FortiGate Security
Lab Guide

for FortiOS 7.2

FORTINET
Training Institute

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

FORTINET

8/30/2022

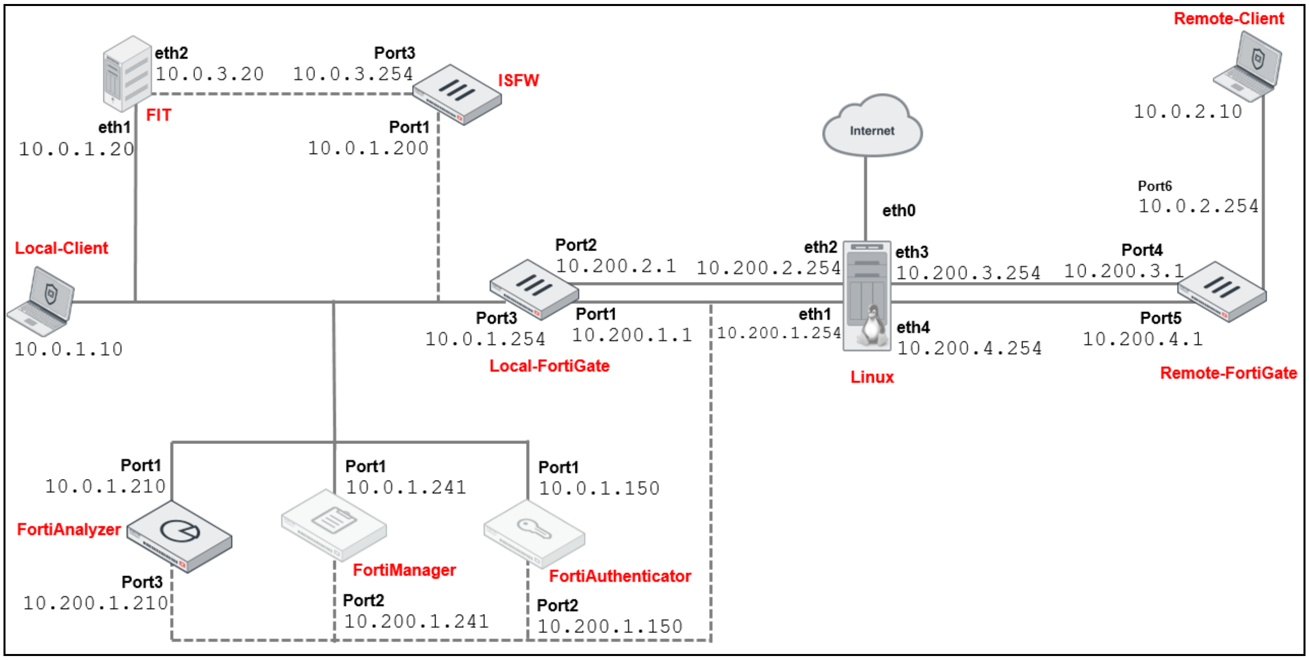
TABLE OF CONTENTS

Change Log

This table includes updates to the *FortiGate Security 7.2 Lab Guide* dated 6/13/2022 to the updated document version dated 8/30/2022.

Change	Location
Updated SSL inspection on Inbound traffic	Lab 6 exercise 2
Various formatting fixes	Entire guide
Fixed step based on latest Firefox version	Lab 6 exercise 1 and 2

Network Topology



Lab 1: FortiGate Introduction

In this lab, you will learn about FortiGate administration through the CLI and GUI. You will also back up and restore a configuration file, as well as create a new administrator account and modify administrator access permissions.

Objectives

- Access the FortiGate CLI
- Back up and restore configuration files
- Locate the FortiGate model and FortiOS firmware build in a configuration file
- Create a new administrator user
- Restrict administrator access

Time to Complete

Estimated: 25 minutes

VM Usernames and Passwords

VM	Username	Password
Local-Client	Administrator	password
Remote-Client	Administrator	password
Local-FortiGate	admin	password
Remote-FortiGate	admin	password
ISFW	admin	password
FortiAnalyzer	admin	password

Exercise 1: Working With the CLI

In this exercise, you will access a FortiGate using the CLI.

Explore the CLI

You will become familiar with the FortiGate CLI.

To explore the CLI

1. Go to the Local-FortiGate CLI.
2. At the login prompt, type `admin`.
3. In the **Password** field, type `password`, and then press `Enter`.
4. Enter the following command:

```
get system status
```

This command displays basic status information about FortiGate. The output includes the FortiGate device serial number, operation mode, and so on. When the `More` prompt appears on the CLI, perform one of the following actions:

Action	Command
To continue scrolling	Press the space bar.
To scroll one line at a time	Press `Enter`.
To exit	Type `q`.

5. Enter the following command:

```
get ?
```

The `?` character is not displayed on the screen.

This command shows all options that the CLI will accept after the `# get` command. Depending on the command, you may need to enter additional words to completely specify a configuration option.

6. Press the up arrow key.

   This displays the previous `get system status` command.

7. Try some of the control key sequences shown in the following table:

Action	Command
Previous command	Up arrow
Next command	Down arrow
Beginning of line	`Ctrl` + `a`
End of line	`Ctrl` + `e`
Back one word	`Ctrl` + `b`
Forward one word	`Ctrl` + `f`
Delete current character	`Ctrl` + `d`
Clear screen	`Ctrl` + `l`
Abort command and exit	`Ctrl` + `c`
Auto repeat history	`Ctrl` + `p`

8. Enter the following command:

   ```
   execute ?
   ```

   This command lists all options that the CLI accepts after the `execute` command.

9. Type `exe`, and then press the `Tab` key.

   Notice that the CLI completes the current word.

10. Press the space bar, and then press the `Tab` key three times.

    Each time you press the `Tab` key, the CLI replaces the second word with the next possible option for the `execute` command, in alphabetical order.

You can abbreviate most commands. In lessons and labs, many of the commands that you see are in abbreviated form. For example, instead of typing `execute`, you can type `exe`.

Use this technique to reduce the number of keystrokes that are required to enter a command. Often, experts can configure FortiGate faster using the CLI than using the GUI.

If there are other commands that start with the same characters, your abbreviation must be long enough to be specific, so that FortiGate can distinguish them. Otherwise, the CLI displays an error message about ambiguous commands.

11. On a new line, enter the following command to view the port3 interface configuration (hint: try using the shortcuts you just learned about):

    ```
    show system interface port3
    ```

12. Enter the following command:

    ```
    show full-configuration system interface port3
    ```

Stop and think!

Compare both outputs. How are they different?

The `show full-configuration` command displays all the configuration settings for the interface. The `show` command displays only those values that are different from the default values.

Exercise 2: Generating Configuration Backups

In this exercise, you will learn how to generate and restore cleartext and encrypted configuration backups. The configuration files that backups produce enable you to restore FortiGate to an earlier configuration.

Restore a Configuration From a Backup

You will restore a configuration from a backup.

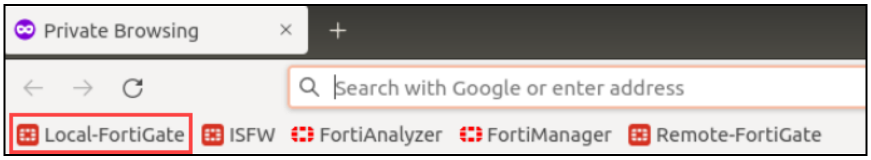
To restore a configuration from a backup

1. Log in to the Local-Client VM with the username `Administrator` and password `password`.

> The first time that you log in, you may need to click and drag the screen from the bottom to bring up the login prompt.

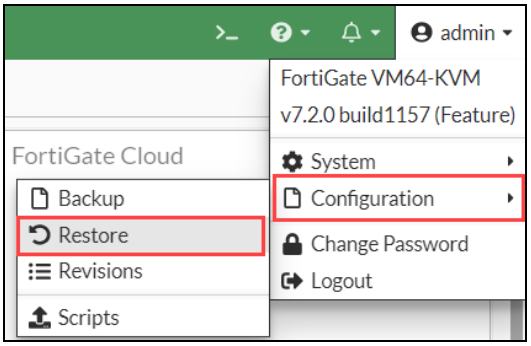
2. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.

> You can also access the Local-FortiGate GUI from the bookmarks bar in the Mozilla Firefox browser.

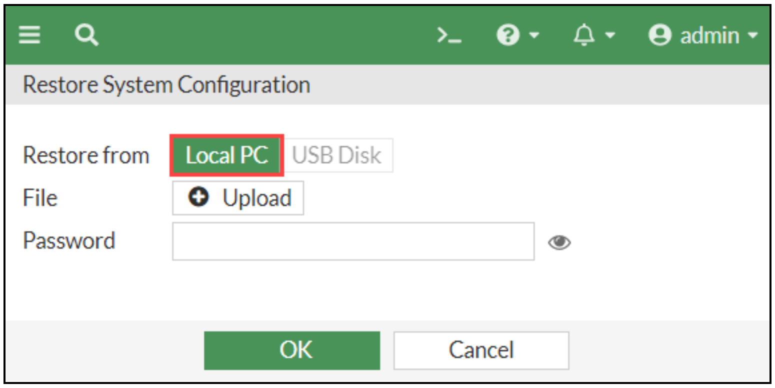


> All lab exercises were tested running Firefox on the Local-Client and Remote-Client VMs. To get consistent results, you should use Firefox to access both the internet and the FortiGate GUIs in this virtual environment.

3. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



4. Click **Upload** to select the backup configuration file from your local PC.



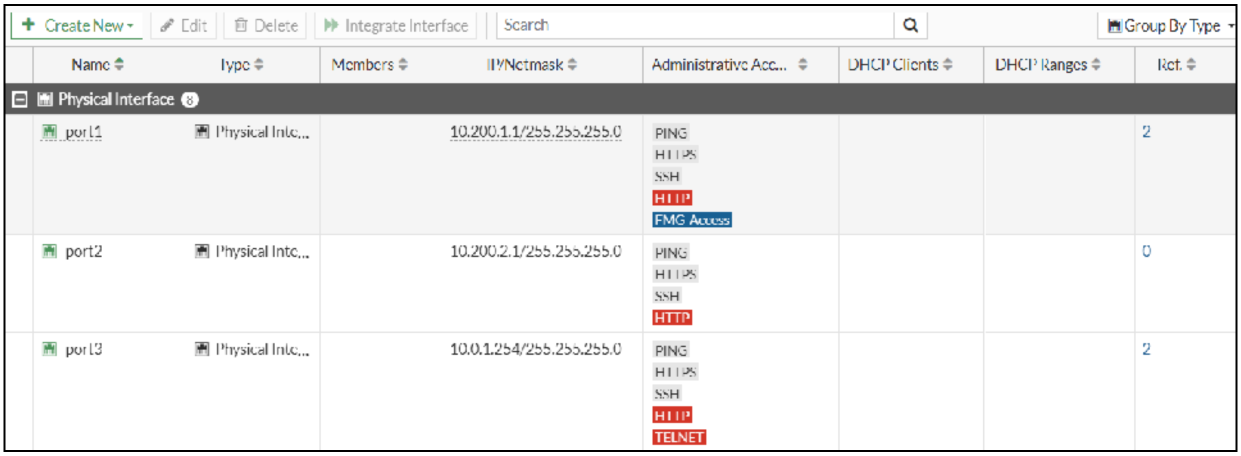
Restore System Configuration

Restore from	[✓ Local PC] USB Disk
File	Upload
Password	

5. Click **Desktop** > **Resources** > **FortiGate-Security** > **Introduction** > `local-initial.conf`, and then click **Open**.
6. Click **OK**.
7. Click **OK** to reboot.

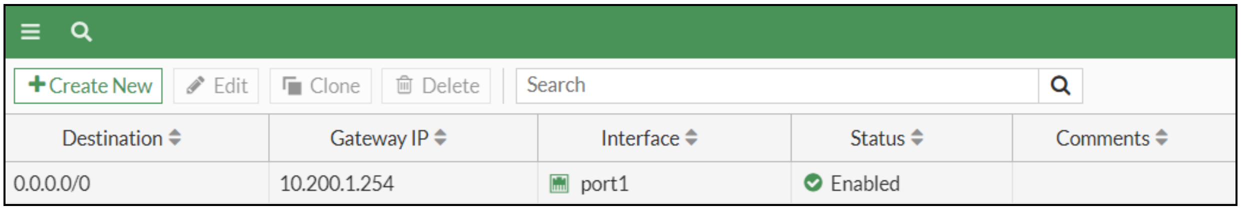
   After your browser uploads the configuration, FortiGate reboots automatically. This takes approximately 30–45 seconds.

8. When the Local-FortiGate GUI login page reappears after reboot, log in with the username `admin` and password `password`.
9. Click **Network** > **Interfaces**, and then verify that the network interface settings were restored.



Name	Type	Members	IP/Netmask	Administrative Acc...	DHCP Clients	DHCP Ranges	Ref.
Physical Interface 8							
port1	Physical Inte...		10.200.1.1/255.255.255.0	PING HTTPS SSH HTTP FMG Access			2
port2	Physical Inte...		10.200.2.1/255.255.255.0	PING HTTPS SSH HTTP			0
port3	Physical Inte...		10.0.1.254/255.255.255.0	PING HTTPS SSH HTTP TELNET			2

10. Click **Network** > **Static Routes**, click the **+** sign to expand the IPv4 routes, and then verify that the default route was restored.



Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	10.200.1.254	port1	✓ Enabled	

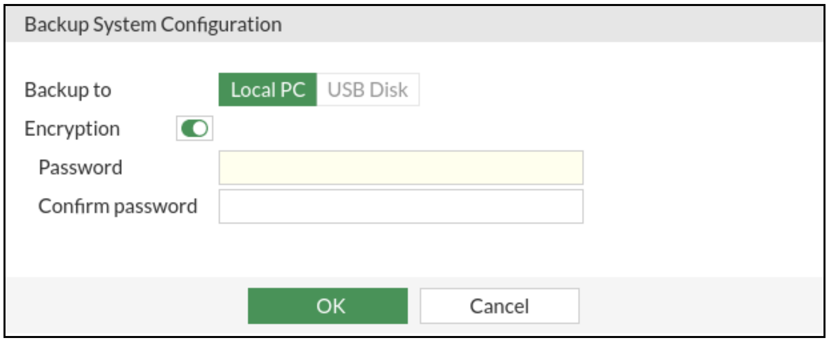
Back Up and Encrypt a Configuration File

Always back up the configuration before making changes to FortiGate (even if the change seems minor or unimportant). There is no *undo*. You should carefully consider the pros and cons of an encrypted backup before you begin encrypting backups. While your configuration, including things like private keys, remains private, an encrypted file hampers troubleshooting because Fortinet Support cannot read the file. Consider saving backups in plaintext, and storing them in a secure place instead.

You will create an encrypted file with the backup of the FortiGate current configuration.

To save an encrypted configuration backup

1. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.
2. On the Local-FortiGate GUI, in the upper-right corner, click **admin**, and then click **Configuration** > **Backup**.
3. On the **Backup System Configuration** page, enable **Encryption**.
4. In the **Password** and **Confirm password** fields, type `fortinet`.


Backup System Configuration

Backup to: Local PC | USB Disk

Encryption: ●

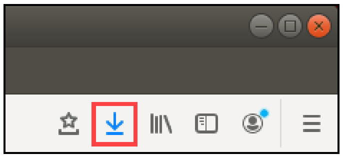
Password:

Confirm password:

5. Click **OK**.
6. Select **Save File**, and then click **Cancel**.

   The Firefox browser saves the encrypted configuration file in the **Downloads** folder, by default. Ensure that you record the password and store it in a secure place.

You can access downloaded files by clicking the blue down arrow in the upper-right corner of the browser.



Restore an Encrypted Configuration Backup

Restoring from a backup enables you to return FortiGate to a previous configuration. As a word of caution, if you cannot recall the password required to decrypt an encrypted backup, you will not be able to restore FortiGate to the backup. Ensure that you record the password and store it in a secure place.

You will restore the configuration backup that you created in the previous procedure.

Take the Expert Challenge!

Restore the configuration from the encrypted backup.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Compare the Headers of Two Configuration Files on page 16.

To restore an encrypted configuration backup

1. On the Local-FortiGate GUI, in the upper-right corner, click **admin**, and then click **Configuration** > **Restore**.
2. On the **Restore System Configuration** page, click **Upload**.
3. Browse to your **Downloads** folder, and then select the configuration file that you created in the previous procedure.
4. In the **Password** field, type `fortinet`, and then click **OK**.
5. Click **OK** to confirm that you want to restore the configuration.

   FortiGate reboots.

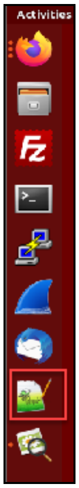
Compare the Headers of Two Configuration Files

When you troubleshoot issues, or when you restore FortiGate to an earlier OS version or build, it is useful to know where to find the version and build number in a configuration file. This task shows you where to find this information.

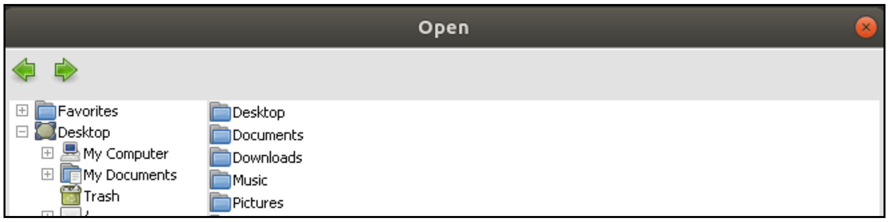
You will open and compare two configuration files using Notepad++.

To compare the headers of two configuration files

1. On the Local-Client VM, click the Notepad++ icon.



2. Click **File** > **Open**, and then browse to the **Downloads** folder to open the encrypted configuration file.

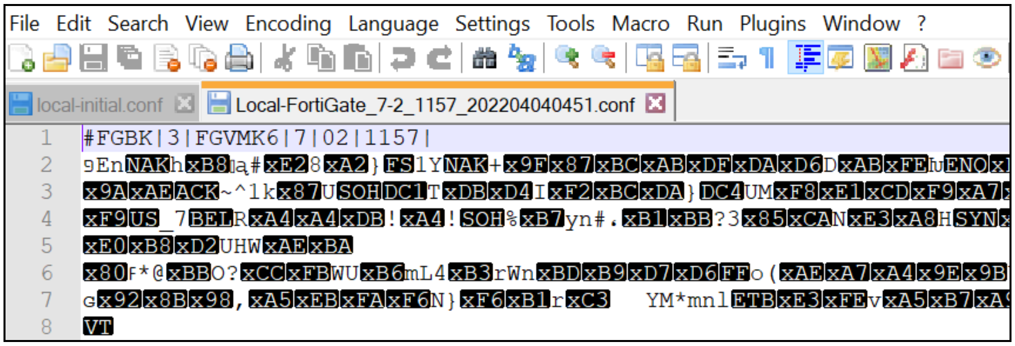


3. Click **File** > **Open**, and then browse to the initial configuration file:
   `Desktop\Resources\FortiGate-Security\Introduction\local-initial.conf`

   The configuration file opens in a second tab in Notepad++.

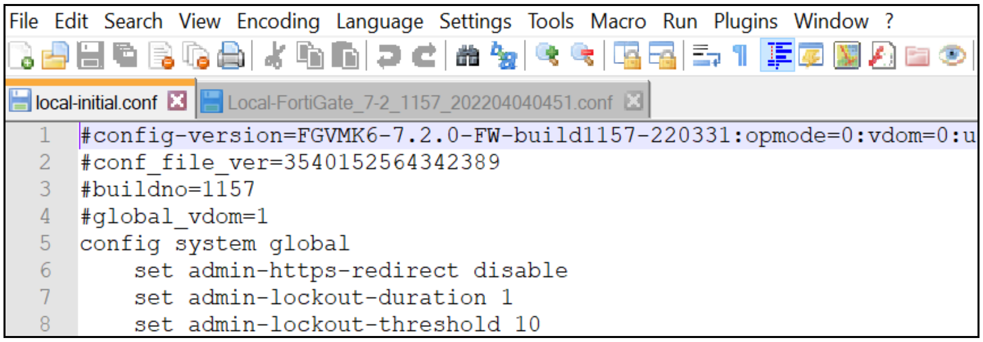
4. Compare the headers in the two files.

   The following example is an encrypted file:


File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
local-initial.conf
Local-FortiGate_7-2_1157_202204040451.conf

```
#FGBK|3|FGVMK6|7|02|1157|
9EnNAKhxB8ąą#xE28xA2}FS1YNAK+x9Fx87xBCxABxDFxDAxD6DxABxFEuENOx
x9AxAEACK~^1kx87USOHDC1TxDBxD4IxF2xBCxDA}DC4UMxF8xE1xCDxF9xA7x
xF9US_7BELRxA4xA4xDB!xA4!SOH%xB7yn#.xB1xBB?3x85xCANxE3xA8HSYNx
xE0xB8xD2UHWxAExBA
x80F*@xBBO?xCCxFBWUxB6mL4xB3rWnxBDxB9xD7xD6FFo(xAExA7xA4x9Ex9B
Gx92x8Bx98,xA5xEBxFAxF6N}xF6xB1rxC3    YM*mnlETBxE3xFEvxA5xB7xA
VT
```

   The following example is a cleartext file:


File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
local-initial.conf
Local-FortiGate_7-2_1157_202204040451.conf

```
#config-version=FGVMK6-7.2.0-FW-build1157-220331:opmode=0:vdom=0:u
#conf_file_ver=3540152564342389
#buildno=1157
#global_vdom=1
config system global
    set admin-https-redirect disable
    set admin-lockout-duration 1
    set admin-lockout-threshold 10
```

In both the cleartext and encrypted configuration files, the top line acts as a header, and lists the firmware and model that this configuration belongs to.

5. Close the two tabs in Notepad++, and then close the application.

Exercise 3: Configuring Administrator Accounts

FortiGate offers many options for configuring administrator privileges. For example, you can specify the IP addresses that administrators are allowed to connect from.

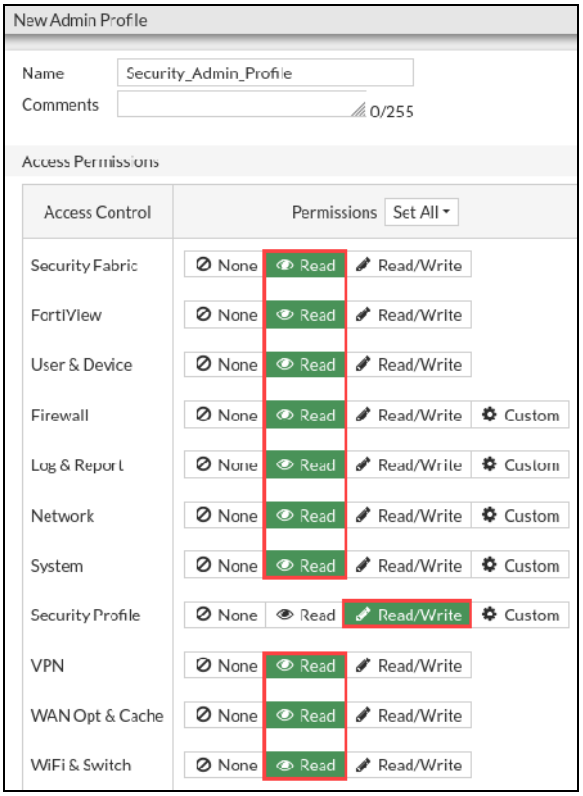
In this exercise, you will work with administrator profiles and administrator user accounts. An administrator profile is a role that is assigned to an administrator user that defines what the user is permitted to do on the FortiGate GUI and CLI.

Configure a User Administrator Profile

You will create a new user administrator profile that has read-only access for most of the configuration settings.

To configure a user administrator profile

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **System** > **Admin Profiles**.
3. Click **Create New**.
4. In the **Name** field, type `Security_Admin_Profile`.
5. In the permissions table, set **Security Profile** to **Read/Write**, and then set all other permissions to **Read**.



New Admin Profile

Name: Security_Admin_Profile

Comments: 0/255

Access Permissions

Access Control	Permissions Set All
Security Fabric	None [✓ Read] Read/Write
FortiView	None [✓ Read] Read/Write
User & Device	None [✓ Read] Read/Write
Firewall	None [✓ Read] Read/Write Custom
Log & Report	None [✓ Read] Read/Write Custom
Network	None [✓ Read] Read/Write Custom
System	None [✓ Read] Read/Write Custom
Security Profile	None Read [✓ Read/Write] Custom
VPN	None [✓ Read] Read/Write
WAN Opt & Cache	None [✓ Read] Read/Write
WiFi & Switch	None [✓ Read] Read/Write

6. Click **OK** to save the changes.

Create an Administrator Account

You will create a new administrator account. You will assign the account to the administrator profile you created in the previous procedure. The administrator will have read-only access to most of the configuration settings.

To create an administrator account

1. On the Local-FortiGate GUI, click **System** > **Administrators**.
2. Click **Create New**, and then click **Administrator** to add a new administrator account.
3. On the **New Administrator** page, configure the following settings:

Field	Value
Username	Security
Type	Local User
Password	fortinet
Confirm Password	fortinet
Administrator Profile	Security_Admin_Profile

Administrator names and passwords are case sensitive. You can't include characters, such as `< > ( ) # "`, in an administrator account name

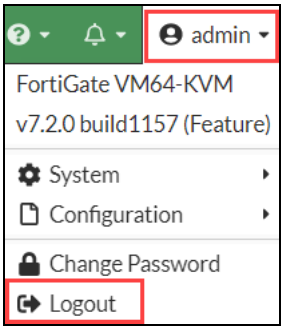
4. Click **OK** to save the changes.

Test the New Administrator Account

You will confirm that the new administrator account has read-write access to only the security profiles configuration.

To test the new administrator account

1. Continuing on the Local-FortiGate GUI, click **admin**, and then click **Logout** to log out of the **admin** account GUI session.



2. Log back in to the Local-FortiGate GUI with the username `Security` and password `fortinet`.
3. In the **FortiGate Setup** window, click **Later**.
4. Enable **Don't show again**, and then click **OK** to close the FortiOS introduction window.
5. Explore the permissions that are listed in the GUI.

