to the internal interface.

Seq.#	Source	Destination	Schedule	Service	Action	NAT
▶ internal1 (Local LAN) - wan1 (1 - 1)						
▼ NativeMac - internal1 (Local LAN) (2 - 2)						
2	NativeMac_range	Internal	always	ALL	ACCEPT	Enable
▶ Implicit (3 - 3)						

2. Creating a security policy for remote access to the Internet

Under **Policy & Objects > Policy > IPv4**, create a security policy

allowing remote users to access the Internet securely through the FortiGate unit.

Set **Incoming Interface** to the tunnel interface and set **Source Address** to **all**.

Set **Outgoing Interface** to the Internet-facing interface and **Destination Address** to **all**.

Set **Service** to **ALL** and enable **NAT**.

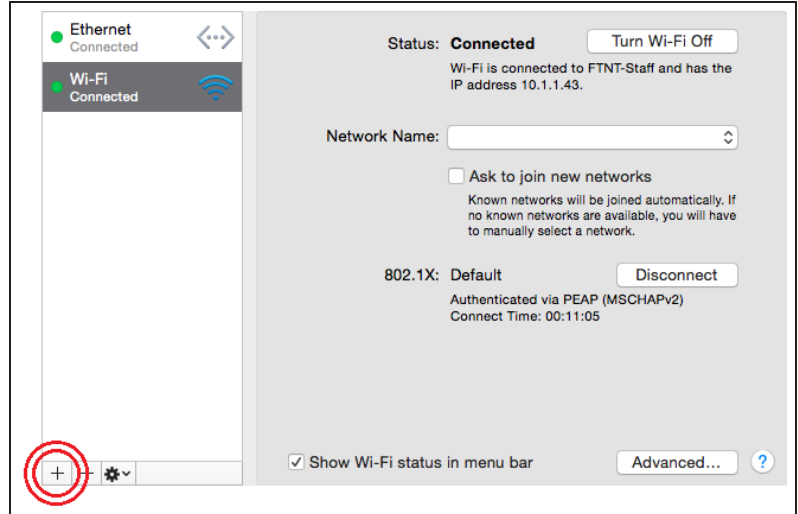
Incoming Interface	NativeMac	+
Source Address	all	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	wan1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	
Firewall / Network Options		
<input checked="" type="checkbox"/> NAT		
<input checked="" type="radio"/> Use Outgoing Interface Address	<input type="checkbox"/> Fixed Port	
<input type="radio"/> Use Dynamic IP Pool	Click to add...	

The policy should appear in the policy list at **Policy & Objects > Policy > IPv4**.

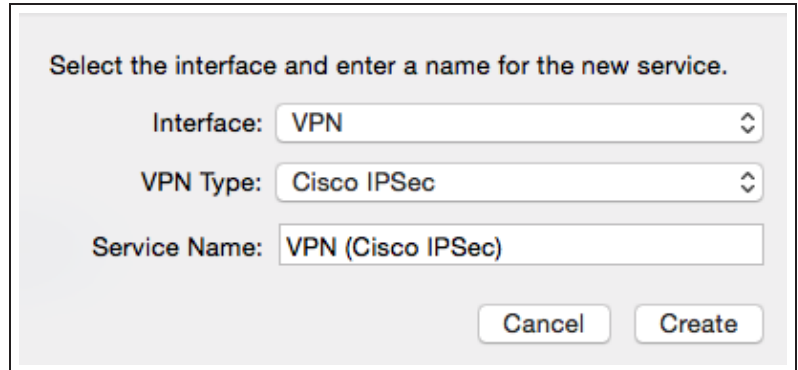
Seq.#	Source	Destination	Schedule	Service	Action	NAT
▶ internal1 (Local LAN) - wan1 (1 - 1)						
▼ NativeMac - internal1 (Local LAN) (2 - 2)						
2	NativeMac_range	Internal	always	ALL	ACCEPT	Enable
▼ NativeMac - wan1 (3 - 3)						
3	all	all	always	ALL	ACCEPT	Enable
▶ Implicit (4 - 4)						

3. Connecting to the IPsec VPN using the native Mac client

On the Mac, go to **System Preferences** > **Network** and click the **Plus (+)** button.



Set **Interface** to **VPN**, set **VPN Type** to **Cisco IPsec**, and click **Create**.



Set the **Server Address** to the FortiGate IP address, configure the network account details for the remote user, then click **Authentication Settings**.

The screenshot shows a VPN configuration window. On the left, there is a status bar with three items: 'Ethernet Connected' with a green dot and a bidirectional arrow icon, 'Wi-Fi Connected' with a green dot and a Wi-Fi signal icon, and 'VPN (C...IPSec) Not Configured' with a red dot and a padlock icon. Below this is a large empty white area. At the bottom left of this area are three small icons: a plus sign, a minus sign, and a gear icon with a downward arrow. On the right side of the window, the status is 'Not Configured'. Below this, there are three input fields: 'Server Address' with the value '172.20.120.82', 'Account Name' with the value 'ckent', and 'Password' with six dots. Below the password field is a button labeled 'Authentication Settings...'. Below that is a 'Connect' button. At the bottom right, there is a checkbox labeled 'Show VPN status in menu bar' which is unchecked, and an 'Advanced...' button with a question mark icon.

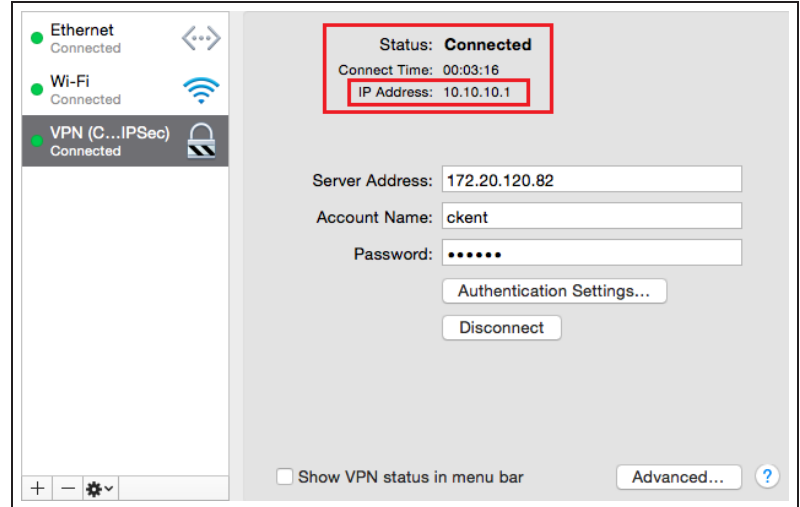
Select **Shared Secret** and enter the pre-shared key you created **above**, then click **OK**.

The screenshot shows a 'Machine Authentication' dialog box. It has a title 'Machine Authentication:'. Below the title are two radio buttons. The first is 'Shared Secret' with a selected radio button and a text input field containing six dots. The second is 'Certificate' with an unselected radio button and a 'Select...' button. Below these is a 'Group Name:' label followed by an empty text input field. At the bottom right are two buttons: 'Cancel' and 'OK'.

4. Results

On the Mac, ensure that the VPN is selected and click **Connect**. The **Status** should change to **Connected** and you should be given an **IP Address** in the range specified [above](#).

You should also be able to browse the Internet, protected by whichever profiles you applied to the security policy created in [the above step](#).

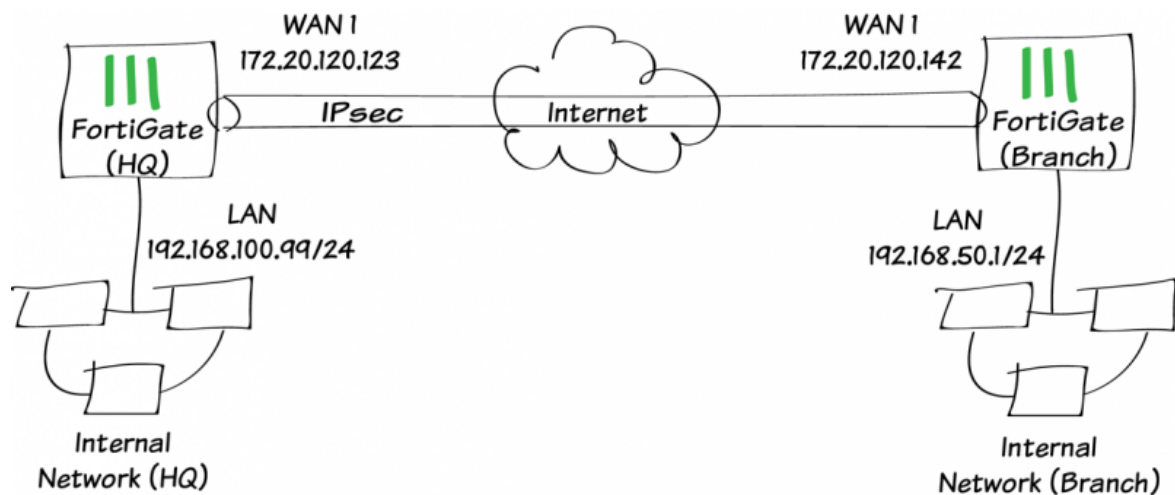


On the FortiGate unit, go to **VPN > Monitor > IPsec Monitor** and verify that the tunnel **Status** is **Up**, and that there are **Incoming** and **Outgoing Data**.

Name	Type	Remote Gateway	Username	Status	Incoming Data	Outgoing
NativeMac_0	Dialup - Cisco Firewall	172.20.120.221		Up	862.49 KB	2.06 MB

For further reading, check out [IPsec VPN in the web-based manager](#) in the [FortiOS 5.2 Handbook](#).

Site-to-site IPsec VPN with two FortiGates



In this example, you will allow transparent communication between two networks that are located behind different FortiGates at different offices using route-based IPsec VPN. The VPN will be created on both FortiGates by using the VPN Wizard's **Site to Site FortiGate** template.

In this example, one office will be referred to as HQ and the other will be referred to as Branch.

1. Configuring the HQ IPsec VPN

On the HQ FortiGate, go to **VPN > IPsec > Wizard** and select **Site to Site - FortiGate**.

1 VPN Setup 2 Authentication 3 Policy & Routing

Name

Template

- Dialup - FortiClient (Windows, Mac OS, Android)
- Site to Site - FortiGate
- Dialup - iOS (Native)
- Dialup - Android (Native L2TP/IPsec)
- Dialup - Cisco Firewall
- Site to Site - Cisco
- Custom VPN Tunnel (No Template)

< Back Next > Cancel

In the **Authentication** step, set the Branch FortiGate's IP as the **Remote Gateway** (in the example, *172.20.120.142*). After you enter the gateway, an available interface will be assigned as the **Outgoing Interface**. If you wish to use a different interface, select **Change**.

Set a secure **Pre-shared Key**

VPN Setup 2 Authentication 3 Policy & Routing

HQ-to-Branch : Site to Site - FortiGate

Remote Gateway

Outgoing Interface wan1 (Detected via routing lookup) [Change]

Authentication Method Pre-shared Key Signature

Pre-shared Key

Hide Characters

< Back Next > Cancel

In the **Policy & Routing** section, set **Local Interface** to your **lan** interface. The **Local Subnet** will be added automatically. Set **Remote Subnets** to the Branch FortiGate's local subnet (in the example, *192.168.50.0/24*).

VPN Setup > Authentication > 3 Policy & Routing

HQ-to-Branch : Site to Site - FortiGate

Local Interface: lan

Local Subnets: 192.168.100.0/24

Remote Subnets: 192.168.50.0/24

< Back Create Cancel

A summary page shows the configuration created by the wizard, including firewall addresses, firewall address groups, a static route, and security policies.

✔ The VPN has been set up

Summary of Created Objects

Phase 1 Interface	<i>HQ-to-Branch</i>
Phase 2 Interfaces	<i>HQ-to-Branch</i>
Static Routes	<i>192.168.50.0/24</i>
Local Address Group	<i>HQ-to-Branch_local</i>
Remote Address Group	<i>HQ-to-Branch_remote</i>
Local to Remote Policy	<i>2</i>
Remote to Local Policy	<i>3</i>

2. Configuring the Branch IPsec VPN

On the Branch FortiGate, go to **VPN > IPsec > Wizard** and select **Site to Site - FortiGate**.

1 VPN Setup 2 Authentication 3 Policy & Routing

Name

Template

- Dialup - FortiClient (Windows, Mac OS, Android)
- Site to Site - FortiGate
- Dialup - iOS (Native)
- Dialup - Android (Native L2TP/IPsec)
- Dialup - Cisco Firewall
- Site to Site - Cisco
- Custom VPN Tunnel (No Template)

< Back Next > Cancel

In the **Authentication** step, set the HQ FortiGate's IP as the **Remote Gateway** (in the example, *172.20.120.123*). After you enter the gateway, an available interface will be assigned as the **Outgoing Interface**. If you wish to use a different interface, select **Change**.

Set the same **Pre-shared Key** that was used for HQ's VPN.

1 VPN Setup 2 Authentication 3 Policy & Routing

Branch-to-HQ : Site to Site - FortiGate

Remote Gateway

Outgoing Interface wan1 (Detected via routing lookup) [\[Change\]](#)

Authentication Method Pre-shared Key Signature

Pre-shared Key

Hide Characters

< Back Next > Cancel

In the **Policy & Routing** section, set **Local Interface** to your **lan** interface. The **Local Subnet** will be added automatically. Set **Remote Subnets** to the HQ FortiGate's local subnet (in the example, *192.168.100.0/24*).

A summary page shows the configuration created by the wizard, including firewall addresses, firewall address groups, a static route, and security policies.

✔ The VPN has been set up

Summary of Created Objects

Phase 1 Interface	<i>Branch-to-HQ</i>
Phase 2 Interfaces	<i>Branch-to-HQ</i>
Static Routes	<i>192.168.100.0/24</i>
Local Address Group	<i>Branch-to-HQ_local</i>
Remote Address Group	<i>Branch-to-HQ_remote</i>
Local to Remote Policy	<i>1</i>
Remote to Local Policy	<i>2</i>

3. Results

A user on either of the office networks should be able to connect to any address on the other office network transparently.

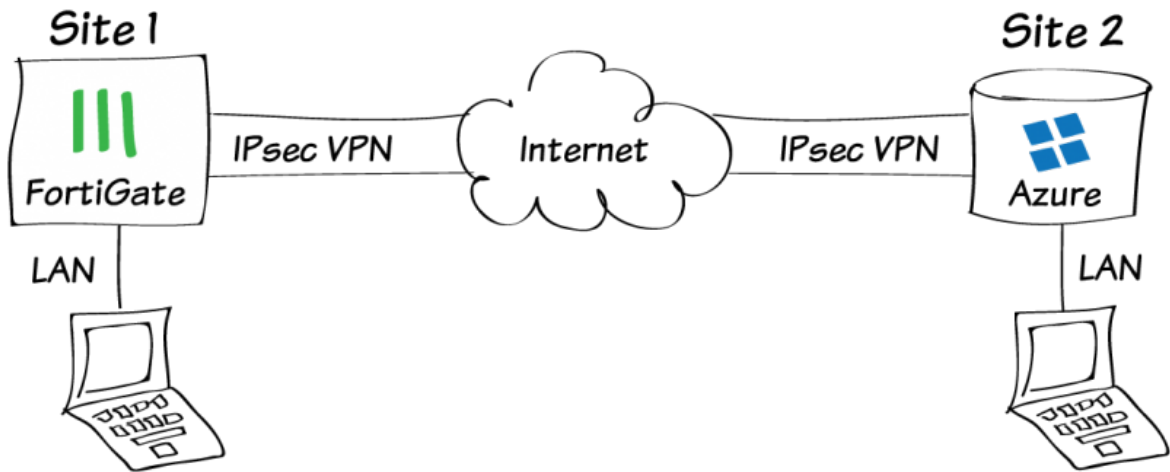
If you need to generate traffic to test the connection, ping the Branch FortiGate's internal interface from the HQ's internal network.

Go to **VPN > Monitor > IPsec Monitor** to verify the status of the VPN tunnel. Ensure that its **Status** is **Up** and that traffic is flowing.

Name	Type	Remote Gateway	Status	Incoming Data	Outgoing Data
Branch-to-HQ	Site to Site - FortiGate	172.20.120.236	Up	1.63 KB	1.56 KB

For further reading, check out [Gateway-to-gateway configurations](#) in the [FortiOS 5.2 Handbook](#).

IPsec VPN to Microsoft Azure



The following recipe describes how to configure a site-to-site IPsec VPN tunnel. In this example, one site is behind a FortiGate and another site is hosted on Microsoft Azure™, for which you will need a valid Microsoft Azure profile.

Using FortiOS 5.2, the example demonstrates how to configure the tunnel between each site, avoiding overlapping subnets, so that a secure tunnel can be established with the desired security profiles applied.

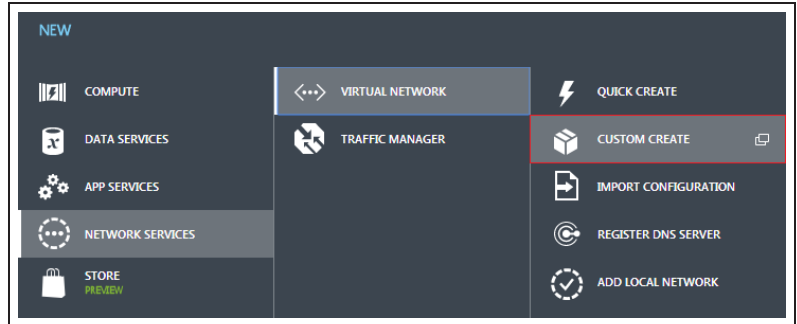
A video of this recipe is available [here](#).

1. Configuring the Microsoft Azure™ virtual network

Log into Microsoft Azure and click New in the lower-left corner to add a new service.



From the prompt, select **Network Services > Virtual Network > Custom Create**.



Under 'Virtual Network Details', enter a **Name** for the VPN and a **Location** where you want the VMs to reside, then click the **Next** arrow.

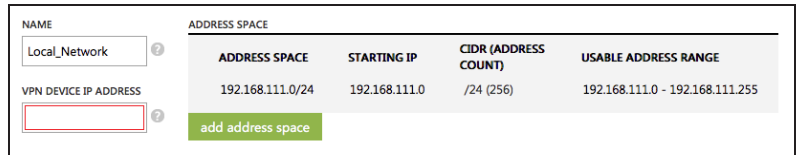
A screenshot of the 'Virtual Network Details' form. It has two input fields: 'NAME' with the value 'Site2SiteVPN' and 'LOCATION' with a dropdown menu set to 'East US'.

Under 'DNS Servers and VPN Connectivity', enable the **Configure a site-to-site VPN** checkbox and enter DNS server information if required.

A screenshot of the 'DNS Servers and VPN Connectivity' section. It features a table for 'DNS SERVERS' with columns for 'ENTER NAME' and 'IP ADDRESS'. To the right, there are two sections: 'POINT-TO-SITE CONNECTIVITY' with a checkbox for 'Configure a point-to-site VPN' (unchecked), and 'SITE-TO-SITE CONNECTIVITY' with a checkbox for 'Configure a site-to-site VPN' (checked) and a checkbox for 'Use ExpressRoute' (unchecked).

Click the **Next** arrow.

Under 'Site-to-Site Connectivity', enter a **Name** and **IP Address** for the FortiGate device.

A screenshot of the 'Site-to-Site Connectivity' section. It shows a table with columns for 'NAME', 'ADDRESS SPACE', 'STARTING IP', 'CIDR (ADDRESS COUNT)', and 'USABLE ADDRESS RANGE'. The 'NAME' field contains 'Local_Network'. The 'ADDRESS SPACE' field contains '192.168.111.0/24'. The 'STARTING IP' field contains '192.168.111.0'. The 'CIDR (ADDRESS COUNT)' field contains '/24 (256)'. The 'USABLE ADDRESS RANGE' field contains '192.168.111.0 - 192.168.111.255'. Below the table, there is a red-bordered input field for 'VPN DEVICE IP ADDRESS' and a green 'add address space' button.

Under Address Space, include a **Starting IP** and **CIDR (Address Count)** for the tunnel, avoiding overlapping subnets.

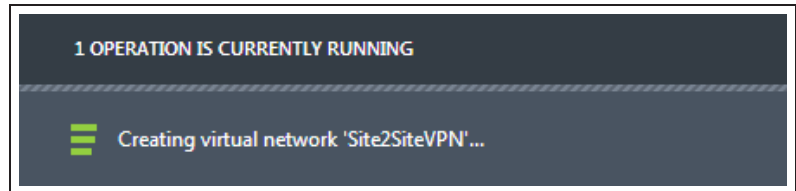
Click the **Next** arrow.

Under 'Virtual Network Address Spaces', configure the desired address space or accept the default settings.

Select **add gateway subnet** to configure a gateway IP and click the Checkmark in the lower-right corner to accept the configuration.

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
10.0.0.0/8	10.0.0.0	/8 (16777...	10.0.0.4 - 10.255.255.254
SUBNETS			
Subnet-1	10.11.12.0	/24 (251)	10.11.12.4 - 10.11.12.254
Gateway	10.11.13.0	/29 (3)	10.11.13.4 - 10.11.13.6
add subnet	add gateway subnet		

After accepting the configuration, you will have to wait a short period of time for the virtual network to be created, but it shouldn't be long.

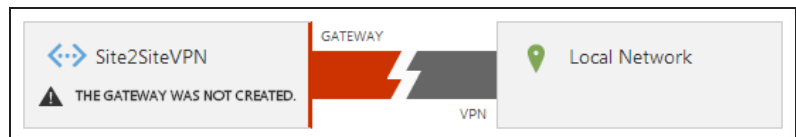


2. Creating the Microsoft Azure™ virtual network gateway

On the 'networks' home screen, click the name of the virtual network you just created.

NAME	STATUS
Site2SiteVPN →	✓ Created

Under this virtual network, go to the **Dashboard**. You will notice that the gateway has not yet been created. You will create the gateway in this step.

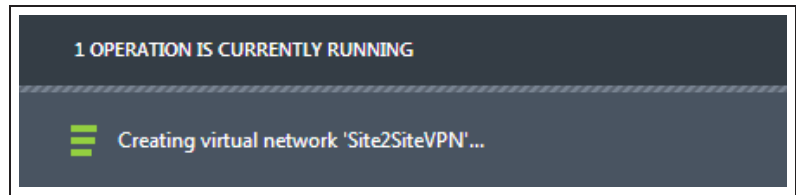


At the bottom of the screen, select **Create Gateway > Dynamic Routing**.

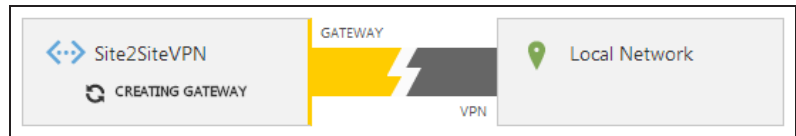
When prompted, select **Yes**.



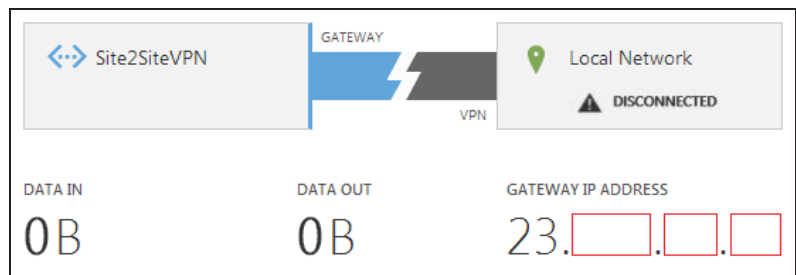
The operation to create the virtual network gateway will run. The process takes a short amount of time.



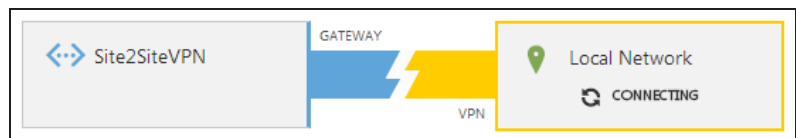
Azure will indicate to you that the gateway is being created. You may wish to leave this running for a few minutes as wait periods in excess of 10 minutes are common.



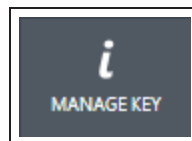
When the operation is complete, the status changes and you are given a **Gateway IP Address**.



The gateway will then attempt to connect to the Local Network.

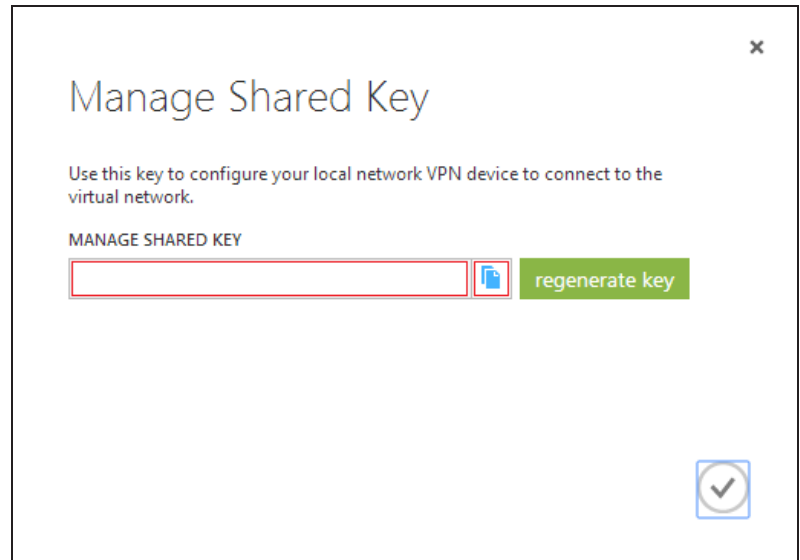


At the bottom of the screen, select **Manage Key**.



The 'Manage Shared Key' dialogue appears. **Copy** the key that is shown. You can select **regenerate key** if you want to copy a different key.

Click the **Checkmark** when you are confident that the key is copied.



You are now ready to configure the FortiGate endpoint of the tunnel.

3. Configuring the FortiGate tunnel

Go to **VPN > IPsec > Wizard** and select **Custom VPN Tunnel (No Template)**.

Enter a **Name** for the tunnel and click **Next**.



Enter the desired parameters. Set the **Remote Gateway** to **Static IP Address**, and include the gateway **IP Address** provided by Microsoft Azure.

Set the **Local Interface** to **wan1**.

Under **Authentication**, enter the **Pre-shared Key** provided by Microsoft Azure.

Disable **NAT Traversal** and **Dead Peer Detection**.

Under **Authentication**, ensure that you enable **IKEv2** and set **DH Group** to **2**.

Enable the encryption types shown and set the **Keylife** to **56660** seconds.

The screenshot shows the configuration page for a Site2Site VPN tunnel. The Name is 'Site2Site' and the Enable IPsec Interface Mode checkbox is checked. Under the Network section, the IP Version is set to IPv4, the Remote Gateway is 'Static IP Address', the Local Interface is 'wan1', and the Mode Config, NAT Traversal, and Dead Peer Detection checkboxes are all disabled.

Name	Site2Site
Comments	Comments
Enable IPsec Interface Mode	<input checked="" type="checkbox"/>
Network	
IP Version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Remote Gateway	Static IP Address
IP Address	
Local Interface	wan1
Mode Config	<input type="checkbox"/>
NAT Traversal	<input type="checkbox"/>
Dead Peer Detection	<input type="checkbox"/>

The screenshot shows the Authentication and Phase 1 Proposal configuration page. The Method is 'Pre-shared Key' and the Pre-shared Key is masked with dots. The IKE Version is set to 2. Under the Phase 1 Proposal section, there are four proposals with encryption and authentication settings. The Diffie-Hellman Group is set to 2, and the Key Lifetime is 56660 seconds.

Authentication				
Method	Pre-shared Key			
Pre-shared Key <input type="checkbox"/> Show Key			
IKE				
Version	<input type="radio"/> 1 <input checked="" type="radio"/> 2			
Phase 1 Proposal				
Encryption	AES256	Authentication	SHA1	<input type="checkbox"/> Remove
Encryption	AES256	Authentication	SHA256	<input type="checkbox"/> Remove
Encryption	AES128	Authentication	SHA1	<input type="checkbox"/> Remove
Encryption	AES128	Authentication	SHA256	<input type="checkbox"/> Remove
Diffie-Hellman Group		<input type="checkbox"/> 21 <input type="checkbox"/> 20 <input type="checkbox"/> 19 <input type="checkbox"/> 18 <input type="checkbox"/> 17 <input type="checkbox"/> 16		
		<input type="checkbox"/> 15 <input type="checkbox"/> 14 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 2 <input type="checkbox"/> 1		
Key Lifetime (seconds)	56660			
Local ID				

Scroll down to **Phase 2 Selectors** and set **Local Address** to the local subnet and **Remote Address** to the VPN tunnel endpoint subnet (found under 'Virtual Network Address Spaces in Microsoft Azure).

Enable the encryption types to match Phase 1 and set the **Keylife** to **7200 seconds**.

Phase 2 Selectors

Name	Local Address	Remote Address
Site2Site	192.168.111.0/255.255.255.0	10.11.12.0/255.255.255.0

Edit Phase 2 ✓ ✕

Name: Site2Site
Comments: VPN: Site2Site (Created by VPN wizard)

Local Address: Subnet 192.168.111.0/255.255.255.0
Remote Address: Subnet 10.11.12.0/255.255.255.0

▼ **Advanced...**

Phase 2 Proposal + Add

Encryption	AES128	Authentication	SHA256	Remove
Encryption	AES256	Authentication	SHA256	Remove
Encryption	AES128	Authentication	SHA1	Remove
Encryption	AES256	Authentication	SHA1	Remove

Enable Replay Detection
Enable Perfect Forward Secrecy (PFS)

Local Port: All
Remote Port: All
Protocol: All
Autokey Keep Alive:
Auto-negotiate:
Key Lifetime: Seconds
Seconds: 7200

4. Creating the FortiGate firewall addresses

Go to **Policy & Objects > Objects > Addresses** and configure a firewall address for the local network.

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	<input type="text" value="Internal_Port1"/>
Type	<input type="text" value="Subnet"/>
Subnet / IP Range	<input type="text" value="192.168.111.0/255.255.255.0"/>
Interface	<input type="text" value="any"/>
Visibility	<input checked="" type="checkbox"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Create another firewall object for the Azure VPN tunnel subnet.

Category	<input checked="" type="radio"/> Address <input type="radio"/> IPv6 Address <input type="radio"/> Multicast Address
Name	<input type="text" value="AzureVPN-tunnel"/>
Type	<input type="text" value="Subnet"/>
Subnet / IP Range	<input type="text" value="10.11.12.0/255.255.255.0"/>
Interface	<input type="text" value="any"/>
Visibility	<input checked="" type="checkbox"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

5. Creating the FortiGate firewall policies

Go to **Policy & Objects > Policy > IPv4** and create a new policy for the site-to-site connection that allows outgoing traffic

Set the **Source Address** and **Destination Address** using the firewall objects you just created.

Incoming Interface	<input type="text" value="internal1"/> +
Source Address	<input type="text" value="Internal_Port1"/> +
Source User(s)	<input type="text" value="Click to add..."/>
Source Device Type	<input type="text" value="Click to add..."/>
Outgoing Interface	<input type="text" value="Site2Site"/> +
Destination Address	<input type="text" value="AzureVPN-tunnel"/> +
Schedule	<input type="text" value="always"/>
Service	<input type="text" value="ALL"/> +
Action	<input type="text" value="ACCEPT"/>

When you are done, create another policy for the same connection to allow incoming traffic.

This time, invert the **Source Address** and **Destination Address**.

Incoming Interface	Site2Site
Source Address	AzureVPN-tunnel
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	internal1
Destination Address	Internal_Port1
Schedule	always
Service	ALL
Action	ACCEPT

6. Results

Go to **VPN > Monitor > IPsec > Monitor**. Right-click the tunnel you created and select **Bring Up** to activate the tunnel.

Name	Type	Remote Gateway	Username	Status
Site2Site	Static IP or Dynamic DNS			Down

Go to **Log & Report > Event Log > VPN**.

Name	Type	Remote Gateway	Username	Status
Site2Site	Static IP or Dynamic DNS			Up

Select an entry to view more information and verify the connection.

Go to **Log & Report > Event Log > VPN**.

Select an entry to view more information and verify the connection.

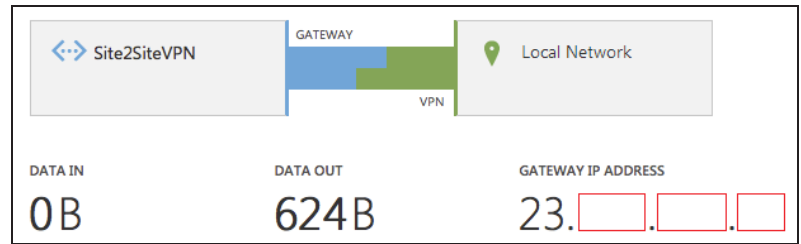
#	Date/Time	Level	Action	Status	Message	VPN Tunnel
12	15:23:04	*****	phase2-up		IPsec phase 2 status change	Site2Site
13	15:23:04	*****	install_sa		install IPsec SA	Site2Site
14	15:23:04	*****	negotiate	success	negotiate IPsec phase 2	Site2Site
15	15:23:04	*****	negotiate	success	progress IPsec phase 1	Site2Site
16	15:23:04	*****	negotiate	success	negotiate IPsec phase 1	Site2Site

1 / 1582 [Total: 79053]

Action	negotiate	Assigned IP	N/A
Cookies	9de897c069896c80/31b2351571a476b2	Date/Time	15:23:04 (1407770584)
ESP Authentication	HMAC_SHA1	ESP Transform	ESP_AES
Group	N/A	IPsec Local IP	69.171.153.181
IPsec Remote IP	23.100.122.11	Level	notice *****
Local Port	500	Log Description	negotiate IPsec phase 2
Log ID	37186	Message	negotiate IPsec phase 2
Outgoing Interface	ppp1	Remote Port	500
Role	Initiator	Status	success
Sub Type	vpn	Timestamp	8/11/2014, 3:23:04 PM
User	N/A	VPN Tunnel	Site2Site
Virtual Domain	root	XAUTH Group	N/A
XAUTH User	N/A		

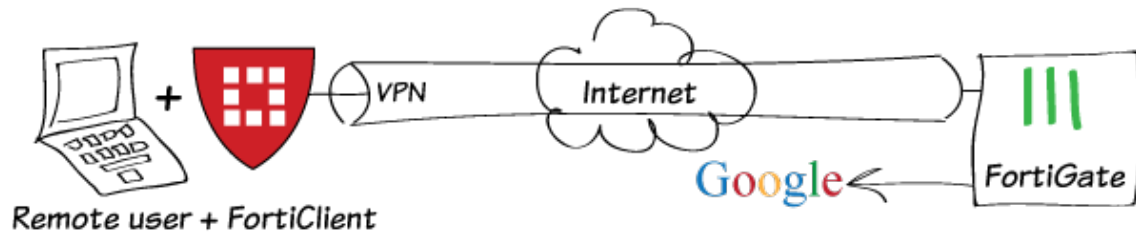
Return to the Microsoft Azure virtual network **Dashboard**. The status of the tunnel will show as **Connected**.

Data In and **Data Out** will indicate that traffic is flowing.



For further reading, check out [Gateway-to-gateway configurations](#) in the [FortiOS 5.2 Handbook](#).

Remote Internet browsing using a VPN



In this recipe, you will use remote IPsec and SSL VPN tunnels to bypass Internet access restrictions.

Restricted Internet access is simulated with a Web Filter profile that blocks google.com. You will create FortiClient SSL and IPsec VPN tunnels to bypass the web filter, connect to a remote FortiGate unit, and transparently browse the Internet to google.com.

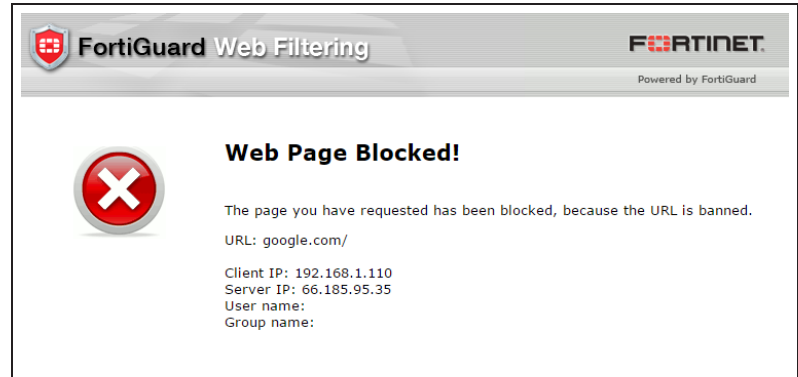
The recipe assumes that a "vpn_users" user group and a Local LAN firewall address have already been created.