   You should see that this account can configure only security profiles.

6. Log out of the GUI.

Restrict Administrator Access

You will restrict access for FortiGate administrators. Only administrators connecting from a trusted subnet are allowed access. This is useful if you must restrict the access points that administrators connect to FortiGate from.

To restrict administrator access

1. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI with the username `admin` and password `password`.
2. Click **System** > **Administrators**.
3. Edit the **Security** account.
4. Enable **Restrict login to trusted hosts**, and then set **Trusted Host 1** to the `10.200.3.0/24`address.
5. Click **OK** to save the changes.
6. Log out of the GUI.

Test the Restricted Access

You will verify that a **Security** administrator outside the `10.200.3.0/24` subnet can't access FortiGate.

To test the restricted access

1. On the Local-Client VM, log out of the Local-FortiGate GUI session as the **admin** user.
2. Try to log in to the `Security` account with the password `fortinet`.

   Authentication will fail.

3. Log in to the Remote-Client VM with the username `Administrator` and password `password`.
4. On the Remote-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.200.1.1` with the username `Security` and password `fortinet`.

What is the result this time?

Stop and think!

Why were you able to log in using the **admin** account and not the **Security** account from the Local-Client VM directly connecting to the Local-FortiGate GUI?

This is because **Trusted Host** is set on the **Security** administrator account but not on the **admin** account.

5. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
6. Enter the following CLI commands to add `10.0.1.0/24` as the second trusted IP subnet (**Trusted Host 2**) to the **Security** administrator account:

```
config system admin
   edit Security
      set trusthost2 10.0.1.0/24
end
```

7. Return to the Local-Client VM.
8. Open a browser, and then try to log in to the Local-FortiGate GUI at `10.0.1.254` with the username `Security` and password `fortinet`.

   You should be able to log in.

Lab 2: Firewall Policies

In this lab, you will configure firewall policies on Local-FortiGate, and then perform various tests on the Local-Client VM to confirm that traffic is matching the appropriate firewall policies based on the configuration.

Objectives

- Configure firewall objects and firewall policies
- Configure source and destination matching in firewall policies
- Apply service and schedule objects to a firewall policy
- Configure firewall policy logging options
- Reorder firewall policies
- Read and understand logs
- Use policy lookup to find a matching policy

Time to Complete

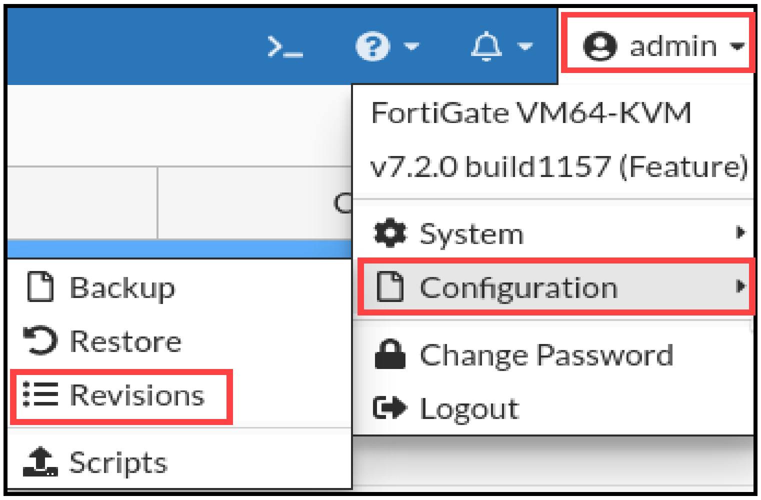
Estimated: 25 minutes

Prerequisites

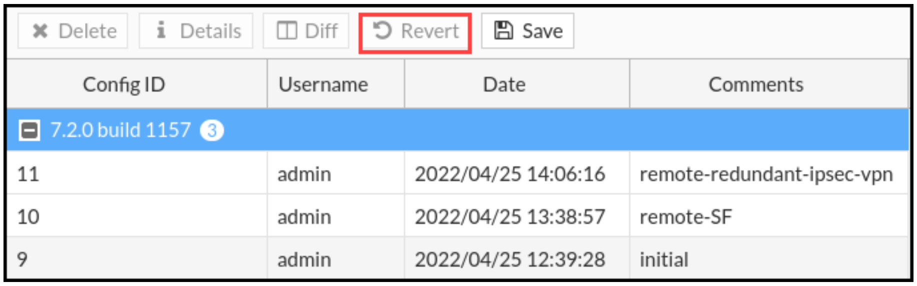
Before beginning this lab, you must restore configuration files to Remote-FortiGate, ISFW, and Local-FortiGate.

To restore the Remote-FortiGate configuration file

1. Connect to the Remote-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.

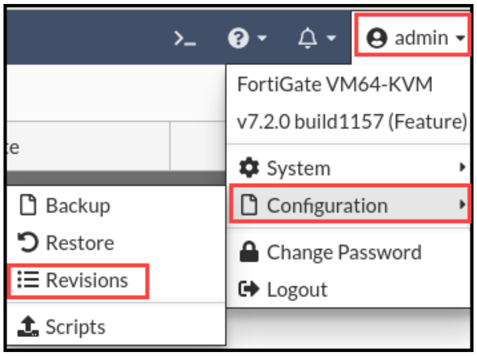


Config ID	Username	Date	Comments
7.2.0 build 1157 3			
11	admin	2022/04/25 14:06:16	remote-redundant-ipsec-vpn
10	admin	2022/04/25 13:38:57	remote-SF
9	admin	2022/04/25 12:39:28	initial

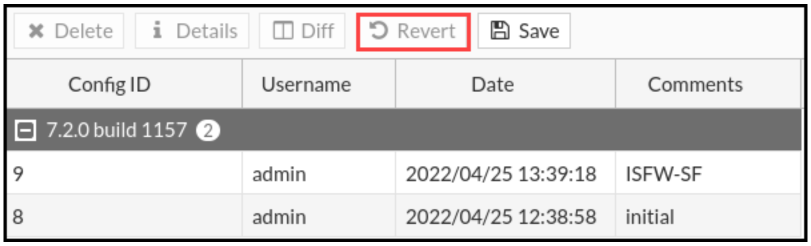
5. Click **OK** to reboot.

To restore the ISFW configuration file

1. Connect to the ISFW GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.

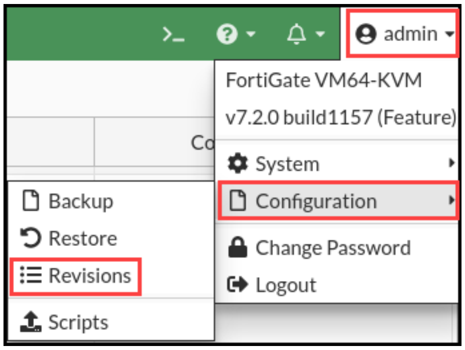


Config ID	Username	Date	Comments
7.2.0 build 1157 (2)			
9	admin	2022/04/25 13:39:18	ISFW-SF
8	admin	2022/04/25 12:38:58	initial

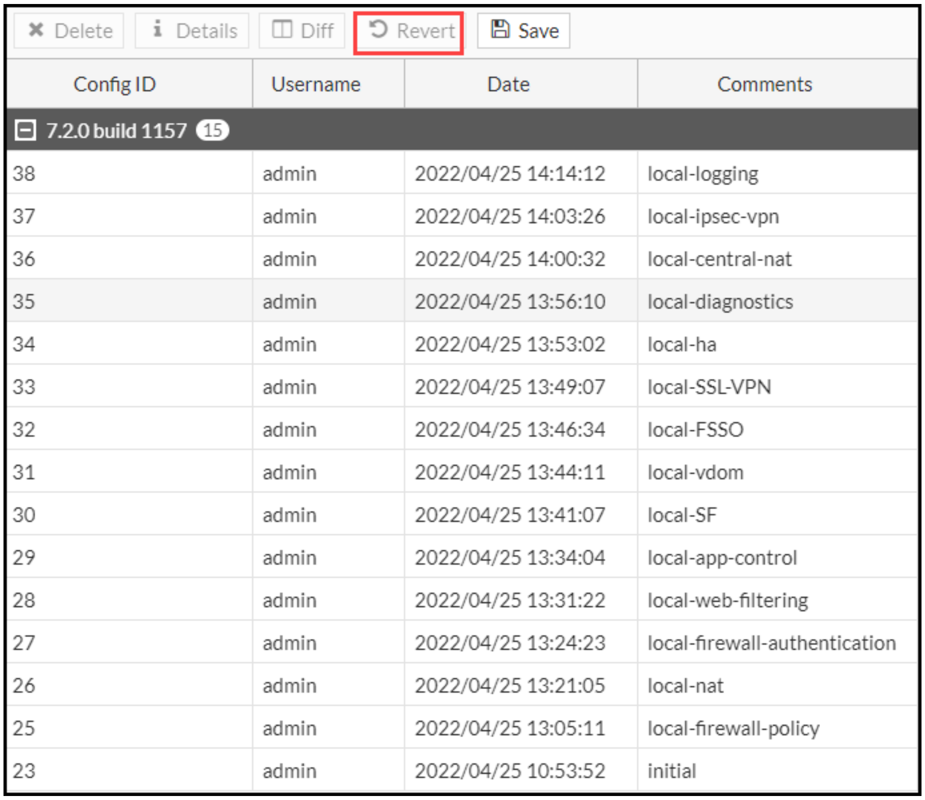
5. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **local-firewall-policy**, and then click **Revert**.



Config ID	Username	Date	Comments
7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

Exercise 1: Creating Firewall Address Objects and Firewall Policies

In this exercise, you will configure firewall address objects. You will also configure an IPv4 firewall policy that you will apply firewall address objects to, along with a schedule, services, and log options. Then, you will test the firewall policy by passing traffic through it and checking the logs for your traffic.

At its core, FortiGate is a firewall, so almost everything that it does to your traffic is related to your firewall policies.

Create Firewall Address Objects

By default, FortiGate has many preconfigured, well-known address objects in the factory default configuration. However, if those objects don't meet the needs of your organization, you can configure more.

To create a firewall address object

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Addresses**.
3. Click **Create New** > **Address**.
4. Configure the following settings:

Field	Value
Name	LOCAL_SUBNET
Type	Subnet
IP/Netmask	10.0.1.0/24
Interface	any

5. Click **OK**.

Create a Firewall Policy

First, you will disable the existing firewall policy. Then, you will create a more specific firewall policy using the firewall address object that you created in the previous procedure. You will also select specific services and configure log settings.

To disable an existing firewall policy

1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Right-click the **Full_Access** firewall policy, and then in the **Set Status** field, select **Disable**.

To create a firewall policy

1. Continuing in the **Policy & Objects** > **Firewall Policy** section, click **Create New** to add a new firewall policy.
2. Configure the following settings:

Field	Value
Name	Internet_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL_ICMP, HTTP, HTTPS, DNS, SSH **Tip**: Type the service name in the search box to quickly find it, and then click the service object to add it to the policy.
Action	ACCEPT
NAT	<enable>
Log Allowed Traffic	<enable> and select **All Sessions**
Generate Logs when Session Starts	<enable>
Enable this policy	<enable>

3. Leave all other settings at the default values, and then click **OK** to save the changes.

When you create firewall policies, remember that FortiGate is a stateful firewall. As a result, you need to create only one firewall policy that matches the direction of the traffic that initiates the session.

Test the Firewall Policy and View the Generated Logs

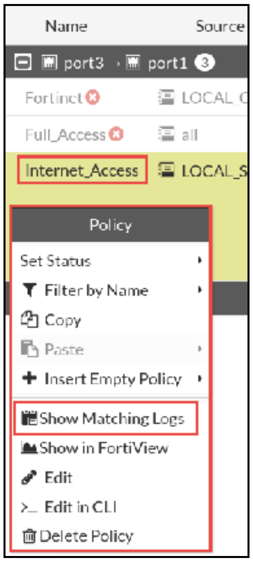
Now that you configured the firewall policy, you will test it by passing traffic through it and viewing the generated logs.

To test and view logs for a firewall policy

1. On the Local-Client VM, open several web browser tabs, and connect to several external websites, such as:

- www.google.com
- kb.fortinet.com
- docs.fortinet.com
- www.bbc.com

2. Return to the browser tab with the Local-FortiGate GUI, and then click **Policy & Objects** > **Firewall Policy**.
3. Right-click the **Internet_Access** policy, and then click **Show Matching Logs**.



4. Identify the log entries for your internet browsing traffic.

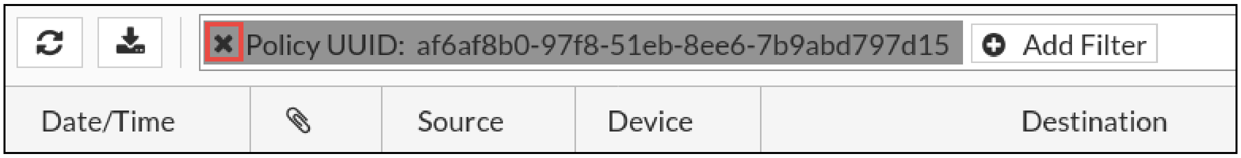
   With the current settings, you should have a few log messages that have **Accept: session start** in the **Result** column. These are the session start logs.