1. Starting point

In this example, we simulate restricted Internet access using a Web Filtering profile to block Google.

With the user situated behind this FortiGate, google.com cannot be accessed, and instead the FortiGuard "Web Page Blocked" message appears.

For the user to bypass this Web Filter, the following VPN configurations must be made on a remote FortiGate (which is not blocked by any filter), and the user must connect to it using **FortiClient**.

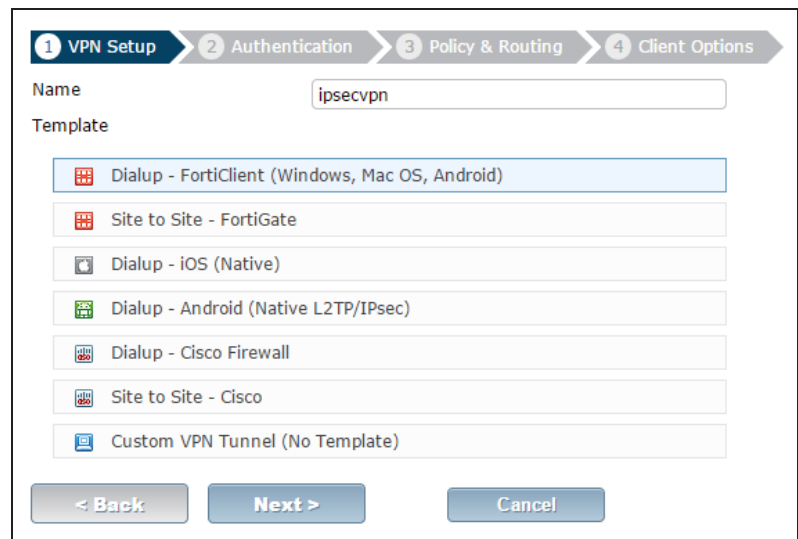


2. Configuring the IPsec VPN

On the remote Fortigate, go to **VPN > IPsec > Wizard**.

Name the VPN connection and select **Dial Up - FortiClient (Windows, Mac OS, Android)** and click **Next**.

The tunnel name must not have any spaces in it.



Set the **Incoming Interface** to the internet-facing interface. In this case, **wan1**.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key and select the **vpn_users** user group, then click **Next**.

The pre-shared key is a credential for the VPN and should differ from the user's password.

Set **Local Interface** to the internal interface and set **Local Address** to the local LAN address.

Enter an IP range for VPN users in the **Client Address Range** field.

*The IP range you enter here prompts FortiOS to create a new firewall object for the VPN tunnel using the name of your tunnel followed by the **_range** suffix (in this case, **ipsecvpn_range**).*

In addition, FortiOS automatically creates a security policy to allow remote users to access the internal network.

The screenshot shows the 'Authentication' step of the VPN Setup wizard. The wizard progress bar at the top indicates: 1. VPN Setup (checked), 2. Authentication (active), 3. Policy & Routing, and 4. Client Options. The configuration title is 'ipsecvpn : Dialup - FortiClient (Windows, Mac OS, Android)'. The 'Incoming Interface' is set to 'wan1'. The 'Authentication Method' is 'Pre-shared Key' (selected with a radio button), with 'Signature' as an alternative. The 'Pre-shared Key' field contains seven dots, and the 'Hide Characters' checkbox is checked. The 'User Group' is set to 'vpn_users'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

The screenshot shows the 'Policy & Routing' step of the VPN Setup wizard. The wizard progress bar at the top indicates: 1. VPN Setup (checked), 2. Authentication (checked), 3. Policy & Routing (active), and 4. Client Options. The configuration title is 'ipsecvpn : Dialup - FortiClient (Windows, Mac OS, Android)'. The 'Local Interface' is set to 'internal'. The 'Local Address' is set to 'Local LAN' (indicated by a yellow icon and a green plus sign). The 'Client Address Range' is '10.10.110.1-10.10.110.10'. The 'Subnet Mask' is '255.255.255.0'. Under 'DNS Server', 'Use System DNS' is selected with a radio button, and 'Specify' is an alternative. The 'Enable IPv4 Split Tunnel' checkbox is unchecked, and the 'Allow Endpoint Registration' checkbox is checked. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

Click **Next** and select **Client Options** as desired.

The screenshot shows the 'Client Options' step of the VPN Setup wizard. The progress bar at the top indicates the following steps: VPN Setup, Authentication, Policy & Routing, and Client Options (4). The main configuration area contains a text field with the value 'ipsecvpn : Dialup - FortiClient (Windows, Mac OS, Android)'. Below this are three checkboxes: 'Save Password' (checked), 'Auto Connect' (unchecked), and 'Always Up (Keep Alive)' (unchecked). At the bottom, there are three buttons: '< Back', 'Create', and 'Cancel'.

When using the IPsec VPN Wizard, an IPsec firewall address range is automatically created using the name of the tunnel you entered into the Wizard. The Wizard also creates an **IPsec -> internal** IPv4 policy, so all that is left is to create the Internet access policy. See [Step 4](#).

3. Configuring the SSL VPN

Go to **VPN > SSL > Portals**, highlight the **full-access** portal, and select **Edit**.

The screenshot shows the 'SSL VPN Portals' table in the FortiGate GUI. The table has columns for Name, Tunnel Mode, Web Mode, and Ref. The 'full-access' portal is highlighted, and the 'Edit' button is circled in red.

Name	Tunnel Mode	Web Mode	Ref.
full-access	✓	✓	1
tunnel-access	✓	✗	0
web-access	✗	✓	1

Disable **Split Tunneling** so that all VPN traffic will go through the FortiGate firewall.

The screenshot shows the configuration page for the 'full-access' portal. The 'Name' field contains 'full-access'. The 'Enable Tunnel Mode' checkbox is checked. The 'Enable Split Tunneling' checkbox is unchecked and circled in red. The 'Source IP Pools' field contains 'SSLVPN_TUNNEL_ADDR1'.

Go to **VPN > SSL > Settings**. Under **Connection Settings** set **Listen on Port** to **10443**.

The screenshot shows the 'Connection Settings' page for SSL-VPN portals. The 'Listen on Interface(s)' field contains 'wan1'. The 'Listen on Port' field contains '10443' and is circled in red. Below the port field, it says 'Web mode access will be listening at https://172.20.120.230:10443'.

Under **Authentication/Portal Mapping**, assign the **vpn_users** user group to the **full-access** portal, and assign **All Other Users/Groups** to the desired portal.

Authentication/Portal Mapping

By default, all users see the same SSL-VPN portal. The following table allows you to assign different portals to different users and groups.

Users/Groups	Realm	Portal
vpn_users	/	full-access
All Other Users/Groups	/	web-access

By default, the FortiGate has an **ssl.root** firewall address. All that is left is to create the Internet access policy, as described in the following step.

4. Creating security policies for VPN access to the Internet

Go to **Policy & Objects > Policy > IPv4**.

Create two security policies allowing remote users to access the Internet securely through the FortiGate unit; one for each VPN tunnel.

Set **Incoming Interface** to the tunnel interface and set **Source Address** to **all**.

For SSL VPN, set **Source User(s)** to the **vpn_users** user group.

Set **Outgoing Interface** to **wan1** and **Destination Address** to **all**.

Set **Service** to **ALL** and ensure that you enable **NAT**.

Incoming Interface: ipsecvpn
 Source Address: all
 Source User(s): Click to add...
 Source Device Type: Click to add...
 Outgoing Interface: wan1
 Destination Address: all
 Schedule: always
 Service: ALL
 Action: ACCEPT

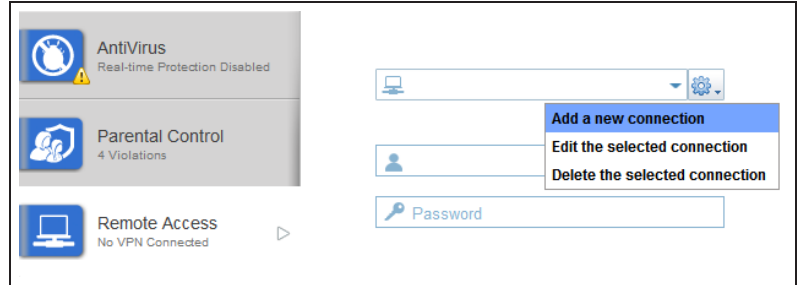
Firewall / Network Options
 NAT
 Use Outgoing Interface Address Fixed Port

Incoming Interface: ssl.root (SSL VPN interface)
 Source Address: all
 Source User(s): vpn_users
 Outgoing Interface: wan1
 Destination Address: all
 Schedule: always
 Service: ALL
 Action: ACCEPT

Firewall / Network Options
 NAT

5. Configuring FortiClient for IPsec and SSL VPN

Open FortiClient, go to **Remote Access** and add new connections for both VPNs.

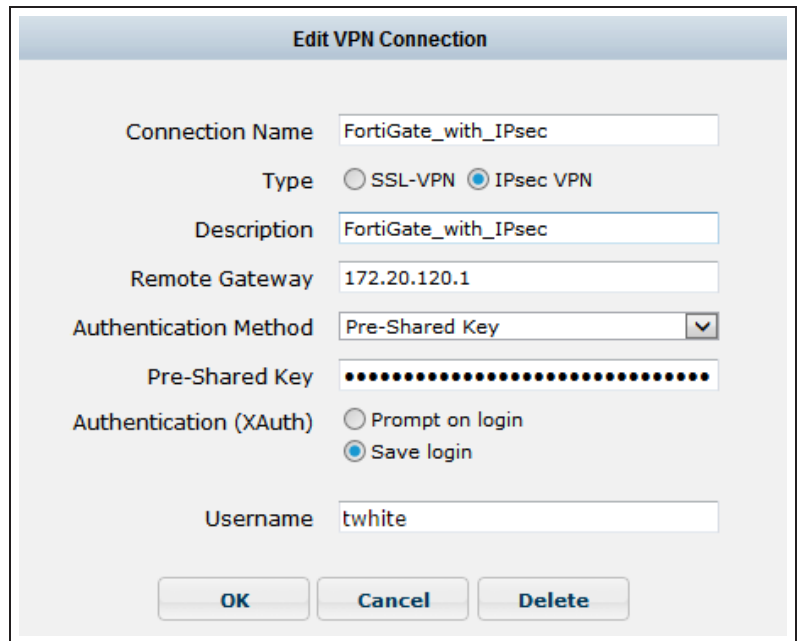


Provide a **Connection Name** and set the **Type** to either **IPsec VPN** or **SSL VPN** depending on the VPN configuration.

Set **Remote Gateway** to the FortiGate IP address.

- For IPsec VPN, set **Authentication Method** to **Pre-Shared Key** and enter the key below.
- For SSL VPN, set **Customize Port** to **10443**.

(Optional) For **Username**, enter a username from the **vpn_users** user group.



Edit VPN Connection

Connection Name:

Type: SSL-VPN IPsec VPN

Description:

Remote Gateway:

Customize port:


Authentication: Prompt on login Save login


Username:


Client Certificate:

Do not Warn Invalid Server Certificate:


Select the new connection, enter the username and password, and click **Connect**.

 **AntiVirus**
Real-time Protection Disabled

 **Parental Control**
4 Violations

 **Remote Access**
No VPN Connected

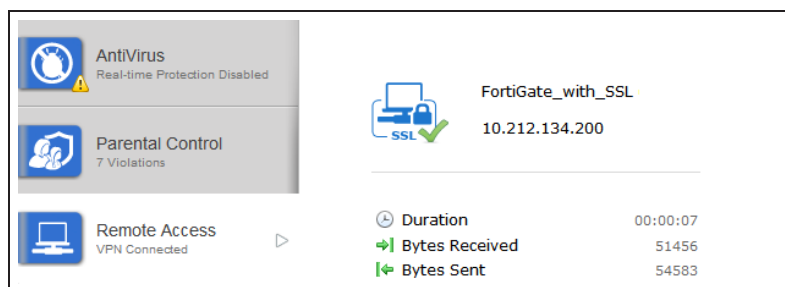
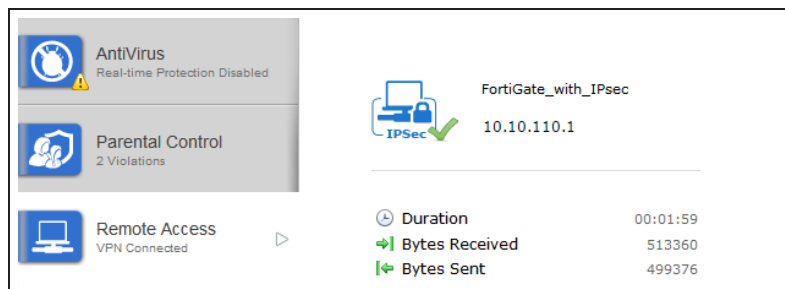
If prompted with a server authentication warning, select **Yes**.

 This page requires a secure connection which includes server authentication.

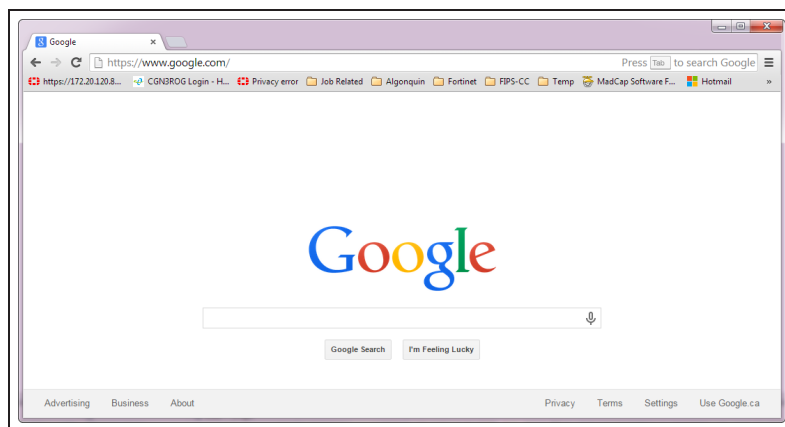
The Certificate Issuer for this site is untrusted or unknown. Do you wish to proceed?

6. Results

From FortiClient start an IPsec or SSL VPN session. Once the connection is established, the FortiGate assigns the user an IP address and FortiClient displays the status of the connection, including the IP address, connection duration, and bytes sent and received.

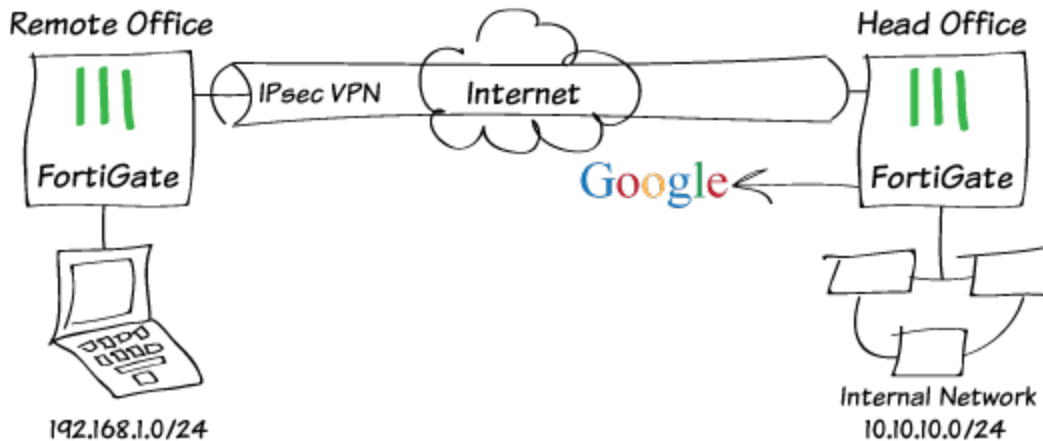


With the tunnel up, you can now visit [google.com](https://www.google.com) without being blocked, since the Internet traffic is handled by the remote FortiGate and the web filter on the local FortiGate has been bypassed.



For further reading, check out [IPsec VPN in the web-based manager](#) in the [FortiOS 5.2 Handbook](#).

Remote browsing using site-to-site IPsec VPN



In this recipe, you will configure a site-to-site, also called gateway-to-gateway, IPsec VPN between an office with Internet access restrictions (Remote Office) and an office without these restrictions (Head Office) so that the Remote Office can access the Internet through the Head Office, avoiding the restrictions.

To bypass this restriction, this example shows how create a site-to-site VPN to connect the Remote Office FortiGate unit to the Head Office FortiGate unit, and allow Remote Office staff to transparently browse the Internet to google.com using the Head Office's Internet connection.

Note that both FortiGates run FortiOS firmware version 5.2.2 and have static IP addresses on Internet-facing interfaces. You will also need to know the Remote Office's gateway IP address.

1. Configuring IPsec VPN on the Head Office FortiGate

In a real world scenario, a Remote Office's ISP or something in their local Internet may be blocking access to Google, or any other site for that matter.

On the Head Office FortiGate, go to **VPN > IPsec > Wizard**.

Name the VPN, select **Site to Site - FortiGate**, and click **Next**.

1 VPN Setup > 2 Authentication > 3 Policy & Routing

Name: Head Office

Template:

- Dialup - FortiClient (Windows, Mac OS, Android)
- Site to Site - FortiGate**
- Dialup - iOS (Native)
- Dialup - Android (Native L2TP/IPsec)
- Dialup - Cisco Firewall
- Site to Site - Cisco
- Custom VPN Tunnel (No Template)

< Back Next > Cancel

Set the **Remote Gateway** to the Remote Office FortiGate IP address

The Wizard should select the correct **Outgoing Interface** when you click anywhere else in the window. Depending on your configuration, you may have to manually set the outgoing interface.

Select **Pre-shared Key** for the **Authentication Method**.

Enter a pre-shared key then click **Next**.

The pre-shared key is a credential for the VPN and should differ from the user's password. Both FortiGate's must have the same pre-shared key.

VPN Setup > 2 Authentication > 3 Policy & Routing

Head Office : Site to Site - FortiGate

Remote Gateway: 10.10.20.1

Outgoing Interface: port1 (Detected via routing lookup) [Change]

Authentication Method: Pre-shared Key Signature

Pre-shared Key: ●●●●●●

Hide Characters

< Back Next > Cancel

Under **Policy & Routing**, set the **Local Interface** to the interface connected to the Head Office internal network.

For **Local Subnets**, enter the subnet range of the Head Office internal network. Depending on your configuration, this may be set automatically by the wizard.

For **Remote Subnets**, enter the subnet range of the Remote Office internal network then click **Create**.

The VPN Wizard informs you that a static route has been created, as well as two security policies and two address objects, which are added to two address groups (also created).

The screenshot shows the 'Policy & Routing' step of the VPN Wizard. At the top, there are three progress indicators: 'VPN Setup' (checked), 'Authentication' (checked), and 'Policy & Routing' (active, with a '3'). Below this is a title bar 'Head Office : Site to Site - FortiGate'. The main area contains three input fields: 'Local Interface' with a dropdown menu showing 'port2', 'Local Subnets' with a text box containing '10.10.10.0/24' and a help icon, and 'Remote Subnets' with a text box containing '192.168.1.0/24' and a help icon. At the bottom, there are three buttons: '< Back', 'Create', and 'Cancel'.

The screenshot shows the 'Summary of Created Objects' screen after the VPN setup. At the top, the progress indicators are: 'VPN Setup' (checked), 'Authentication' (checked), and 'Policy & Routing' (checked). Below this is a title bar 'Head Office : Site to Site - FortiGate'. A green checkmark icon is followed by the text 'The VPN has been set up'. Below this is the heading 'Summary of Created Objects' and a table listing the created objects:

Phase 1 Interface	Head Office
Phase 2 Interfaces	Head Office
Static Routes	192.168.1.0/24
Local Address Group	Head Office_local
Remote Address Group	Head Office_remote
Local to Remote Policy	1
Remote to Local Policy	2

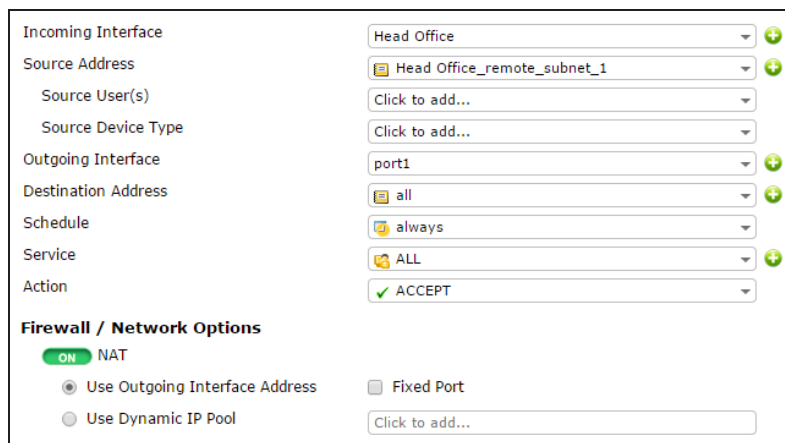
At the bottom, there are two buttons: 'Add Another' and 'Show Tunnel List'.

Create a security policy to allow the Remote Office to have Internet access. Go to **Policy & Objects > Policy > IPv4** and select **Create New**.

Set **Incoming Interface** to the VPN interface created by the VPN wizard and set **Source Address** to the remote office address group created by the VPN wizard.

Set **Outgoing Interface** to the Internet-facing interface and set **Destination Address** to **all**.

Enable **NAT** and (optionally) enforce any company security profiles.



The screenshot shows the configuration for a Firewall Policy. The fields are as follows:

Incoming Interface	Head Office
Source Address	Head Office_remote_subnet_1
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	port1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

Firewall / Network Options

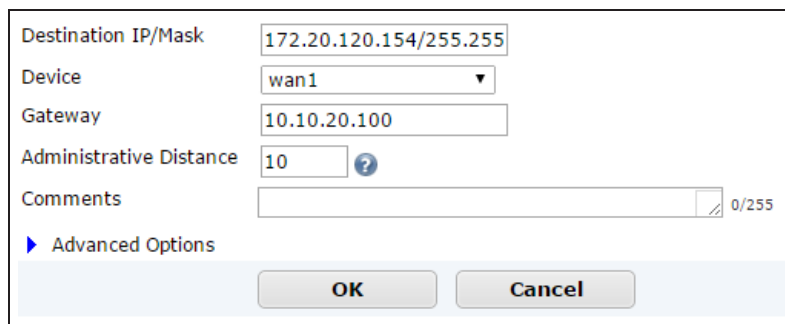
- NAT
- Use Outgoing Interface Address
- Use Dynamic IP Pool
- Fixed Port

Click to add... (for Fixed Port)

2. Adding a route on the Remote Office FortiGate

On the Remote Office FortiGate, create a static route that forwards traffic destined for the Head Office FortiGate to the ISP's Internet gateway.

(In this example, the Head Office FortiGate IP address is 172.20.120.154 so the destination IP/Mask is 172.20.120.154/255.255.255.0 and the ISP's gateway IP address is 10.10.20.100.)



The screenshot shows the configuration for a Static Route. The fields are as follows:

Destination IP/Mask	172.20.120.154/255.255
Device	wan1
Gateway	10.10.20.100
Administrative Distance	10
Comments	0/255

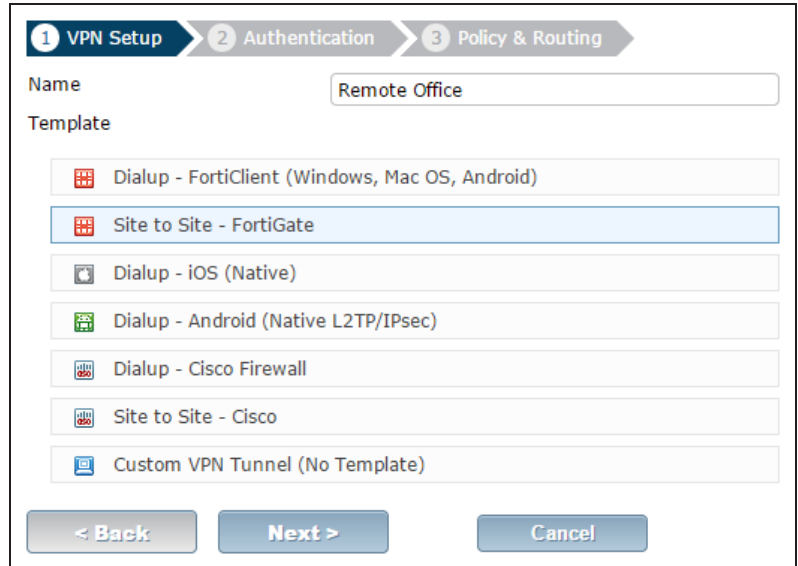
Advanced Options

OK Cancel

3. Configuring IPsec VPN on the Remote Office FortiGate

On the Remote Office FortiGate, go to **VPN > IPsec > Wizard**.

Name the VPN, select **Site to Site - FortiGate**, and click **Next**.



1 VPN Setup 2 Authentication 3 Policy & Routing

Name Remote Office

Template

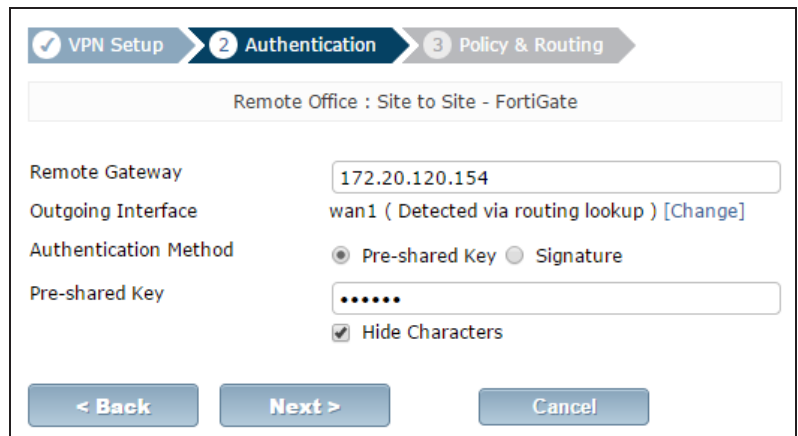
- Dialup - FortiClient (Windows, Mac OS, Android)
- Site to Site - FortiGate**
- Dialup - iOS (Native)
- Dialup - Android (Native L2TP/IPsec)
- Dialup - Cisco Firewall
- Site to Site - Cisco
- Custom VPN Tunnel (No Template)

< Back Next > Cancel

Set the **Remote Gateway** to the Head Office FortiGate IP address.

The Wizard should select the correct **Outgoing Interface**.

Select **Pre-shared Key** for the **Authentication Method** and enter the same **Pre-shared Key** as you entered in **Step 1**.



1 VPN Setup 2 Authentication 3 Policy & Routing

Remote Office : Site to Site - FortiGate

Remote Gateway 172.20.120.154

Outgoing Interface wan1 (Detected via routing lookup) [Change]

Authentication Method Pre-shared Key Signature

Pre-shared Key
 Hide Characters

< Back Next > Cancel

Under **Policy & Routing**, set the **Local Interface** to the interface connected to the Remote Office internal network.

For **Local Subnets**, enter the subnet range of the Remote Office internal network.

For **Remote Subnets**, enter the subnet range of the Head Office internal network then click **Create**.

The VPN Wizard informs you that a static route has been created, as well as two address groups and two security policies.

The screenshot shows the 'Policy & Routing' configuration page for a Remote Office Site-to-Site VPN. The progress bar at the top indicates that 'VPN Setup' and 'Authentication' are completed, and 'Policy & Routing' is the current step. The configuration fields are as follows:

Field	Value
Local Interface	internal1 (Local LAN)
Local Subnets	192.168.1.0/24
Remote Subnets	10.10.10.0/24

At the bottom, there are three buttons: '< Back', 'Create', and 'Cancel'.

The screenshot shows the 'Summary of Created Objects' screen after the VPN configuration is complete. A green checkmark and the text 'The VPN has been set up' are displayed at the top. Below this is a table summarizing the objects created:

Object Type	Object Name
Phase 1 Interface	Remote Office
Phase 2 Interfaces	Remote Office
Static Routes	10.10.10.0/24
Local Address Group	Remote Office_local
Remote Address Group	Remote Office_remote
Local to Remote Policy	2
Remote to Local Policy	3

At the bottom, there are two buttons: 'Add Another' and 'Show Tunnel List'.

Allow Internet traffic from the remote office to enter the VPN tunnel.

On the Remote Office FortiGate, go to **Policy & Objects > Policy > IPv4**.

Edit the outbound security policy created by the VPN Wizard.

Change the **Destination Address** to **all** so that the policy accepts Internet traffic.

The screenshot shows the configuration page for a security policy. The 'Destination Address' field is highlighted with a red box and contains the value 'all'. The configuration is as follows:

Incoming Interface	internal1 (Local LAN)
Source Address	Remote Office_local
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	Remote Office
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

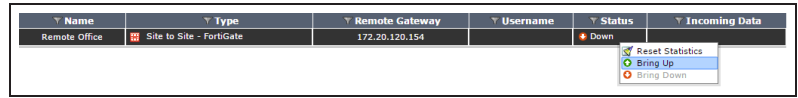
4. Establishing the tunnel

On either FortiGate, go to **VPN > Monitor > IPsec Monitor**.

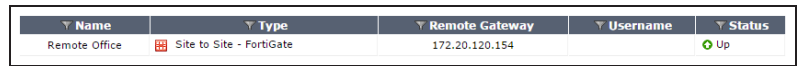
Right-click the newly created tunnel and select **Bring Up**.

If the tunnel is established, the **Status** column will read **Up** on both of the FortiGates.

Name	Type	Remote Gateway	Username	Status	Incoming Data
Remote Office	Site to Site - FortiGate	172.20.120.154		Down	

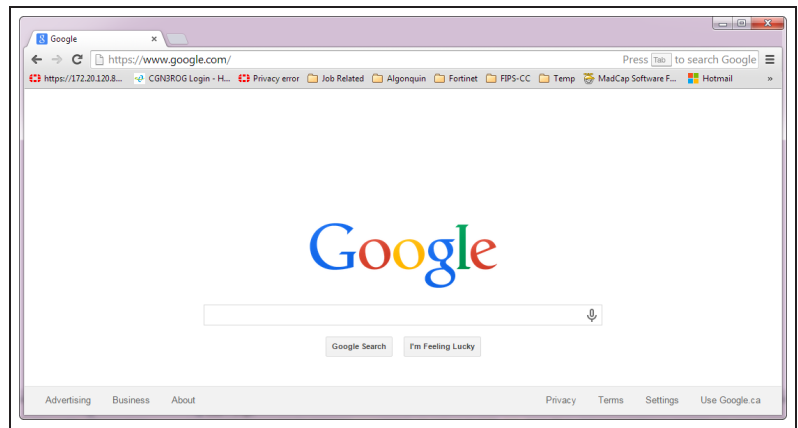


Name	Type	Remote Gateway	Username	Status	Incoming Data
Remote Office	Site to Site - FortiGate	172.20.120.154		Up	



6. Results

With the tunnel up, you can now visit [google.com](https://www.google.com/) without being blocked, since the Internet traffic is handled by the Head Office FortiGate and the access restrictions on the remote FortiGate have been bypassed.



For further reading, check out [IPsec VPN in the web-based manager](#) in the [FortiOS 5.2 Handbook](#).

IPsec troubleshooting

This section contains tips to help you with some common challenges of IPsec VPNs.

The options to configure policy-based IPsec VPN are unavailable.

Go to **System > Config > Features**. Select Show More and turn on Policy-based IPsec VPN.

The VPN connection attempt fails.

If your VPN fails to connect, check the following:

- Ensure that the pre-shared keys match exactly.
- Ensure that both ends use the same P1 and P2 proposal settings.
- Ensure that you have allowed inbound and outbound traffic for all necessary network services, especially if services such as DNS or DHCP are having problems.
- Check that a static route has been configured properly to allow routing of VPN traffic.
- Ensure that your FortiGate unit is in NAT/Route mode, rather than Transparent.
- Check your NAT settings, enabling NAT traversal in the Phase 1 configuration while disabling NAT in the security policy.
- Ensure that both ends of the VPN tunnel are using Main mode, unless multiple dial-up tunnels are being used.
- If you have multiple dial-up IPsec VPNs, ensure that the Peer ID is configured properly on the FortiGate and that clients have specified the correct Local ID.
- If you are using FortiClient, ensure that your version is compatible with the FortiGate firmware by reading the FortiOS Release Notes.
- Ensure that the Quick Mode selectors are correctly configured. If part of the setup currently uses firewall addresses or address groups, try changing it to either specify the IP addresses or use an expanded address range.
- If XAUTH is enabled, ensure that the settings are the same for both ends, and that the FortiGate unit is set to Enable as Server.
- If your FortiGate unit is behind a NAT device, such as a router, configure port forwarding for UDP ports 500 and 4500.
- Remove any Phase 1 or Phase 2 configurations that are not in use. If a duplicate instance of the VPN tunnel appears on the IPsec Monitor, reboot your FortiGate unit to try and clear the entry.

If you are still unable to connect to the VPN tunnel, run the diagnostic command in the CLI:

```
diag debug application ike -1
diag debug enable
```

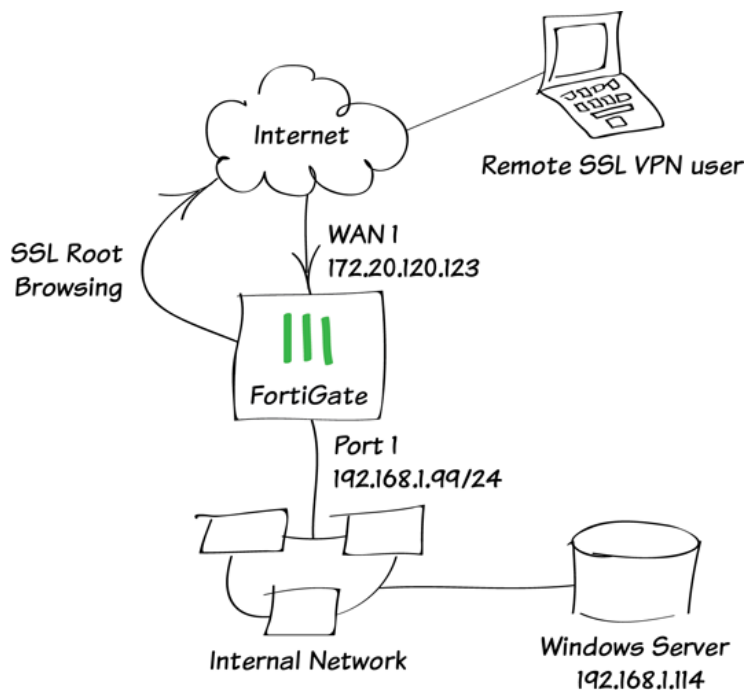
The resulting output may indicate where the problem is occurring. When you are finished, disable the diagnostics by using the following command:

```
diag debug reset  
diag debug disable
```

The VPN tunnel goes down frequently.

If your VPN tunnel goes down often, check the Phase 2 settings and either increase the **Keylife** value or enable **Autokey Keep Alive**.

SSL VPN for remote users



This example provides remote users with access to the corporate network using SSL VPN and connect to the Internet through the corporate FortiGate unit. During the connecting phase, the FortiGate unit will also verify that the remote user's antivirus software is installed and current.

A video of this recipe can be found [here](#).

1. Creating an SSL VPN portal for remote users

Go to VPN > SSL > Portals.

Edit the **full-access** portal. The full-access portal allows the use of tunnel mode and/or web mode. In this scenario we are using both modes.

Enable Split Tunneling is *not* enabled so that all Internet traffic will go through the FortiGate unit and be subject to the corporate security profiles.

The screenshot shows the configuration page for an SSL VPN portal named 'full-access'. The interface is divided into several sections:

- Name:** full-access
- Enable Tunnel Mode:** . Sub-options: Enable Split Tunneling. Source IP Pools: SSLVPN_TUNNEL_ADDR1.
- Enable IPv6 Tunnel Mode:** . Sub-options: Enable IPv6 Split Tunneling. Source IPv6 Pools: SSLVPN_TUNNEL_IPv6_ADDR1.
- Client Options:** Save Password, Auto Connect, Always Up (Keep Alive).
- Enable Web Mode:** . Sub-options: Portal Message: Welcome to SSL VPN Service; Theme: Blue; Page Layout: (selected layout icon); Include Status Information; Include Connection Tool; Include FortiClient Download; Prompt Mobile Users to Download FortiClient Application; Include Login History; Enable User Bookmarks.
- Predefined Bookmarks:** A table with columns Name, Type, Location, and Description. It shows 'No matching entries found'.
- Limit Users to One SSL-VPN Connection at a Time:**

Buttons for OK and Cancel are at the bottom.