   When sessions close, there is a separate log entry for the amount of data that was sent and received.

Enabling **Generate Logs when Session Starts** in the firewall policy will generate twice the amount of log messages. You should use this option only when this level of detail is absolutely necessary.

When you click **Show Matching Logs** in the firewall policy, it adds the **Policy UUID** filter in the forward traffic logs.

5. In the **Forward Traffic** logs, click **X** to remove the **Policy UUID** filter.


Policy UUID: af6af8b0-97f8-51eb-8ee6-7b9abd797d15

When you remove the **Policy UUID** filter, the logs are displayed unfiltered. You will use the logs in upcoming labs.

Exercise 2: Reordering Firewall Policies and Firewall Policy Actions

In the applicable interface pair section, FortiGate looks for a matching policy, beginning at the top. Usually, you should put more specific policies at the top—otherwise, more general policies will match the traffic first, and more granular policies will never be applied.

In this exercise, you will create a new firewall policy with more specific settings, such as the source, destination, and service, and you will set the action to **DENY**. Then, you will move this firewall policy above the existing firewall policies and observe the behavior that reordering the firewall policies creates.

Create a Firewall Policy

You will create a new firewall policy to match a specific source, destination, and service, and you will set the action to **DENY**.

The firewall address LINUX_ETH1 with IP/netmask `10.200.1.254/32` is preconfigured for you, and you will use this address when you create the firewall policy.

Take the Expert Challenge!

Configure a firewall policy on the Local-FortiGate GUI using the following settings:

- Name the firewall policy **Block_Ping**.
- Use port3 as the incoming interface and port1 as the outgoing interface.
- Block all ping traffic from the `10.0.1.0/24` subnet destined for the `10.200.1.254` address. Use the preconfigured address objects **LOCAL_SUBNET** and **LINUX_ETH1**.
- Enable log violation traffic.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you have performed these steps, see Test the Reordering of a Firewall Policy on page 31.

To create a firewall policy

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Firewall Policy**, and then click **Create New**.
3. Configure the following settings:

Field	Value
Name	Block_Ping
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	LINUX_ETH1
Schedule	always
Service	PING **Tip**: Type the service name in the search box to quickly find it, and then click the service object to add it to the policy.
Action	DENY
Log Violation Traffic	<enable>
Enable this policy	<enable>

4. Click **OK** to save the changes.

Test the Reordering of a Firewall Policy

Now that your configuration is ready, you will test it by moving the **Block_Ping** firewall policy above the **Internet_Access** firewall policy. The objective is to confirm that, after you reorder the firewall policies, the following occurs:

- Traffic is matched to a more specific firewall policy.
- The policy ID remains the same.

To confirm traffic matches a more granular firewall policy after reordering the policies

1. On the Local-Client VM, open a terminal.
2. Ping the destination address (**LINUX_ETH1**) that you configured in the **Block_Ping** firewall policy.

```
ping 10.200.1.254
```

Stop and think!

Why are you still able to ping the destination address, even though you just configured a policy to block it?

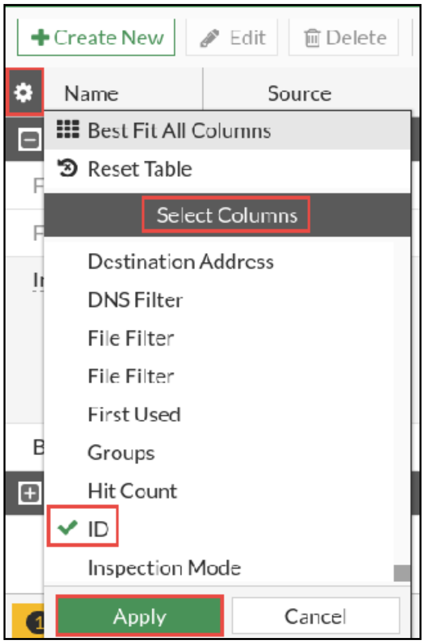
The ping should still work because it matches the **ACCEPT** policy and not the **DENY** policy that you created. The **Block_Ping** policy was never checked because the traffic matched the policy at the top (**Internet_Access**). This demonstrates the behavior that FortiGate looks for a matching policy, beginning at the top.

3. Leave the terminal window open and running.
4. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.

5. Hover over the **Name** column.

   A settings icon appears beside **Name**.

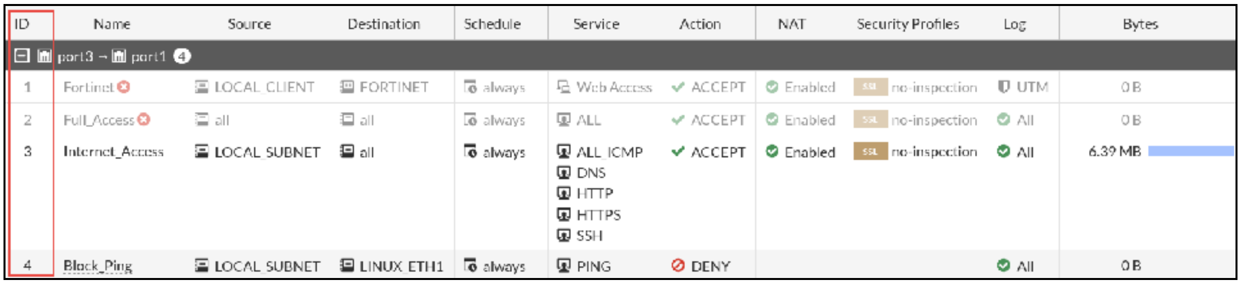
6. Click the settings icon, scroll down to the **Select Columns** section, select the **ID** column, and then click **Apply**.



   The **ID** column appears as the last column in the table.

7. Drag the **ID** column to the left of the **Name** column, so it becomes the first column in the table.

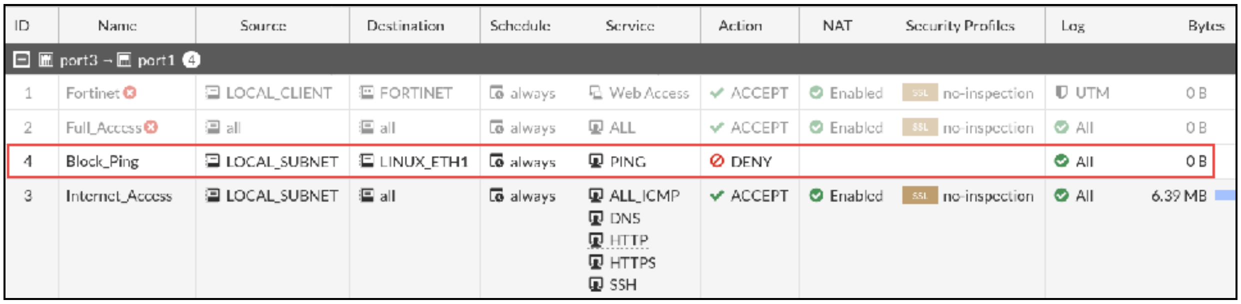
   Note the current **ID** values for both the **Internet_Access** and **Block_Ping** firewall policies.



ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
port3 → port1 4										
1	Fortinet	LOCAL_CLIENT	FORTINET	always	Web Access	✓ ACCEPT	Enabled	SSL no-inspection	UTM	0 B
2	Full_Access	all	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	All	0 B
3	Internet_Access	LOCAL_SUBNET	all	always	ALL_ICMP DNS HTTP HTTPS SSH	✓ ACCEPT	Enabled	SSL no-inspection	All	6.39 MB
4	Block_Ping	LOCAL_SUBNET	LINUX_ETH1	always	PING	DENY			All	0 B

8. In the **ID** column, drag the **Block_Ping** firewall policy up, and place it above the **Internet_Access** firewall policy.

   When you move the **Block_Ping** policy up, the **ID** value remains the same.



ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
port3 → port1 4										
1	Fortinet	LOCAL_CLIENT	FORTINET	always	Web Access	✓ ACCEPT	Enabled	SSL no-inspection	UTM	0 B
2	Full_Access	all	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	All	0 B
4	Block_Ping	LOCAL_SUBNET	LINUX_ETH1	always	PING	DENY			All	0 B
3	Internet_Access	LOCAL_SUBNET	all	always	ALL_ICMP DNS HTTP HTTPS SSH	✓ ACCEPT	Enabled	SSL no-inspection	All	6.39 MB

If the changes that you made are not displayed, refresh the page. Alternatively, you can log out of the FortiGate GUI, and then log back in.

9. On the Local-Client VM, review the terminal window that is running the continuous ping.

   You should see that the pings now fail.

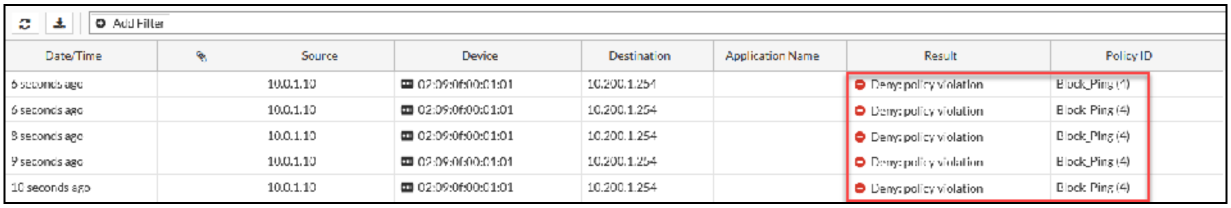
Stop and think!

Why are the pings failing?

This demonstrates the outcome of the policy reordering. After moving the more granular policy above the general access policy, the traffic is matched to the more granular policy and, based on the **DENY** action, the traffic stops being processed.

10. Close the terminal window.
11. On the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.

    You should see many policy violation logs reporting the blocked ping.



Date/Time		Source	Device	Destination	Application Name	Result	Policy ID
6 seconds ago		10.0.1.10	02:09:0f:00:01:01	10.200.1.254		Deny: policy violation	Block_Ping (4)
6 seconds ago		10.0.1.10	02:09:0f:00:01:01	10.200.1.254		Deny: policy violation	Block Ping (4)
8 seconds ago		10.0.1.10	02:09:0f:00:01:01	10.200.1.254		Deny: policy violation	Block_Ping (4)
9 seconds ago		10.0.1.10	02:09:0f:00:01:01	10.200.1.254		Deny: policy violation	Block_Ping (4)
10 seconds ago		10.0.1.10	02:09:0f:00:01:01	10.200.1.254		Deny: policy violation	Block Ping (4)

Clear the log filter that you applied in the previous exercise.

Exercise 3: Applying ISDB Objects as Destinations

FortiGate can match destination traffic using address objects or internet service database (ISDB) objects. ISDB objects are predefined entries that FortiGuard regularly updates and contain a database of IP addresses, protocols, and port numbers that the most common internet services use.

You can use ISDB objects to allow or deny traffic to well-known internet destinations, without having to configure the IP addresses, protocols, or ports that those destinations use in the firewall policy.

In this exercise, you will apply an ISDB object as the destination criteria in a firewall policy to block traffic to a well-known internet service.

Review the ISDB

You will review the entries in the ISDB.

To review the ISDB

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Internet Service Database**.
3. Expand the **Predefined Internet Services** and **IP Reputation Database** sections.
4. Double-click any entry, and then click **View/Edit Entries**.

   You can see the corresponding IP addresses, ports, and protocols that the internet service uses.
5. Click **Return**.

Configure a Firewall Policy Destination as an ISDB Object

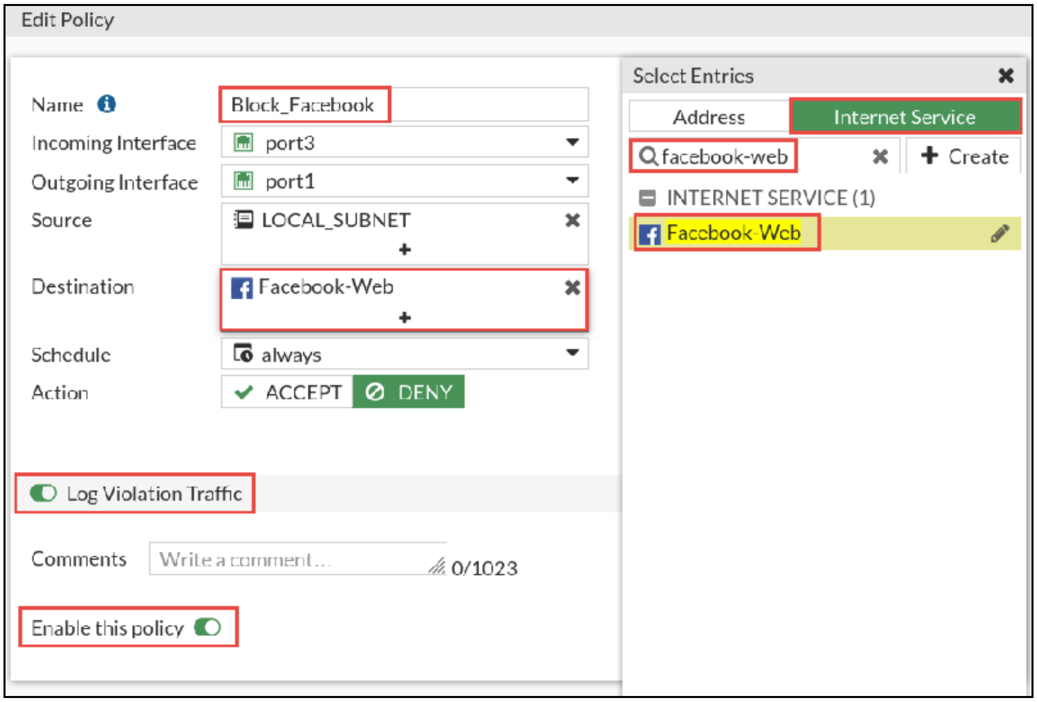
You will modify an existing firewall policy and use an ISDB object as a destination.