Select **Create New** in the Predefined Bookmarks area to add a bookmark for a remote desktop link/connection.

Bookmarks are used as links to internal network resources.

You must include a username and password. You will create this user in the next step, so be sure to use the same credentials.

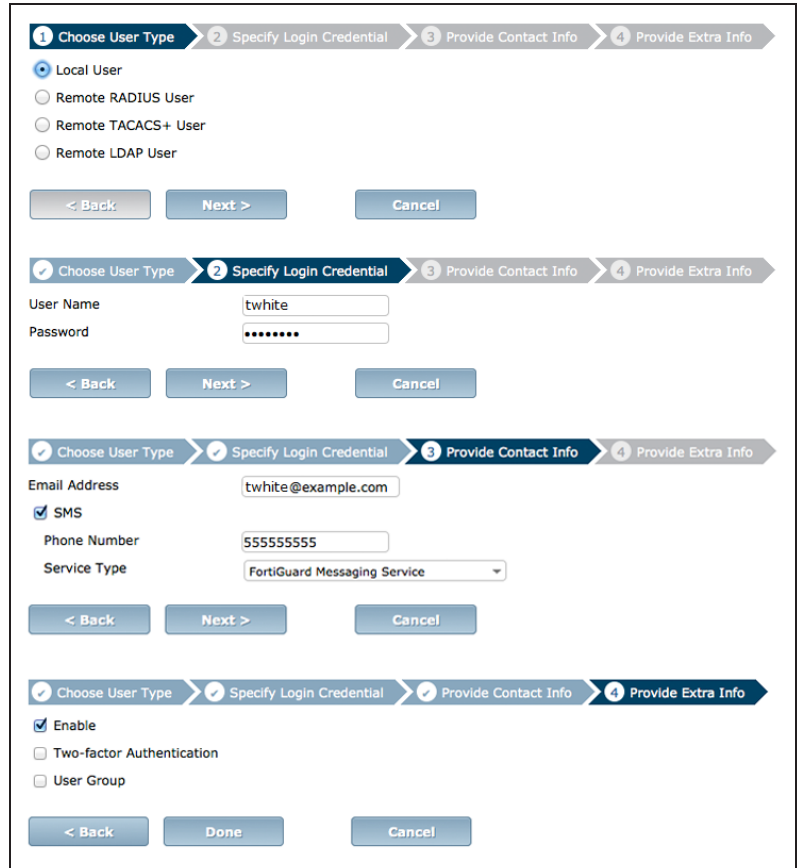
New Bookmark	
Category	Remote Desktop
Name	Windows Server
Type	RDP
Host	192.168.1.114
Screen Width	1024
Screen Height	768
Full Screen Mode	<input checked="" type="checkbox"/>
Username	twhite
Password	•••••
Keyboard Layout	English, US.
Description	

OK Cancel

2. Creating a user and a user group

Go to **User & Device > User > User Definition**.

Add a remote user with the **User Creation Wizard** (in the example, *twhite*, with the same credentials used for the predefined bookmark).



The image shows four sequential screenshots of the User Creation Wizard:

- Step 1: Choose User Type** - Radio buttons for Local User (selected), Remote RADIUS User, Remote TACACS+ User, and Remote LDAP User. Buttons: < Back, Next >, Cancel.
- Step 2: Specify Login Credential** - Text fields for User Name (twhite) and Password (masked with dots). Buttons: < Back, Next >, Cancel.
- Step 3: Provide Contact Info** - Text field for Email Address (twhite@example.com), checked SMS checkbox, text field for Phone Number (55555555), and dropdown for Service Type (FortiGuard Messaging Service). Buttons: < Back, Next >, Cancel.
- Step 4: Provide Extra Info** - Checked Enable checkbox, unchecked Two-factor Authentication and User Group checkboxes. Buttons: < Back, Done, Cancel.

Go to **User & Device > User > User Groups**.

Add the user *twhite* to a user group for SSL VPN connections.



The image shows the User Groups configuration page:

- Name:** sslvpn_group
- Type (RSSO):** Firewall (selected), Fortinet Single Sign-On (FSSO), Guest, RADIUS Single Sign-On
- Members:** twhite (with add and remove icons)
- Remote groups:** A table with columns Remote Server and Group Name. The table is empty, showing "No matching entries found".
- Buttons: Add, Edit, Delete, OK, Cancel.

3. Adding an address for the local network

Go to **Policy & Objects > Objects > Addresses**.

Add the address for the local network. Set **Subnet / IP Range** to the local subnet and set **Interface** to an internal port.

Category: Address IPv6 Address Multicast Address

Name: Local LAN

Type: Subnet

Subnet / IP Range: 192.168.1.0/255.255.255.0

Interface: port1

Visibility:

Comments: Write a comment... 0/255

Buttons: OK, Cancel

4. Configuring the SSL VPN tunnel

Go to **VPN > SSL > Settings** and set **Listen on Interface(s)** to wan1.

Set **Listen on Port** to 443 and **Specify custom IP ranges**.

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s): wan1

Listen on Port: 443

Restrict Access: Allow access from any host Limit access to specific hosts

Idle Logout: Logout users when inactive for specified period Never logout inactive users

Inactive For: 5000 (Seconds)

Server Certificate: Fortinet_Factory

Require Client Certificate:

Tunnel Mode Client Settings

Once connected in tunnel mode, clients will receive these settings.

Address Range: Automatically assign addresses Specify custom IP ranges

IP Ranges: SSLVPN_TUNNEL_ADDR1, SSLVPN_TUNNEL_IPv6_ADDR1

Under **Authentication/Portal Mapping**, add the SSL VPN user group.

Users/Groups	Realm	Portal
sslvpn_group	/	full-access
All Other Users/Groups	/	web-access

5. Adding security policies for access to the Internet and internal network

Go to **Policy & Objects > Policy > IPv4**.

Add a security policy allowing access to the internal network through the *ssl.root* VPN tunnel interface.

Set **Incoming Interface** to *ssl.root*.

Set **Source Address** to *all* and select the **Source User** group you created in step 2.

Set **Outgoing Interface** to the local network interface so that the remote user can access the internal network.

Set **Destination Address** to *all*, enable **NAT**, and configure any remaining firewall and security options as desired.

Add a second security policy allowing SSL VPN access to the Internet.

For this policy, **Incoming Interface** is set to *ssl.root* and **Outgoing Interface** is set to *wan1*.

Incoming Interface	ssl.root (sslvpn tunnel interface) +
Source Address	all +
Source User(s)	sslvpn_group X +
Source Device Type	Click to add...
Outgoing Interface	lan +
Destination Address	all +
Schedule	always +
Service	ALL +
Action	ACCEPT +
Firewall / Network Options	
<input checked="" type="checkbox"/> NAT	
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...
<input type="radio"/> Use Central NAT Table	

Incoming Interface	ssl.root (sslvpn tunnel interface) +
Source Address	all +
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1 +
Destination Address	all +
Schedule	always +
Service	ALL +
Action	ACCEPT +

6. Setting the FortiGate unit to verify users have current AntiVirus software

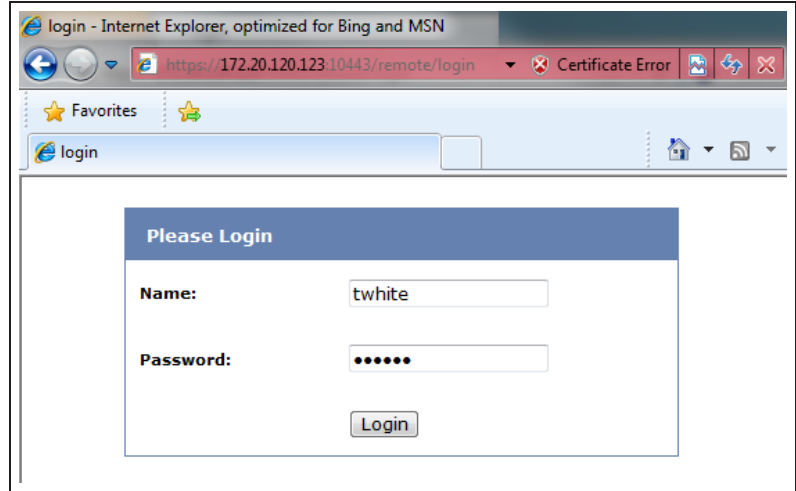
Go to **System > Status > Dashboard**.

In the **CLI Console** widget, enter the commands on the right to enable the host to check for compliant AntiVirus software on the remote user's computer.

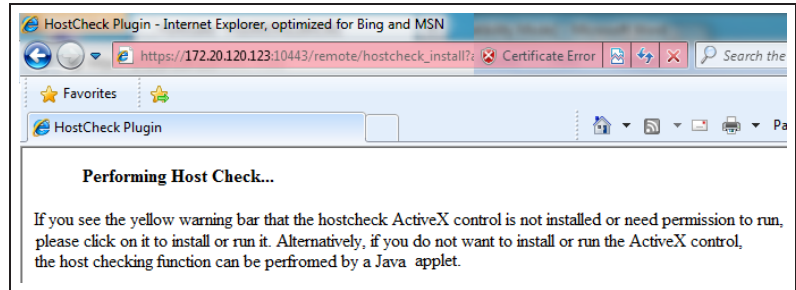
```
config vpn ssl web portal
edit full-access
set host-check av
end
end
```


7. Results

Log into the portal using the credentials you created in step 2.

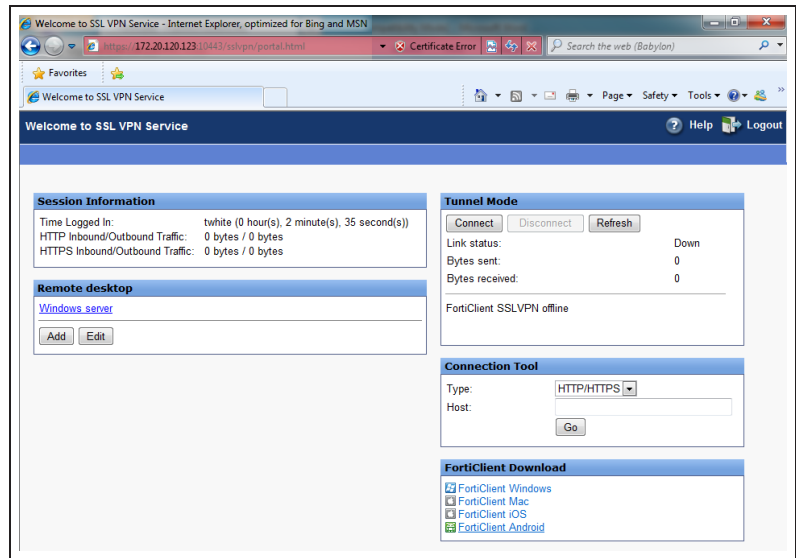


The FortiGate unit performs the host check.

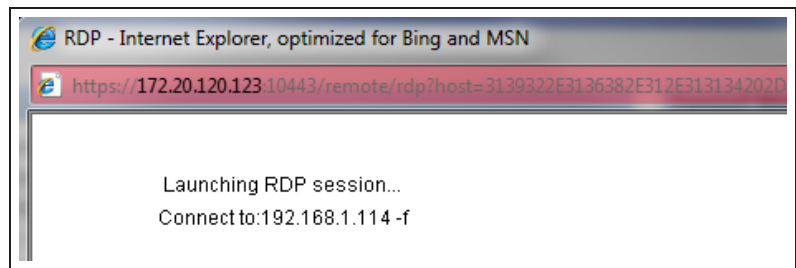


After the check is complete, the portal appears.

You may need to install the FortiClient application using the available download link.






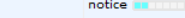
Select the bookmark **Remote Desktop** link to begin an RDP session.



Go to **VPN > Monitor > SSL-VPN Monitor** to verify the list of SSL users. The Web Application description indicates that the user is using web mode.

No.	User	Source IP	Begin Time	Description
1	twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
	Subsession			Web Application:RDP 192.168.1.114

Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.

Dst	192.168.1.114	Virtual Domain	root
Received	85591	Source Country	Reserved
Sent / Received	8.71 KB / 83.58 KB	Duration	36
Sent	8923	Application Details	
Group	N/A	Service	RDP
Protocol	6	User	 twhite
Destination Country	Reserved	Dst Port	3389
roll	65389	Status	
Timestamp	Wed Apr 17 14:13:11 2013	Tran Display	noop
Sequence Number	2700	Policy ID	11
Src Interface	wan1	Src	 twhite (172.20.120.23)
VPN	sslvpn_web_mode	Sent Packets	71
Level	notice 	VPN Type	sslvpn
Src Port	53712	Log ID	13
Sub Type	forward	Threat	
Received Packets	98	Date/Time	14:13:11 (Wed Apr 17 14:13:11 2013)
Dst Interface	port1		

In the **Tunnel Mode** widget, select **Connect** to enable the tunnel.

Tunnel Mode

Connect
Disconnect
Refresh

Link status: Up




Bytes sent: 46865

Bytes received: 118096

FortiClient SSLVPN connected to server

Select the bookmark **Remote Desktop** link to begin an RDP session.

RDP - Internet Explorer, optimized for Bing and MSN

https://172.20.120.123:10443/remote/rdp?host=31393
Certificate Error

Launching RDP session...

Connect to:192.168.1.114 -f

Go to **VPN > Monitor > SSL-VPN Monitor** to verify the list of SSL users.

The tunnel description indicates that the user is using tunnel mode.

Go to **Log & Report > Traffic Log > Forward Traffic** and view the details for the SSL entry.

Delete					
	No.	User	Source IP	Begin Time	Description
<input type="checkbox"/>	1	twhite	172.20.120.23	Wed Apr 17 11:41:06 2013	
<input type="checkbox"/>		Subsession			Tunnel IP:10.212.134.200



Dst	192.168.1.114	Virtual Domain	root
Received	326664	Source Country	Reserved
Sent / Received	54,36 KB / 319.01 KB	Duration	83
Sent	55665	Application Details	
Group	N/A	Service	RDP
Protocol	6	User	twhite
Destination Country	Reserved	Dst Port	3389
roll	65389	Status	✓
Timestamp	Wed Apr 17 14:17:15 2013	Tran Display	noop
Sequence Number	3618	Policy ID	11
Src Interface	wan1	Src	twhite (172.20.120.23)
VPN	sslvpn_web_mode	Sent Packets	329
Level	notice	VPN Type	sslvpn
Src Port	53820	Log ID	13
Sub Type	forward	Threat	
Received Packets	407	Date/Time	14:17:15 (Wed Apr 17 14:17:15 2013)
Dst Interface	unknown-0		

Go to **Log & Report > Traffic Log > Forward Traffic**.

Internet access occurs simultaneously through the FortiGate unit.

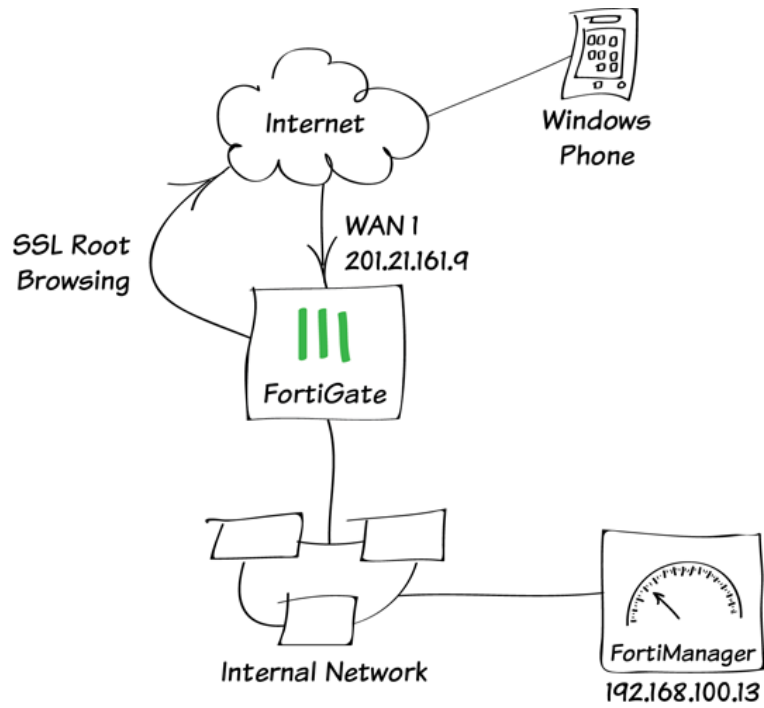
#	Date/Time	Src Interface	Dst Interface	Src	Dst	Service	Policy ID	Sent / Received
1	14:26:05	ssl.root	wan1	10.212.134.200	74.125.133.95	HTTP	8	168 B / 88 B
2	14:26:04	ssl.root	wan1	10.212.134.200	173.194.77.94	HTTP	8	168 B / 88 B
3	14:26:04	ssl.root	wan1	10.212.134.200	173.194.43.79	HTTP	8	168 B / 88 B
4	14:26:03	ssl.root	wan1	10.212.134.200	66.171.121.34 (fortinet.com)	HTTP	8	535 B / 938 B
5	14:25:57	ssl.root	wan1	10.212.134.200	74.121.50.17 (www.pages03.net)	HTTP	8	880 B / 537 B
6	14:25:44	ssl.root	wan1	10.212.134.200	208.91.113.212	HTTPS	8	3.30 KB / 7.44 KB
7	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30	KERBEROS	8	520 B / 1.64 KB
8	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30	KERBEROS	8	1.71 KB / 321 B
9	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30	KERBEROS	8	404 B / 367 B
10	14:24:39	ssl.root	wan1	10.212.134.200	213.199.179.159	40031/tcp	8	512 B / 469 B
11	14:24:37	ssl.root	wan1	10.212.134.200	213.199.179.159	HTTP	8	168 B / 128 B
12	14:24:37	ssl.root	wan1	10.212.134.200	132.246.2.6 (www.msfncsi.com)	HTTP	8	305 B / 387 B

Select an entry to view more information.

Dst	 66.171.121.34 (fortinet.com)	Virtual Domain	root
Received	938	Source Country	Reserved
Src NAT IP	172.20.120.123	Sent / Received	535 B / 938 B
Duration	17	Sent	535
Src NAT Port	54165	Application Details	
Service	HTTP	Protocol	6
Destination Country	United States	Dst Port	80
roll	65389	Status	close
Timestamp	Wed Apr 17 14:26:03 2013	Tran Display	snat
Sequence Number	8096	Policy ID	8
Src Interface	ssl.root	Src	10.212.134.200
Sent Packets	6	Level	notice 
Src Port	54165	Log ID	13
Sub Type	forward	Threat	
Received Packets	5	Date/Time	14:26:03 (Wed Apr 17 14:26:03 2013)
Dst Interface	wan1		

For further reading, check out [Basic SSL VPN configuration](#) in the [FortiOS 5.2 Handbook](#).

SSL VPN for Windows Phone 8.1



In this example, you will connect to a private network with a Windows Phone, using an SSL VPN.

1. Creating a VPN portal with custom bookmarks

Go to **VPN > SSL > Portals** and create a new portal.

Enable both **Tunnel Mode** and **Web Mode**. Disable **Split Tunneling** and set **Source IP Pools** to use the default SSL VPN tunnel address range.

Under **Predefined Bookmarks**, create bookmarks to access resources on the internal network.

Name: PORTAL_PBI

Enable Tunnel Mode

Enable Split Tunneling

Source IP Pools: SSLVPN_TUNNEL_ADDR1

Client Options: Save Password Auto Connect Always Up (Keep Alive)

Enable Web Mode

Portal Message: Bem-Vindo a VPN SSL - FGT_110C

Theme: Blue

Page Layout:

Include Status Information

Include Connection Tool

Include FortiClient Download

Prompt Mobile Users to Download FortiClient Application

Include Login History

Enable User Bookmarks

Predefined Bookmarks

Name	Type	Location	Description
▼ WEB_APPS (6)			
FortiAnalyzer_WEB	HTTP/HTTPS	192.168.100.12	192.168.100.12
FortiManager_WEB	HTTP/HTTPS	192.168.100.13	192.168.100.13
VMWare_ESXi	HTTP/HTTPS	192.168.100.150	192.168.100.150
Windows Server 20...	RDP Native	192.168.100.10	
Fortigate_SSH	SSH	192.168.100.1	192.168.100.1
SERVER_FTP	FTP	192.168.100.10	192.168.100.10

Limit Users to One SSL-VPN Connection at a Time

2. Creating a user and user group

Go to **User & Device > User > User Definition** and create a new local user.

The screenshot shows a four-step wizard for creating a user:

- Step 1: Choose User Type**
 - Local User
 - Remote RADIUS User
 - Remote TACACS+ User
 - Remote LDAP User
- Step 2: Specify Login Credential**
 - User Name:
 - Password:
- Step 3: Provide Contact Info**
 - Email Address:
 - SMS
 - Phone Number:
 - Service Type:
- Step 4: Provide Extra Info**
 - Enable
 - Two-factor Authentication
 - User Group

Go **User & Device > User > User Groups** and create a new user group. Set **Members** to include the new user.

The screenshot shows the configuration for a user group:

- Name:
- Type (RSSO): Firewall Fortinet Single Sign-On (FSSO) Guest RADIUS Single Sign-On
- Members:
- Remote groups:
 - Buttons: Add, Edit, Delete
 - Table:

Remote Server	Group Name
No matching entries found	

3. Configuring the VPN tunnel

Go to **VPN > SSL > Settings** and set **Listen on Interface(s)** to **wan1**.

Set **Listen on Port** to **10443** and **Specify custom IP ranges** using the default SSL VPN tunnel addresses.

Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s) X +
This is generally your external interface (i.e. wan1)

Listen on Port

Restrict Access Allow access from any host Limit access to specific hosts

Idle Logout Logout users when inactive for specified period Never logout inactive users

Inactive For (Seconds)

Server Certificate

Require Client Certificate

Tunnel Mode Client Settings

Once connected in tunnel mode, clients will receive these settings.

Address Range Automatically assign addresses Specify custom IP ranges

IP Ranges X +
 X

Under **Authentication/Portal Mapping**, add the new user group.

Users/Groups	Realm	Portal
sslvpn_group	/	full-access
All Other Users/Groups	/	web-access

4. Creating security policies

Go to **Policy & Objects > Policy > IPv4**.

Add a security policy allowing access to the internal network through the *ssl.root* VPN tunnel interface.

Set **Incoming Interface** to **ssl.root**.

Set **Source Address** to **all** and select the **Source User** new user group.

Set **Outgoing Interface** to the local network interface so that the remote user can access the internal network.

Set **Destination Address** to **all**, enable **NAT**, and configure any remaining firewall and security options as desired.

Incoming Interface +

Source Address +

Source User(s) X +

Source Device Type

Outgoing Interface +

Destination Address +

Schedule

Service +

Action

Firewall / Network Options

NAT








Use Destination Interface Address Fixed Port

Use Dynamic IP Pool

Use Central NAT Table

Add a second security policy allowing SSL VPN access to the Internet.

For this policy, **Incoming Interface** is set to **ssl.root** and **Outgoing Interface** is set to your Internet-facing interface.

Incoming Interface	ssl.root (sslvpn tunnel interface) 
Source Address	all 
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan1 
Destination Address	all 
Schedule	always 
Service	ALL 
Action	ACCEPT 

3. Results

Using your Window Phone's web browser, access the portal. The portal's address is the IP address of your Internet-facing interface with the port the SSL VPN tunnel is listening to, and it must be accessed using HTTPS (in the example, <https://201.21.161.9:10443>).

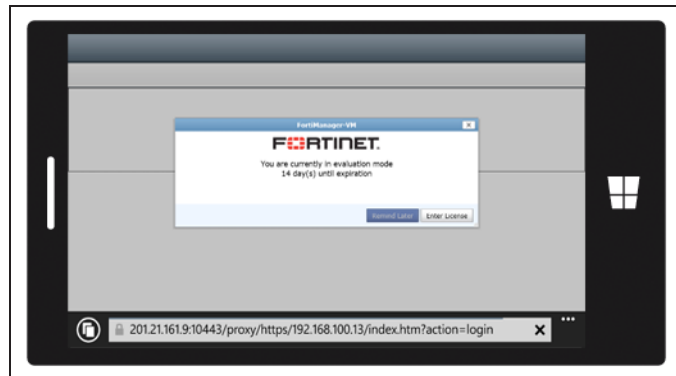
Log in using the credentials for your SSL VPN user.



After your credentials are accepted, you will be able to see the VPN portal.

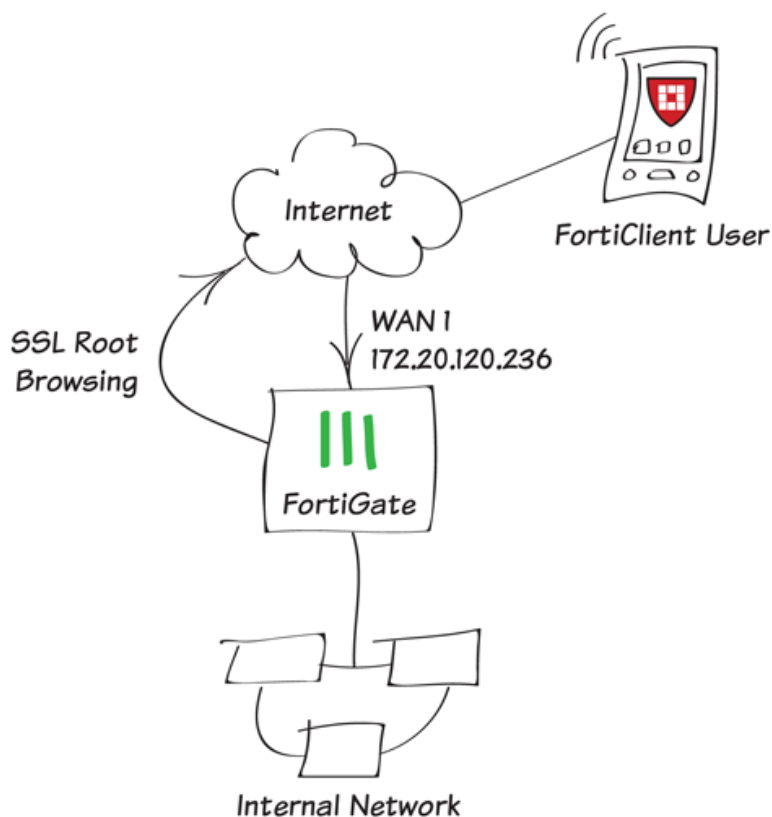


Select one of the pre-defined bookmarks (in the example, the bookmark for a FortiManager device). You will be able to access the network resource.



For further reading, check out [The SSL VPN web portal](#) in the [FortiOS 5.2 Handbook](#).

SSL VPN using FortiClient for iOS



In this recipe, you will create an SSL VPN that remote users connect to using FortiClient running on iOS.

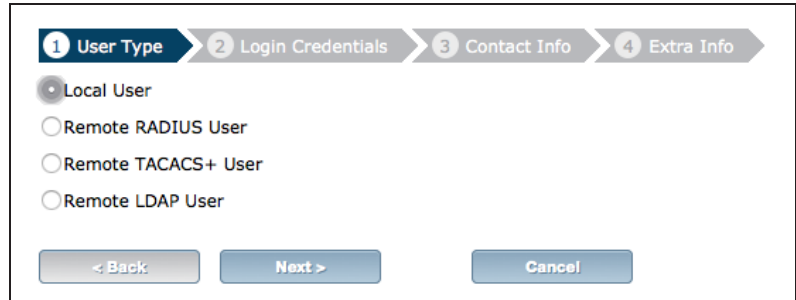
When a user using an iOS device connects to this SSL VPN, they can access servers and data on the internal network. They can also securely browse the Internet using the FortiGate's Internet connection.

This example uses FortiClient 5.2.0.028 for iOS. FortiClient can be downloaded from www.forticlient.com.

1. Creating users and a user group

Go to **User & Device > User > User Definition**.

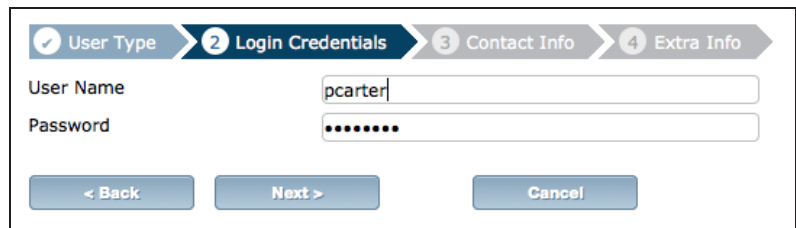
Add as many local users as required with the **User Creation Wizard**.



1 User Type 2 Login Credentials 3 Contact Info 4 Extra Info

Local User
 Remote RADIUS User
 Remote TACACS+ User
 Remote LDAP User

< Back Next > Cancel



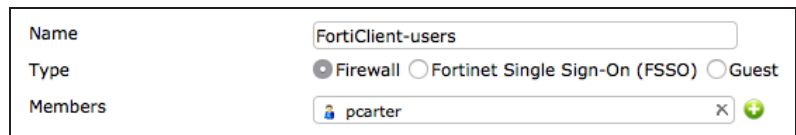
1 User Type 2 Login Credentials 3 Contact Info 4 Extra Info

User Name pcarter
Password

< Back Next > Cancel

Go to **User & Device > User > User Groups**.

Create a user group for FortiClient users and add the new user(s) to the group.



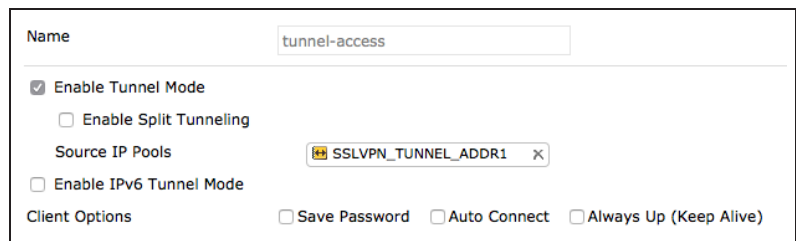
Name FortiClient-users
Type Firewall Fortinet Single Sign-On (FSSO) Guest
Members pcarter

2. Creating an SSL VPN portal

Go to **VPN > SSL > Portals**.

Edit the **tunnel-access** portal. This portal supports tunnel mode by default.

Enable Split Tunneling is *not* enabled so that all SSL VPN traffic will go through the FortiGate unit.



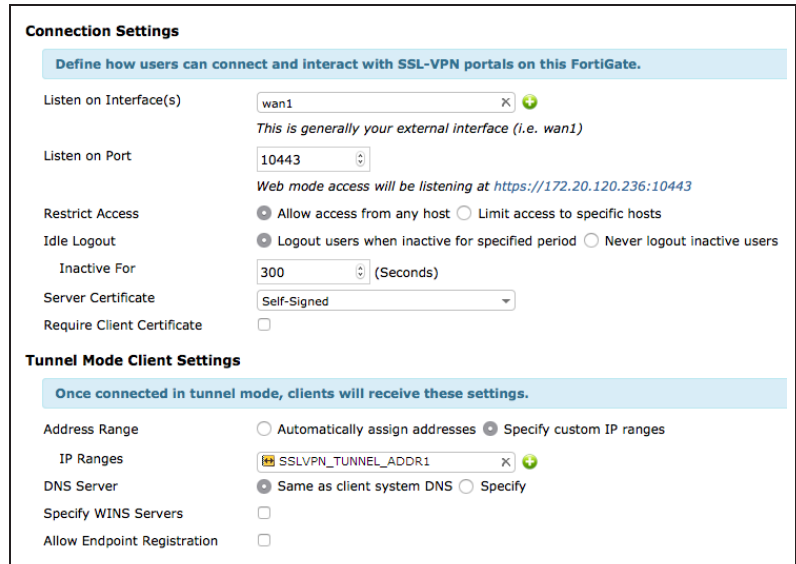
Name tunnel-access

Enable Tunnel Mode
 Enable Split Tunneling
Source IP Pools SSLVPN_TUNNEL_ADDR1
 Enable IPv6 Tunnel Mode
Client Options Save Password Auto Connect Always Up (Keep Alive)

3. Configuring the SSL VPN tunnel

Go to **VPN > SSL > Settings** and set **Listen on Interface(s)** to wan1.

Set **Listen on Port** to 10443 and **Specify custom IP ranges**. Use the default IP Range, `SSLVPN_TUNNEL_ADDR1`.



Connection Settings
Define how users can connect and interact with SSL-VPN portals on this FortiGate.

Listen on Interface(s)
This is generally your external interface (i.e. wan1)

Listen on Port
Web mode access will be listening at https://172.20.120.236:10443

Restrict Access Allow access from any host Limit access to specific hosts

Idle Logout Logout users when inactive for specified period Never logout inactive users

Inactive For (Seconds)

Server Certificate

Require Client Certificate

Tunnel Mode Client Settings
Once connected in tunnel mode, clients will receive these settings.

Address Range Automatically assign addresses Specify custom IP ranges

IP Ranges

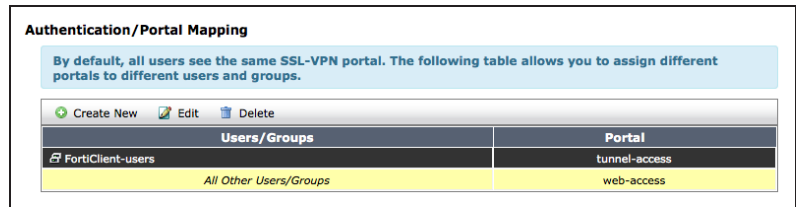
DNS Server Same as client system DNS Specify

Specify WINS Servers

Allow Endpoint Registration

At the bottom of the page, under **Authentication/Portal Mapping**, add the FortiClient user group.

If necessary, map a portal for **All Other Users/Groups**.



Authentication/Portal Mapping
By default, all users see the same SSL-VPN portal. The following table allows you to assign different portals to different users and groups.

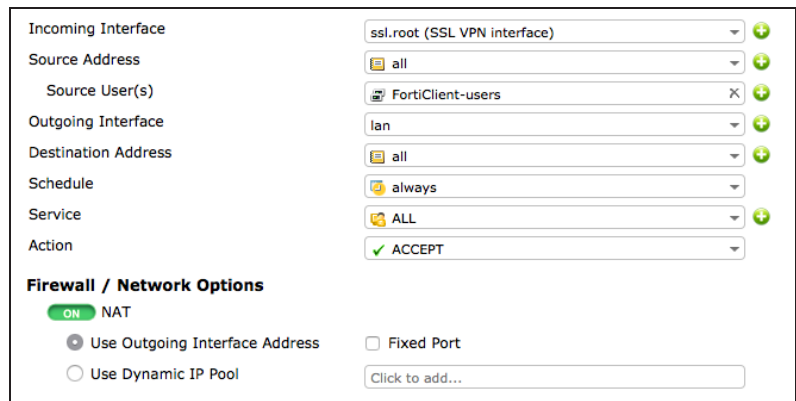
Users/Groups	Portal
FortiClient-users	tunnel-access
All Other Users/Groups	web-access

4. Adding security policies for access to the Internet and internal network

Go to **Policy & Objects > Policy > IPv4**. Create a security policy allowing SSL VPN user to access the internal network.

Set **Incoming Interface** to `ssl.root`. Set **Source Address** to `all` and **Source User** to the new user group. Set **Outgoing Interface** to the local network interface so that the remote user can access the internal network.

Set **Destination Address** to `all`, enable **NAT**, and configure any remaining



Incoming Interface

Source Address

Source User(s)

Outgoing Interface

Destination Address

Schedule

Service

Action

Firewall / Network Options

NAT

Use Outgoing Interface Address Fixed Port

Use Dynamic IP Pool

firewall and security options as desired.

Add a second security policy allowing SSL VPN users to access the Internet.

For this policy, **Incoming Interface** is set to **ssl.root** and **Outgoing Interface** is set to **wan1**.

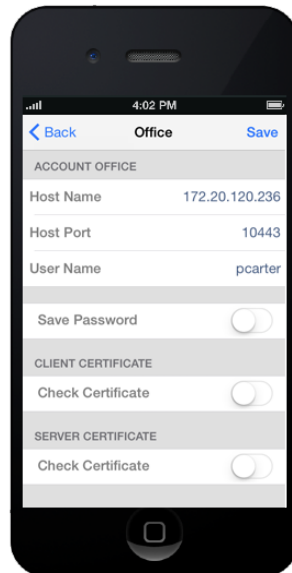
Incoming Interface	ssl.root (SSL VPN interface)	+
Source Address	all	+
Source User(s)	FortiClient-users	X +
Outgoing Interface	wan1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	
Firewall / Network Options		
<input checked="" type="checkbox"/> ON NAT		
<input checked="" type="radio"/> Use Outgoing Interface Address		
<input type="radio"/> Use Dynamic IP Pool		
<input type="checkbox"/> Fixed Port		
<input type="text" value="Click to add..."/>		

5. Configuring FortiClient for SSL VPN in iOS

Install **FortiClient** on the iOS device.

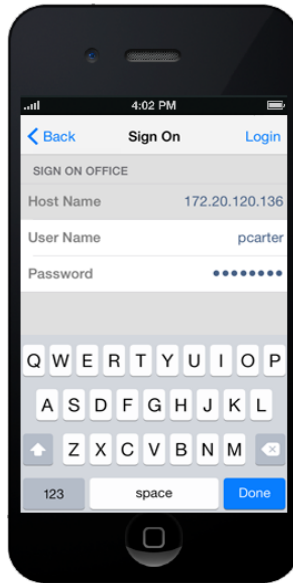
Add a new VPN Gateway.

Set **Host Name** to the FortiGate's IP (in the example, *172.20.120.236*), set **Host Port** to *10443*, and set **User Name** to match the new user account.

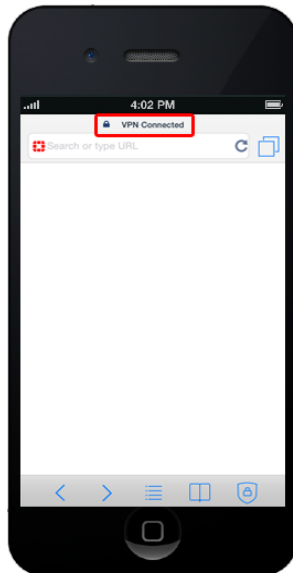


6. Results

Select the VPN in FortiClient. Enter the **Password** and select **Login**.



You will be able to connect to the VPN.



On the FortiGate, go to **VPN > Monitor > SSL-VPN Monitor** to see that the user has connected.

<input type="checkbox"/>	No.	User	Source IP	Begin Time
<input type="checkbox"/>	1	pcarter	172.20.130.254	Thu Jan 15 10:44:34 2015

For further reading, check out [FortiClient](#) in the [FortiOS 5.2 Handbook](#).

SSL VPN troubleshooting

This page contains tips to help you with some common challenges for SSL VPN.

There is no response from the SSL VPN URL.

Go to **VPN > SSL > Settings** and check the SSL VPN port assignment. Also, verify that the SSL VPN policy is configured correctly.

You receive an error stating that the web page cannot be found.

Check the URL you are attempting to connect to. It should follow this pattern:

https://:/remote/login.

Ensure that you are using the correct port number for the part of the URL.

FortiClient cannot connect.

Read the [Release Notes](#) to ensure that the version of FortiClient you are using is compatible with your version of FortiOS.

When you attempt to connect using FortiClient or in Web mode, you receive the following error message: "Unable to logon to the server. Your user name or password may not be configured properly for this connection. (-12)."

Ensure that cookies are enabled in your browser. Also, if you are using a remote authentication server, ensure that the FortiGate is able to communicate with it.

The tunnel connects but there is no communication.

Go to **Router > Static > Static Routes** (or **System > Network > Routing** on some FortiGate models) and ensure that there is a static route to direct packets destined for the tunnel users to the SSL VPN interface.

You can connect remotely to the VPN tunnel but are unable to access the network resources.

Go to **Policy & Objects > Policy > IPv4** and check the policy allowing VPN access to the local network. If the destination address is set to all, create a firewall address for the internal network. Change the destination address and attempt to connect remotely again.

Users are unable to download the SSL VPN plugin.

Go to at **VPN > SSL > Portals** to check the VPN Portal to ensure that the option to **Limit Users to One SSL-VPN Connection at a Time** is disabled. This allows users to connect to the resources on the portal page while also connecting to the VPN through FortiClient.

Users are being assigned to the wrong IP range.

Ensure that the same IP Pool is used in VPN Portal and VPN Settings to avoid conflicts. If there is a conflict, the portal settings will be used.

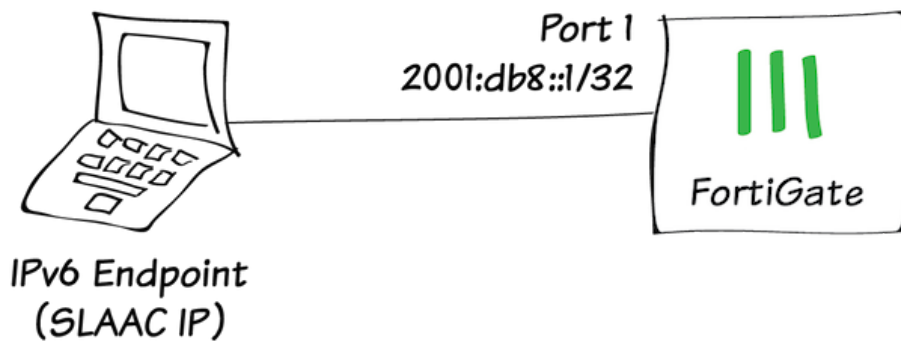
IPv6

Internet Protocol version 6 (IPv6) is the most significant advance in traditional Internet communications protocol. The IPv6 address scheme is based on a 128-bit address, rather than the 32-bit addresses used by IPv4, allowing IPv6 to have a much higher address limit of over 340 undecillion possible addresses (that is 340 followed by 36 zeros).

FortiGates support IPv6 in a wide variety of network configurations.

- [Creating an IPv6 interface using SLAAC](#)

Creating an IPv6 interface using SLAAC



In this example you will configure your FortiGate to use Stateless Address Auto Configuration (SLAAC) to assign IPv6 addresses to IPv6-enabled devices on your internal network.

The IPv6 address block used in this recipe (2001:db8::/32) is reserved for documentation purposes and will not work on your network. If you're not sure how to determine the correct IPv6 address for your environment, refer to the [FortiOS IPv6 Handbook Chapter](#).

1. Enabling IPv6

Go to **System > Config > Features** and make sure that **IPv6** is turned **ON**.



2. Configuring a FortiGate interface for IPv6

Go to **System > Network > Interfaces** and edit the interface connected to your internal network (in the example, port1).

Set the **IPv6 Addressing mode** to **Manual**

and enter the **IPv6 Address/Prefix** for the interface (in this example, 2001:db8::1/32).

Interface Name	port1(00:09:0F:BC:0E:68)
Alias	<input type="text"/>
Link Status	Up
Type	Physical Interface
Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> Dedicated to Extension Device
IP/Network Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
IPv6 Addressing mode	<input checked="" type="radio"/> Manual <input type="radio"/> DHCP
IPv6 Address/Prefix	<input type="text" value="2001:db8::1/32"/>

The interface can have both IPv4 and IPv6 addressing. This example only includes IPv6 addressing.

Enter this CLI command to add the router advertisements and specific IPv6 prefixes required to configure SLAAC on the interface.

```
config system interface
edit port1
config ipv6
set ip6-address 2001:db8::1/32
set ip6-send-adv enable
config ip6-prefix-list
edit 2001:db8::/32
set autonomous-flag enable
set onlink-flag enable
end
end
end
```

The `set ip6-address` option is not required since you already added an IPv6 address to the interface from the GUI. But its included in the example to show the complete CLI configuration.

3. Adding IPv6 firewall addresses

Go to **Policy & Objects > Objects > Addresses > Create New**.

Add an IPv6 firewall address that matches the IPv6 address added to the port1 interface.

Category	<input type="radio"/> Address <input checked="" type="radio"/> IPv6 Address
Name	port1-IPv6-address
Type	Subnet
IPv6 Address	2001:db8::1/32
Visibility	<input checked="" type="checkbox"/>
Comments	matches the port1 IPv6 address 30/255

4. 'Bouncing' the IPv6 interface

You can now 'bounce' the port1 interface (bring the interface down and then back up). Go to **System > Network > Interfaces**, edit the port1 interface and set the **Administrative Access** to **Down**. Select **OK**, then edit the interface again and set the **Administrative Access** back to **Up**. This causes a router advertisement using the Neighbor Discovery Protocol, which performs address autoconfiguration and determines the reachability of neighboring nodes.

Alternatively, you can reboot the FortiGate or wait for the next router advertisement.

5. Results

Connect a computer to the port1 interface. Configure the computer to get an IPv6 address automatically. Then, from a command prompt or terminal session enter the command `ipconfig` to view the computer's IP configuration.

```
IPv6 Address.....: 2001:db8::44d2:ed21:9733:9245
```

You should see that an IPv6 address has been assigned with the prefix advertised on the port1 interface.

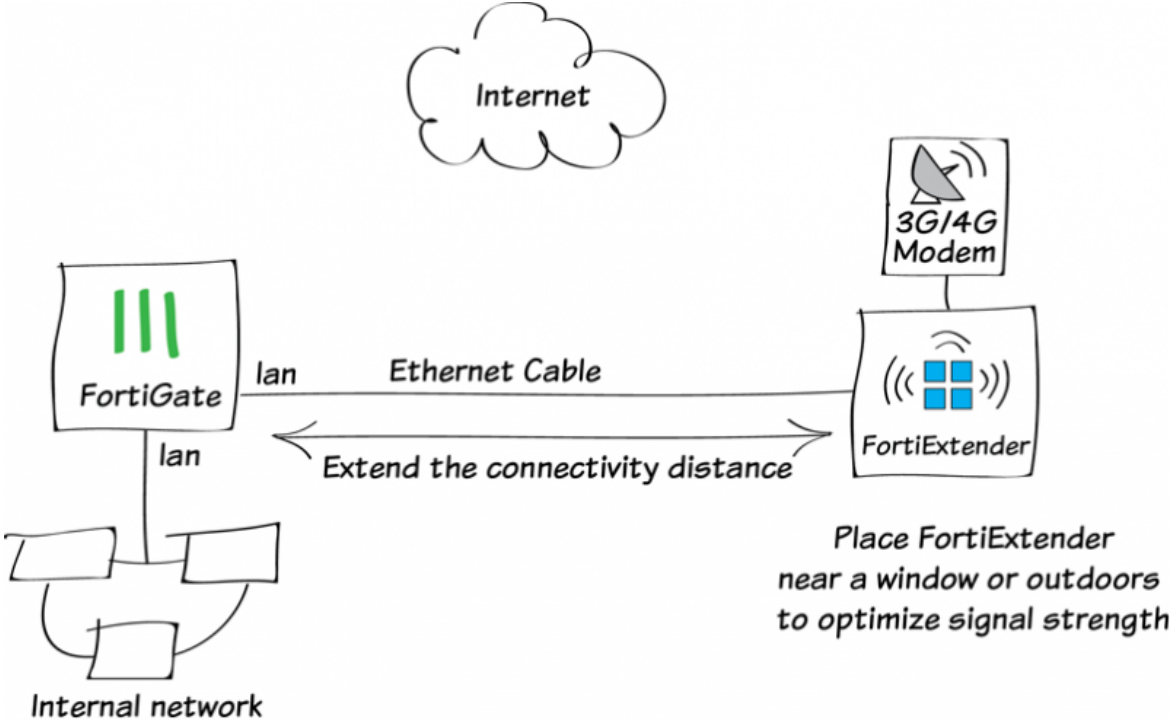
For further reading, check out [IPv6](#) in the [FortiOS 5.2 Handbook](#).

Fortinet Integration

This section contains information about using other Fortinet products alongside a FortiGate. For more information about any of the Fortinet products used in these recipes, go to www.fortinet.com.

- [FortiExtender installation](#)
- [WiFi with external RADIUS authentication \(FortiAuthenticator\)](#)
- [Remotely accessing FortiRecorder through a FortiGate](#)

FortiExtender installation



This example shows how to set an internet connection using a 3G/4G modem and a FortiExtender. A FortiExtender is used when the FortiGate unit is located in an area without 3G/4G network coverage, the FortiExtender can be placed near a window or outdoors.

For information about the compatibility of FortiExtender and various modems, see the [FortiGate and FortiExtender Modem Compatibility Matrix](#).

1. Installing the 3G/4G modem in the FortiExtender

Remove the housing cover of the FortiExtender and use the provided USB extension cable to connect your 3G/4G modem to the device.

For more information on installing the 3G/4G modem, see the QuickStart Guide.



2. Connecting the FortiExtender

Use an Ethernet cable to connect the FortiExtender to the **lan** interface of a FortiGate unit.

Once connected, FortiGate can control FortiExtender and modem.

Enable FortiExtender in the FortiGate's CLI.

CAPWAP service must be enabled on the port to which FortiExtender is connected, **lan** interface in this example.

```
config system global
  set fortiextender enable
  set wireless-controller enable
end

config system interface
  edit lan
    append allowaccess capwap
  end
end
```


Once enabled, it appears as a virtual WAN interface in the FortiGate, such as **fext-wan1**. Go to **System > Network > Interface** to verify **fext-wan1** interface.






lan	Hardware Switch (16)
fext-wan1	FortiExtender

3. Configuring the FortiExtender

Go to **System > Network > FortiExtender** and authorize the FortiExtender.

Once authorized, you can see the status of the FortiExtender.

Primary	
Serial Number	FX100B3X14000077
Administrative Status	 Deauthorized [Authorize]

Primary	
Serial Number	FX100B3X14000077
Model	FX100B
Administrative Status	 Authorized [Deauthorize]
Link Status	 Up [Details]
MAC Address	8:5b:e:5b:71:d0
IP Address	192.168.1.100
OS Version	FX100B-v1.0-build024 [Upgrade]
Network	 N/A
Data Usage	
Current Usage	
	
Last Month Usage	
	
Configure Settings Diagnostics	

4. Modem settings

The FortiExtender unit allows for two modes of operation for the modem; On Demand and Always Connect.

Go to **System > Network > FortiExtender** and click on **Configuring Settings**.

Select **Always Connect** for **Dial Mode** and keep other settings to default.

Settings for FX100B3X14000077 - Primary

- ▼ **Modem Settings**
 - Dial Mode On Demand Always Connect
 - Redial Limit
 - Quota Limit (MB)
- ▼ **PPP Authentication**
 - Username
 - Password
 - Authentication Protocol
- ▶ **General**
- ▶ **GSM / LTE**
- ▶ **CDMA**

5. Configuring the FortiGate

Go to **Router > Static > Static Routes** and add new route through **fext-wan1** interface.

Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Device	<input type="text" value="fext-wan1"/>
Gateway	<input type="text" value="0.0.0.0"/>
Distance	<input type="text" value="5"/> (1-255, Default=10)
Priority	<input type="text" value="0"/> (0-4294967295)
Comments	<input type="text" value="Write a comment..."/>

Go to **Policy & Objects > Policy > IPv4** and create a new security policy allowing traffic from **lan** interface to **fext-wan1** interface.

Incoming Interface	lan	
Source Address	all	
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	fext-wan1	
Destination Address	all	
Schedule	always	
Service	ALL	
Action	ACCEPT	

Firewall / Network Options

NAT

Use Destination Interface Address Fixed Port

Use Dynamic IP Pool

Use Central NAT Table

Web Cache

WAN Optimization

6. Results

Browse the Internet and go to **Policy & Objects > Policy > IPv4** to verify the Count.

Seq.#	ID	Source	Destination	Count
▼ ike-bgp-fgt1 - lan (1 - 1)				
4	8	all	all	0 Packets / 0 B
▼ lan - fext-wan1 (2 - 2)				
6	9	all	all	8,441 Packets / 2.19 MB
▼ lan - ike-bgp-fgt1 (3 - 3)				
3	7	all	all	0 Packets / 0 B
▼ lan - wan1 (4 - 4)				
5	10	all	all	974,394 Packets / 664.12 MB

Go to **Log & Report > Traffic Log > Forward Traffic**.

You can see that traffic flowing from **lan** interface to **fext-wan1** interface.

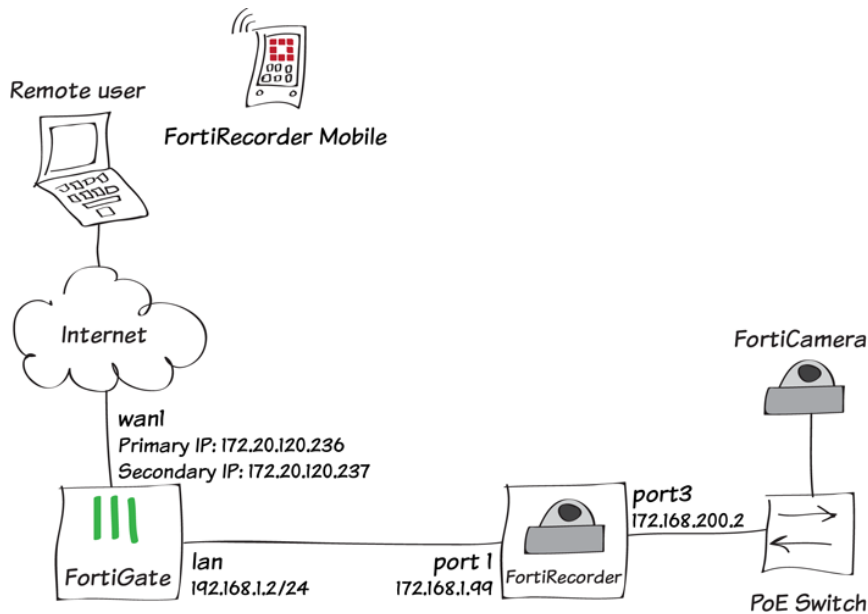
▼ Date...	▼ Policy ...	▼ Src Interface	▼ Dst Interface
15:38:03	9	lan	fext-wan1
15:37:47	9	lan	fext-wan1
15:37:43	9	lan	fext-wan1
15:37:39	9	lan	fext-wan1
15:37:35	9	lan	fext-wan1
15:37:31	9	lan	fext-wan1
15:37:19	9	lan	fext-wan1
15:37:07	9	lan	fext-wan1
15:36:59	9	lan	fext-wan1
15:36:55	9	lan	fext-wan1
15:36:31	9	lan	fext-wan1
15:36:27	9	lan	fext-wan1

Select an entry for details.

Action	ip-conn	Date/Time	15:35:51 (1405006551)
Destination	10.10.80.25	Dst Interface	fext-wan1
Dst Port	161	Level	warning ■■■■ ■■■■
Log ID	11	Policy ID	9
Security Events		Sent / Received	N/A / N/A
Sequence Number	10016	Source	192.168.1.101
Src Interface	lan	Src Port	56442
Sub Type	forward	Threat	262144
Threat Score	1375731722	Timestamp	7/10/2014, 3:35:51 PM
Virtual Domain	root		

For further reading, check out [FortiExtender](#) in the [FortiOS 5.2 Handbook](#).

Remotely accessing FortiRecorder through a FortiGate



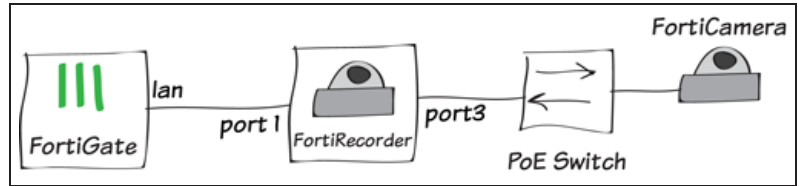
In this recipe, you set up a FortiGate with a secondary IP to provide remote access to a FortiRecorder. This allows you to securely view live FortiCamera video feeds over the Internet, using either the FortiRecorder GUI, FortiRecorder Mobile, or FortiRecorder Central.

This recipe employs a secondary IP and two port forwarding virtual IPs to forward HTTPS and Real Time Streaming Protocol (RTSP) packets from the Internet to the FortiRecorder. To use a secondary IP address you must have a second Internet IP address for your FortiRecorder. Instead of adding this IP address to the FortiRecorder, you add it to your FortiGate and forward traffic for the FortiRecorder IP address through the FortiGate.

1. Connect the hardware

Connect your devices as shown in the diagram.

In this example, the FortiCamera connects to a PoE switch, which is then connected to **port3** on the FortiRecorder. The FortiRecorder's **port1** connects to the FortiGate **lan** interface.



2. Configuring the FortiRecorder and FortiCamera

On the FortiRecorder, go to **System > Network > Interface** and edit **port1**. Set a manual **IP/Netmask** for the interface that is on the same subnet as the FortiGate **lan** interface (in the example, *192.168.1.99*).

Set **Access** to allow HTTPS and any other protocols you require. If you are using FortiRecorder Central, you must enable **FRC-Central**.

Interface name: port1 (8c:89:a5:5f:a5:a5)

Discover cameras on this port

Addressing Mode

Manual

IP/Netmask: /

IPv6/Netmask: /

DHCP

Retrieve default gateway and DNS from server

Connect to server

Access

HTTPS PING HTTP FRC-Central

SSH SNMP TELNET

MTU

Override default MTU value (1500)

(bytes)

Administrative status Up Down

Edit **port3**. Make sure that **Discover cameras on this port** is enabled. Set a manual **IP/Netmask** for the interface.

Interface name: port3 (8c:89:a5:5f:a5:a7)

Discover cameras on this port

Addressing Mode

Manual

IP/Netmask: /

IPv6/Netmask: /

DHCP

Retrieve default gateway and DNS from server

Connect to server

Go to **System > Network > DHCP** and create a new DHCP server. Set **Interface** to **port3** and **Gateway** to port3's IP address (in the example, *192.168.200.2*).

Create a new **DHCP IP Range** that is on the same subnet as port3.

ID:

Enable DHCP server:

Interface:

Gateway:

DNS options:

DNS server 1:

DNS server 2:

Domain:

Netmask:

Auto Config Setting

Lease time (Seconds):

Conflicted IP timeout (Seconds):

DHCP IP Range

Start	End
192.168.2.100	192.168.2.200

Go to **System > Network > Routing**. Add a default route that uses the IP address of the FortiGate's lan interface (in the example, 192.168.1.2). Set **Interface** to **port1**.

Destination IP/netmask:	0.0.0.0	/	0
Interface:	port1		
Gateway:	192.168.1.2		

Go to **Camera > Configuration > Camera**. Click on **Force Discover** to have connected cameras displayed.

Camera Name	Vendor	Model	Version	Location	Address	MAC Address	Profile	Status
FCM-MB13-605a	Fortinet	FCM-MB13			192.168.200.101	00:22:14:ce:60:5a		Not Configured

The FortiCamera will appear on the list, with the **Status** column displayed as **Not Configured**.

Select the FortiCamera and select **Configure**. Set the unit's **Name** and **Location**, and **Profile**, as well as any other required configuration settings.

If you do not have any profiles already created, you will have to configure one. For more information, see the [FortiRecorder 2.0.0 Administration guide](#).

Enabled:	<input checked="" type="checkbox"/>	
Name:	big-sister	
Location:	everywhere	
Vendor:	Fortinet	Camera detail
Model:	FCM-MB13	
Address mode:	Wired	
Address:	192.168.200.101	Port: 443
Transport type:	UDP	Port: 554
Profile:	Motion-detect	New... Edit...

3. Adding a secondary IP to the FortiGate

From the FortiGate GUI, go to **System > Network > Interfaces** and edit your Internet-facing interface.

Enable **Secondary IP Address** and create a new **IP/Network Mask** for the interface.

Secondary IP Address	
IP/Network Mask	172.20.120.237/255.255.255.0
Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> CAPWAP <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET

Adding a secondary IP address allows the FortiGate and the network to see two IP addresses, the primary and the secondary, that terminate at the interface.

In this example, the primary IP address is used to connect to the FortiGate, while the secondary IP will be used to connect to the FortiRecorder.

Interface Name: wan1(00:09:0F:B0:EB:EA)

Alias: []

Link Status: Up

Type: Physical Interface

Addressing mode: Manual DHCP PPPoE Dedicated to Extension Device

IP/Network Mask: 172.20.120.237/255.255.255.0

IPv6 Addressing mode: Manual DHCP

IPv6 Address/Prefix: ::/0

Administrative Access: HTTPS PING HTTP FMG-Access CAPWAP

SSH SNMP FCT-Access

Auto IPsec Request

IPv6 Administrative Access: HTTPS PING HTTP FMG-Access CAPWAP

SSH SNMP

DHCP Server: Enable

Security Mode: None

Device Management: Detect and Identify Devices

Enable Explicit Web Proxy:

Listen for RADIUS Accounting Messages:

Secondary IP Address:

IP / Network Mask	Administrative Access
172.20.120.237/255.255.255.0	

4. Creating virtual IPs

From the FortiGate GUI, go to **Policy & Objects > Objects > Virtual IPs**. Create the two virtual IPs: one for HTTPS traffic and one for RTSP traffic.

For both virtual IPs, set **External Interface** to your Internet-facing interface, **External IP Address/Range** to the secondary IP of that interface (in the example, 172.20.120.237) and the **Mapped IP Address/Range** to the IP of port1 on the FortiRecorder unit (in the example, 192.168.1.99).

Enable **Port Forwarding** and use the standard port for each protocol. HTTPS uses TCP port 443 and RTSP uses TCP port 554.

VIP Type: IPv4 VIP IPv6 VIP NAT46 VIP NAT64 VIP

Name: FortiRecorder_HTTPS

Comments: [] 0/255

Interface: wan1

Type: Static NAT

Source Address Filter

External IP Address/Range: 172.20.120.237 - 172.20.120.237

Mapped IP Address/Range: 192.168.1.99 - 192.168.1.99

Port Forwarding

Protocol: TCP UDP SCTP ICMP

External Service Port: 443 - 443

Map to Port: 443 - 443

VIP Type IPv4 VIP IPv6 VIP NAT46 VIP NAT64 VIP

Name

Comments 0/255

Interface

Type **Static NAT**

Source Address Filter

External IP Address/Range -

Mapped IP Address/Range -

Port Forwarding

Protocol TCP UDP SCTP ICMP

External Service Port -

Map to Port -

If you are using FortiRecorder Central, you must create a third virtual IP to allow TCP port 8550.

VIP Type IPv4 VIP IPv6 VIP NAT46 VIP NAT64 VIP

Name

Comments 0/255

Interface

Type **Static NAT**

Source Address Filter

External IP Address/Range -

Mapped IP Address/Range -

Port Forwarding

Protocol TCP UDP SCTP ICMP

External Service Port -

Map to Port -

5. Creating a security policy to access to the FortiRecorder

Go to **Policy & Object > Policy > IPv4** and create a new policy that allows access to the FortiRecorder from the Internet.

Set **Incoming Interface** to your Internet-facing interface, **Outgoing Interface** to lan, and **Destination Address** to the new virtual IPs.

Incoming Interface +

Source Address +

Source User(s)

Source Device Type

Outgoing Interface +

Destination Address X +
 X
 X

Schedule

Service +

Action

Firewall / Network Options

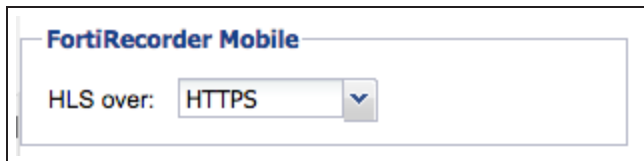
ON NAT

Use Outgoing Interface Address Fixed Port

Use Dynamic IP Pool

6. Configuring FortiRecorder Mobile for iOS

On your FortiRecorder, go to **System > Configuration > Options**. Set **FortiRecorder Mobile** to use **HLS over HTTPS**.



You can also connect using HLS over HTTP, as long as you add another virtual IP to allow TCP port 80.

FortiRecorder Mobile for iOS

Download the FortiRecorder Mobile app onto your iOS device.

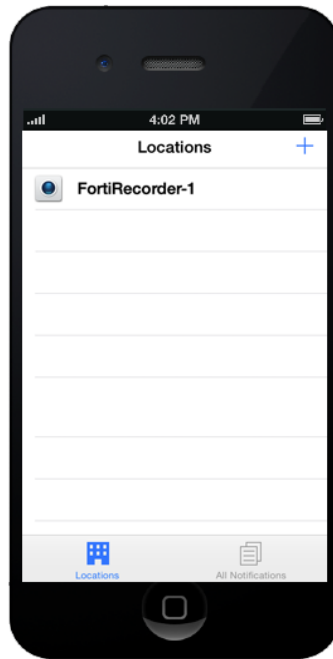
If you will connect using HTTPS, the iOS device must be able to verify the FortiRecorder certificate. To do this, you can either sign the FortiRecorder local certificate with one of the world's largest certificate authorities, whose CA certificate are trusted by the iOS device, or install the CA certificate on the iOS device, if the CA certificate is not trusted by the iOS device. For information about this, see the technical note [Provisioning CA Certificate to iOS Devices for FortiRecorder Mobile](#).

Open FortiRecorder Mobile. Use the **+** to add a new location.

Enter the information for the FortiRecorder device, including the **Address** (in the example, *172.20.120.237*) and the admin account **username** and **password**.



The FortiRecorder is shown in the list of **Locations**.

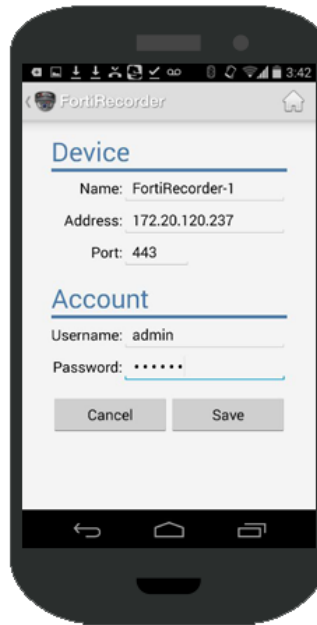


FortiRecorder Mobile for Android

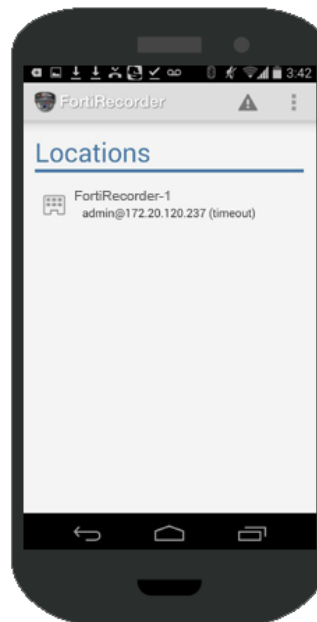
Download the FortiRecorder Mobile app onto your Android device.

Open FortiRecorder Mobile. Select **Add Location**.

Enter the information for the FortiRecorder device, including the **Address** (in the example, *172.20.120.237*) and the admin account **username** and **password**.



The FortiRecorder is shown in the list of **Locations**.



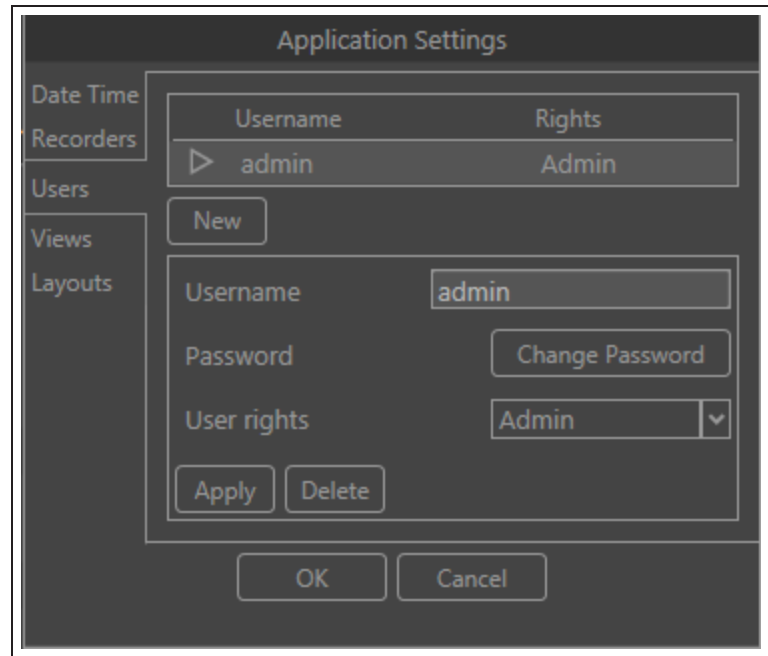
7. Configuring FortiRecorder Central

FortiRecorder Central is a Windows-based video management system that is used to connect and view information from several FortiRecorder units at the same time. It can be downloaded at the [Fortinet Support website](#).

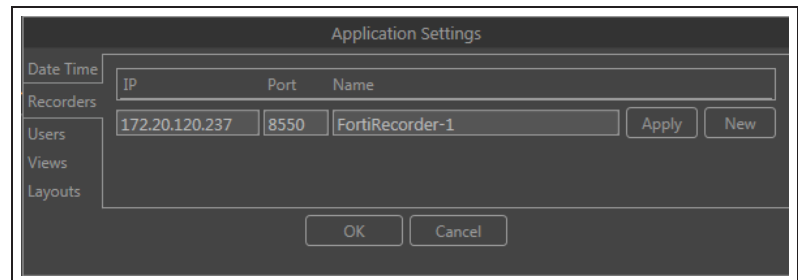
The recipe was written using FortiRecorder Central 1.0.0.

From FortiRecorder Central, use the **Settings** cogwheel in the top right corner to go to **Settings > Users**. Make sure the admin account settings are identical to those on the FortiRecorder because FortiRecorder Central has to be able to log into FortiRecorder using these credentials.

All FortiRecorders must use the same admin credentials in order to be used by FortiRecorder Central.



Go to **Settings > Recorders**. Set the IP to the FortiGate's secondary IP (in this example, `172.20.120.237`).



The FortiRecorder will appear in the list of devices, with its connected cameras listed underneath.

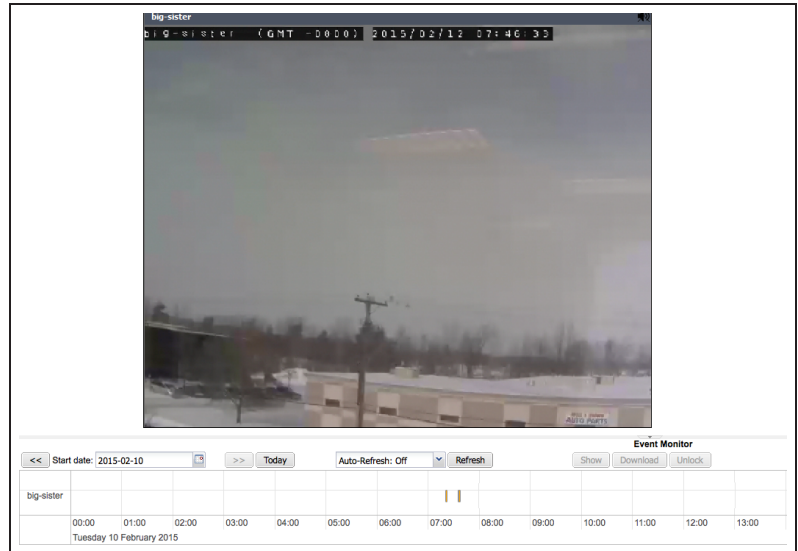


8. Results

From the Internet you can browse to the secondary IP address, using HTTPS (in the example, <https://172.20.120.237>). The FortiRecorder GUI login screen appears.

Go to **Monitor > Video Monitor** to see the live video feed from the FortiCamera.

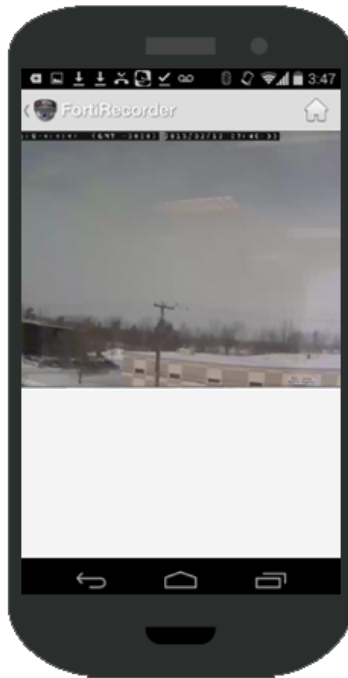
*Quicktime 6.0 or higher is required to view the **Video Monitor**.*



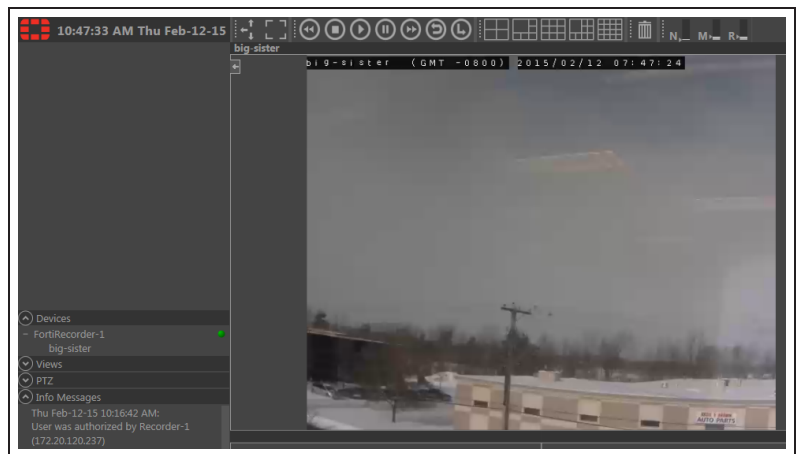
In FortiRecorder Mobile for iOS, go to the **Locations** list and select the FortiRecorder. A list of the available cameras will be shown. Click on the camera you wish to view.