To configure an internet service as a destination

1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Right-click the **ID** column for the **Block_Ping** firewall policy, and then click **Edit.**
3. Change the **Name** to **Block_Facebook**.
4. Click **Destination**, and then in the right pane, click **LINUX_ETH1** to clear it.
5. Click **Internet Service**.
6. Select **Facebook-Web**.

Type the internet service object name in the search box to quickly find it, and then click the object to add it to the policy.

Your configuration should look like the following example:



Edit Policy

Name: Block_Facebook

Incoming Interface: port3

Outgoing Interface: port1

Source: LOCAL_SUBNET

Destination: Facebook-Web

Schedule: always

Action: ✓ ACCEPT [✓ DENY]

Log Violation Traffic

Comments: Write a comment... 0/1023

Enable this policy

Select Entries

Address | Internet Service

facebook-web

INTERNET SERVICE (1)

Facebook-Web

When **Internet Service** is selected as the **Destination**, you cannot:

- Use **Address** in the **Destination**
- Select **Service** in the firewall policy

7. Click **OK**.

Test the Internet Service Firewall Policy

Now that you configured the firewall policy, you will test it by passing traffic through it.

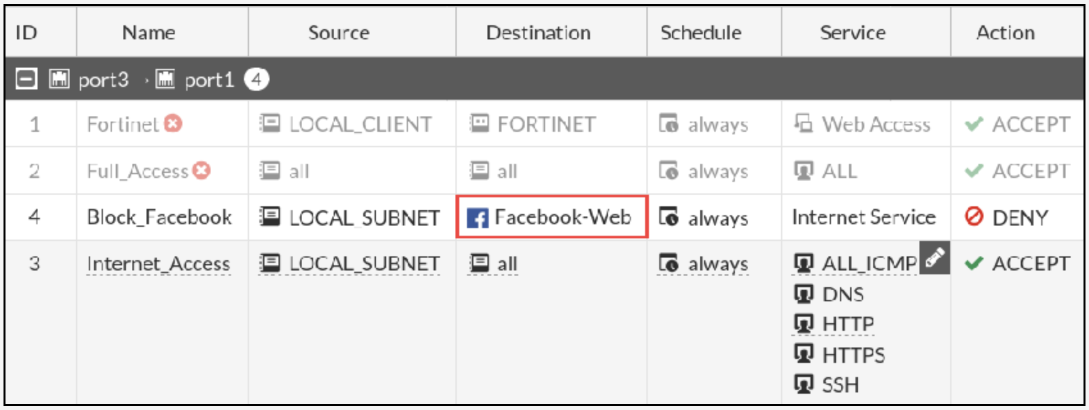
To test the internet service firewall policy

1. On the Local-Client VM, open a few browser tabs, and go to the following websites:
   - www.facebook.com
   - www.twitter.com

Stop and think!

Why is Facebook blocked but Twitter is allowed?

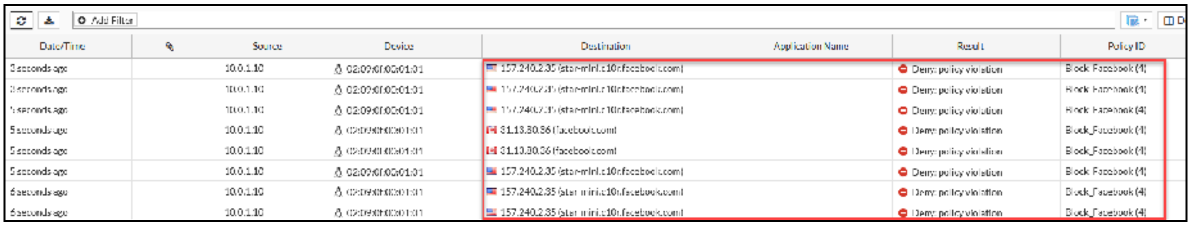
FortiGate checks for the matching policy from top to bottom. Facebook is blocked by the **ID 4** firewall policy because the destination is set to **Facebook-Web**. Twitter is allowed by the **ID 3** firewall policy, which allows internet access.



ID	Name	Source	Destination	Schedule	Service	Action
port3 › port1 4						
1	Fortinet	LOCAL_CLIENT	FORTINET	always	Web Access	✓ ACCEPT
2	Full_Access	all	all	always	ALL	✓ ACCEPT
4	Block_Facebook	LOCAL_SUBNET	Facebook-Web	always	Internet Service	DENY
3	Internet_Access	LOCAL_SUBNET	all	always	ALL_ICMP DNS HTTP HTTPS SSH	✓ ACCEPT

2. On the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.

   You should see many policy violation logs that the **Block_Facebook** policy reported.



Date/Time		Source	Device	Destination	Application Name	Result	Policy ID
3 seconds ago		10.0.1.10	02:09:0f:00:01:01	157.240.2.35 (star-mini.c10r.facebook.com)		Deny: policy violation	Block_Facebook (4)
3 seconds ago		10.0.1.10	02:09:0f:00:01:01	157.240.2.35 (star-mini.c10r.facebook.com)		Deny: policy violation	Block_Facebook (4)
4 seconds ago		10.0.1.10	02:09:0f:00:01:01	157.240.2.35 (star-mini.c10r.facebook.com)		Deny: policy violation	Block_Facebook (4)
5 seconds ago		10.0.1.10	02:09:0f:00:01:01	31.13.80.36 (facebook.com)		Deny: policy violation	Block_Facebook (4)
5 seconds ago		10.0.1.10	02:09:0f:00:01:01	31.13.80.36 (facebook.com)		Deny: policy violation	Block_Facebook (4)
5 seconds ago		10.0.1.10	02:09:0f:00:01:01	157.240.2.35 (star-mini.c10r.facebook.com)		Deny: policy violation	Block_Facebook (4)
6 seconds ago		10.0.1.10	02:09:0f:00:01:01	157.240.2.35 (star-mini.c10r.facebook.com)		Deny: policy violation	Block_Facebook (4)
6 seconds ago		10.0.1.10	02:09:0f:00:01:01	157.240.2.35 (star-mini.c10r.facebook.com)		Deny: policy violation	Block_Facebook (4)

3. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**, right-click the **Block_Facebook** firewall policy, select **Set Status**, and then click **Disable**.

Exercise 4: Using Policy Lookup

FortiGate can find a matching firewall policy based on the policy lookup input criteria. The policy lookup feature basically creates a packet flow over FortiGate without real traffic. From this packet flow, FortiGate can extract a policy ID and highlight it on the GUI policy configuration page.

In this exercise, you will use the policy lookup feature to find a matching firewall policy based on input criteria.

Enable Existing Firewall Policies

As required in the previous exercises, most of the configured firewall policies are currently disabled. Now, you will enable some of the existing firewall policies.

Take the Expert Challenge!

On the Local-FortiGate GUI, enable **Policy Status** for the **Fortinet** and **Full_Access** firewall policies.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you have performed these steps, see Set Up and Test the Policy Lookup Criteria on page 37.

To enable existing firewall policies

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Firewall Policy**.
3. Right-click the **Fortinet** firewall policy, select **Set Status**, and then click **Enable**.
4. Right-click the **Full_Access** firewall policy, select **Set Status**, and then click **Enable**.

Set Up and Test the Policy Lookup Criteria

You will set up the policy lookup criteria. FortiGate searches and highlights the matching firewall policy based on your input criteria.

To set up and test the policy lookup criteria

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**, and then click **Policy Lookup**.
2. Configure the following settings:

Field	Value
Source Interface	port3

Field	Value
Protocol	TCP
Source	10.0.1.100
Source Port	<leave this field empty>
Destination	fortinet.com
Destination Port	443

3. Click **Search**.

   The search matches the **Full_Access** policy, but does not match the more specific **Fortinet** firewall policy.

   In the search criteria, the source address is set to `10.0.1.100`. This source address is not included in the **Fortinet** firewall policy; therefore, the search does not match the **Fortinet** firewall policy.

When FortiGate is performing a policy lookup, it does a series of checks on ingress, stateful inspection, and egress for the matching firewall policy. It performs the checks from *top to bottom* before it provides results for the matching policy.

4. Click **Policy Lookup**, and then change the **Source** to `10.0.1.10`.

   Make sure all the other settings match the settings you configured in step 2.

5. Click **Search**.

   This time, the search matches the **Fortinet** firewall policy, in which the destination is set to the FQDN address object.

Reorder the Firewall Policies

You will reorder the firewall policies. You will move the **Block_Facebook** firewall policy above the **Full_Access** policy.

Take the Expert Challenge!

On the Local-FortiGate GUI, move the **Block_Facebook** firewall policy above the **Full_Access** policy.

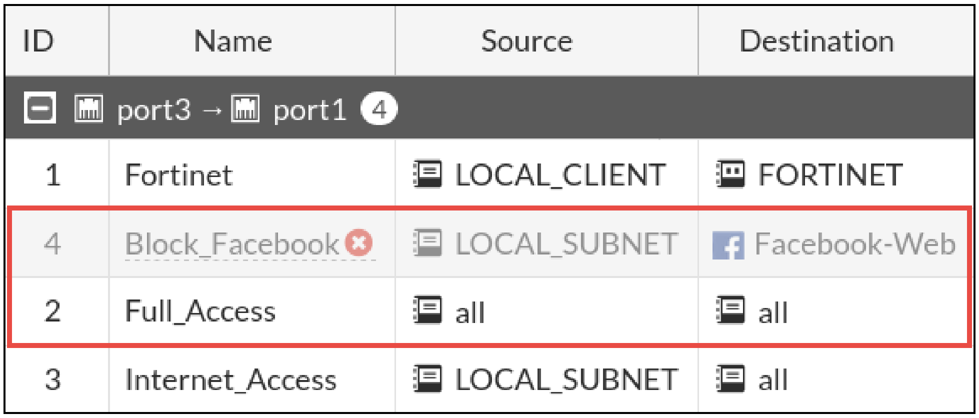
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you have performed these steps, see Retest Policy Lookup After Reordering the Firewall Policies on page 39.

To reorder the firewall policies

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. From the ID column, drag the **Block_Facebook** firewall policy above the **Full_Access** firewall policy.

   The order of the firewall policies should match the following example:



ID	Name	Source	Destination
⊟ port3 → port1 4			
1	Fortinet	LOCAL_CLIENT	FORTINET
4	Block_Facebook ✖	LOCAL_SUBNET	Facebook-Web
2	Full_Access	all	all
3	Internet_Access	LOCAL_SUBNET	all

Retest Policy Lookup After Reordering the Firewall Policies

You will retest the policy lookup feature after reordering the firewall policies.

To retest policy lookup after reordering the firewall policies

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**, and then click **Policy Lookup**.
2. Configure the following settings:

Field	Value
Source Interface	port3
Protocol	TCP
Source	10.0.1.10
Destination	facebook.com
Destination Port	443

3. Click **Search**.

Stop and think!

Why did the search not match the more specific policy, **Block_Facebook**?

When FortiGate is performing a policy lookup, it skips all disabled policies.

The search matches the **Full_Access** policy, but does not match the more specific **Block_Facebook** policy because it is disabled.

4. Right-click the **Block_Facebook** firewall policy, select **Set Status**, and then click **Enable**.
5. Click **Policy Lookup**.

   Make sure all the settings match the settings you configured in step 2.

6. Click **Search**.

   This time the search matches the more specific policy, **Block_Facebook**.

Lab 3: NAT

You can use network address translation (NAT) to perform source NAT (SNAT) and destination NAT (DNAT) for the traffic passing through FortiGate. There are two ways to configure SNAT and DNAT:

- Firewall policy NAT
- Central NAT

In this lab, you will examine how to configure and test firewall policy for DNAT using virtual IP (VIP), and SNAT using IP pool. You will configure and test SNAT using the central SNAT policy, and DNAT using the DNAT policy and VIPs.

Objectives

- Configure DNAT settings using a VIP
- Configure SNAT settings using overload IP pools
- Configure a central NAT policy for SNAT
- Configure DNAT and VIPs for DNAT

Time to Complete

Estimated: 50 minutes

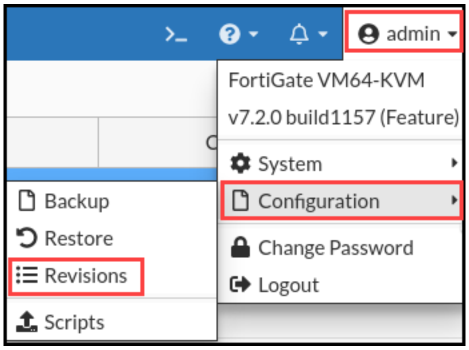
Prerequisites

Before beginning this lab, you must restore a configuration file on each FortiGate.