In FortiRecorder Mobile for Android, go to the **Locations** list and select the FortiRecorder, then select **Cameras**. A list of the available cameras will be shown. Click on the camera you wish to view.



In FortiRecorder Central, click on the listing for the FortiCamera and drag it onto a square in the grid. The live video feed will be shown.



Expert

FortiGate units can be deployed in many ways to meet a wide range of advanced requirements. This section contains recipes and articles (which discuss topics in greater depth than a recipe) about a variety of these configurations.

Recipes and articles in this section are intended for users with a high degree of background knowledge about FortiGates and computer networking, such as users who have completed Fortinet's [Network Security Expert \(NSE\) 4](#) level of training.

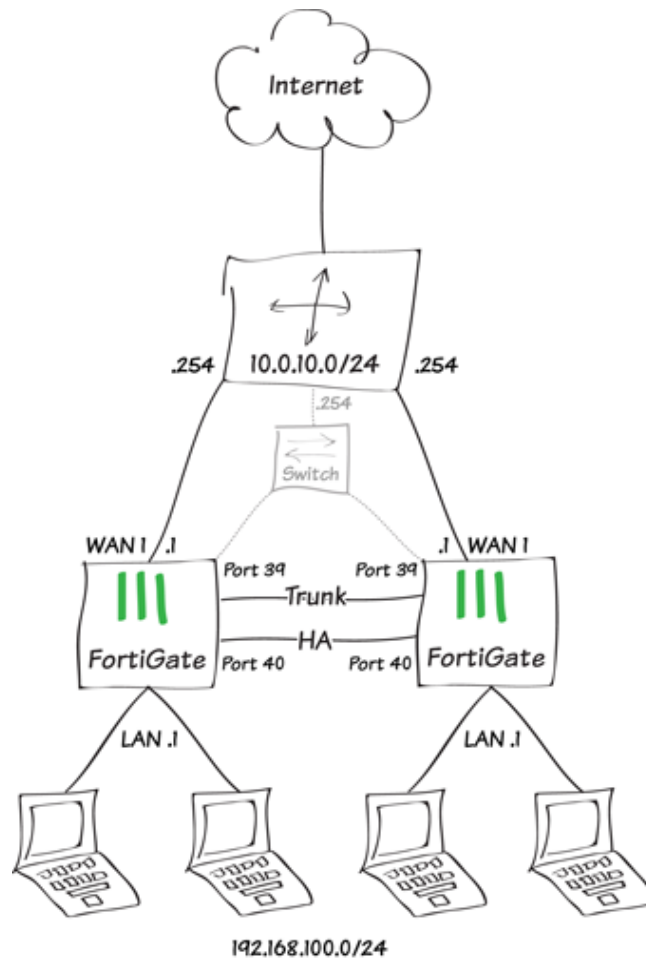
Recipes

- [Redundant architecture](#)
- [BGP over a dynamic IPsec VPN](#)
- [SLBC setup with one FortiController](#)
- [SLBC Active-Passive setup with two FortiControllers](#)
- [SLBC Active-Passive with two FortiControllers and two chassis](#)
- [SLBC Dual Mode setup with two FortiControllers](#)
- [SLBC Active-Passive with four FortiControllers and two chassis](#)

Articles

- [Hub-and-spoke VPN using quick mode selectors](#)

Redundant architecture



The following recipe provides useful instructions for customers with multi-site architecture and redundant firewalls. It is intended for those customers that want to reduce the number of on-site appliances while increasing network security and decreasing Total Cost of Ownership, where the goal is simple, cost-effective reliability.

FortiOS 5.2 introduced many new features that we will use in this configuration, which is therefore not possible on FortiOS 5.0.x or earlier. The recipe is performed with the FortiGate 1xxD/2xxD series.

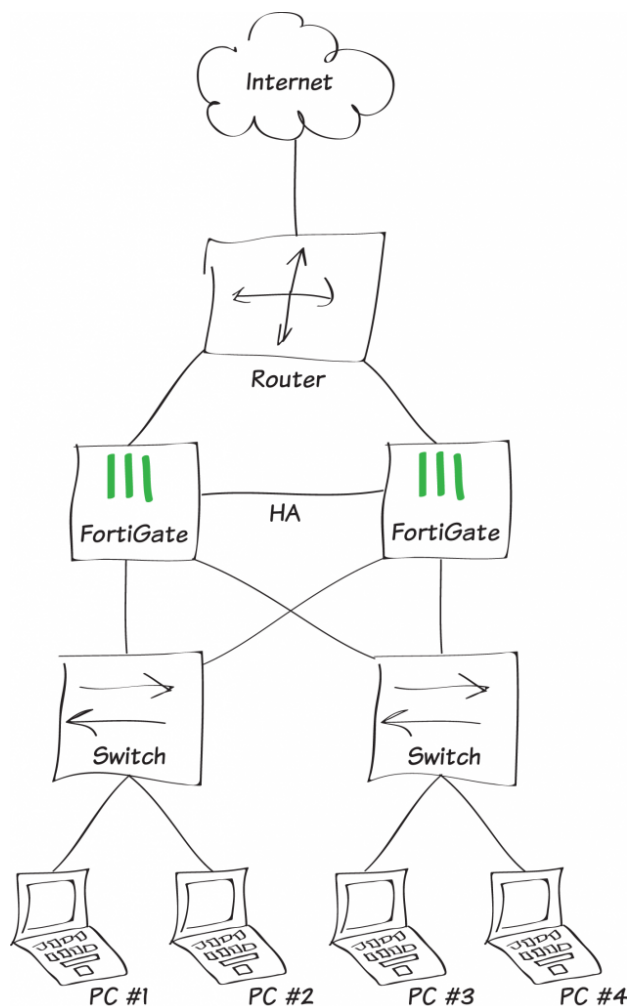
By following the recipe, you will be able to provide your small-site customers with simple, yet secure infrastructure that perfectly matches the UTM approach, where we want to centralize as many security features as possible on a single device or cluster.

The recipe provides task-oriented instructions for administrators to fully complete the installation. It is divided into the following sections:

1. **Scenario:** This section explains the problems that this new network topology solves, including the cases in which the topology should be used.
2. **Topology:** This section includes diagrams of the new topology. It also lists key advantages to this kind of architecture and explains why it solves the problems previously identified in The Scenario.
3. **Configuration:** This section provides step-by-step instructions for configuring the FortiGates within the new topology.

Scenario

In the standard scenario, we assume the following topology as the starting point:



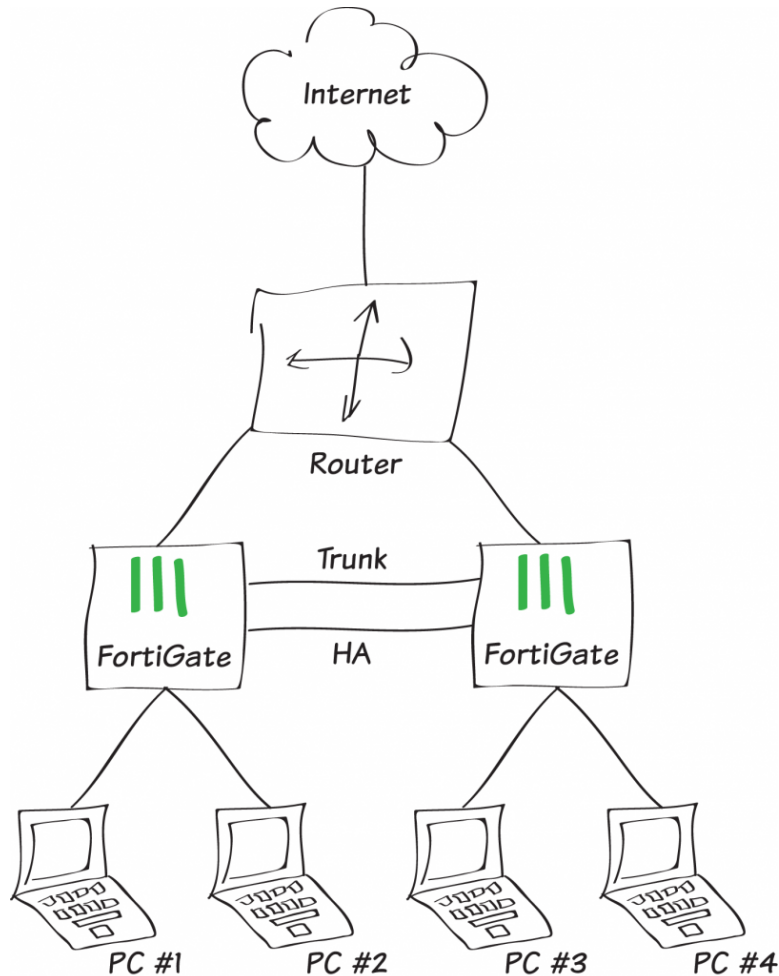
Multi-site customers that want to avoid any “Single Point of Failure” in their remote networks often use this kind of topology. These customers require two FortiGates in Active/Passive mode and therefore two switches on the LAN side to transfer Ethernet payloads to the active FortiGate. There are a few downsides to this approach:

- Four appliances need to be managed and supervised.
- Administrators must know how to work with the Firewall OS and with the Switch OS.
- If one switch fails, the workstations connected won't be able to reach the Internet.
- Most of the firewall ports are not used.

Topology

In this section, we look at the target topology and the scenarios for FortiGate failover. At the end of the section, we discuss the key advantages of adopting the target topology.

2.1 The Target Topology



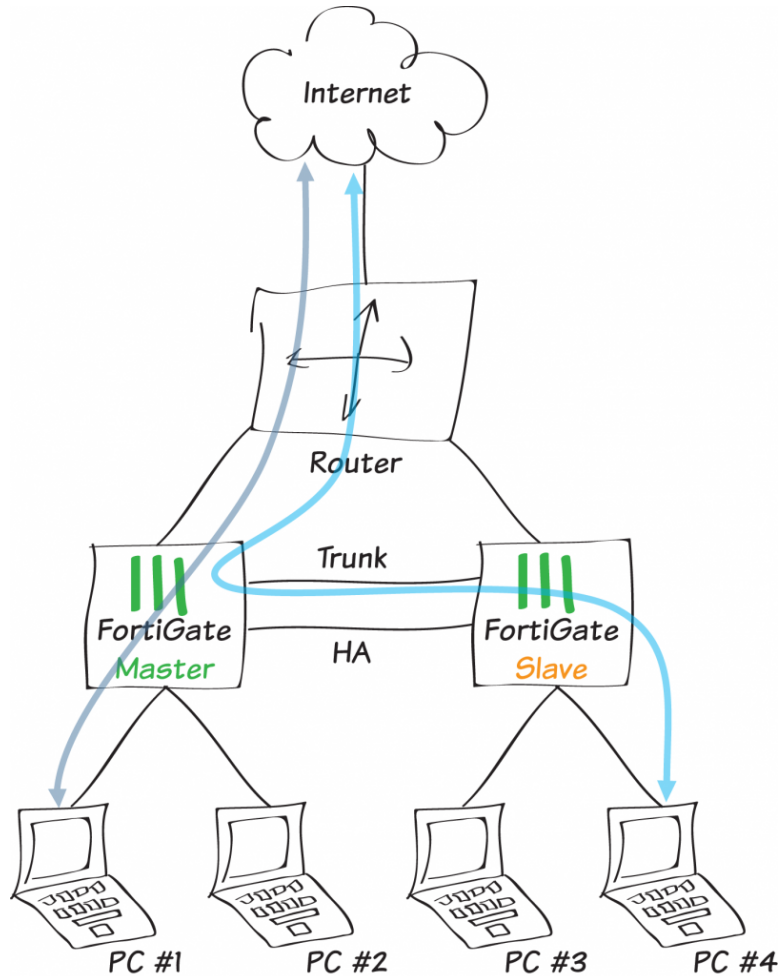
In this new topology, we won't be using additional switches. Instead, we will be using the FortiGate's Integrated Switch Fabric (ISF) solution on both master and slave firewalls.

Note that the target topology uses a FortiGate 2xxD, which has 40 ports. In your configuration, ensure that each FortiGate has enough ports to handle all of the computers in the event of a failover, or switches will still need to be involved.

The administrator will have to configure a trunk link between the two FortiGate physical switches to expand subnets and VLANs from one firewall to the other.

In a FortiGate cluster using FGCP, the slave firewall's ISF can still be used to send traffic destined for the active member across the trunk link.

A representation of the traffic flow appears below:

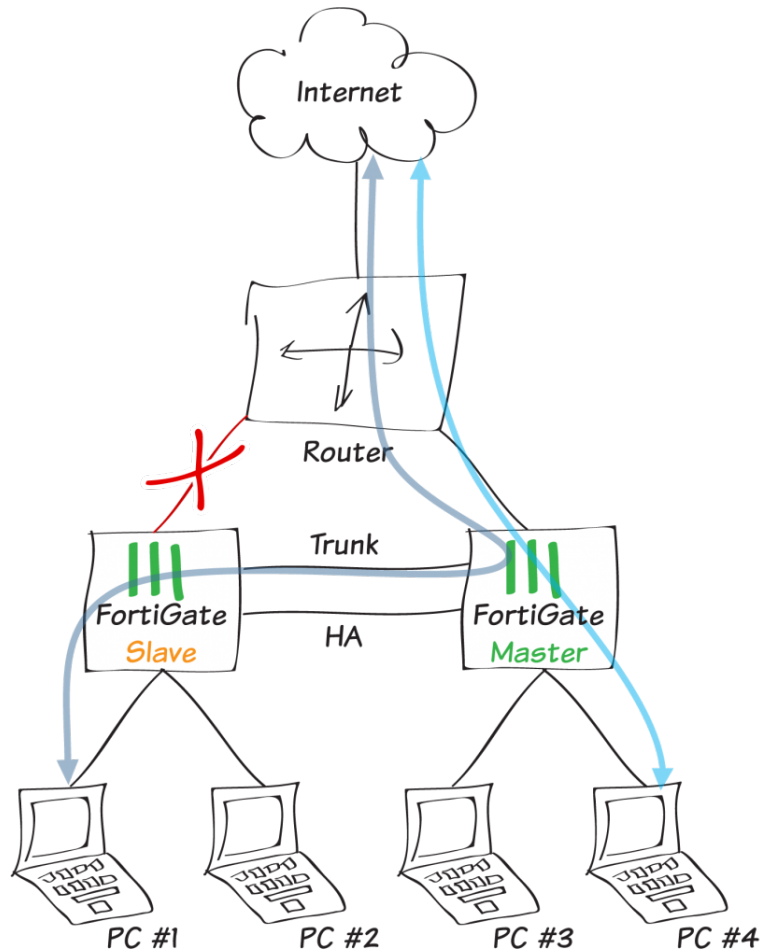


2.2 FortiGate Failover

Case 1: Link failure

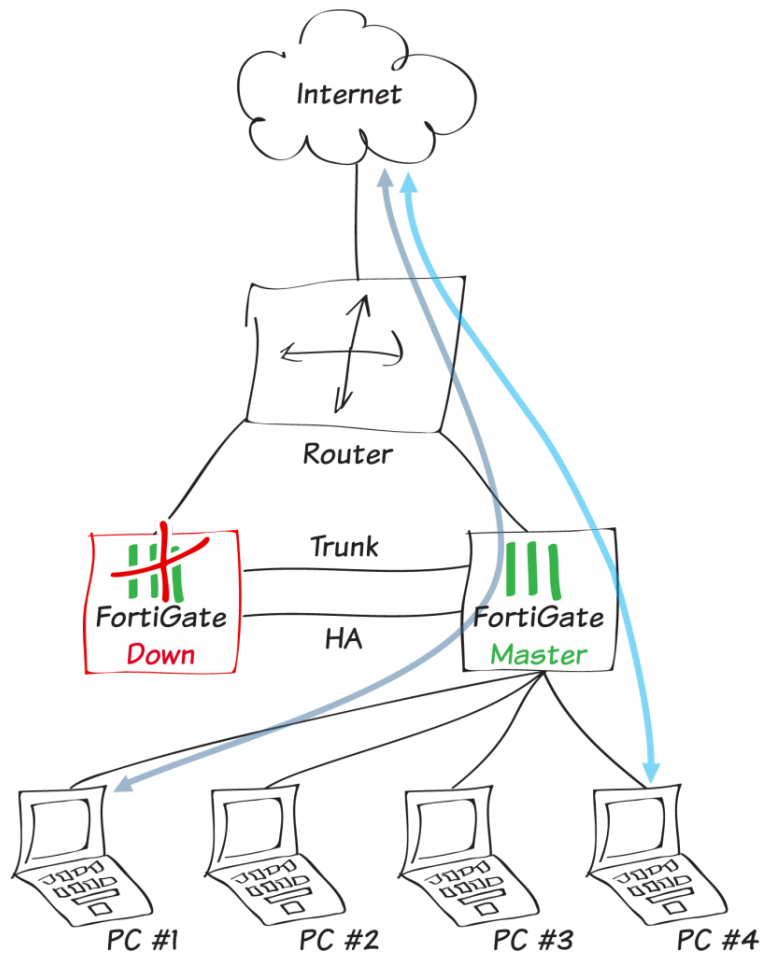
The diagram below represents traffic flow in the event of a failover in the following cases:

- The monitored WAN port, on what was originally the Master FortiGate, fails.
- The link between the router and the original Master FortiGate fails.



Case 2: FortiGate global failure

If the master were to completely fail (including the ISF), the administrator would have to plug the LAN segments into the remaining firewall, just as if one switch were to fail in our standard topology.



2.3 Key Advantages

This new topology offers a few key advantages:

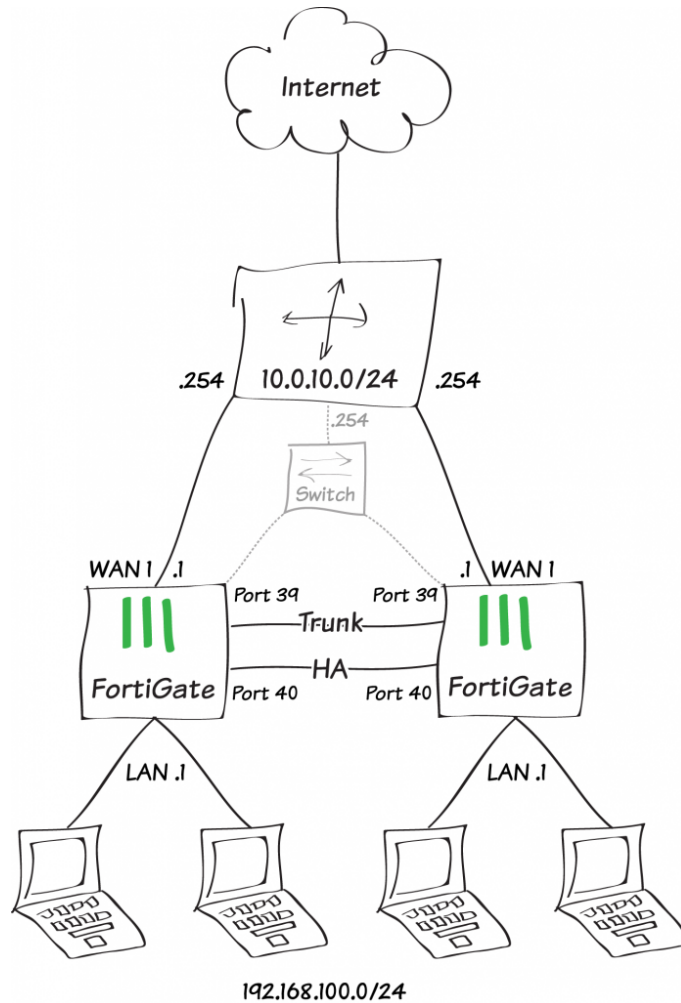
- Only two devices are required, where four are required in the standard topology.
- It is easier for the administrator to manage security and switching on a single device.
- The use of FortiManager simplifies central management.
- There is only one cluster to supervise.

Configuration

In this section, we reproduce the following network topology. Notice how the router has a switch interface. If your router does not have a switch interface, you will have to add an extra switch (noted in gray below), and in the event of a firewall crash, you will have to power cycle the router.

As we will be changing the configuration of the hardware switch, we strongly recommend that you use the management port to follow the steps below.

By default, the FortiGate management IP address is 192.168.1.99/24.



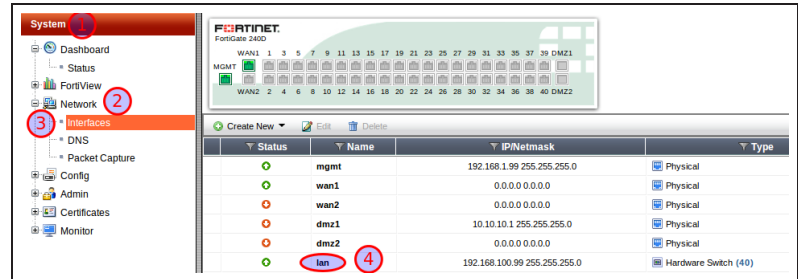
1. Configuring the hardware switch

By default on a FortiGate 1xxD/2xxD, the unit is in Interface mode and all of the internal ports are attached to a hardware switch named **lan**. In this example, we need to use ports 39 and 40 for Trunk and HA respectively.

The first step is to remove ports 39 and 40 from the Hardware Switch lan. Begin by editing the lan interface.

If the unit is in Switch mode, it will have to be reconfigured into Interface mode. For more information, see [Choosing your FortiGate's switch mode](#).

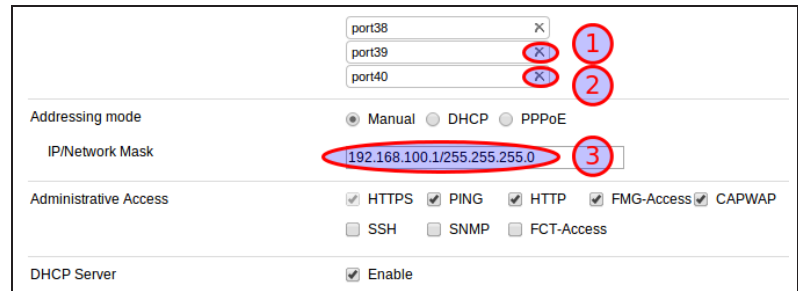
Go to **System > Network > Interfaces** and double-click **lan** in the interface list.



Remove the last two ports in the list, in this case **port39** and **port40**.

Then configure the **IP/Network Mask** with the following address:
192.168.100.1/255.255.255.0

When you are done, accept the change.



The interface list should now look like this:

Status	Name	IP/Netmask	Type
🟢	mgmt	192.168.1.99 255.255.255.0	Physical
🟢	wan1	0.0.0.0 0.0.0.0	Physical
🟠	wan2	0.0.0.0 0.0.0.0	Physical
🟠	dmz1	10.10.10.1 255.255.255.0	Physical
🟠	dmz2	0.0.0.0 0.0.0.0	Physical
🟢	lan	192.168.100.1 255.255.255.0	Hardware Switch (38)
🟠	port39	0.0.0.0 0.0.0.0	Physical
🟠	port40	0.0.0.0 0.0.0.0	Physical

For the trunk port to work properly, we need to configure a vlan ID on the Virtual Switch. This can only be done in the CLI.

```
FGT1 # config system global
FGT1 (global) # set virtual-switch-vlan enable
FGT1 (global) # end
FGT1 # show system global
```

First we need to enable this feature globally. Use the commands shown here:

```
config system global
  set fgd-alert-subscription advisory latest-threat
  set hostname "FGT1"
  set internal-switch-mode interface
  set optimize antivirus
  set timezone 04
  set virtual-switch-vlan enable
end
```

Next, edit the Virtual Switch and set the vlan number:

```
FGT1 # config system virtual-switch
FGT1 (virtual-switch) # edit lan
FGT1 (lan) # set vlan 100
FGT1 (lan) # end
```

You should now be able to see VLAN Switch in the interface list.

▼ Status	▼ Name	▼ IP/Netmask	▼ Type
🟢	mgmt	192.168.1.99 255.255.255.0	Physical
🟢	wan1	0.0.0.0 0.0.0.0	Physical
🔴	wan2	0.0.0.0 0.0.0.0	Physical
🔴	dmz1	10.10.10.1 255.255.255.0	Physical
🔴	dmz2	0.0.0.0 0.0.0.0	Physical
🟢	lan (VLAN ID: 100)	192.168.100.1 255.255.255.0	VLAN Switch (38)
🔴	port39	0.0.0.0 0.0.0.0	Physical
🔴	port40	0.0.0.0 0.0.0.0	Physical

2. Configuring the trunk port

The trunk port will be used to allow traffic to flow between the Virtual Switch of each FortiGate.

Configuring the trunk port is only possible in the CLI:

```
FGT1 # config system interface
FGT1 (interface) # edit port39
FGT1 (port39) # set trunk enable
FGT1 (port39) # end
FGT1 # show system interface port39
config system interface
  edit "port39"
    set [glossary_exclude]vdom[/glossary_exclude] "root"
    set type physical
    set trunk enable
    set [glossary_exclude]snmp[/glossary_exclude]-index 10
  next
end
```

You should now be able to see the trunk port in the interface list.

▼ Status	▼ Name	▼ IP/Netmask	▼ Type
🟢	mgmt	192.168.1.99 255.255.255.0	Physical
🟢	wan1	0.0.0.0 0.0.0.0	Physical
🔴	wan2	0.0.0.0 0.0.0.0	Physical
🔴	dmz1	10.10.10.1 255.255.255.0	Physical
🔴	dmz2	0.0.0.0 0.0.0.0	Physical
🟢	lan (VLAN ID: 100)	192.168.100.1 255.255.255.0	VLAN Switch (38)
🔴	port39	Dedicate as Ethernet Trunk	Physical
🔴	port40	0.0.0.0 0.0.0.0	Physical

3. Configuring HA

We will now configure High Availability. Port 40 will be used for HeartBeat/Sync communications between cluster members. Port Wan1 will be monitored.

Go to **System > Config > HA** and configure High Availability as shown:

The screenshot shows the HA configuration interface. At the top, the Mode is set to 'Active-Passive' (1). The Device Priority is set to 128. There is a checkbox for 'Reserve Management Port for Cluster Member' with a dropdown menu set to 'dmz1'. Below this is the 'Cluster Settings' section, which includes a 'Group Name' field containing 'fgt' (2) and a 'Password' field with masked characters (3). A checkbox for 'Enable Session Pick-up' is checked (4). At the bottom is a table for configuring heartbeat and port monitoring.

	Port Monitor	Heartbeat Interface	
		Enable	Priority(0-512)
dmz1	<input type="checkbox"/>	<input type="checkbox"/>	0
dmz2	<input type="checkbox"/>	<input type="checkbox"/>	0
mgmt	<input type="checkbox"/>		
port39	<input type="checkbox"/>	<input type="checkbox"/>	0
port40	<input type="checkbox"/>	<input checked="" type="checkbox"/> (5)	0
wan1	<input checked="" type="checkbox"/> (6)	<input type="checkbox"/>	50
wan2	<input type="checkbox"/>	<input type="checkbox"/>	50

4. Configuring WAN1 IP routing

Go to **System > Network > Interfaces** and edit **wan1** as shown.

The screenshot shows the configuration page for the WAN1 interface. The interface name is wan1(08:5B:0E:32:5C:E4). The alias is 'Internet', marked with a red circle 1. The link status is 'Up' with a green arrow. The type is 'Physical Interface'. The addressing mode is 'Manual', marked with a red circle 2. The IP/Network Mask is '10.0.10.1/24', marked with a red circle 3. Administrative access options include HTTPS, PING, HTTP, FMG-Access, CAPWAP, SSH, SNMP, and FCT-Access. PING, FMG-Access, and Auto IPsec Request are checked. DHCP Server is disabled. Security Mode is set to 'None'. Device Management 'Detect and Identify Devices' is disabled. Listen for RADIUS Accounting Messages is disabled. Secondary IP Address is disabled. Comments field is empty. Administrative Status is 'Up' with a green arrow. At the bottom, the 'OK' button is marked with a red circle 4.

Go to **Router > Static > Static Routes** and create a new route as shown:

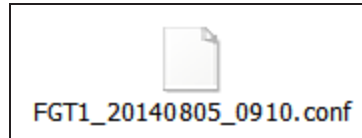
The screenshot shows the configuration page for a static route. The destination IP/Mask is '0.0.0.0/0.0.0.0', marked with a red circle 1. The device is 'wan1', marked with a red circle 2. The gateway is '10.0.10.254', marked with a red circle 3. The distance is '10' (1-255, Default=10). The priority is '0' (0-4294967295). Comments field is empty. At the bottom, the 'OK' button is marked with a red circle 4.

5. Configuring your firewall policies

Go to **Policy & Objects > Policy > IPv4** and configure firewall policies as desired.

6. Replicate the entire configuration on the second device

Once the first FortiGate is configured, the easiest way to configure the second one is to backup the configuration file of the first FortiGate and restore it on the second.



You can change the hostname and HA priority lines directly in the configuration file prior to restoring it on the second FortiGate.

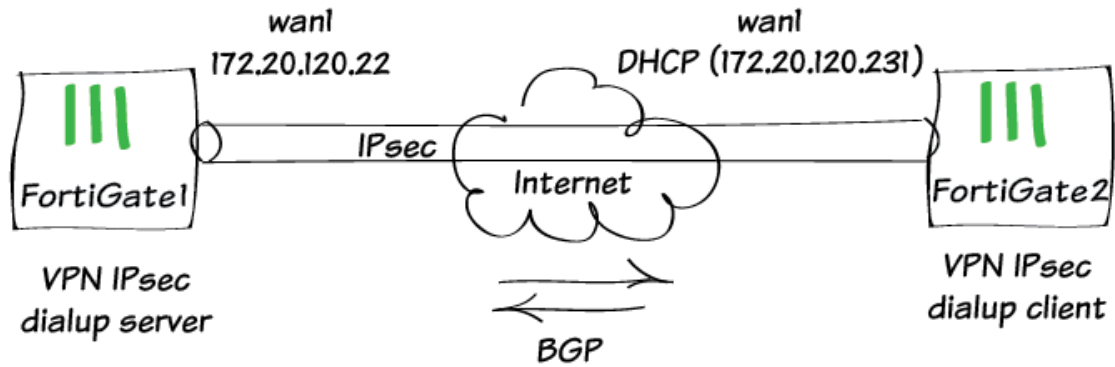
Do not use a text editor, like Notepad or Word, to do this editing. Instead, use a code editor, like Notepad++ or TextWrangler, that won't add unintended content to the file.

Go to **System > Dashboard > Status** and select **Backup** next to **System Configuration** in the **System Information** widget.

Firmware Version	v5.2.0,build0589 (GA) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /2 in Total [Details]

For further reading, check out [High Availability](#) in the [FortiOS 5.2 Handbook](#).

BGP over a dynamic IPsec VPN



This example shows how to create a dynamic IPsec VPN tunnel and allowing BGP peering through it.

1. Configuring IPsec in FortiGate1

Go to **Policy & Objects > Objects > Addresses** and select create new **Address**.

Name	<input type="text" value="Remote_loop_int"/>
Type	<input type="text" value="Subnet"/>
Subnet / IP Range	<input type="text" value="10.10.10.10"/>
Interface	<input type="text" value="any"/>
Visibility	<input checked="" type="checkbox"/>

Then create **Address Group**.

Group Name	<input type="text" value="VPN_DST"/>
Show in Address List	<input checked="" type="checkbox"/>
Members	<input type="text" value="Remote_loop_int"/> <input type="text" value="all"/>

Go to **System > Status** to look for **CLI Console** widget and create phase 1.

```
config vpn ipsec phase1-interface
  edit Dialup
    set type dynamic
    set interface wan1
    set mode aggressive
    set peertype one
    set mode-cfg enable
    set proposal 3des-sha1 aes128-sha1
    set peerid dial
    set assign-ip disable
    set psksecret
  next
end
```

Create phase 2.

```
config vpn ipsec phase2-interface
  edit dial_p2
    set phasename Dialup
    set proposal 3des-sha1 aes128-sha1
    set src-addr-type name
    set dst-addr-type name
    set src-name all
    set dst-name VPN_DST
  next
end
```

2. Configuring BGP in FortiGate1

Go to **System > Network > Interfaces** and create a **Loopback** interface.

Interface Name	loop
Type	Loopback Interface
IP/Network Mask	20.20.20.20/255.255.255.255

Go to **System > Status** to look for **CLI Console** widget and create BGP route.

```
config router bgp
  set as 100
  set router-id 1.1.1.1
  config neighbor
    edit 10.10.10.10
      set ebgp-enforce-multihop enable
      set remote-as 200
      set update-source loop
    next
  end
  config redistribute connected
    set status enable
  end
end
```

3. Adding policies in FortiGate1

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **Dialup** to **loop** interfaces.

Incoming Interface	Dialup
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	loop
Destination Address	all
Schedule	always
Service	BGP
Action	ACCEPT

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **loop** to **Dialup** interfaces.

4. Configuring IPsec in FortiGate 2

Go to **System > Status** to look for **CLI Console** widget and create phase 1.

```
config vpn ipsec phase1-interface
edit Dialup
set interface wan1
set mode aggressive
set mode-cfg enable
set proposal 3des-shal aes128-shal
set localid dial
set remote-gw 172.20.120.22
set assign-ip disable
set psksecret
next
end
```

Create phase 2.

```
config vpn ipsec phase2-interface
edit dial_p2
set phasename Dialup
set proposal 3des-shal aes128-shal
set keepalive enable
next
end
```

5. Configuring BGP in FortiGate 2

Go to **System > Network > Interfaces** and create a **Loopback** interface.

Interface Name	loop
Type	Loopback Interface
IP/Network Mask	<input type="text" value="10.10.10.10/255.255.255.255"/>

Go to **System > Status** to look for **CLI Console** widget and create BGP route.

```
config router bgp
set as 200
set router-id 1.1.1.2
config neighbor
edit 20.20.20.20
set ebgp-enforce-multihop enable
set remote-as 100
set update-source loop
next
end
config redistribute connected
set status enable
end
end
```

6. Adding policies in FortiGate 2

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **Dialup** to **loop** interfaces.

Incoming Interface	Dialup
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	loop
Destination Address	all
Schedule	always
Service	BGP
Action	ACCEPT

Go to **Policy & Objects > Policy > IPv4** and create a policy allowing BGP traffic from **loop** to **Dialup** interfaces.

Incoming Interface	loop
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	Dialup
Destination Address	all
Schedule	always
Service	BGP
Action	ACCEPT

7. Adding a static route in FortiGate 2

Go to **Router > Static > Static Routes** and add a route to the remote Loopback interface via **Dialup** interface.

Destination IP/Mask	20.20.20.20/255.255.25
Device	Dialup
Administrative Distance	10

8. Verifying tunnel is Up

Go to **VPN > Monitor > IPsec Monitor** to verify that the tunnel is **Up**.

Name	Remote Gateway	Status	Incoming Data	Outgoing Data
Dialup_0	172.20.120.231	Up	82.99 MB	987.89 KB

9. Results

From FortiGate 1, Go to **Router > Monitor > Routing Monitor** and verify that routes from FortiGate 2 were successfully advertised to FortiGate 1 via BGP.

Type	Network	Gateway	Interface
Static	0.0.0.0/0	172.20.120.2	wan1
Static	10.10.10.10/32	0.0.0.0	Dialup_0
BGP	10.10.80.0/24	10.10.10.10	
BGP	10.10.100.0/24	10.10.10.10	
Connected	20.20.20.20/32	0.0.0.0	loop
Connected	172.20.120.0/24	0.0.0.0	wan1
Connected	192.168.100.0/24	0.0.0.0	lan

From FortiGate 1, go to **System > Status** to look for **CLI Console** widget and type this command to verify BGP neighbors.

```
get router info bgp summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 8
2 BGP AS-PATH entries
0 BGP community entries
Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ
Up/Down    State/PfxRcd
10.10.10.10    4          200    8257    8237
7      0      0 5d00h01m          4
Total number of neighbors 1
```

From FortiGate 2, go to **Router > Monitor > Routing Monitor** and verify that routes from FortiGate 1 were successfully advertised to FortiGate 2 via BGP.

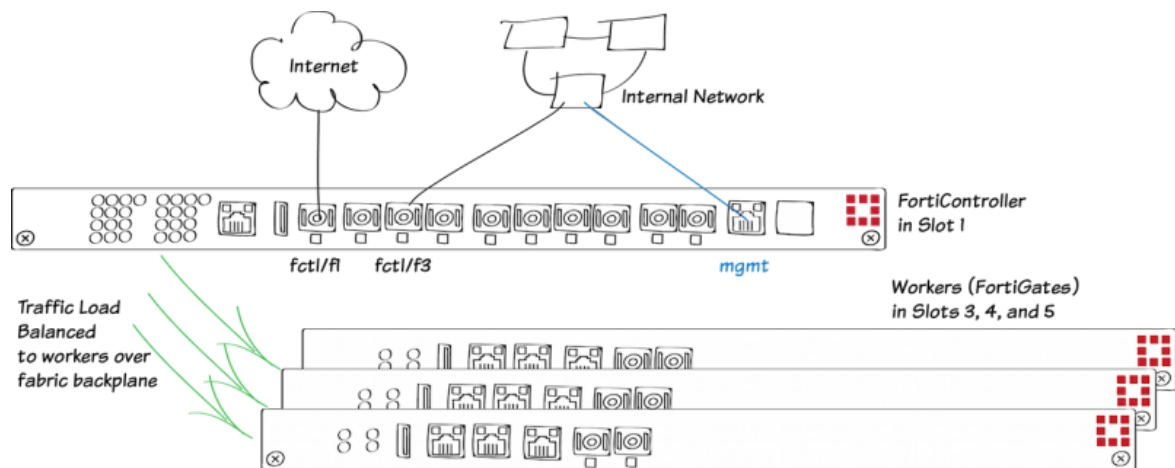
Type	Network	Gateway	Interface
Static	0.0.0.0/0	0.0.0.0	Dialup
Connected	10.10.10.10/32	0.0.0.0	loop
Connected	10.10.80.0/24	0.0.0.0	lan
Connected	10.10.100.0/24	0.0.0.0	dmz
Static	20.20.20.20/32	0.0.0.0	Dialup
Connected	172.20.120.0/24	0.0.0.0	wan1
BGP	192.168.100.0/24	20.20.20.20	

From FortiGate 2, go to **System > Status** to look for **CLI Console** widget and type this command to verify BGP neighbors.

```
get router info bgp summary
BGP router identifier 1.1.1.2, local AS number 200
BGP table version is 11
2 BGP AS-PATH entries
0 BGP community entries
Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ
Up/Down    State/PfxRcd
20.20.20.20    4          100    8341    8361
10      0      0 5d01h32m          3
Total number of neighbors 1
```

For further reading, check out [IPsec VPN](#) and [Border Gateway Protocol \(BGP\)](#) in the [FortiOS 5.2 Handbook](#).

SLBC setup with one FortiController



This example describes the basics of setting up a Session-aware Load Balancing Cluster (SLBC) that consists of one FortiController-5103B, installed in chassis slot 1, and three FortiGate-5001C workers, installed in chassis slots 3, 4, and 5. This SLBC configuration can have up to eight 10Gbit network connections.

For more information about SLBC go [here](#).

1. Hardware setup

Install a FortiGate-5000 series chassis and connect it to power. Install the FortiController in slot 1. Install the workers in slots 3, 4, and 5. Power on the chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally. (To check normal operation LED status see the FortiGate-5000 series documents available [here](#).)

Check the FortiSwitch-ATCA [release notes](#) and install the latest supported firmware on the FortiController and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

2. Configuring the FortiController

Connect to the FortiController GUI (using HTTPS) or CLI (using SSH) with the default IP address (<http://192.168.1.99>) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None). Login using the admin administrator account and no password.

Add a password for the admin administrator account. From the GUI use the **Administrators** widget or from the CLI enter this command.

```
config admin user
  edit admin
    set password <password>
  end
```

Change the FortiController mgmt interface IP address. From the GUI use the **Management Port** widget or from the CLI enter this command.

```
config system interface
  edit mgmt
    set ip 172.20.120.151/24
  end
```

If you need to add a default route for the management IP address, enter this command.

```
config route static
  edit route 1
    set gateway 172.20.120.2
  end
```

Set the chassis type that you are using.

```
config system global
  set chassis-type fortigate-5140
end
```

Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. Since the workers have not been configured yet their status is **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure them.

The screenshot shows a web interface for configuring a cluster. The top section is titled "Config" and contains "Member Management" settings. Below that is a "Membership" table with columns for Worker Blade, Role, Weight, Status, and an action menu. The Status column shows a red circle with a white 'D' for all three slots.

Worker Blade	Role	Weight	Status	
Slot #3	Active	5	Down	[Icons]
Slot #4	Active	5	Down	[Icons]
Slot #5	Active	5	Down	[Icons]

You can also enter the following CLI command to add slots 3, 4, and 5 to the cluster:

```
config load-balance setting
config slots
edit 3
next
edit 4
next
edit 5
end
end
```

You can also enter the following CLI command to configure the external management IP/Netmask and management access to this address:

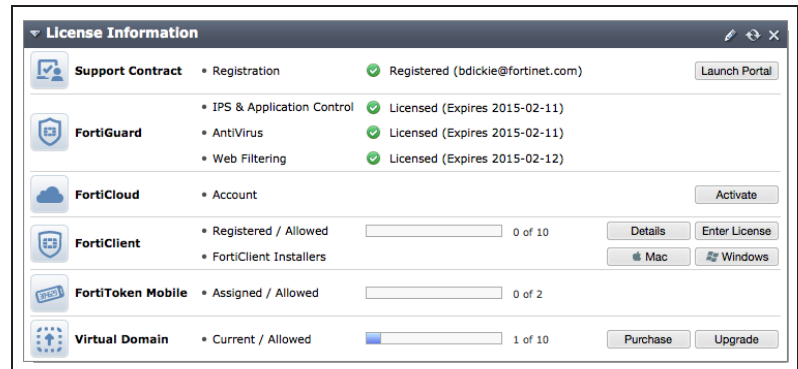
```
config load-balance setting
endset base-mgmt-external-ip 172.20.120.100 255.255.255.0
endset base-mgmt-allowaccess https ssh ping
end
```

3. Adding the workers

Enter this command to reset the workers to factory default settings.

```
execute factoryreset
```

Register and apply licenses to each worker before adding the workers to the SLBC. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**.

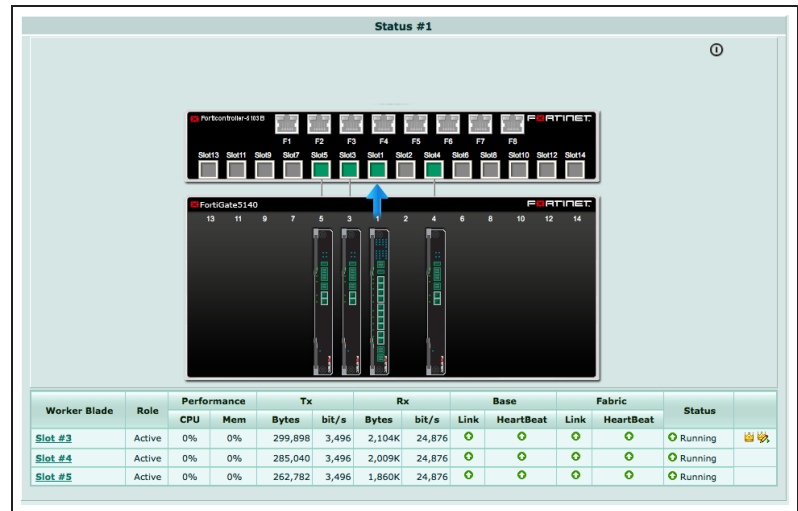


Log into the CLI of each worker and enter this CLI command to set the worker to operate in FortiController mode.

```
config system elbc
  set mode forticontroller
end
```

The worker restarts and joins the cluster. On the FortiController GUI go to **Load Balance > Status**. As the workers restart they should appear in their appropriate slots.

The worker in the lowest slot number usually becomes the primary unit.



4. Results

You can now manage the workers in the same way as you would manage a standalone FortiGate. You can connect to the worker GUI or CLI using the **External Management IP**. If you had configured the worker mgmt1 or mgmt2 interfaces you can also connect to one of these addresses to manage the cluster.

To operate the cluster, connect networks to the FortiController front panel interfaces and connect to a worker GUI or CLI to configure the workers to process the traffic they receive. When you connect to the External Management IP you connect to the primary worker. When you make configuration changes they are synchronized to all workers in the cluster.

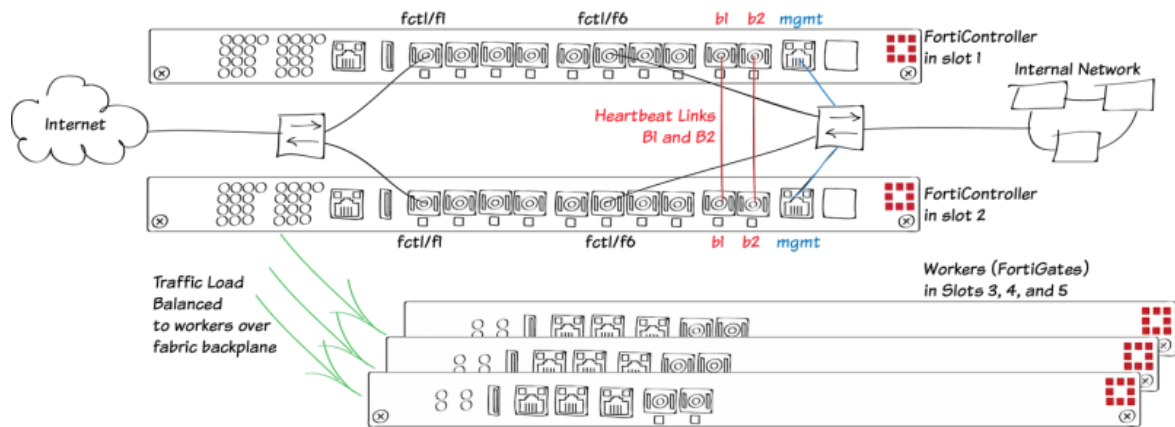
By default on the workers, all FortiController front panel interfaces are in the root VDOM. You can configure the root VDOM or create additional VDOMs and move interfaces into them.

For example, you could connect the Internet to FortiController front panel interface 4 (fctrl/f4 on the worker GUI and CLI) and an internal network to FortiController front panel interface 2 (fctrl/f2 on the worker GUI and CLI). Then enter the root VDOM and add a policy to allow users on the Internal network to access the Internet.

Incoming Interface	fctrl/f3	+
Source Address	Internal-net	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	fctrl/f1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	
Firewall / Network Options		
<input checked="" type="checkbox"/> NAT		
<input checked="" type="radio"/> Use Outgoing Interface Address		
<input type="radio"/> Use Dynamic IP Pool		
		<input type="checkbox"/> Fixed Port
		Click to add...

For further reading, check out the [FortiController Session-aware Load Balancing Guide](#).

SLBC Active-Passive setup with two FortiControllers



This example describes the basics of setting up an active-passive Session-aware Load Balancing Cluster (SLBC) that consists of two FortiController-5103Bs, installed in chassis slots 1 and 2, and three FortiGate-5001C workers, installed in chassis slots 3, 4, and 5. This SLBC configuration can have up to eight redundant 10Gbit network connections.

The FortiControllers in the same chassis to operate in active-passive HA mode for redundancy. The FortiController in slot 1 becomes the primary unit actively processing sessions. The FortiController in slot 2 becomes the subordinate unit, sharing the primary unit's session table. If the primary unit fails the subordinate unit resumes all active sessions.

All networks have redundant connections to both FortiControllers. You also create heartbeat links between the FortiControllers and management links from the FortiControllers to an internal network.

For more information about SLBC go [here](#).

1. Hardware setup

Install a FortiGate-5000 series chassis and connect it to power. Install the FortiControllers in slots 1 and 2. Install the workers in slots 3, 4, and 5. Power on the chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally (to check normal operation LED status, see the FortiGate-5000 series documents available [here](#)).

Create duplicate connections from the FortiController front panel interfaces to the Internet and to the internal network.

Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a backup heartbeat link by connecting the FortiController B2 interfaces together. You can directly connect the interfaces with a patch cable or connect them together through a switch. If you use a switch, it must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301 and 101). These connections establish heartbeat, base control, and base management communication between the FortiControllers. Only one heartbeat connection is required but redundant connections are recommended.

Connect the mgmt interfaces of the both FortiControllers to the internal network or any network from which you want to manage the cluster.

Check the FortiSwitch-ATCA [release notes](#) and install the latest supported firmware on the FortiController and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

2. Configuring the FortiControllers

Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in slot 1 with the default IP address (<http://192.168.1.99>) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None).

Add a password for the admin administrator account. You can either use the GUI **Administrators** widget or enter this CLI command.

```
config admin user
  edit admin
    set password <password>
  end
```

Change the FortiController mgmt interface IP address. Use the **Management Port** widget in the GUI or enter this command. Each FortiController should have a different Management IP address.

```
config system interface
  edit mgmt
    set ip 172.20.120.151/24
  end
```

If you need to add a default route for the

```
config route static
```

management IP address, enter this command.

```
edit 1
  set gateway 172.20.120.2
end
```

Set the chassis type that you are using.

```
config system global
  set chassis-type fortigate-5140
end
```

Configure active-passive HA on the FortiController in slot 1.

From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

Set **Mode** to **Active-Passive**, change the **Group ID**, and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync
-----------	----	------	----	---------	----------------------------	----------------	---------	-----------

Configure

Mode: Active-Passive

Device Priority (0-255): 128

Group ID(0-31): 23

Enable Override:

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy:

Heartbeat Device

Available	Selected
mgmt	b1
	b2

OK Cancel

You can also enter this command:

```
config system ha
  set mode a-p
  set groupid 23
  set hbdev b1 b2
end
```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the Group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a

MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

You can also adjust other HA settings. For example, you could increase the **Device Priority** of the FortiController that you want to become the primary unit, enable **Override** to make sure the FortiController with the highest device priority becomes the primary unit, and change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on your network.

You would only select **Enable chassis redundancy** if your cluster has more than one chassis.

Log into the web-based manager of the FortiController in slot 2 and duplicate the HA configuration of the FortiController in slot 1, except for the Device Priority and override setting, which can be different on each FortiController.

After a short time, the FortiControllers restart in HA mode and form an active-passive cluster. Both FortiControllers must have the same HA configuration and at least one heartbeat link must be connected.

Normally the FortiController in slot 1 is the primary unit, and you can log into the cluster using the management IP address you assigned to this FortiController.

You can confirm that the cluster has been formed by viewing the HA configuration from the the FortiController web-based manager. The display should show both FortiControllers in the cluster.

Since the configuration of all FortiControllers is synchronized, you can complete the configuration of the cluster from the primary FortiController.

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up	Port Worker Failure	In Sync	Elbc sync
FTS13B3912000029	FTS13B3912000029	Master	169.254.128.81	545.32	0	0/0	1	1
FTS13B3912000051	FTS13B3912000051	Slave	169.254.128.82	405.77	0	0/0	1	1

Configure

Mode: Active-Passive

Device Priority (0-255): 128

Group ID(0-31): 10

Enable Override:

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy:

Available: mgmt

Selected: b1, b2

Heartbeat Device

OK Cancel

You can also go to **Load Balance > Status** to see the status of the cluster.

This page should show both FortiControllers in the cluster.

The FortiController in slot 1 is the primary unit (slot icon colored green) and the FortiController in slot 2 is the backup unit (slot icon colored yellow).

Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured yet their status will be **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure them.

Worker Blade	Role	Weight	Status	
Slot #3	Active	5	Down	🗑️ 🛠️ 📄
Slot #4	Active	5	Down	🗑️ 🛠️ 📄
Slot #5	Active	5	Down	🗑️ 🛠️ 📄

You can also enter this command to add slots 3, 4, and 5 to the cluster:

```
config load-balance setting
config slots
edit 3
next
edit 4
next
edit 5
end
end
```

You can also enter this command to set the external management IP/Netmask and configure management access.

```
config load-balance setting
set base-mgmt-external-ip 172.20.120.100 255.255.255.0
set base-mgmt-allowaccess https ssh ping
end
```

Enable base management traffic between FortiControllers.

```
config load-balance setting
config base-mgmt-interfaces
edit b1
next
edit b2
end
end
```

Enable base control traffic between FortiControllers.

```
config load-balance setting
config base-ctrl-interfaces
edit b1
next
edit b2
```

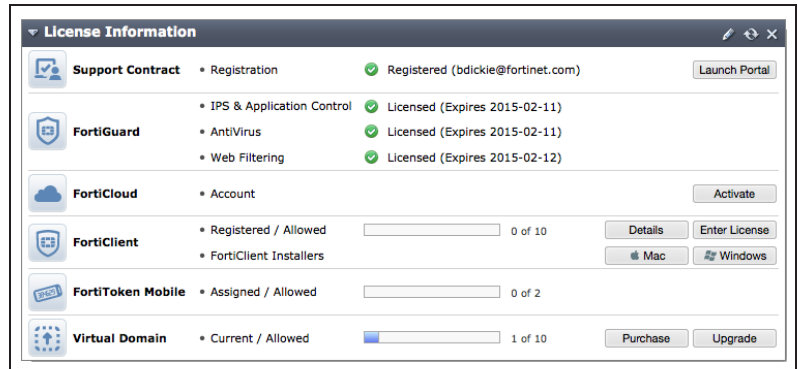
```
end
end
```

3. Adding the workers to the cluster

Reset the workers to factory default settings.

```
execute factoryreset
```

Register and apply licenses to each worker before adding the workers to the SLBC. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**.



Optionally give the mgmt1 and or mgmt2 interfaces of each worker IP addresses and connect them to your network. When a cluster is created, the mgmt1 and mgmt2 IP addresses are not synchronized, so you can connect to and manage each worker separately.

Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

Log into the CLI of each worker and enter this command to set the worker to operate in FortiController mode.

```
config system elbc
set mode forticontroller
end
```

The worker restarts and joins the cluster. On the FortiController GUI go to **Load Balance > Status**. As the workers restart they should appear in their appropriate slots.

Worker Blade	Role	Performance	Tx	Rx	Base	Fabric	Status
		CPU Mem	Bytes bit/s	Bytes bit/s	Link HeartBeat	Link HeartBeat	
Slot #3	Active	0% 0%	104,326 3,496	698,891 24,876	🟢 🟢	🟢 🟢	🟢 Running 🏆
Slot #4	Active	0% 0%	104,394 3,496	698,891 24,876	🟢 🟢	🟢 🟢	🟢 Running
Slot #5	Active	0% 0%	104,394 3,768	698,891 24,876	🟢 🟢	🟢 🟢	🟢 Running

4. Results

You can now connect to the worker GUI or CLI using the **External Management IP** and manage the workers in the same way as you would manage a standalone FortiGate. If you configured the worker mgmt1 or mgmt2 interfaces you can also connect to these interfaces to configure the workers. Configuration changes made to any worker are synchronized to all workers.

Configure the workers to process the traffic they receive from the FortiController front panel interfaces. By default all FortiController front panel interfaces are in the root VDOM. You can keep them in the root VDOM or create additional VDOMs and move interfaces into them.

For example, if you connect the Internet to FortiController front panel interface 1 (fctrl/f1 on the worker GUI and CLI) and the internal network to FortiController front panel interface 6 (fctrl/f6 on the worker GUI and CLI) you would access the root VDOM and add this policy to allow users on the Internal network to access the Internet.

Incoming Interface fctrl/f6 +

Source Address Internal-net +

Source User(s) Click to add...

Source Device Type Click to add...

Outgoing Interface fctrl/f1 +

Destination Address all +

Schedule always

Service ALL +

Action ✓ ACCEPT

Firewall / Network Options

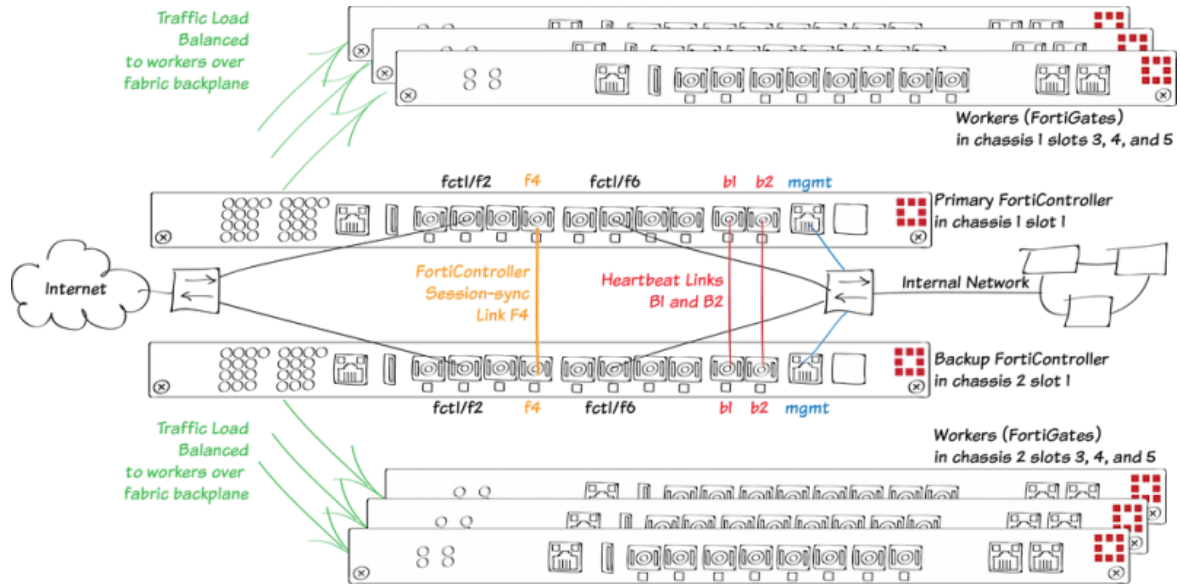
ON NAT

Use Outgoing Interface Address Fixed Port

Use Dynamic IP Pool

For further reading, check out the
[FortiController Session-aware Load
Balancing Guide](#).

SLBC Active-Passive with two FortiControllers and two chassis



This example describes how to setup an active-passive session-aware load balancing cluster (SLBC) consisting of two FortiGate-5000 chassis, two FortiController-5103Bs, and six FortiGate-5001Bs acting as workers, three in each chassis. This SLBC configuration can have up to seven redundant 10Gbit network connections.

The FortiControllers operate in active-passive HA mode for redundancy. The FortiController in chassis 1 slot 1 will be configured to be the primary unit, actively processing sessions. The FortiController in chassis 2 slot 1 becomes the subordinate unit. If the primary unit fails the subordinate unit resumes all active sessions.

All networks in this example have redundant connections to both FortiControllers and redundant heartbeat and base control and management links are created between the FortiControllers using their front panel B1 and B2 interfaces.

This example also includes a FortiController session sync connection between the FortiControllers using the FortiController F4 front panel interface (resulting in the SLBC having a total of seven redundant 10Gbit network connections). (You can use any fabric front panel interface.)

Heartbeat and base control and management traffic uses VLANs and specific subnets. So the switches and network components used must be configured to allow traffic on these VLANs and you should be aware of the subnets used in case they conflict with any connected networks.

This example sets the device priority of the FortiController in chassis 1 higher than the device priority of the FortiController in chassis 2 to make sure that the FortiController in chassis 1 becomes the primary FortiController for the cluster.

For more information about SLBC go [here](#).

1. Hardware setup

Install two FortiGate-5000 series chassis and connect them to power. Ideally each chassis should be connected to a separate power circuit. Install a FortiController in slot 1 of each chassis. Install the workers in slots 3, 4, and 5 of each chassis. The workers must be installed in the same slots in both chassis. Power on both chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally (to check normal operation LED status, see the FortiGate-5000 series documents available [here](#)).

Create duplicate connections from both FortiController front panel interfaces to the Internet and to the internal network.

Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a backup heartbeat link by connecting the FortiController B2 interfaces together. You can directly connect the interfaces with a patch cable or connect them together through a switch. If you use a switch, it must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301 and 101). These connections establish heartbeat, base control, and base management communication between the FortiControllers. Only one heartbeat connection is required but redundant connections are recommended.

Create a FortiController session sync connection between the chassis by connecting the FortiController F4 interfaces. If you use a switch it must allow traffic on the FortiController session sync VLAN (2000). You can use any of the F1 to F8 interfaces. We chose F4 in this example to make the diagram easier to understand.

Connect the mgmt interfaces of the both FortiControllers to the internal network or any network from which you want to manage the cluster.

Check the FortiSwitch-ATCA [release notes](#) and install the latest supported firmware on the FortiController and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

2. Configuring the FortiController in Chassis 1

Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in chassis 1 with the default IP address (<http://192.168.1.99>) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None).

From the Dashboard System Information widget, set the **Host Name** to ch1-slot1. Or enter this command.

```
config system global
    set hostname ch1-slot1
end
```

Add a password for the admin administrator account. You can either use the **Administrators** widget on the

```
config admin user
    edit admin
        set password
```


GUI or enter this command.

```
end
```

Change the FortiController mgmt interface IP address. Use the GUI **Management Port** widget or enter this command.

```
config system interface
edit mgmt
set ip 172.20.120.151/24
end
```

If you need to add a default route for the management IP address, enter this command.

```
config route static
edit 1
set gateway 172.20.120.2
end
```

Set the chassis type that you are using.

```
config system global
set chassis-type fortigate-5140
end
```

Configure Active-Passive HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

Set **Mode** to **Active-Passive**, set the **Device Priority** to 250, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 1 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync
5103-slot1	FT51383912000051	Master	169.254.128.33	247020.05	0	0/1	1	1

Configure

Mode: Active-Passive

Device Priority (0-255): 250

Group ID(0-31): 5

Enable Override:

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy:

Chassis ID(1 - 2): 1

Heartbeat Device

Available: mgmt

Selected: b1, b2

OK Cancel

Enter this command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
set session-sync-port f4
end
```

You can also enter the complete HA

```
config system ha
```

configuration with this command.

```
set mode active-passive
set groupid 5
set priority 250
set override enable
set chassis-redundancy enable
set chassis-id 1
set hbdev b1 b2
set session-sync-port f4
end
```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the Group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

Enable Override is selected to make sure the FortiController in chassis 1 always becomes the primary unit. Enabling override could lead to the cluster renegotiating more often, so once the chassis is operating you can disable this setting.

You can also adjust other HA settings. For example, you could change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on your network. You can also adjust the **Heartbeat Interval** and **Number of Heartbeats** lost to adjust how quickly the cluster determines one of the FortiControllers has failed.

3. Configuring the FortiController in Chassis 2

Log into the FortiController in chassis 2.

```
config system global
    set hostname ch2-slot1
end
```

Enter these commands to set the host name to ch2-slot1 and duplicate the HA configuration of the FortiController in chassis 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10), and set the **Chassis ID** to 2.

```
config system ha
    set mode active-passive
    set groupid 5
    set priority 10
    set chassis-redundancy enable
    set chassis-id 2
    set hbdev b1 b2
    set session-sync-port f4
end
```

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

À

4. Configuring the cluster

After a short time the FortiControllers restart in HA mode and form an active-passive SLBC. Both FortiControllers must have the same HA configuration and at least one heartbeat link (the B1 and B2 interfaces) must be connected. If the FortiControllers are unable to form a cluster, check to make sure that they both have the same HA configuration. Also they can't form a cluster if the heartbeat interfaces (B1 and B2) are not connected.

With the configuration described in the previous steps, the FortiController in chassis 1 should become the primary unit and you can log into the cluster using the management IP address that you assigned to the FortiController in chassis 1.

The FortiController in chassis 2 becomes the backup FortiController. You cannot log into or manage the backup FortiController until you configure the cluster External Management IP and add workers to the cluster. Once you do this you can use the External Management IP address and a special port number to manage the backup FortiController. This is described below. (You can also connect to the backup FortiController CLI using the console port.)

You can confirm that the cluster has been formed by viewing the FortiController HA configuration. The display should show both FortiControllers in the cluster.

Note in some of the screen images in this example the host names shown on the screen images may not match the host names used in the example configuration.

Host Name	SN	Role	IP	Up Time	The number of link-up	Port	Worker	Failure	In Sync	Elbc	sync
FTS13B3912000029	FTS13B3912000029	Master	169.254.128.81	357.50	0		0/0	1	1		
FTS13B3912000051	FTS13B3912000051	Slave	169.254.128.82	53.84	0		0/0	0	1		

Configure

Mode: Active-Passive

Device Priority (0-255): 128

Group ID(0-31): 10

Enable Override:

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy:

Chassis ID(1 - 2): 1

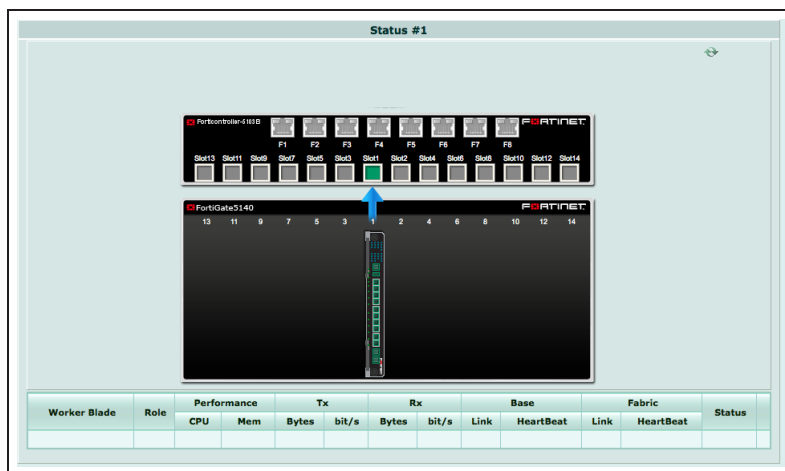
Heartbeat Device: mgmt

Available: mgmt

Selected: b1, b2

OK Cancel

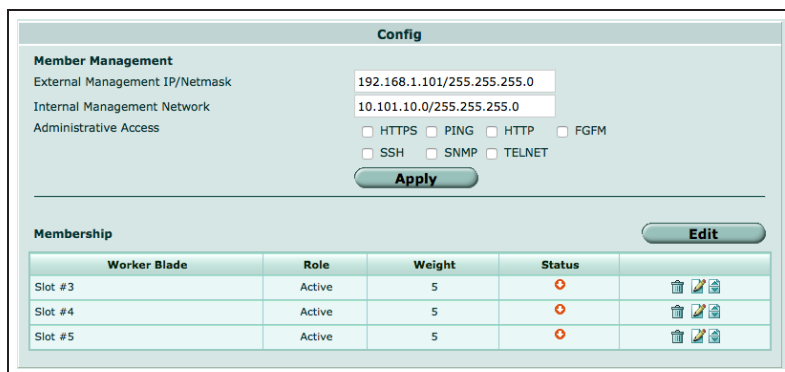
You can also go to **Load Balance > Status** to see the status of the primary FortiController (slot icon colored green).



Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured their status will be **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure all of the devices in the cluster.



You can also enter this command to add slots 3, 4, and 5 to the cluster.

```
config load-balance setting
config slots
edit 3
next
edit 4
next
edit 5
end
end
```

You can also enter this command to set the External Management IP and

```
config load-balance setting
set base-mgmt-external-ip 172.20.120.100 255.255.255.0
```

configure management access.

```
set base-mgmt-allowaccess https ssh ping
end
```

Enable base management traffic between FortiControllers.

```
config load-balance setting
config base-mgmt-interfaces
    edit b1
    next
    edit b2
end
end
```

Enable base control traffic between FortiControllers.

```
config load-balance setting
config base-ctrl-interfaces
    edit b1
    next
    edit b2
end
end
```

5. Adding the workers to the cluster

Reset each worker to factory default settings.

```
execute factoryreset
```

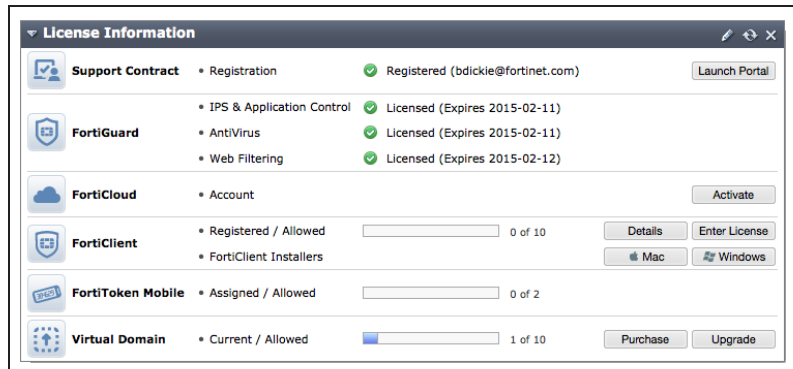
Give the mgmt1 or mgmt2 interface of each worker an IP address and connect these interfaces to your network. This step is optional but useful because when the workers are added to the cluster, these IP addresses are not synchronized, so you can connect to and manage each worker separately.

```
config system interface
edit mgmt1
set ip 172.20.120.120
end
```

Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

```
config system global
    set hostname worker-chassis-1-slot-3
end
```

Register and apply licenses to each worker before adding the workers to the cluster. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**.



Log into the CLI of each worker and enter this command to set the worker to operate in FortiController mode. The worker restarts and joins the cluster.

```
config system elbc
set mode forticontroller
end
```

6. Managing the cluster

After the workers have been added to the cluster you can use the External Management IP to manage the the primary worker. This includes access to the primary worker GUI or CLI, SNMP queries to the primary worker, and using FortiManager to manage the primary worker. As well SNMP traps and log messages are sent from the primary worker with the External Management IP as their source address. And finally connections to FortiGuard for updates, web filtering lookups and so on, all originate from the External Management IP.

You can use the external management IP followed by a special port number to manage individual devices in the cluster. The special port number identifies the protocol (80 for HTTP, 443 for HTTPS, 22 for SSH, 23 for Telnet, 161 for SNMP) and the chassis and slot number of the device you want to connect to. In fact this is the only way to manage the backup FortiController. Some examples:

- To use HTTP to connect to the GUI of the FortiController in chassis 1 slot 1, browse to: **https://172.20.120.100:44311**
- To use HTTP to connect to the GUI of the FortiController in chassis 2 slot 1, (the backup FortiController) browse to: **https://172.20.120.100:44321**
- To use Telnet to connect to the CLI of the worker in chassis 1 slot 4: **telnet 172.20.120.100 2314**
- To use SSH to connect to the CLI the worker in chassis 2 slot 5: **ssh admin@172.20.120.100 -p2225**
- To use SNMP to query the FortiController in chassis 2 slot 1 (the backup FortiController) use port **16121** in the SNMP query.

You can also manage the primary FortiController using the IP address of its mgmt interface, set up when you first configured the primary FortiController. You can also manage the workers by connecting directly to their mgmt1 or mgmt2 interfaces if you set them up. However, the only way to manage the backup FortiController is by using its special port number.

To manage a FortiController using SNMP you need to load the FORTINET-CORE-MIB.mib file into your SNMP

manager. You can get this MIB file from the Fortinet support site, in the same location as the current FortiController firmware (select the FortiSwitchATCA product).

On the primary FortiController GUI go to **Load Balance > Status**. As the workers in chassis 1 restart they should appear in their appropriate slots.

The primary FortiController should be the FortiController in chassis 1 slot 1. The primary FortiController status display includes a **Config Master** link that you can use to connect to the primary worker.

Worker Blade	Role	Performance		Tx		Rx		Base		Fabric		Status
		CPU	Mem	Bytes	bit/s	Bytes	bit/s	Link	HeartBeat	Link	HeartBeat	
Slot #3	Active	0%	0%	443,698	3,768	4,951K	23,024	🟢	🟢	🟢	🟢	Running 🏠
Slot #4	Active	0%	0%	434,206	3,496	4,897K	23,024	🟢	🟢	🟢	🟢	Running
Slot #5	Active	0%	0%	427,538	3,768	4,870K	23,024	🟢	🟢	🟢	🟢	Running

Log into the backup FortiController GUI (for example by browsing to <https://172.20.120.100:44321>) and go to **Load Balance > Status**. As the workers in chassis 2 restart they should appear in their appropriate slots.

The backup FortiController Status page shows the status of the workers in chassis 2 and does not include the **Config Master** link.

Worker Blade	Role	Performance		Tx		Rx		Base		Fabric		Status
		CPU	Mem	Bytes	bit/s	Bytes	bit/s	Link	HeartBeat	Link	HeartBeat	
Slot #3	Active	0%	0%	1,682K	3,496	8,410K	24,876	🟢	🟢	🟢	🟢	Running 🏠
Slot #4	Active	0%	0%	1,643K	3,768	8,301K	24,876	🟢	🟢	🟢	🟢	Running
Slot #5	Active	0%	0%	1,620K	3,496	8,305K	24,876	🟢	🟢	🟢	🟢	Running

7. Results - Configuring the workers

Configure the workers to process the traffic they receive from the FortiController front panel interfaces. By default all FortiController front panel interfaces are in the worker root VDOM. You can keep them in the root VDOM or create additional VDOMs and move interfaces into them.

For example, if you connect the Internet to FortiController front panel 2 interfaces (fctrl/f2 on the worker GUI and CLI) and the internal network to FortiController front panel 6 interfaces (fctrl/f6) you would access the root VDOM and add this policy to allow users on the Internal network to access the Internet.

Incoming Interface	fctrl/f6	+
Source Address	Internal_NET	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	fctrl/f2	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	

Firewall / Network Options

NAT

Use Outgoing Interface Address Fixed Port

Use Dynamic IP Pool

8. Results - Checking the cluster status

You can use the following get and diagnose commands to show the status of the cluster and all of the devices in it.

Log into the **primary FortiController** CLI and enter this command to view the system status of the primary FortiController.

For example, you can use SSH to log into the primary FortiController CLI using the external management IP:

```
ssh admin@172.20.120.100 -p2211
```

```
get system status
Version: FortiController-5103B
v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000029
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: chl-slot1
Current HA mode: a-p, master
System time: Sat Sep 13 06:51:53 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)
```

Enter this command to view the load balance status of the primary FortiController and its workers. The command output shows the workers in slots 3, 4, and 5, and status information about each one.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
Working: 3 [ 3 Active 0 Standby]
Ready: 0 [ 0 Active 0 Standby]
Dead: 0 [ 0 Active 0 Standby]
```



```

Total:      3 [ 3 Active  0 Standby]

Slot 3: Status:Working  Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"
Slot 4: Status:Working  Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"
Slot 5: Status:Working  Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"

```

Enter this command from the primary FortiController to show the HA status of the primary and backup FortiControllers. The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (this case 0 for each FortiController) the number of failed workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (status=alive) and the B2 interfaces are not (status=dead). The cluster can still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

```

diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.41,
uptime=62581.81, chassis=1(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=2
force-state(0:none) hbdevs: local_interface=      b1 best=yes
                          local_interface=      b2 best=no

ch2-slot1(FT513B3912000051), Slave(priority=1), ip=169.254.128.42,
uptime=1644.71, chassis=2(1)
  slot: 1
  sync: conf_sync=0, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=2
force-state(0:none) hbdevs: local_interface=      b1 last_hb_time=66430.35
status=alive

```

```
local_interface= b2 last_hb_time= 0.00 status=dead
```

Log into the **backup FortiController** CLI and enter this command to view the status of the backup FortiController.