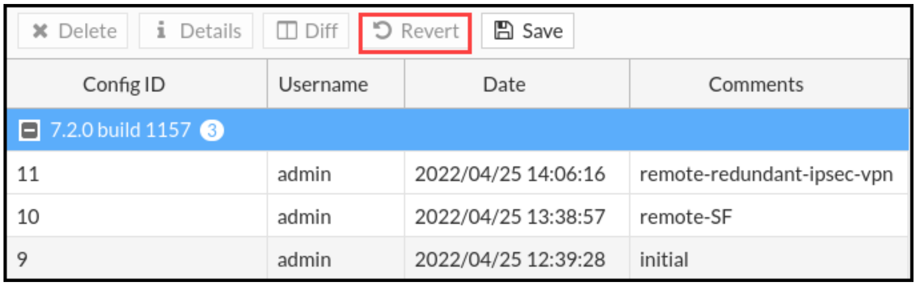
> Make sure that you restore the correct configuration on each FortiGate using the following steps. Failure to restore the correct configuration on each FortiGate will prevent you from doing the lab exercises.

To restore the Remote-FortiGate configuration file

1. Connect to the Remote-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click **+** to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.

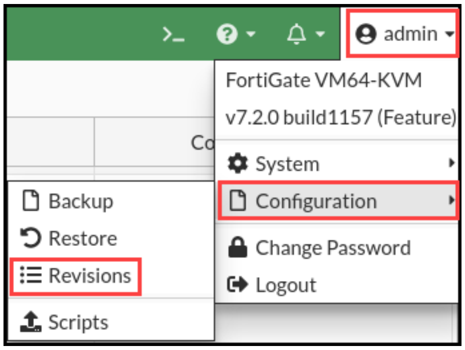


Config ID	Username	Date	Comments
7.2.0 build 1157 (3)			
11	admin	2022/04/25 14:06:16	remote-redundant-ipsec-vpn
10	admin	2022/04/25 13:38:57	remote-SF
9	admin	2022/04/25 12:39:28	initial

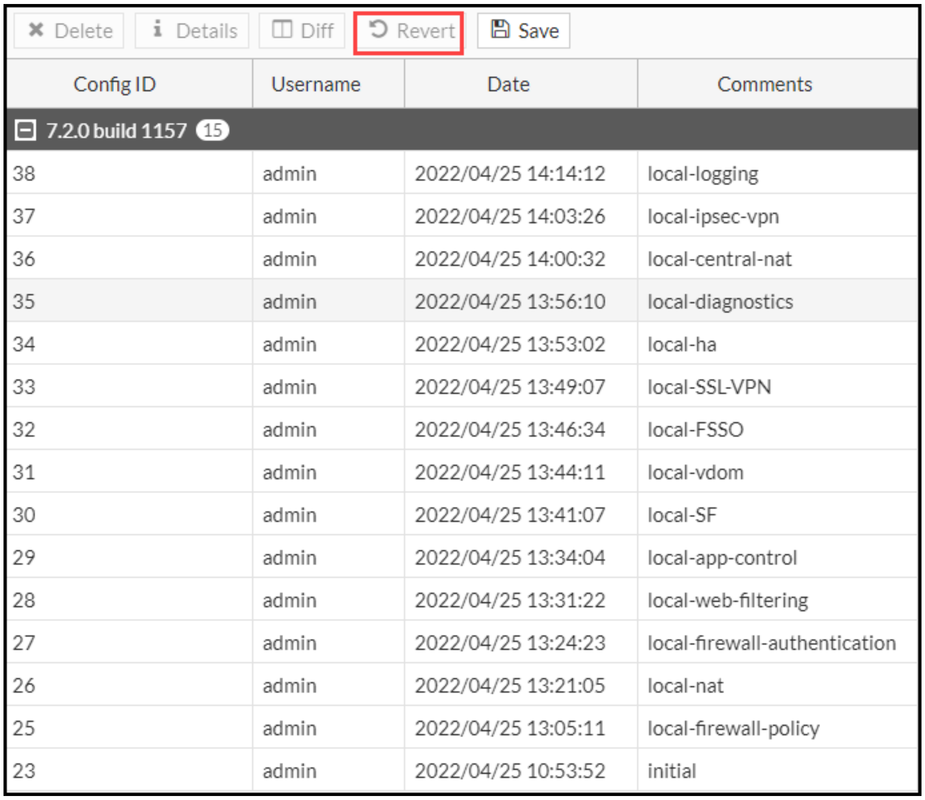
5. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click **+** to expand the list.
4. Select the configuration with the comment **local-nat**, and then click **Revert**.



Config ID	Username	Date	Comments
7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

Exercise 1: Configuring DNAT Settings Using a VIP

VIPs are typically used to translate external, or public, IP addresses to internal, or private, IP addresses.

In this exercise, you will examine how to configure a VIP for the Local-Client VM. Then, you will create an egress-to-ingress firewall policy and apply the VIP. This allows internet connections to the Local-Client VM. You will also verify the DNAT and SNAT behavior using CLI commands.

Create a VIP

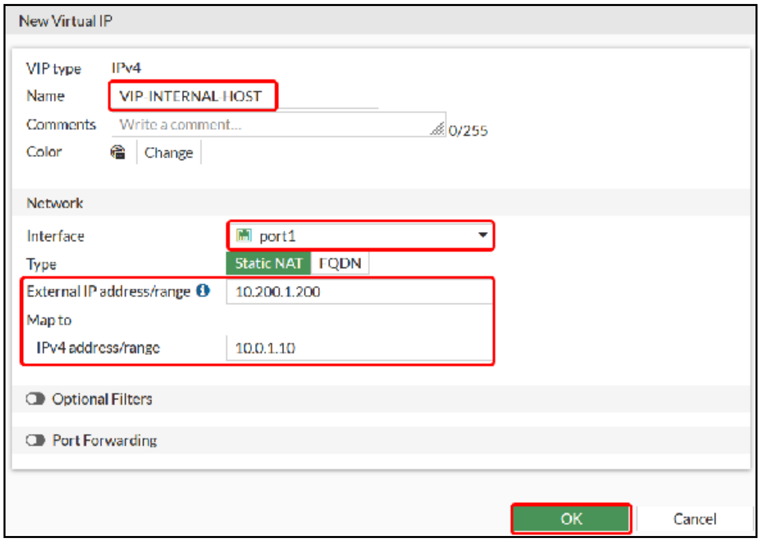
For DNAT on FortiGate, you use a VIP as the destination address field of a firewall policy.

You will configure the VIP to map the Local-Client VM (10.0.1.10) to 10.200.1.200, which is part of the port1 subnet. To refer to the lab diagram, see Network Topology on page 8.

To create a VIP

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Virtual IPs**.
3. Click **Create New**, and then select **Virtual IP**.
4. Configure the following settings:

Field	Value
Name	VIP-INTERNAL-HOST
Interface	port1 This port is connected to the internet with IP address 10.200.1.1/24.
External IP address/range	10.200.1.200 This IP address is in the same range as the port1 subnet.
Mapped IP address/range	10.0.1.10



New Virtual IP

VIP type IPv4

Name VIP-INTERNAL-HOST

Comments Write a comment... 0/255

Color Change

Network

Interface port1

Type Static NAT FQDN

External IP address/range 10.200.1.200

Map to

IPv4 address/range 10.0.1.10

5. Click **OK**.

Create a Firewall Policy

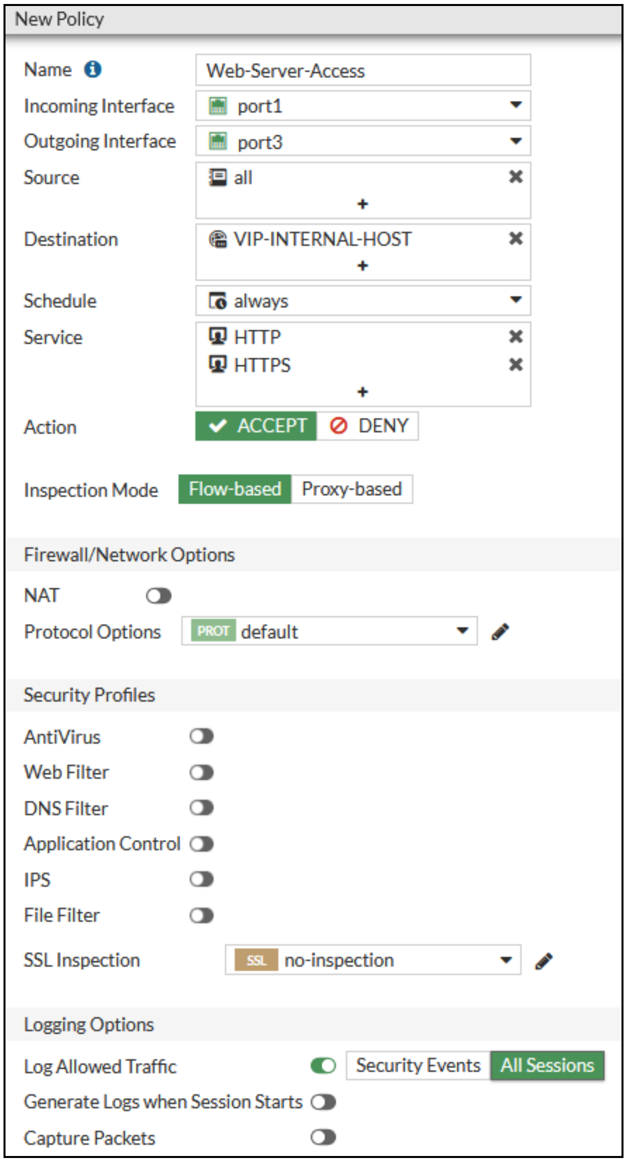
You will configure a new firewall policy using the VIP that you just created as the destination address.

To create a firewall policy

1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	Web-Server-Access
Incoming Interface	port1
Outgoing Interface	port3
Source	all
Destination	VIP-INTERNAL-HOST **Tip**: This is listed under the **VIRTUAL IP/SERVER** section.
Schedule	always
Service	HTTP, HTTPS **Tip**: In the right pane, type the name in the search box, and then click services to add.
Action	ACCEPT

4. In the **Firewall/Network Options** section, disable **NAT**.
5. In the **Logging Options** section, enable **Log Allowed Traffic**, and then select **All Sessions**.
6. Click **OK**.



New Policy

Name: Web-Server-Access
Incoming Interface: port1
Outgoing Interface: port3
Source: all
Destination: VIP-INTERNAL-HOST
Schedule: always
Service: HTTP, HTTPS
Action: [✓ ACCEPT] DENY

Inspection Mode: [✓ Flow-based] Proxy-based

Firewall/Network Options

NAT: ○
Protocol Options: PROT default

Security Profiles

AntiVirus: ○
Web Filter: ○
DNS Filter: ○
Application Control: ○
IPS: ○
File Filter: ○
SSL Inspection: SSL no-inspection

Logging Options

Log Allowed Traffic: ● Security Events [✓ All Sessions]
Generate Logs when Session Starts: ○
Capture Packets: ○

Test the VIP Firewall Policy

Now that you have configured a firewall policy with the VIP as the destination, you can test your VIP by accessing it from the Remote-Client VM, which is behind the Remote-FortiGate internal network. A Linux machine acts as a router between the two FortiGate devices, and routes the traffic from the Remote-FortiGate to the Local-FortiGate. For more information, see Network Topology on page 8.

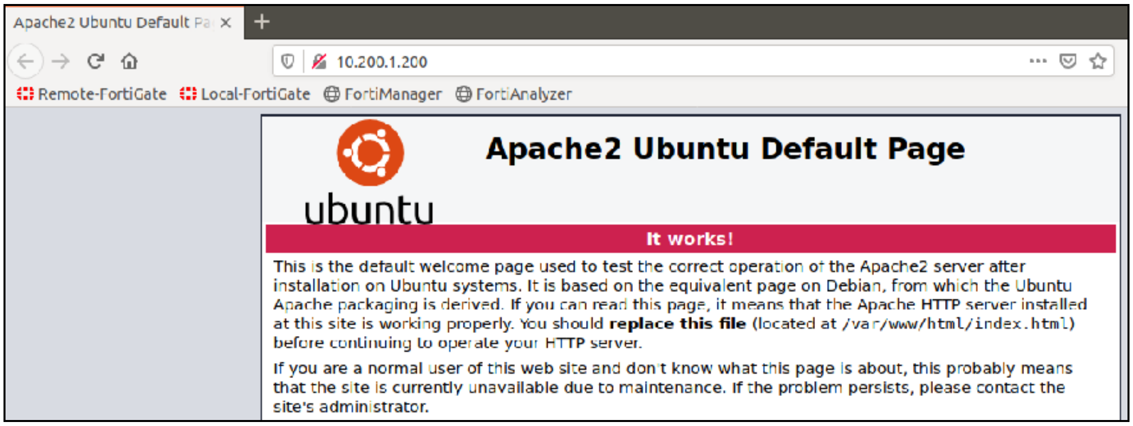
You will also test how the source address is translated by the VIP when traffic leaves the Local-Client VM.

To test VIPs (DNAT)

1. On the Remote-Client VM, open a browser, and then browse to the following URL:

   ```
   http://10.200.1.200
   ```

   If the VIP operation is successful, a simple web page opens.



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

2. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
3. Enter the following command to check the destination NAT entries in the session table:

   ```
   get system session list
   ```

   The following example shows a sample output:

   ```
   Local-FortiGate# get system session list
   PROTO EXPIRE SOURCE SOURCE-NAT DESTINATION DESTINATION-NAT
   tcp 3594 10.200.3.1:49478 - 10.200.1.200:80 10.0.1.10:80
   ```

   You will notice that the destination address `10.200.1.200` is translated to `10.0.1.10`, which is the mapping you configured in the VIP.

The HTTP session may have been deleted by the time you run the `get system session list` command. You can repeat steps 1–3 to generate a new HTTP connection and, therefore, another HTTP session through Local-FortiGate.

Test SNAT

As a result of the VIP (which is a static NAT), FortiGate uses the VIP external address as the NAT IP address when performing SNAT for the ingress-to-egress direction of the traffic, provided the matching outgoing firewall policy has NAT enabled. That is, FortiGate doesn't use the egress interface address.

To test SNAT

1. Return to the Local-FortiGate CLI session, and then enter the following command to clear any existing sessions:

   ```
   diagnose sys session clear
   ```

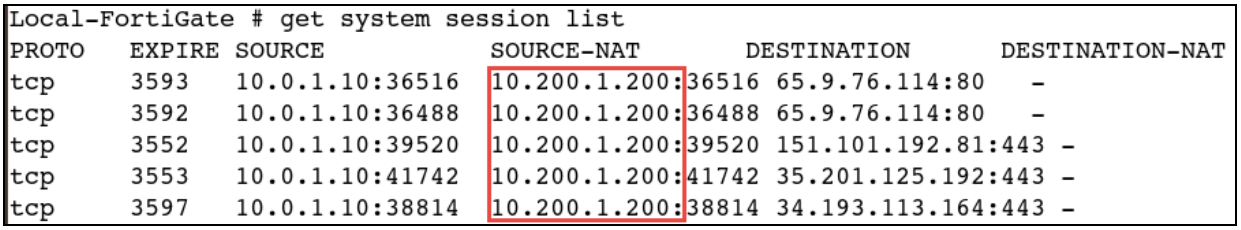
The `diagnose sys session clear` CLI command clears all sessions, including the SSH session you created. This is expected behavior.

This clears the session to the Local-FortiGate from the Local-Client VM.

2. Close the Local-FortiGate CLI window.
3. On the Local-Client VM, open a few browser tabs, and connect to a few websites, such as:
   - www.fortinet.com
   - www.yahoo.com
   - www.bbc.com
4. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
5. Enter the following command to view the session information:

   ```
   get system session list
   ```

   The following example shows a sample output:



```
Local-FortiGate # get system session list
PROTO   EXPIRE SOURCE            SOURCE-NAT          DESTINATION        DESTINATION-NAT
tcp     3593   10.0.1.10:36516   10.200.1.200:36516 65.9.76.114:80     -
tcp     3592   10.0.1.10:36488   10.200.1.200:36488 65.9.76.114:80     -
tcp     3552   10.0.1.10:39520   10.200.1.200:39520 151.101.192.81:443 -
tcp     3553   10.0.1.10:41742   10.200.1.200:41742 35.201.125.192:443 -
tcp     3597   10.0.1.10:38814   10.200.1.200:38814 34.193.113.164:443 -
```

The outgoing connections from the Local-Client VM are now translated with the VIP address `10.200.1.200`, instead of the firewall egress interface IP address (`10.200.1.1`).

This is a behavior for SNAT when using a static NAT VIP. That is, when you enable NAT on a policy, the external address of a static NAT VIP takes precedence over the destination interface IP address if the source address of the connections matches the VIP internal address.

6. Close the Local-FortiGate CLI window.
7. Close all browser tabs except the Local-FortiGate GUI.

Exercise 2: Using Dynamic NAT With IP Pools

IP pools are used to translate the source address to an address from that pool, rather than the egress interface address.

Currently, Local-FortiGate translates the source IP address of all traffic generated from the Local-Client VM to 10.200.1.200 because the internal address of the VIP matches the address of Local-Client, and the VIP is a static NAT VIP.

In this exercise, you will examine how to create an IP pool, apply it to the ingress-to-egress firewall policy, and verify the SNAT address using CLI commands.

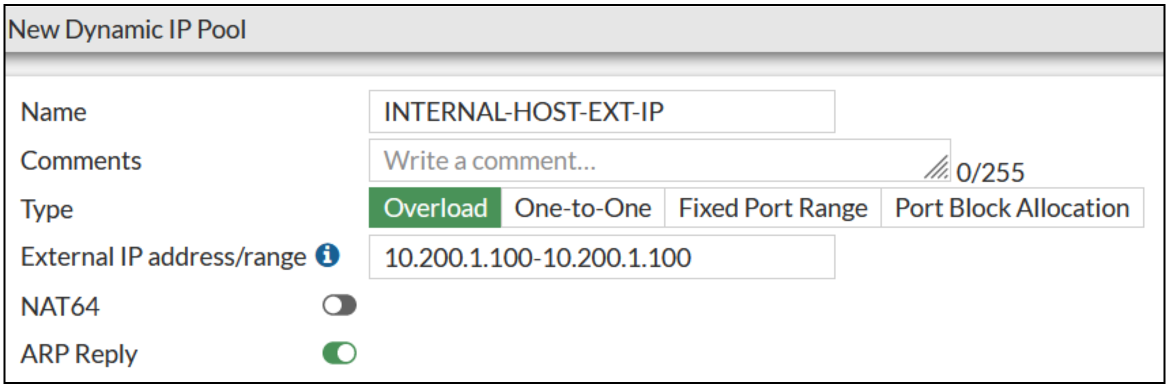
Create an IP Pool

You will create an IP pool from the range of public IP addresses available on the egress port (port1).

To create an IP pool

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **IP Pools**.
3. Click **Create New**, and then configure the following settings:

Field	Value
Name	INTERNAL-HOST-EXT-IP
Type	Overload
External IP address/range	10.200.1.100-10.200.1.100



New Dynamic IP Pool

Name	INTERNAL-HOST-EXT-IP
Comments	Write a comment... 0/255
Type	[✓ Overload] One-to-One Fixed Port Range Port Block Allocation
External IP address/range	10.200.1.100-10.200.1.100
NAT64	○
ARP Reply	●

4. Click **OK**.

Edit a Firewall Policy to Use the IP Pool

You will apply the IP pool to change the behavior from static NAT to dynamic NAT on the ingress-to-egress firewall policy.

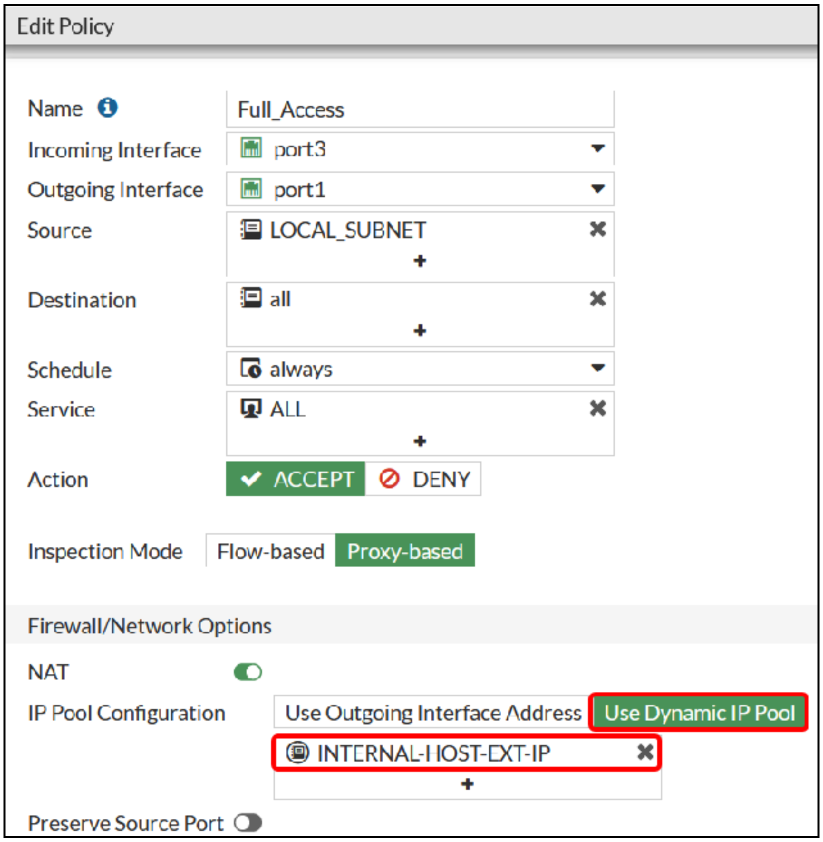
To edit the firewall policy

1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Right-click the **Full_Access** firewall policy, and then click **Edit.**
3. In the **Firewall / Network Options** section, configure the following settings:

Field	Value
NAT	<enable>
IP Pool Configuration	Use Dynamic IP Pool

4. Click the **+** sign that appeared when you clicked **Use Dynamic IP Pool**, and then in the right pane, click **INTERNAL-HOST-EXT-IP**.

   Your configuration will look similar to the following example:



Edit Policy

Name	Full_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY
Inspection Mode	Flow-based [✓ Proxy-based]

Firewall/Network Options

NAT	●
IP Pool Configuration	Use Outgoing Interface Address [✓ Use Dynamic IP Pool] INTERNAL-HOST-EXT-IP
Preserve Source Port	○

5. Click **OK.**

Test Dynamic NAT With IP Pools

Now that your configuration is ready, you can test dynamic NAT with IP pools by browsing to a few external sites on the internet. If successful, you will see that the Local-Client VM IP address (10.0.1.10) is translated to the IP pool address of 10.200.1.100.

To test dynamic NAT with IP pools

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following commands to clear sessions sourced from `10.0.1.10`:

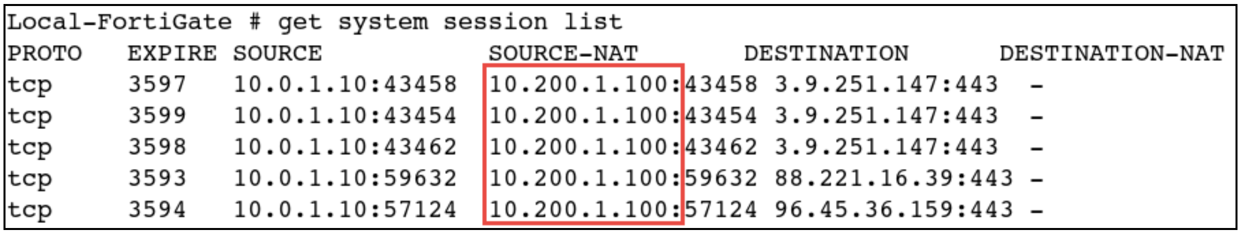
```
diagnose sys session filter clear
diagnose sys session filter src 10.0.1.10
diagnose sys session clear
```

You built the filter to match sessions sourced from `10.0.1.10`. This way, when you run the `diagnose sys session clear` CLI command, it clears only the sessions sourced from `10.0.1.10`. As a result, your SSH session is not disconnected. This is why it is important to build the session filter before using the `session clear` command.

3. On the Local-Client VM, open a few browser tabs, and connect to a few websites, such as:
   - www.fortinet.com
   - www.yahoo.com
   - www.bbc.com
4. On the Local-FortiGate CLI, enter the following command to verify the SNAT address that the sessions are using:

```
get system session list
```

The following image shows a sample output:



```
Local-FortiGate # get system session list
PROTO   EXPIRE SOURCE          SOURCE-NAT          DESTINATION        DESTINATION-NAT
tcp     3597   10.0.1.10:43458 10.200.1.100:43458 3.9.251.147:443   -
tcp     3599   10.0.1.10:43454 10.200.1.100:43454 3.9.251.147:443   -
tcp     3598   10.0.1.10:43462 10.200.1.100:43462 3.9.251.147:443   -
tcp     3593   10.0.1.10:59632 10.200.1.100:59632 88.221.16.39:443 -
tcp     3594   10.0.1.10:57124 10.200.1.100:57124 96.45.36.159:443 -
```

Notice that the SNAT address is now `10.200.1.100`, as configured in the IP pool, and the IP pool has overridden the static NAT VIP.

5. Close the Local-FortiGate CLI window.
6. Close all browser tabs except the Local-FortiGate GUI.

Exercise 3: Configuring Central SNAT

A central SNAT policy is applied to multiple firewall policies, based on a configured central rule.

In this exercise, you will examine how to configure a central SNAT policy and test it.