To use SSH:

```
ssh admin@172.20.120.100 -p2221
```

```
get system status
Version: FortiController-5103B
v5.0,build0020,131118 (Patch 3)
Branch Point: 0020
Serial-Number: FT513B3912000051
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: ch2-slot1
Current HA mode: a-p, backup
System time: Sat Sep 13 07:29:04 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)
```

Enter this command to view the status of the backup FortiController and its workers.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: N/A
Blades:
  Working: 3 [ 3 Active 0 Standby]
  Ready:   0 [ 0 Active 0 Standby]
  Dead:    0 [ 0 Active 0 Standby]
  Total:   3 [ 3 Active 0 Standby]

Slot 3: Status:Working Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good Data: Good
Status Message:"Running"
Slot 4: Status:Working Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good Data: Good
Status Message:"Running"
Slot 5: Status:Working Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good Data: Good
Status Message:"Running"
```

Enter this command from the backup FortiController to show the HA status of the backup and primary FortiControllers. Notice that the backup FortiController is shown first. The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (this case 0 for each FortiController) the number of failed

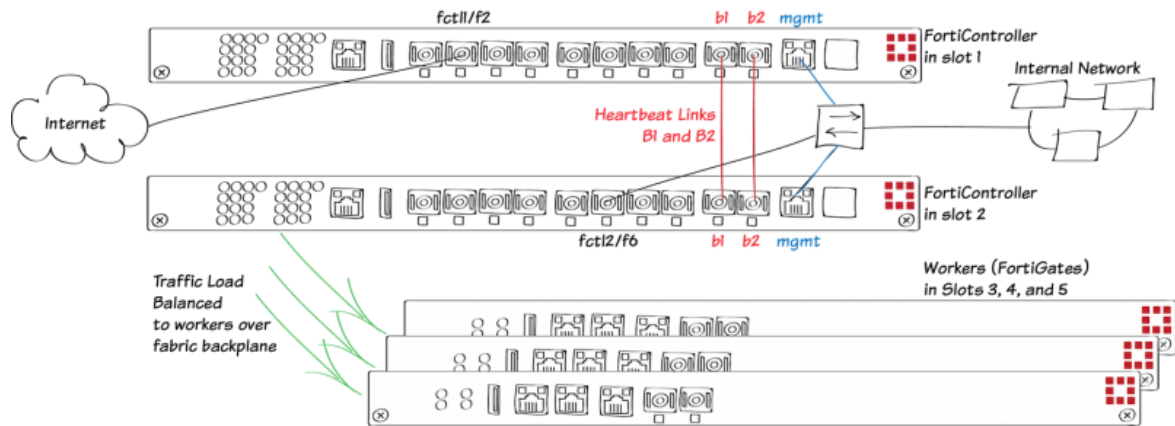
workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (status=alive) and the B2 interfaces are not (status=dead). The cluster can still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch2-slot1 (FT513B3912000051), Slave (priority=1), ip=169.254.128.42,
uptime=3795.92, chassis=2 (1)
  slot: 1
  sync: conf_sync=0, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)   hbdevs: local_interface=          b1 best=yes
  local_interface=          b2 best=no

ch1-slot1 (FT513B3912000029), Master (priority=0), ip=169.254.128.41,
uptime=64732.98, chassis=1 (1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3 (connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)   hbdevs: local_interface=          b1 last_hb_time=68534.90
status=alive
  local_interface=          b2 last_hb_time=          0.00   status=dead
```

For further reading, check out the
[FortiController Session-aware Load
Balancing Guide](#).

SLBC Dual Mode setup with two FortiControllers



This example describes the basics of setting up a dual mode Session-aware Load Balancing Cluster (SLBC) that consists of two FortiController-5103Bs, installed in chassis slots 1 and 2, and three FortiGate-5001C workers, installed in chassis slots 3, 4, and 5. This SLBC configuration can have up to 16 10Gbit network connections.

The two FortiControllers in the same chassis to operate in dual mode to double the number of network interfaces available. In dual mode, two FortiControllers load balance traffic to multiple workers. Traffic can be received by both FortiControllers and load balanced to all of the workers in the chassis. In dual mode configuration the front panel interfaces of both FortiControllers are active.

In a dual FortiController-5103B cluster this means up to 16 10Gbyte network interfaces are available. The interfaces of the FortiController in slot 1 are named fct1/f1 to fct1/f8 and the interfaces of the FortiController in slot 2 are named fct2/f1 to fct2/f8.

All networks have single connections to the first or second FortiController. One or more heartbeat links are created between the FortiControllers. Redundant heartbeat links are recommended. The heartbeat links use the front panel B1 and B2 interfaces.

If one of the FortiControllers fails, the remaining FortiController keeps processing traffic received by its front panel interfaces. Traffic to and from the failed FortiController is lost.

For more information about SLBC go [here](#).

1. Hardware setup

Install a FortiGate-5000 series chassis and connect it to power. Install the FortiControllers in slots 1 and 2. Install the workers in slots 3, 4, and 5. Power on the chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally (to check normal operation LED status, see the FortiGate-5000 series documents available [here](#)).

Create connections from the FortiController front panel interfaces to the Internet and to the internal network.

Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a backup heartbeat link by connecting the FortiController B2 interfaces together. You can directly connect the interfaces with a patch cable or connect them together through a switch. If you use a switch, it must allow traffic on the heartbeat VLAN (default 999) and the base control and management VLANs (301 and 101). These connections establish heartbeat, base control, and base management communication between the FortiControllers. Only one heartbeat connection is required but redundant connections are recommended.

Connect the mgmt interfaces of the both FortiControllers to the internal network or any network from which you want to manage the cluster.

Check the FortiSwitch-ATCA [release notes](#) and install the latest supported firmware on the FortiController and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

2. Configuring the FortiControllers

Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in slot 1 with the default IP address (<http://192.168.1.99>) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None).

Add a password for the admin administrator account. You can either use the **Administrators** widget in the GUI or enter the following command in the CLI.

```
config admin user
edit admin
    set password password
end
```

Change the FortiController mgmt interface IP address. Use the **Management Port** widget in the GUI or enter the following command in the CLI.

```
config system interface
edit mgmt
    set ip 172.20.120.151/24
end
```

If you need to add a default route for the management IP address, enter this command.

```
config route static
edit 1
    set gateway 172.20.120.2
end
```

Set the chassis type that you are using.

```
config system global
    set chassis-type fortigate-5140
end
```

Configure dual Mode HA on the FortiController in slot 1.

From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

Set **Mode** to **Dual Mode**, change the **Group ID**, and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

High Availability

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync
Cluster Members								

Configure

Mode: Dual Mode

Device Priority (0-255): 128

Group ID(0-31): 4

Enable Override:

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy:

Heartbeat Device

Available	Selected
mgmt	b1 b2

OK Cancel

You can also enter this CLI command:

```
config system ha
    set mode dual
    set groupid 4
    set hbdev b1 b2
end
```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the Group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

You can also adjust other HA settings. For example, you could increase the **Device Priority** of the FortiController that you want to become the primary unit, enable **Override** to make sure the FortiController with the highest device priority becomes the primary unit, and change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on your network.

You would only select **Enable chassis redundancy** if your cluster has more than one chassis.

Log into the web-based manager of the FortiController in slot 2 and duplicate the HA configuration of the FortiController in slot 1, except for the Device Priority and override setting, which can be different on each FortiController.

After a short time, the FortiControllers restart in HA mode and form a dual mode cluster. Both FortiControllers must have the same HA configuration and at least one heartbeat link must be connected.

Normally the FortiController in slot 1 is the primary unit, and you can log into the cluster using the management IP address you assigned to this FortiController.

If the FortiControllers are unable to form a cluster, check to make sure that they both have the same HA configuration. Also they can't form a cluster if the heartbeat interfaces (B1 and B2) are not connected.

You can confirm that the cluster has been formed by viewing the HA configuration from the the FortiController web-based manager. The display should show both FortiControllers in the cluster.

Since the configuration of the FortiControllers is synchronized, you can complete the configuration of the cluster from the primary FortiController.

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up	Port Worker Failure	In Sync	Elbc sync
FT513B3912000029	FT513B3912000029	Master	169.254.128.33	1894.42	0	0/0	1	1
FT513B3912000051	FT513B3912000051	Slave	169.254.128.34	827.73	0	0/0	1	1

Configure

Mode: Dual Mode

Device Priority (0-255): 128

Group ID(0-31): 4

Enable Override:

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy:

Available: mgmt

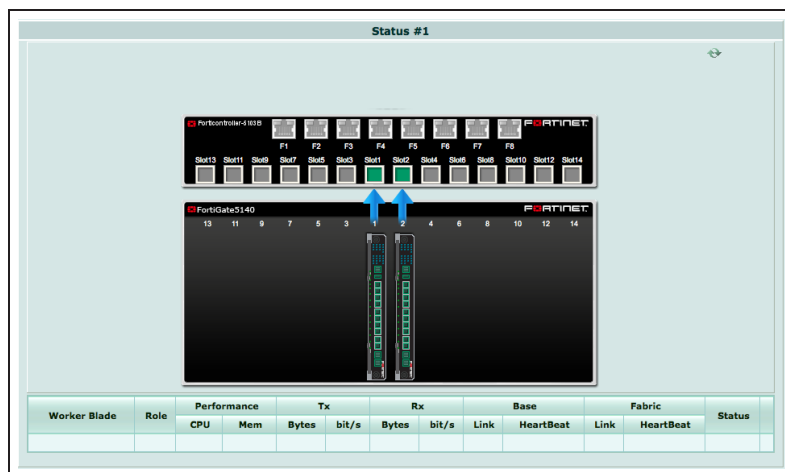
Selected: b1, b2

Heartbeat Device

OK Cancel

You can also go to **Load Balance > Status** to see the status of the cluster. This page should show both FortiControllers in the cluster.

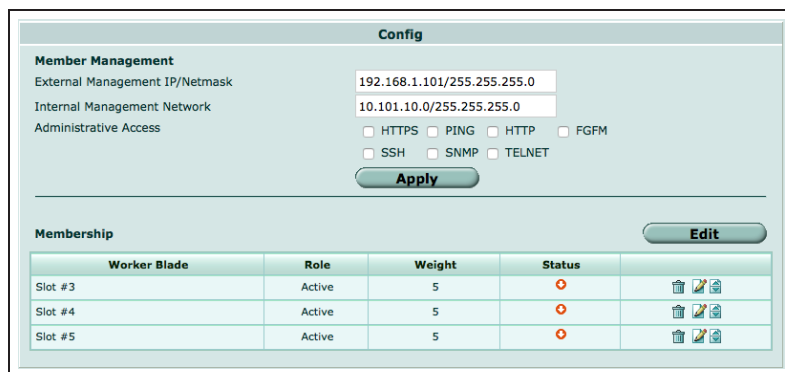
Since both FortiControllers are active their slot icons are both colored green.



Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured yet their status will be **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure them.



You can also enter this command to add slots 3, 4, and 5 to the cluster.

```
config load-balance setting
config slots
edit 3
next
edit 4
next
edit 5
end
end
```

You can also enter this command to configure the external management IP/Netmask and management access to

```
config load-balance setting
set base-mgmt-external-ip 172.20.120.100 255.255.255.0
set base-mgmt-allowaccess https ssh ping
```


this address.

Enable base management traffic between FortiControllers.

```
end
config load-balance setting
config base-mgmt-interfaces
    edit b1
    next
    edit b2
end
end
```

Enable base control traffic between FortiControllers.

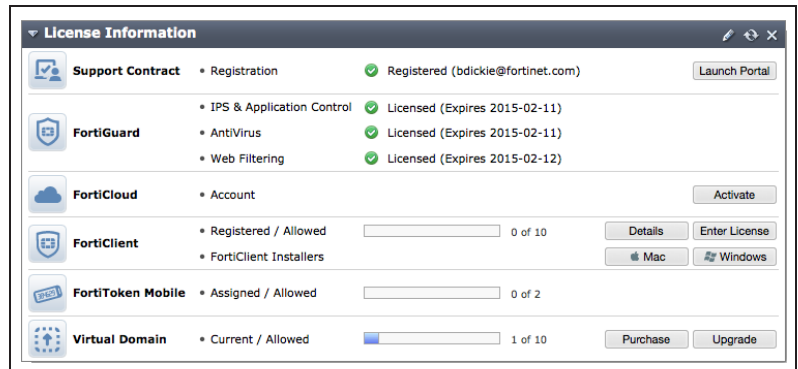
```
config load-balance setting
config base-ctrl-interfaces
    edit b1
    next
    edit b2
end
end
```

3. Adding the workers to the cluster

Reset the workers to factory default settings.

```
execute factoryreset
```

Register and apply licenses to each worker before adding the workers to the SLBC. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**.



Optionally give the mgmt1 and or mgmt2 interfaces of each worker IP addresses and connect them to your network. When a cluster is created, the mgmt1 and mgmt2 IP addresses are not synchronized, so you can connect to and manage each worker separately.

Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

Log into the CLI of each worker and enter this command to set the worker to operate in FortiController mode.

```
config system elbc
    set mode dual-forticontroller
end
```

The worker restarts and joins the cluster. On the FortiController GUI go to **Load Balance > Status**. As the workers restart they should appear in their appropriate slots.

Worker Blade	Role	Performance	Tx	Rx	Base	Fabric	Status
		CPU Mem	Bytes	bit/s	Bytes	bit/s	Link HeartBeat
Slot #3	Active	0% 0%	1,262K 3,496	8,591K 23,024	23,024	23,024	Running
Slot #4	Active	0% 0%	1,262K 3,496	8,596K 23,024	23,024	23,024	Running
Slot #5	Active	0% 0%	1,263K 3,496	8,603K 23,024	23,024	23,024	Running

4. Results

You can now connect to the worker GUI or CLI using the **External Management IP** and manage the workers in the same way as you would manage a standalone FortiGate. If you configured the worker mgmt1 or mgmt2 interfaces you can also connect to these interfaces to configure the workers. Configuration changes made to any worker are synchronized to all workers.

Configure the workers to process the traffic they receive from the FortiController front panel interfaces. By default all FortiController front panel interfaces are in the root VDOM. You can keep them in the root VDOM or create additional VDOMs and move interfaces into them.

For example, if you connect the Internet to FortiController front panel interface 2 of the FortiController in slot 1 (fctrl1/f2 on the worker GUI and CLI) and the internal network to FortiController front panel interface 6 of the FortiController in slot 2 (fctrl2/f6 on the worker GUI and CLI) you would access the root VDOM and add this policy to allow users on the Internal network to access the Internet.

Incoming Interface fctrl2/f6

Source Address Internal_NET

Source User(s) Click to add...

Source Device Type Click to add...

Outgoing Interface fctrl1/f2

Destination Address all

Schedule always

Service ALL

Action ACCEPT

Firewall / Network Options

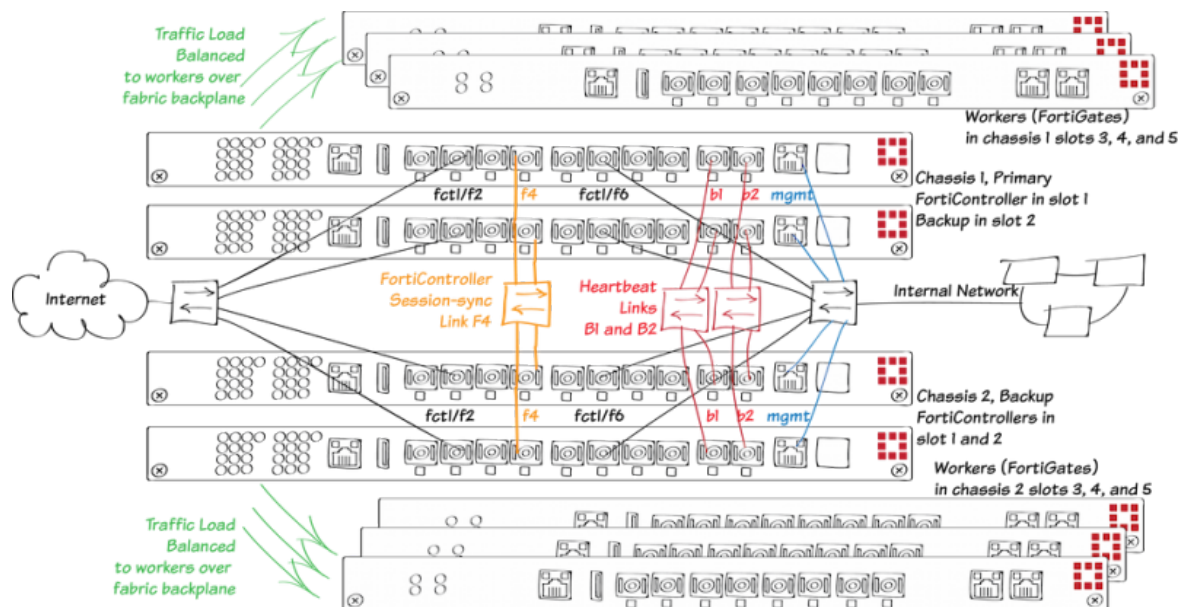
ON NAT

Use Outgoing Interface Address Fixed Port

Use Dynamic IP Pool

For further reading, check out the
[FortiController Session-aware Load
Balancing Guide](#).

SLBC Active-Passive with four FortiControllers and two chassis



This example describes how to setup an active-passive session-aware load balancing cluster (SLBC) consisting of two FortiGate-5000 chassis, four FortiController-5103Bs two in each chassis, and six FortiGate-5001Bs acting as workers, three in each chassis. This SLBC configuration can have up to seven redundant 10Gbit network connections.

The FortiControllers operate in active-passive HA mode for redundancy. The FortiController in chassis 1 slot 1 will be configured to be the primary unit, actively processing sessions. The other FortiControllers become the subordinate units.

In active-passive HA with two chassis and four FortiControllers, both chassis have two FortiControllers in active-passive HA mode and the same number of workers. Network connections are duplicated to the redundant FortiControllers in each Load chassis and between chassis for a total of four redundant data connections to each network.

All traffic is processed by the primary unit. If the primary unit fails, all traffic fails over to the chassis with two functioning FortiControllers and one of these FortiControllers becomes the new primary unit and processes all traffic. If the primary unit in the second chassis fails as well, one of the remaining FortiControllers becomes the primary unit and processes all traffic.

Heartbeat and base control and management communication is established between the chassis using the FortiController B1 and B2 interfaces. Only one heartbeat connection is required but redundant connections are recommended. Connect all of the B1 and all of the B2 interfaces together using switches. This example shows using one switch for the B1 connections and another for the B2 connections. You could also use one switch for both the B1 and B2 connections but using separate switches provides more redundancy.

The following VLAN tags and subnets are used by traffic on the B1 and B2 interfaces:

- Heartbeat traffic uses VLAN 999.
- Base control traffic on the 10.101.11.0/255.255.255.0 subnet uses VLAN 301.
- Base management on the 10.101.10.0/255.255.255.0 subnet uses VLAN 101

This example also includes a FortiController session sync connection between the FortiControllers using the FortiController F4 front panel interface (resulting in the SLBC having a total of seven redundant 10Gbit network connections). (You can use any fabric front panel interface, F4 is used in this example to make the diagram clearer.) FortiController-5103B session sync traffic uses VLAN 2000.

This example sets the device priority of the FortiController in chassis 1 slot 1 higher than the device priority of the other FortiControllers to make sure that the FortiController in chassis 1 slot 1 becomes the primary FortiController for the cluster. Override is also enabled on the FortiController in chassis 1 slot 1. Override may cause the cluster to negotiate more often to select the primary unit. This makes it more likely that the unit that you select to be the primary unit will actually be the primary unit; but enabling override can also cause the cluster to negotiate more often.

For more information about SLBC go [here](#).

1. Hardware setup

Install two FortiGate-5000 series chassis and connect them to power. Ideally each chassis should be connected to a separate power circuit. Install FortiControllers in slot 1 and 2 of each chassis. Install the workers in slots 3, 4, and 5 of each chassis. The workers must be installed in the same slots in both chassis. Power on both chassis.

Check the chassis, FortiController, and FortiGate LEDs to verify that all components are operating normally (to check normal operation LED status, see the FortiGate-5000 series documents available [here](#)).

Create redundant connections from all four FortiController front panel interfaces to the Internet and to the internal network.

Create a heartbeat link by connecting the FortiController B1 interfaces together. Create a backup heartbeat link by connecting the FortiController B2 interfaces together.

Create a FortiController session sync connection between the chassis by connecting the FortiController F4 interfaces together.

Connect the mgmt interfaces of all of the FortiControllers to the internal network or any network from which you want to manage the cluster.

Check the FortiSwitch-ATCA [release notes](#) and install the latest supported firmware on the FortiControllers and on the workers. Get FortiController firmware from the Fortinet Support site. Select the FortiSwitch-ATCA product.

2. Configuring the FortiController in Chassis 1 Slot 1

This will become the primary FortiController. To make sure this is the primary FortiController it will be assigned the highest device priority and override will be enabled. Connect to the GUI (using HTTPS) or CLI (using SSH) of the FortiController in chassis 1 slot 1 with the default IP address (<http://192.168.1.99>) or connect to the FortiController CLI through the console port (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None).

From the Dashboard System Information widget, set the **Host Name** to ch1-slot1. Or enter this command.

```
config system global
  set hostname ch1-slot1
end
```

Add a password for the admin administrator account. You can either use the **Administrators** widget on the GUI or enter this command.

```
config admin user
  edit admin
  set password
end
```

Change the FortiController mgmt

```
config system interface
```

interface IP address. Use the GUI **Management Port** widget or enter this command.

```
edit mgmt
set ip 172.20.120.151/24
end
```

If you need to add a default route for the management IP address, enter this command.

```
config route static
edit 1
set gateway 172.20.120.2
end
```

Set the chassis type that you are using.

```
config system global
set chassis-type fortigate-5140
end
```

Configure Active-Passive HA. From the FortiController GUI **System Information** widget, beside **HA Status** select **Configure**.

Set **Mode** to **Active-Passive**, set the **Device Priority** to 250, change the **Group ID**, select **Enable Override**, enable **Chassis Redundancy**, set **Chassis ID** to 1 and move the **b1** and **b2** interfaces to the **Selected** column and select **OK**.

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure In Sync	Elbc sync
5103-slot1	FT513B3912000051	Master	169.254.128.33	247020.05	0	0/1	1

Configure

Mode: Active-Passive

Device Priority (0-255): 250

Group ID(0-31): 5

Enable Override:

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy:

Chassis ID(1 - 2): 1

Available: mgmt

Selected: b1, b2

OK Cancel

Enter this command to use the FortiController front panel F4 interface for FortiController session sync communication between FortiControllers.

```
config system ha
set session-sync-port f4
end
```

You can also enter the complete HA configuration with this command.

```
config system ha
set mode active-passive
set groupid 15
set priority 250
```

```
set override enable
set chassis-redundancy enable
set chassis-id 1
set hbdev b1 b2
set session-sync-port f4
end
```

If you have more than one cluster on the same network, each cluster should have a different **Group ID**. Changing the Group ID changes the cluster interface virtual MAC addresses. If your group ID setting causes a MAC address conflict you can select a different Group ID. The default Group ID of 0 is not a good choice and normally should be changed.

You can also adjust other HA settings. For example, you could change the **VLAN to use for HA heartbeat traffic** if it conflicts with a VLAN on your network. You can also adjust the **Heartbeat Interval** and **Number of Heartbeats** lost to adjust how quickly the cluster determines one of the FortiControllers has failed.

3. Configuring the FortiController in Chassis 1 Slot 2

Log into the FortiController in chassis 1 slot 2.

```
config system global
  set hostname ch1-slot2
end
```

Enter these commands to set the host name to ch1-slot2, to configure the mgmt interface, and to duplicate the HA configuration of the FortiController in slot 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10).

```
config system interface
  edit mgmt
  set ip 172.20.120.152/24
end
```

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

```
config system ha
  set mode active-passive
  set groupid 15
  set priority 10
  set chassis-redundancy enable
  set chassis-id 1
  set hbdev b1 b2
  set session-sync-port f4
end
```

4. Configuring the FortiController in Chassis 2 Slot 1

Log into the FortiController in chassis 2 slot 1.

```
config system global
  set hostname ch2-slot1
end
```

Enter these commands to set the host

name to ch2-slot1, to configure the mgmt interface, and to duplicate the HA configuration of the FortiController in chassis 1 slot 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10), and set the **Chassis ID** to 2.

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

```
config system interface
  edit mgmt
    set ip 172.20.120.251/24
  end

config system ha
  set mode active-passive
  set groupid 15
  set priority 10
  set chassis-redundancy enable
  set chassis-id 2
  set hbdev b1 b2
  set session-sync-port f4
end
```

5. Configuring the FortiController in Chassis 2 Slot 2

Log into the FortiController in chassis 2 slot 2.

Enter these commands to set the host name to ch2-slot2, to configure the mgmt interface, and to duplicate the HA configuration of the FortiController in chassis 1 slot 1. Except, do not select **Enable Override** and set the **Device Priority** to a lower value (for example, 10), and set the **Chassis ID** to 2.

All other configuration settings are synchronized from the primary FortiController when the cluster forms.

```
config system global
  set hostname ch2-slot2
end

config system interface
  edit mgmt
    set ip 172.20.120.252/24
  end

config system ha
  set mode active-passive
  set groupid 15
  set priority 10
  set chassis-redundancy enable
  set chassis-id 2
  set hbdev b1 b2
  set session-sync-port f4
end
```

6. Configuring the cluster

After a short time the FortiControllers restart in HA mode and form an active-passive SLBC. All of the FortiControllers must have the same HA configuration and at least one heartbeat link (the B1 and B2 interfaces) must be connected. If the FortiControllers are unable to form a cluster, check to make sure that they all have the same HA configuration. Also they can't form a cluster if the heartbeat interfaces (B1 and B2) are not connected.

With the configuration described in the previous steps, the FortiController in chassis 1 slot 1 should become the primary unit and you can log into the cluster using the management IP address that you assigned to this FortiController.

The other FortiControllers become backup FortiControllers. You cannot log into or manage the backup FortiControllers until you configure the cluster External Management IP and add workers to the cluster. Once you do this you can use the External Management IP address and a special port number to manage the backup FortiControllers. This is described below. (You can also connect to any backup FortiController CLI using their console port.)

You can confirm that the cluster has been formed by viewing the FortiController HA configuration. The display should show both FortiControllers in the cluster.

High Availability

Cluster Members

Host Name	SN	Role	IP	Up Time	The number of link-up Port	Worker Failure	In Sync	Elbc sync
ch1-slot1	FT513B3912000029	Master	169.254.128.121	1075.00	0	0/3	1	1
ch2-slot1	FT513B3912000051	Slave	169.254.128.124	423.61	0	0/0	0	0
ch2-slot2	FT513B3913000168	Slave	169.254.128.123	273.87	0	0/3	0	1
ch1-slot2	FT513B3914000006	Slave	169.254.128.122	703.38	0	0/3	1	1

Configure

Mode: Active-Passive

Device Priority (0-255): 250

Group ID(0-31): 5

Enable Override:

Heartbeat interval(200-1000ms): 250

Number of heartbeats lost(2-255): 5

VLAN to use for HA heartbeat traffic(1-4094): 999

Enable Chassis Redundancy:

Chassis ID(1 - 2): 1

Available: mgmt

Selected: b1, b2

Heartbeat Device

OK Cancel

You can also go to **Load Balance > Status** to see the status of the primary FortiController (slot icon colored green).

Status #1

FortiGate 5140

FortiGate 5140

Worker Blade	Role	Performance		Tx		Rx		Base		Fabric		Status
		CPU	Mem	Bytes	bit/s	Bytes	bit/s	Link	HeartBeat	Link	HeartBeat	

Go to **Load Balance > Config** to add the workers to the cluster by selecting **Edit** and moving the slots that contain workers to the **Members** list.

The **Config** page shows the slots in which the cluster expects to find workers. If the workers have not been configured for SLBC operation their status will be **Down**.

Configure the **External Management IP/Netmask**. Once you have connected workers to the cluster, you can use this IP address to manage and configure all of the devices in the cluster.

You can also enter this command to add slots 3, 4, and 5 to the cluster.

You can also enter this command to set the External Management IP and configure management access.

Enable base management traffic between FortiControllers.

Enable base control traffic between FortiControllers.

Worker Blade	Role	Weight	Status	
Slot #3	Active	5	Down	
Slot #4	Active	5	Down	
Slot #5	Active	5	Down	

```
config load-balance setting
config slots
  edit 3
  next
  edit 4
  next
  edit 5
  end
end
```

```
config load-balance setting
  set base-mgmt-external-ip 172.20.120.100 255.255.255.0
  set base-mgmt-allowaccess https ssh ping
end
```

```
config load-balance setting
config base-mgmt-interfaces
  edit b1
  next
  edit b2
  end
end
```

```
config load-balance setting
config base-ctrl-interfaces
  edit b1
  next
  edit b2
```

```
end
end
```

7. Adding the workers to the cluster

Reset each worker to factory default settings.

```
execute factoryreset
```

Give the mgmt1 or mgmt2 interface of each worker an IP address and connect these interfaces to your network. This step is optional but useful because when the workers are added to the cluster, these IP addresses are not synchronized, so you can connect to and manage each worker separately.

```
config system interface
edit mgmt1
set ip 172.20.120.120
end
```

Optionally give each worker a different hostname. The hostname is also not synchronized and allows you to identify each worker.

```
config system global
set hostname worker-chassis-1-slot-3
end
```

Register each worker and apply licenses to each worker before adding the workers to the cluster. This includes **FortiCloud** activation, **FortiClient** licensing, and **FortiToken** licensing, and entering a license key if you purchased more than 10 **Virtual Domains**.

Product	Status	Details	Buttons
Support Contract	Registered	Registered (bdickie@fortinet.com)	Launch Portal
FortiGuard	IPS & Application Control	Licensed (Expires 2015-02-11)	
	AntiVirus	Licensed (Expires 2015-02-11)	
	Web Filtering	Licensed (Expires 2015-02-12)	
FortiCloud	Account		Activate
FortiClient	Registered / Allowed	0 of 10	Details Enter License
	FortiClient Installers		Mac Windows
FortiToken Mobile	Assigned / Allowed	0 of 2	
Virtual Domain	Current / Allowed	1 of 10	Purchase Upgrade

Log into the CLI of each worker and enter this command to set the worker to operate in FortiController mode. The worker restarts and joins the cluster.

```
config system elbc
set mode forticontroller
end
```

À

8. Managing the cluster

After the workers have been added to the cluster you can use the External Management IP to manage the the primary worker. This includes access to the primary worker GUI or CLI, SNMP queries to the primary worker, and using FortiManager to manage the primary worker. As well SNMP traps and log messages are sent from the primary worker with the External Management IP as their source address. And finally connections to FortiGuard for updates, web filtering lookups and so on, all originate from the External Management IP.

You can use the external management IP followed by a special port number to manage individual devices in the cluster. The special port number identifies the protocol (80 for HTTP, 443 for HTTPS, 22 for SSH, 23 for Telnet, 161 for SNMP) and the chassis and slot number of the device you want to connect to. In fact this is the only way to manage the backup FortiControllers. Some examples:

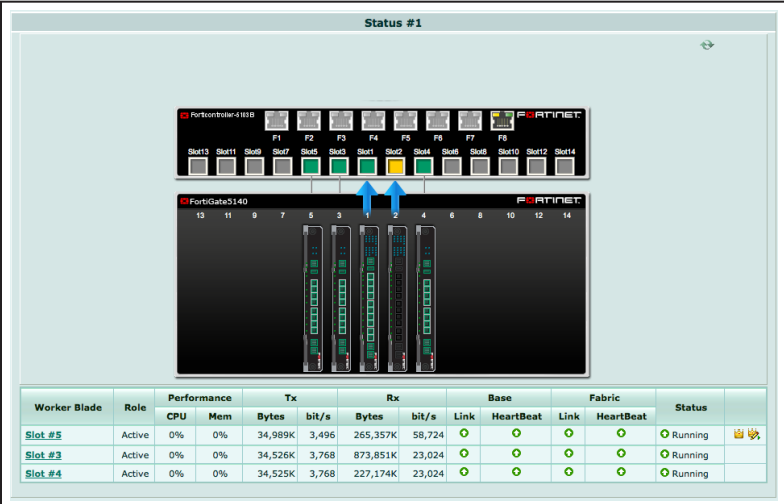
- To use HTTP to connect to the GUI of the FortiController in chassis 1 slot 2, browse to: **https://172.20.120.100:44312**
- To use HTTP to connect to the GUI of the FortiController in chassis 2 slot 1, browse to: **https://172.20.120.100:44321**
- To use Telnet to connect to the CLI of the worker in chassis 2 slot 4: **telnet 172.20.120.100 2324**
- To use SSH to connect to the CLI the worker in chassis 1 slot 5: **ssh admin@172.20.120.100 -p2215**
- To use SNMP to query the FortiController in chassis 1 slot 2 use port **16112** in the SNMP query.

You can also manage the primary FortiController using the IP address of its mgmt interface, set up when you first configured the primary FortiController. You can also manage the workers by connecting directly to their mgmt1 or mgmt2 interfaces if you set them up. However, the only way to manage the backup FortiControllers is by using its special port number (or a serial connection to the Console port).

To manage a FortiController using SNMP you need to load the FORTINET-CORE-MIB.mib file into your SNMP manager. You can get this MIB file from the Fortinet support site, in the same location as the current FortiController firmware (select the FortiSwitchATCA product).

On the primary FortiController GUI go to **Load Balance > Status**. As the workers in chassis 1 restart they should appear in their appropriate slots.

The primary FortiController should be the FortiController in chassis 1 slot 1. The primary FortiController status display includes a **Config Master** link that you can use to connect to the primary worker.



The screenshot displays the 'Status #1' page in the FortiController GUI. At the top, there is a rack of FortiGate5140 units. The units are labeled with ports F1 through F8 and slots Slot1 through Slot14. Two blue arrows point to Slot 1 and Slot 2. Below the rack, a table provides performance metrics for the worker blades.

Worker Blade	Role	Performance	Tx	Rx	Base	Fabric	Status					
		CPU	Mem	Bytes	bit/s	Bytes	bit/s	Link	HeartBeat	Link	HeartBeat	
Slot #5	Active	0%	0%	34,989K	3,496	265,357K	58,724	🟢	🟢	🟢	🟢	Running 🏠👤
Slot #3	Active	0%	0%	34,526K	3,768	873,851K	23,024	🟢	🟢	🟢	🟢	Running
Slot #4	Active	0%	0%	34,525K	3,768	227,174K	23,024	🟢	🟢	🟢	🟢	Running

Log into a backup FortiController GUI (for example by browsing to <https://172.20.120.100:44321> to log into the FortiController in chassis 2 slot 1) and go to **Load Balance > Status**. If the workers in chassis 2 are configured correctly they should appear in their appropriate slots.

The backup FortiController Status page shows the status of the workers in chassis 2 and does not include the **Config Master** link.

Worker Blade	Role	Performance		Tx		Rx		Base			Fabric			Status
		CPU	Mem	Bytes	bit/s	Bytes	bit/s	Link	HeartBeat	Link	HeartBeat	Link	HeartBeat	
Slot #3	Active	0%	0%	329,702	3,768	8,679K	92,052	🟢	🟢	🟢	🟢	🟢	🟢	🟢 Running
Slot #4	Active	0%	0%	329,702	3,768	2,171K	23,024	🟢	🟢	🟢	🟢	🟢	🟢	🟢 Running
Slot #5	Active	0%	0%	329,702	3,768	2,171K	23,024	🟢	🟢	🟢	🟢	🟢	🟢	🟢 Running

9. Results - Configuring the workers

Configure the workers to process the traffic they receive from the FortiController front panel interfaces. By default all FortiController front panel interfaces are in the worker root VDOM. You can keep them in the root VDOM or create additional VDOMs and move interfaces into them.

For example, if you connect the Internet to FortiController front panel interface 2 (fctrl/f2 on the worker GUI and CLI) and the internal network to FortiController front panel interface 6 (fctrl/f6) you can access the root VDOM and add a policy to allow users on the Internal network to access the Internet.

Incoming Interface fctrl/f6

Source Address Internal_NET

Source User(s) Click to add...

Source Device Type Click to add...

Outgoing Interface fctrl/f2

Destination Address all

Schedule always

Service ALL

Action ACCEPT

Firewall / Network Options

ON NAT

Use Outgoing Interface Address Fixed Port

Use Dynamic IP Pool

10. Results - Primary FortiController cluster status

Log into the **primary FortiController CLI** and enter this command to view the system status of the primary FortiController.

For example, you can use SSH to log into the primary FortiController CLI using the external management IP:

```
ssh admin@172.20.120.100 -p2211
```

```
get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000029
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: chl-slot1
Current HA mode: a-p, master
System time: Sun Sep 14 08:16:25 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time (US&Canada)
```

Enter this command to view the load balance status of the primary FortiController and its workers. The command output shows the workers in slots 3, 4, and 5, and status information about each one.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
  Working: 3 [ 3 Active 0 Standby]
  Ready:   0 [ 0 Active 0 Standby]
  Dead:    0 [ 0 Active 0 Standby]
  Total:   3 [ 3 Active 0 Standby]

Slot 3: Status:Working  Function:Active
  Link:   Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
Slot 4: Status:Working  Function:Active
  Link:   Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
Slot 5: Status:Working  Function:Active
  Link:   Base: Up      Fabric: Up
  Heartbeat: Management: Good  Data: Good
  Status Message:"Running"
```

Enter this command from the primary FortiController to show the HA status of the FortiControllers. The command output shows a lot of information about the cluster including the host names and chassis and slot locations of the FortiControllers, the number of sessions each FortiController is processing (this case 0 for each FortiController) the number of failed workers (0 of 3 for each FortiController), the number of FortiController front panel interfaces that are connected (2 for each FortiController) and so on. The final two lines of output also show that the B1 interfaces are connected (status=alive) and the B2 interfaces are not (status=dead). The cluster can

still operate with a single heartbeat connection, but redundant heartbeat interfaces are recommended.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=4416.18, chassis=1(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none) hbdevs: local_interface=      b1 best=yes
                        local_interface=      b2 best=no

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123, uptime=1181.62, chassis=2(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none) hbdevs: local_interface=      b1 last_hb_time= 4739.97  status=alive
                        local_interface=      b2 last_hb_time=  0.00  status=dead

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=335.79, chassis=2(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none) hbdevs: local_interface=      b1 last_hb_time= 4739.93  status=alive
                        local_interface=      b2 last_hb_time=  0.00  status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4044.46, chassis=1(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none) hbdevs: local_interface=      b1 last_hb_time= 4740.03  status=alive
                        local_interface=      b2 last_hb_time=  0.00  status=dead
```

II. Results - Chassis 1 Slot 2 FortiController status

Log into the **chassis 1 slot 2 FortiController CLI** and enter this command to view the status of this backup FortiController.

To use SSH:
ssh admin@172.20.120.100 -p2212


```
get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3914000006
BIOS version: 04000010
System Part-Number: P08442-04
Hostname: chl-slot2
Current HA mode: a-p, backup
System time: Sun Sep 14 12:44:58 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time(US&Canada)
```

Enter this command to view the status of this backup FortiController and its workers.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: slot-3
Blades:
  Working:  3 [  3 Active  0 Standby]
  Ready:    0 [  0 Active  0 Standby]
  Dead:     0 [  0 Active  0 Standby]
  Total:    3 [  3 Active  0 Standby]

Slot  3: Status:Working  Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"

Slot  4: Status:Working  Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"

Slot  5: Status:Working  Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"
```

Enter this command from the FortiController in chassis 1 slot 2 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 1 slot 2 is shown first.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
chl-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4292.69, chassis=1(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1
  session: total=0, session_sync=in sync
```

```

state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)  hbdevs: local_interface=      b1 best=yes
                    local_interface=      b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=4664.49, chassis=1(1)
slot: 1
sync: conf_sync=1, elbc_sync=1, conn=3(connected)
session: total=0, session_sync=in sync
state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)  hbdevs: local_interface=      b1 last_hb_time= 4958.88  status=alive
                    local_interface=      b2 last_hb_time=  0.00  status=dead

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123, uptime=1429.99, chassis=2(1)
slot: 1
sync: conf_sync=1, elbc_sync=1, conn=3(connected)
session: total=0, session_sync=in sync
state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)  hbdevs: local_interface=      b1 last_hb_time= 4958.88  status=alive
                    local_interface=      b2 last_hb_time=  0.00  status=dead

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=584.20, chassis=2(1)
slot: 2
sync: conf_sync=1, elbc_sync=1, conn=3(connected)
session: total=0, session_sync=in sync
state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)  hbdevs: local_interface=      b1 last_hb_time= 4958.88  status=alive
                    local_interface=      b2 last_hb_time=  0.00  status=dead

```

12. Results - Chassis 2 Slot 1 FortiController status

Log into the **chassis 2 slot 1 FortiController CLI** and enter this command to view the status of this backup FortiController.

To use SSH:

```
ssh admin@172.20.120.100 -p2221
```

```

get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3912000051
BIOS version: 04000009
System Part-Number: P08442-04
Hostname: ch2-slot1
Current HA mode: a-p, backup
System time: Sun Sep 14 12:53:09 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time (US&Canada)

```

Enter this command to view the status of this backup FortiController and its workers.

```
get load-balance status
ELBC Master Blade: slot-3
Confsync Master Blade: N/A
Blades:
Working: 3 [ 3 Active 0 Standby]
Ready: 0 [ 0 Active 0 Standby]
Dead: 0 [ 0 Active 0 Standby]
Total: 3 [ 3 Active 0 Standby]

Slot 3: Status:Working Function:Active
Link: Base: Up Fabric: Up
Heartbeat: Management: Good Data: Good
Status Message:"Running"
Slot 4: Status:Working Function:Active
Link: Base: Up Fabric: Up
Heartbeat: Management: Good Data: Good
Status Message:"Running"
Slot 5: Status:Working Function:Active
Link: Base: Up Fabric: Up
Heartbeat: Management: Good Data: Good
Status Message:"Running"
```

Enter this command from the FortiController in chassis 2 slot 1 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 2 slot 1 is shown first.

```
diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123, uptime=1858.71, chassis=2(1)
slot: 1
sync: conf_sync=1, elbc_sync=1
session: total=0, session_sync=in sync
state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none) hbdevs: local_interface= b1 best=yes
local_interface= b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=5093.30, chassis=1(1)
slot: 1
sync: conf_sync=1, elbc_sync=1, conn=3(connected)
session: total=0, session_sync=in sync
state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none) hbdevs: local_interface= b1 last_hb_time= 2074.15 status=alive
local_interface= b2 last_hb_time= 0.00 status=dead
```

```

ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=1013.01, chassis=2(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)  hbdevs: local_interface=      b1 last_hb_time= 2074.15  status=alive
                    local_interface=      b2 last_hb_time=  0.00  status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4721.60, chassis=1(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)  hbdevs: local_interface=      b1 last_hb_time= 2074.17  status=alive
                    local_interface=      b2 last_hb_time=  0.00  status=dead

```

13. Results - Chassis 2 Slot 2 FortiController status

Log into the **chassis 2 slot 2 FortiController CLI** and enter this command to view the status of this backup FortiController.

To use SSH:

```
ssh admin@172.20.120.100 -p2222
```

```

get system status
Version: FortiController-5103B v5.0,build0024,140815
Branch Point: 0024
Serial-Number: FT513B3913000168
BIOS version: 04000010
System Part-Number: P08442-04
Hostname: ch2-slot2
Current HA mode: a-p, backup
System time: Sun Sep 14 12:56:45 2014
Daylight Time Saving: Yes
Time Zone: (GMT-8:00)Pacific Time (US&Canada)

```

Enter this command to view the status of the backup FortiController and its workers.

```

get load-balance status
  ELBC Master Blade: slot-3
  Confsync Master Blade: N/A
  Blades:
    Working:  3 [  3 Active  0 Standby]
    Ready:    0 [  0 Active  0 Standby]
    Dead:     0 [  0 Active  0 Standby]
    Total:    3 [  3 Active  0 Standby]

    Slot 3: Status:Working  Function:Active

```

```

Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"
Slot 4: Status:Working  Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"
Slot 5: Status:Working  Function:Active
Link:      Base: Up      Fabric: Up
Heartbeat: Management: Good  Data: Good
Status Message:"Running"

```

Enter this command from the FortiController in chassis 2 slot 2 to show the HA status of the FortiControllers. Notice that the FortiController in chassis 2 slot 2 is shown first.

```

diagnose system ha status
mode: a-p
minimize chassis failover: 1
ch2-slot2(FT513B3913000168), Slave(priority=3), ip=169.254.128.124, uptime=1276.77, chassis=2(1)
  slot: 2
  sync: conf_sync=1, elbc_sync=1
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)  hbdevs: local_interface=      b1 best=yes
                        local_interface=      b2 best=no

ch1-slot1(FT513B3912000029), Master(priority=0), ip=169.254.128.121, uptime=5356.98, chassis=1(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)  hbdevs: local_interface=      b1 last_hb_time= 1363.89  status=alive
                        local_interface=      b2 last_hb_time=  0.00  status=dead

ch2-slot1(FT513B3912000051), Slave(priority=2), ip=169.254.128.123, uptime=2122.58, chassis=2(1)
  slot: 1
  sync: conf_sync=1, elbc_sync=1, conn=3(connected)
  session: total=0, session_sync=in sync
  state: worker_failure=0/3, intf_state=(port up:)=0
  force-state(0:none)  hbdevs: local_interface=      b1 last_hb_time= 1363.97  status=alive
                        local_interface=      b2 last_hb_time=  0.00  status=dead

ch1-slot2(FT513B3914000006), Slave(priority=1), ip=169.254.128.122, uptime=4985.27, chassis=1(1)
  slot: 2

```

```
sync: conf_sync=1, elbc_sync=1, conn=3(connected)
session: total=0, session_sync=in sync
state: worker_failure=0/3, intf_state=(port up:)=0
force-state(0:none)  hbdevs: local_interface=      b1 last_hb_time= 1363.89  status=alive
                    local_interface=      b2 last_hb_time=  0.00  status=dead
```

For further reading, check out the
[FortiController Session-aware Load
Balancing Guide](#).

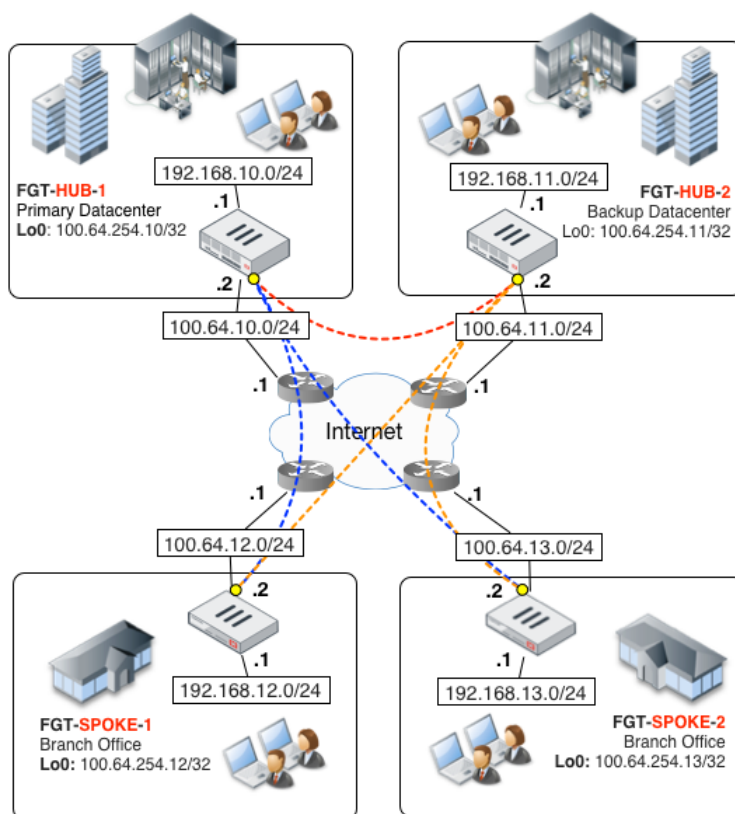
Hub-and-spoke VPN using quick mode selectors

In this expert cookbook article and an included example recipe, we will explore a scalable approach to setting up a large number of spoke VPNs by using quick mode selector source definitions on the spoke FortiGates and the dialup VPN configurations on the hub FortiGates.

We will also explore how redundant spoke VPN tunnels can be configured in order to offer maximum redundancy for environments with critical availability requirements. We will be authenticating the VPN tunnels using X-Auth in order to ensure separate credentials for each spoke.

This recipe is based on FortiOS firmware version 5.2, so some of the steps shown may not be the same as with other versions of the firmware.

The sample topology for this advanced cookbook article follows:



This topology consists of 2 hub networks and 2 spoke networks, using private IP ranges, separated by a simulated Internet, with 100.64.0.0/16 representing the Internet. Each FortiGate also has a loopback interface that is routable across the VPN.

The diagram topology shows the VPN tunnels along with their redundant links:

- The **red** dotted line showing the VPN tunnel connection between the primary and backup data centers; in this case, our two hubs.
- The **blue** dotted line showing the VPN tunnel connection between the primary datacenter and the branch offices; the spokes in the scenario.
- The **orange** dotted line shows the VPN tunnel connection between the backup datacenter and the branch offices.

While the topology shown in the diagram can be built using individual static tunnels between each site, this would not scale well if addition spokes grow to a significant number. There would also be limited support for dynamically addressed sites. This strategy put forth by this article offers a solution to these issues by using a single phase 1 dialup definition on the hub FortiGates with additional spoke tunnels being added, without any changes to the hubs beyond that of adding additional user accounts for each additional spoke.

Spoke authentication is maintained by with X-Auth, which keeps the authentication of the individual tunnels separate in such a way that the use of a Pre-Shared Key alone is insufficient to authenticate a tunnel. A Public Key Infrastructure can also be used, provided that separate key-pairs are used for each VPN tunnel to maintain the segregation of the spokes.

The key points of this design are:

- Each hub FortiGate is configured with a dialup interface-mode Phase1 using X-Auth.
- Each spoke has its own user account on the hub FortiGates. In this example, local accounts are used on each hub, but a RADIUS or LDAP authentication server could be used on the back end, eliminating the need to managed the accounts on the FortiGates.
- Spoke FortiGates are configured to propagate their local subnets using quick mode selectors (specifically, a source object).
- When a new spoke tunnel is connected, the hub FortiGate validates the shared secret along with the X-Auth credentials provided by the spoke FortiGate.
- Spokes FortiGates can have dynamically assigned IP addresses such as those given out by DSL or cable ISPs.
- The hub FortiGates each insert a reverse route pointing to newly established tunnel interfaces, for any of the subnets provided by the spoke FortiGate's source quick mode selectors.
- Each spoke FortiGate uses configured static routes to direct traffic that needs to go to the datacenter(s) through the VPN tunnels destined for the hubs. The static route to the backup hub is set to a higher priority number value, making it the less preferred route. There is also an option where you can send all of your traffic from the spokes through the VPN tunnel by default. This can be done by configuring the WAN interface to route all traffic through the public IP address of the hub FortiGate. This is what our example configuration is set to do.
- We need to aware of any potential points where asymmetrical routing could occur as it relates to traffic

returning to the spokes (This is essentially the response to a request coming back through a different route than it took to get there). This can be a potential problem especially when communicating to hosts that are connected to both data centers and we happen to be redistributing spoke routes using a dynamic routing protocol with hub sites using OSI Layer 3 networking devices. In this case, we would ensure that the backup hub's redistributed routes are less preferred than the primary hub's routes. In all cases, it is important to have a clear view of the routing flows between each endpoint and to keep "diag debug flow" in our toolbox to diagnose those potential asymmetric routing issues. In our example, we would want to route traffic destined to resources in each respective hub directly to that hub, rather than have it cross the inter-datacenter VPN tunnel, and have default routing flow to the primary hub under normal circumstances.

The Hub FortiGates

Let's look at the relevant configuration points of the hub FortiGates (These will be identical on each hub FortiGate:

While the GUI can be used for these steps, we are going to use the CLI to keep things simple and avoid potential confusion that may be caused by changes in the GUI's layout.

Create the IPsec tunnel:

```
config vpn ipsec phase1-interface
  edit "SPOKES"
    set type dynamic
    set interface "port1"
    set mode aggressive
    set peertype one
    set proposal aes256-sha256
    set xauthtype auto
    set authusrgrp "SPOKE-GRP"
    set peerid "SPOKES"
    set psksecret SuperSecretSpokeSecret
  next
end
```

```
config vpn ipsec phase2-interface
  edit "SPOKES-P2"
    set phasename "SPOKES"
    set proposal aes256-sha256
    set keepalive enable
  next
end
```

Create a user for each of the spokes:

```
config user local
  edit "SPOKE1"
    set type password
```

```
set passwd Spoke1SuperSecret
next
edit "SPOKE2"
set type password
set passwd Spoke2SuperSecret
next
end
```

Create a user group and include the spoke members:

```
config user group
edit "SPOKE-GRP"
set member "SPOKE1" "SPOKE2"
next
end
```

Create the firewall policies

```
config firewall policy
edit 1
set srcintf "port2" "loop0"
set dstintf "SPOKES"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
next
edit 2
set srcintf "SPOKES"
set dstintf "port2" "loop0"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
next
end
```

A few of the above configuration aspects require further explanation:

- **Aggressive mode:** We are using this mode in order to ensure that these dialup spokes are terminated on the right dialup phase1. If the hub unit has other dialup phase1 (for FortiClient VPN users, for instance), the hub would otherwise be unable to distinguish between each dialup phase1. A few of the above configuration aspects require further explanation:

- **X-Auth:** As previously stated, this allows us to authenticate each connecting spoke unit to a local group, which is defined in the above configuration as currently containing two user accounts (our example has two spokes). Provisioning additional spokes on the hub would simply involve adding additional user accounts.
- **Policies:** As usual, we must always configure policies in order for traffic to flow. IPsec Phase1 follows a special rule in which tunnels will not even attempt to come up unless they have at least one policy referring to them (this happens to be a good trick to know when you want to disable an IPsec VPN tunnel without deleting its configuration).

The Spoke FortiGates

With the hub FortiGates configured and ready for incoming connections, the spoke FortiGates can be configured. Below is the steps for configuring SPOKE1. To configure additional spoke FortiGates change the unit specific information.

Create the IPsec tunnel

```

config vpn ipsec phase1-interface
  edit "HUB-PRIMARY"
    set interface "port1"
    set mode aggressive
    set proposal aes256-sha256
    set localid "SPOKES"
    set xauthtype client
    set authusr "SPOKE1"
    set authpasswd Spoke1SuperSecret
    set mesh-selector-type subnet
    set remote-gw 100.64.10.2
    set psksecret SuperSecretSpokeSecret
  next
  edit "HUB-BACKUP"
    set interface "port1"
    set mode aggressive
    set proposal aes256-sha256
    set localid "SPOKES"
    set xauthtype client
    set authusr "SPOKE1"
    set authpasswd Spoke1SuperSecret
    set mesh-selector-type subnet
    set remote-gw 100.64.11.2
    set psksecret SuperSecretSpokeSecret
  next
end

config vpn ipsec phase2-interface
  edit "PRIMARY-P2"
    set phase1name "HUB-PRIMARY"
    set proposal aes256-sha256

```

```

set keepalive enable
set src-addr-type name
set dst-addr-type name
set src-name "VPN_SUBNETS"
set dst-name "all"
next
edit "BACKUP-P2"
set phase1name "HUB-BACKUP"
set proposal aes256-sha256
set keepalive enable
set src-addr-type name
set dst-addr-type name
set src-name "VPN_SUBNETS"
set dst-name "all"
next
end

```

Creating addresses for the subnets

```

config firewall address
  edit "NET_192.168.12.0/24"
  set subnet 192.168.12.0 255.255.255.0
  next
  edit "NET_100.64.254.12/32"
  set subnet 100.64.12.254 255.255.255.255
  next
end

```

Creating an address group for the subnets

```

config firewall addrgrp
  edit "VPN_SUBNETS"
  set member "NET_100.64.254.12/32" "NET_192.168.12.0/24"
  next
end

```

Configuring static routes

Use edit 0 to create a route with the next unused number.

```

config router static
  edit 0
  set dst 100.64.11.2 255.255.255.255
  set device "port1"
  next
  edit 0
  set dst 100.64.10.2 255.255.255.255

```

```
set device "port1"
next
edit 0
set device "HUB-PRIMARY"
next
edit 0
set device "HUB-BACKUP"
set priority 20
next
end
```

Configuring the firewall policies

Use edit 0 to create a policy with the next unused number.

```
config firewall policy
edit 0
set srcintf "port2" "loop0"
set dstintf "HUB-PRIMARY"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
next
edit 0
set srcintf "HUB-PRIMARY"
set dstintf "port2" "loop0"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
next
edit 0
set srcintf "port2" "loop0"
set dstintf "HUB-BACKUP"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
next
edit 0
set srcintf "HUB-BACKUP"
```

```

set dstintf "port2" "loop0"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
next
end

```

Each spoke configuration calls for similar Phase1 parameters, but differs for the rest of the configuration in a few keys areas:

- **Aggressive mode:** As the hub is validating the inbound ID, we have configured our peer ID to the matching string "SPOKES".
- **X-Auth:** Our spokes are acting as X-auth clients, and each of our unit is using distinct credentials passed to the hub device during IKE phase1 negotiation.
- **Phase 2 quick mode selectors:** As the title of this recipe suggests, this is where the spoke provisioning routing automation happens. We've defined address objects, added them to a group, and performed the configuration found in Phase2. There is however a peculiarity where if we have more than one subnet behind our spoke unit, the "set mesh-selector-type subnet" command must be configured to ensure multiple Phase2 SAs are negotiated for each subnet listed in our group.
- **Routing:** As previously expressed, we have configured our default routing to flow through the primary hub (blue links) and failover routing to the backup hub (orange links, using route priority adjustment). Notice that we are explicitly routing each hub's public IP through the public Internet to ensure that traffic will not flow through the VPN tunnel (and result in flapping).

Where the spoke configurations will be different

As explained earlier, the spoke FortiGate configurations will be slightly different on each individual spoke. The settings will be similar on all of the spoke with the following exceptions:

- **X-Auth:** Our spokes are acting as X-auth clients, and each of our unit is using distinct credentials passed to the hub device during IKE phase1 negotiation.

```

config vpn ipsec phase1-interface
edit "HUB-PRIMARY"
  set authusr (The account will be the one associated with the specific spoke)
  set authpasswd (The password will be the one associated with the specific spoke)
next
edit "HUB-BACKUP"
  set authusr (The account will be the one associated with the specific spoke)
  set authpasswd (The password will be the one associated with the specific spoke)
next
end

```

- **Phase 2 quick mode selectors:** This is where the spoke routing automation happens. We've defined address objects, added them to a group, and performed the configuration found in Phase2. There is however a peculiarity where if we have more than one subnet behind our spoke unit, the following setting must be used to ensure multiple Phase2 SAs are negotiated for each subnet listed in our group:

```

config vpn ipsec phase1-interface
edit <name>
set mesh-selector-type subnet
end
end

```

- **Routing:** This won't necessarily be different between the different spoke FortiGates, but as previously mentioned, in this example recipe we have configured our default routing to flow through the primary hub and failover routing to the backup hub. Notice that we are explicitly routing each hub's public IP through the public Internet to ensure that traffic will not flow through the VPN tunnel (and result in flapping).

Results

And this concludes our VPN configuration! But this recipe would not be complete without a very important verification step. Let's look at the routing table on the **hub**:

```

HUB # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
S*      0.0.0.0/0 [10/0] via 192.168.56.2, port1
S       100.64.254.12/32 [15/0] is directly connected, HUB_0S
100.64.254.13/24 [15/0] is directly connected, HUB_1
C       192.168.11.0/24 is directly connected, port2
S       192.168.12.0/24 [15/0] is directly connected, HUB_0S
192.168.13.0/24 [15/0] is directly connected, HUB_1
C       192.168.56.0/24 is directly connected, port1

```

As can be seen above, our spoke subnets have been automatically injected into the hub's routing tables. A closer look at the VPN details of one spoke confirms that the hub received the negotiated subnets during quick mode negotiation and inserted distinct SAs for each SA.

```

FGT1 # get vpn ipsec tunnel details
gateway
name: 'HUB_0'
type: route-based
local-gateway: 192.168.56.11:0 (static)
remote-gateway: 192.168.56.12:0 (dynamic)
mode: ike-v1
interface: 'port1' (2)
rx packets: 56 bytes: 8736 errors: 0
tx packets: 41 bytes: 3444 errors: 0
dpd: enabled/negotiated idle: 5000ms retry: 3 count: 0
selectors
name: 'HUB-P2'
auto-negotiate: disable
mode: tunnel

```

```

src: 0:0.0.0.0-255.255.255.255:0
dst: 0:192.168.12.0-192.168.12.255:0
-----OUTPUT TRUNCATED-----
selectors
name: 'HUB-P2'
auto-negotiate: disable
mode: tunnel
src: 0:0.0.0.0-255.255.255.255:0
dst: 0:100.64.254.12-100.64.254.12:0
-----OUTPUT TRUNCATED-----

```

If you require communication between the spokes, this can be routed through the hub FortiGates. The only change to the example recipe's configuration is an addition policy on each of the hub FortiGates which defines the both the Incoming Interface and the Outgoing Interface as the VPN Dialup Interface (in this example, SPOKES)

On the Spoke FortiGates, once the poke tunnels have been established, you can see the default route to the primary datacenter and the alternate though less preferred route to the backup datacenter by running the command `get router info routing-table all`

```

FGT-SPOKE-1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
S* 0.0.0.0/0 [10/0] is directly connected, HUB-PRIMARY [10/0] is
directly connected, HUB-BACKUP, [20/0]
S 100.64.10.2/32 [10/0] is directly connected, port1
S 100.64.11.2/32 [10/0] is directly connected, port1
C 100.64.12.0/24 is directly connected, port1
C 100.64.254.12/32 is directly connected, lo0
C 192.168.12.0/24 is directly connected, port2

```

We can test the failover function by shutting down the port1 interface on the primary hub. This will bring down the VPN between the primary hub and the spokes. Once the DPD detects the fault, traffic switches over to the backup hub as shown here:

```

FGT-SPOKE-1 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
S* 0.0.0.0/0 [10/0] is directly connected, HUB-BACKUP, [20/0]
S 100.64.10.2/32 [10/0] is directly connected, port1
S 100.64.11.2/32 [10/0] is directly connected, port1
C 100.64.12.0/24 is directly connected, port1
C 100.64.254.12/32 is directly connected, lo0
C 192.168.12.0/24 is directly connected, port2

```


Final notes

- The technique shown here does not involve dynamic routing so this configuration and its very straight forward template can be easily used to scale up the topology to include thousands of spoke sites.
- To make it even easier, this configuration can be entirely built and automated with FortiManager, which has support for provisioning hub-and-spoke dialup topologies.

Glossary

- BGP:** Border Gateway Protocol is primarily used to connect the networks of large organizations that have two or more ISP connections, or between other autonomous systems. If used in such a situation, a FortiGate can use BGP for routing.
- BYOD:** Bring Your Own Device (also called device management) is the practice of allowing network users to access an organization's (usually wireless) network with their own computers, smart phones, tablets and other devices. BYOD has a major impact on networks with large and diverse user bases, such as educational institutions, but also affects large and small business networks.
- CA:** A certificate authority (CA) is an entity that issues digital certificates, which are used to establish secure connections over a network, typically the Internet. The CA acts as a trusted third-party by verifying the identity of a certificate's owner: for example, the certificate found when you go to <https://www.facebook.com> is verified as belonging to Facebook.
- Certificates:** In networking, certificates (including public key certificates, digital certificates, and identity certificates) provide digital signatures for websites or other electronic communication and allow you to verify whether a digital identity is legitimate.. A FortiGate can use certificates for many things, including SSL inspection and user authentication.
- CLI:** The Command Line Interface is a text-based interface used to configure a FortiGate unit. Most steps in the FortiGate Cookbook use the Graphical User Interface (see GUI), but some configuration options are only available using the CLI.
- DHCP:** Dynamic Host Configuration Protocol is a networking protocol that allows devices to request network parameters, such as IP addresses, automatically from a DHCP server, reducing the need to assign these settings manually. A FortiGate can function as a DHCP server for your network and can also receive its own network parameters from an external DHCP server.
- Dial-up/dynamic VPN:** A dial-up VPN, also called a dynamic VPN, is a type of IPsec VPN where one of the endpoints has a dynamic IP address.
- DMZ:** A Demilitarized Zone is an interface on a FortiGate unit that provides external users with secure access to a protected subnet on the internal network without giving them access to other parts of the network. This is most commonly done for subnets containing web servers, which must be accessible from the Internet. The DMZ interface will only allow traffic that has been explicitly allowed in the FortiGate's configuration. FortiGate models that do not have a DMZ interface can use other interfaces for this purpose.
- DNS:** Domain Name System is used by devices connecting to the Internet to locate websites by mapping a domain name to a website's IP address. For example, a DNS server maps the domain name www.fortinet.com to the IP address 66.171.121.34. Your FortiGate unit controls which DNS servers the network uses. A FortiGate can also function as a DNS server.
- DSR:** In a typical load balancing scenario, server responses to client requests are routed through a load balancer on their way back to the client. The load balancer examines the headers of each response and can insert a cookie before sending the server response on to the client. In a Direct Server Return (DSR) configuration, the server receiving a client request responds directly to the client IP, bypassing the load balancer. Because the load balancer only processes incoming requests, load balancing performance is dramatically improved when using

DSR in high bandwidth applications. In such applications, it is not necessary for the load balancer to receive and examine the server's responses. So the client makes a request and the server simply streams a large amount of data to the client.

Dynamic IP address:

A dynamic IP address is one that can change without the device's user having to do anything. Dynamic IP addresses allow networks to control the IP addresses of devices that connect to them. This allows you to connect portable devices to different networks without needing to manually change their IP addresses.

Dynamic IP addresses are set by network protocols, most often DHCP.

ECMP:

Equal Cost Multipath Routing allows next-hop packet forwarding to a single destination to occur over multiple best paths that have the same value in routing metric calculations. ECMP is used by a FortiGate for a variety of purposes, including load balancing.

Explicit Proxy:

Explicit proxy is a type of configuration where all clients are configured to allow requests to go through a proxy server, which is a server used as an intermediary for requests from clients seeking resources from other servers. When a FortiGate uses explicit proxy, the clients sending traffic are given the IP address and port number of the proxy server.

FortiAP:

A FortiAP unit is a wireless Access Point that can be managed by a FortiGate. Most FortiAP functions can also be accomplished using a FortiWiFi unit.

FortiClient:

The FortiClient software provides a variety of features, including antivirus, web filtering, firewall, and parental controls, to individual computers and mobile devices. It can also be used to connect to a FortiGate using either an SSL or IPsec VPN.

FortiClient is available for Windows, Mac OSX, iOS, and Android, and can be set up quickly. After being installed, it automatically updates its virus definition files, does a full system scan once per week, and much more.

FortiClient can be downloaded at www.forticlient.com.

FortiOS:

FortiOS is the operating system used by FortiGate and FortiWiFi units. It is also referred to as firmware.

FTP:

File Transfer Protocol is a standard protocol used to transfer computer files from one host to another host over a computer network, usually the Internet, using FTP client and server applications.

Gateway:

A gateway is the IP address that traffic is sent to if it needs to reach resources that are not located on the local subnet. In most FortiGate configurations, a default route using a gateway provided by an Internet service provider must be set to allow Internet traffic.

GUI:

The Graphical User Interface, also known as the web-based manager, is a graphics-based interface used to configure a FortiGate unit and is an alternative to using the Command Line Interface (see CLI). You can connect to the GUI using either a web browser or FortiExplorer. Most steps in the FortiGate Cookbook use the GUI.

HTTP:

Hypertext Transfer Protocol is a protocol used for unencrypted communication over computer networks, including the Internet, where it is used to access websites. FortiGate units handle more HTTP traffic than any other protocol.

HTTPS:

Hypertext Transfer Protocol Secure is a protocol that secures HTTP communications using the Secure Sockets Layer (SSL) protocol. HTTPS is the most commonly used secure communication protocol on the Internet.

- Interfaces:** Interfaces are the points at which communication between two different environments takes place. These points can be physical, like the Ethernet ports on a FortiGate, or logical, like a VPN portal.
- IP address:** An Internet Protocol address is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication. FortiGate units can use IP addresses to filter traffic and determine whether to allow or deny traffic. Both IP version 4 and IP version 6 (see IPv4 and IPv6) are supported by your FortiGate.
- IPsec:** Internet Protocol Security is used 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 achieved by the use of gateways.
- Subnet Mask:** A subnet mask is the part of an IP address that is used to determine if two addresses are on the same subnet by allowing any network enabled device, such as a FortiGate, to separate the network address and the host address. This lets the device determine if the traffic needs to be sent through a gateway to an external network or if it is being sent to host on the local network.
- URL:** A Uniform Resource Locator is a text string that refers to a network resource. The most common use for URLs is on the Internet, where they are also known as web addresses.
- URLs are used by a FortiGate to locate websites on the Internet and can also be used in web filtering to block specific sites from being accessed.
- VDOM:** Virtual Domains are used to divide a single FortiGate unit into two or more virtual instances of FortiOS that function separately and can be managed independently.
- VLAN:** Virtual Local Area Networks are used to logically divide a single local area network (LAN) into different parts that function independently. A FortiGate uses VLANs to provide different levels of access to users connecting to the same LAN.
- VoIP:** Voice over Internet Protocol is a protocol that is used to allow voice communications and multimedia sessions

over Internet Protocol sessions, including the Internet. VoIP protocol is used by a FortiGate when traffic needs to reach a connected VoIP phone or FortiVoice unit.

VPN:

A Virtual Private Network is a private network that acts as a virtual tunnel across a public network, typically the Internet, and allows remote users to access resources on a private network. There are two main types of VPNs that can be configured using a FortiGate unit: IPsec VPN (see IPsec) and SSL VPN (see SSL).

WAN/WAN 1:

The WAN or WAN1 port on your FortiGate unit is the interface that is most commonly used to connect the FortiGate to a Wide Area Network, typically the Internet. Some FortiGate models have a WAN2 port, which is commonly used for redundant Internet connections.



The FortiGate Cookbook contains a variety of step-by-step examples of how to integrate a FortiGate unit into your network and apply features such as security profiles, wireless networking, and VPN.

Using the FortiGate Cookbook, you can go from idea to execution in simple steps, configuring a secure network for better productivity with reduced risk.

Written for FortiOS 5.2