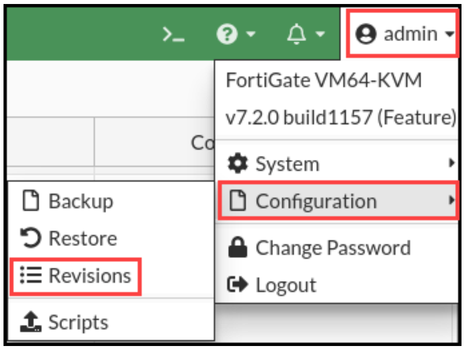
Prerequisites

Before beginning this lab, you must restore a configuration for central NAT to Local-FortiGate.

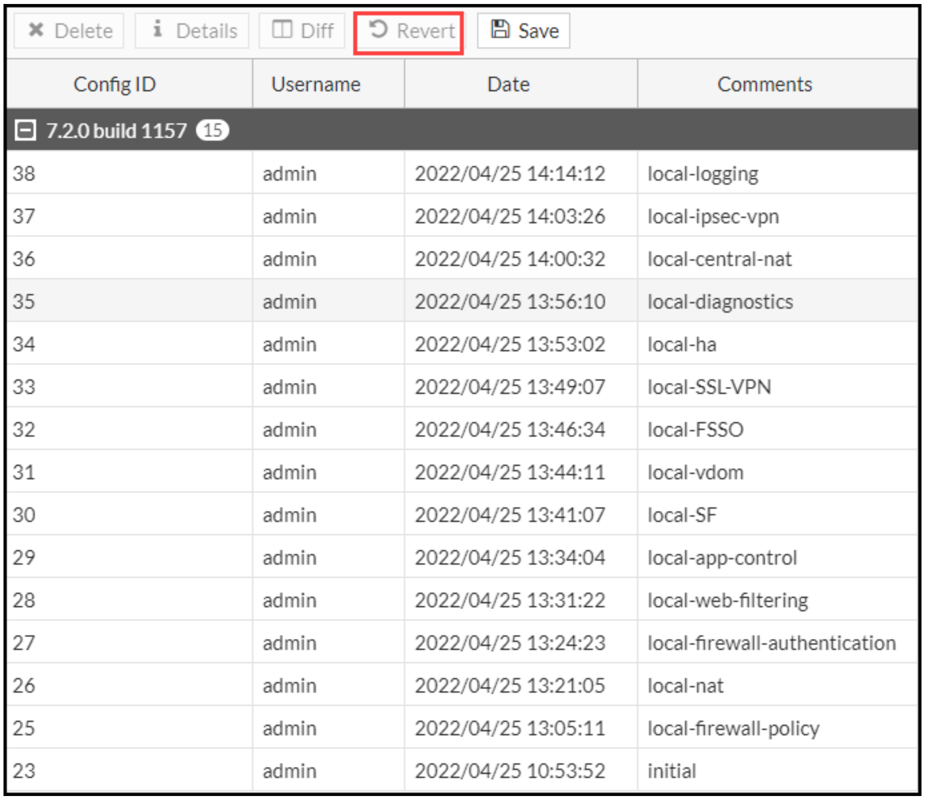
⚠ Make sure to restore the correct configuration for Local-FortiGate using the following steps. Failure to restore the correct configuration on Local-FortiGate will prevent you from doing the lab exercise.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click **+** to expand the list.
4. Select the configuration with the comment **local-central-nat**, and then click **Revert**.

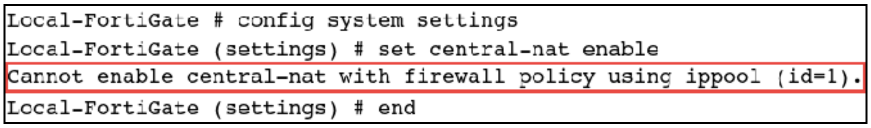


Config ID	Username	Date	Comments
7.2.0 build 1157 (15)			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

When enabling central NAT, you must first remove VIP and IP pool references from the existing firewall policies.

For example, if you try to enable central NAT without removing VIP and IP pool references from the existing firewall policies, you will see the following error:



```
Local-FortiGate # config system settings
Local-FortiGate (settings) # set central-nat enable
Cannot enable central-nat with firewall policy using ippool (id=1).
Local-FortiGate (settings) # end
```

To prevent this error from occurring during this exercise, the following changes were made as part of the configuration restoration:

- The IP pool was removed from the **Full_Access** firewall policy (policy **ID 1**), and the VIP address was removed from the **Web-Server-Access** firewall policy (policy **ID 2**), because central NAT can be enabled only if none of the firewall policies have IP pools and VIPs associated with them.
- The VIP you added in a previous exercise to test the firewall policy SNAT was removed.
- Central NAT was enabled.

You will notice all the changes listed above after you load `local-central-nat.conf` in the firewall.

Configure a Central SNAT Policy

You will configure a central SNAT policy using the IP pool you created in the previous exercise.

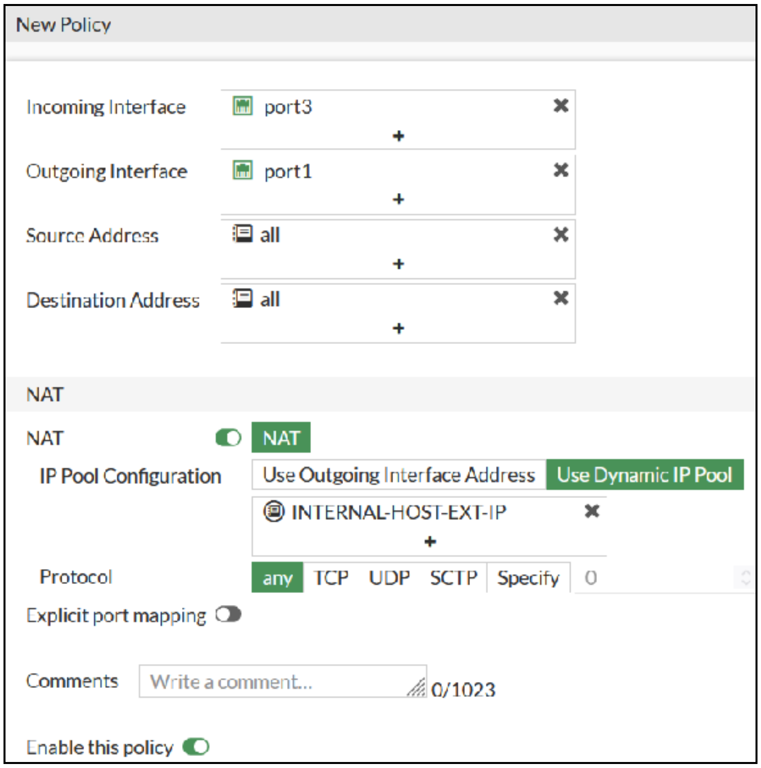
To review the IP pool configuration

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **IP Pools**.
3. Review the settings of **INTERNAL-HOST-EXT-IP**.

To configure a central SNAT policy

1. On the Local-FortiGate GUI, click **Policy & Objects** > **Central SNAT**.
2. Click **Create New**, and then configure the following settings:

Field	Value
Incoming Interface	port3
Outgoing Interface	port1
Source Address	all
Destination Address	all
NAT	<enable>
IP Pool Configuration	Use Dynamic IP Pool Click **+**, and then select **INTERNAL-HOST-EXT-IP**.
Protocol	any



New Policy

Incoming Interface: port3

Outgoing Interface: port1

Source Address: all

Destination Address: all

NAT

NAT: NAT

IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool

INTERNAL-HOST-EXT-IP

Protocol: any TCP UDP SCTP Specify 0

Explicit port mapping

Comments: Write a comment... 0/1023

Enable this policy

3. Keep the default values for the remaining settings, and then click **OK** to save the changes.

NAT is enabled on the central SNAT policy.

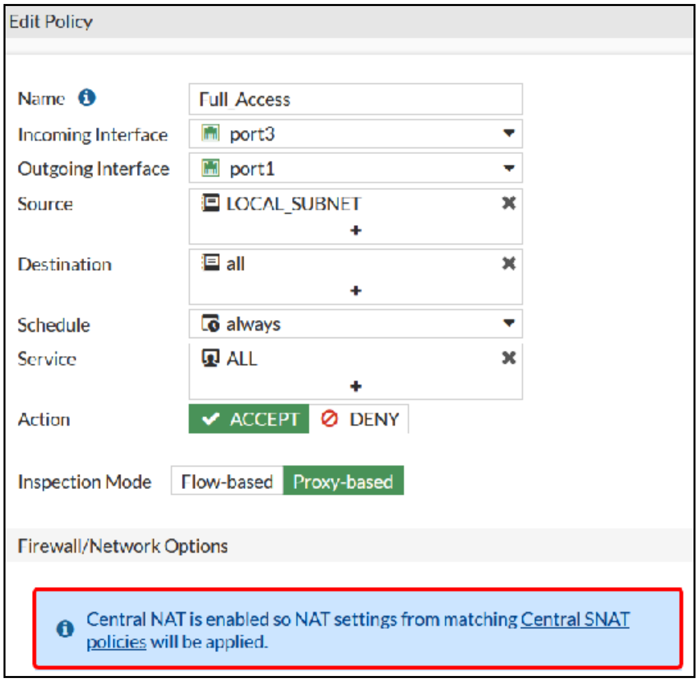
If no central SNAT or matching central SNAT rule exists, FortiGate creates the session using the original source IP address and no NAT is applied.

Review the Firewall Policy

You will review the firewall policy.

To verify that NAT is enabled on the firewall policy

1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Right-click the **Full_Access** firewall policy, and then click **Edit**.
3. Review the **Firewall/Network Options** of the **Full_Access** policy.



Edit Policy

Name	Full Access
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY
Inspection Mode	Flow-based Proxy-based

Firewall/Network Options

Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.

There is no option for enabling NAT or using IP pools. In central NAT mode, the SNAT policy controls whether or not NAT is used.

4. Click **Cancel**.

Test Central SNAT

Now that your configuration is ready, you will test the behavior of the central SNAT policy.

To test central SNAT

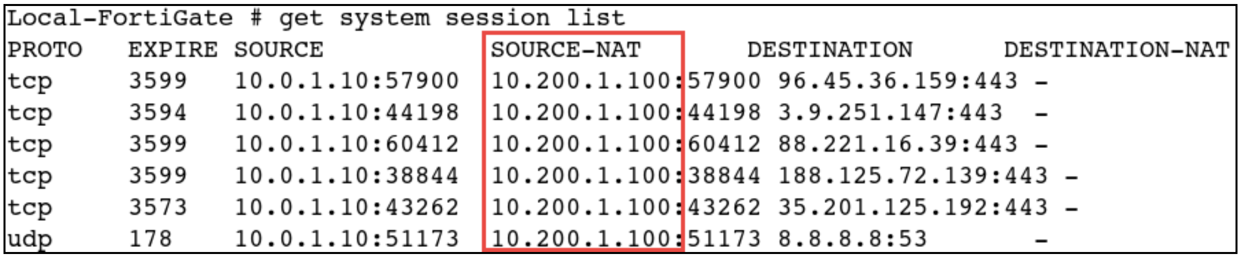
1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following commands to clear sessions sourced from `10.0.1.10`:

```
diagnose sys session filter clear
diagnose sys session filter src 10.0.1.10
diagnose sys session clear
```

3. Close the Local-FortiGate CLI window.
4. On the Local-Client VM, open a few browser tabs, and connect to a few websites, such as:
   - www.fortinet.com
   - www.yahoo.com
   - www.bbc.com
5. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
6. Enter the following command to verify the SNAT IP address that those sessions are using:

```
get system session list
```

The following image shows a sample output:



```
Local-FortiGate # get system session list
PROTO    EXPIRE SOURCE           SOURCE-NAT           DESTINATION        DESTINATION-NAT
tcp      3599    10.0.1.10:57900  10.200.1.100:57900 96.45.36.159:443 -
tcp      3594    10.0.1.10:44198  10.200.1.100:44198 3.9.251.147:443  -
tcp      3599    10.0.1.10:60412  10.200.1.100:60412 88.221.16.39:443 -
tcp      3599    10.0.1.10:38844  10.200.1.100:38844 188.125.72.139:443 -
tcp      3573    10.0.1.10:43262  10.200.1.100:43262 35.201.125.192:443 -
udp      178     10.0.1.10:51173  10.200.1.100:51173 8.8.8.8:53         -
```

Notice that the SNAT address is now `10.200.1.100`, which matches the IP pool configured in the central SNAT policy.

7. Close the Local-FortiGate CLI.
8. Close all browser tabs except the Local-FortiGate GUI.

Field	Value

Field	Value
Incoming Interface	port3
Outgoing Interface	port1
NAT	Enabled

A central SNAT policy is processed from *top to bottom*, similar to firewall policies.

Exercise 4: Configuring and Testing DNAT and VIPs

In firewall policy NAT, a VIP is selected in the firewall policy as the destination address. In central NAT, when you configure DNAT and VIPs, FortiGate automatically creates a rule in the kernel to allow DNAT to occur, and no additional configuration is required.

In this exercise, you will examine how to configure and test the behavior of central DNAT.

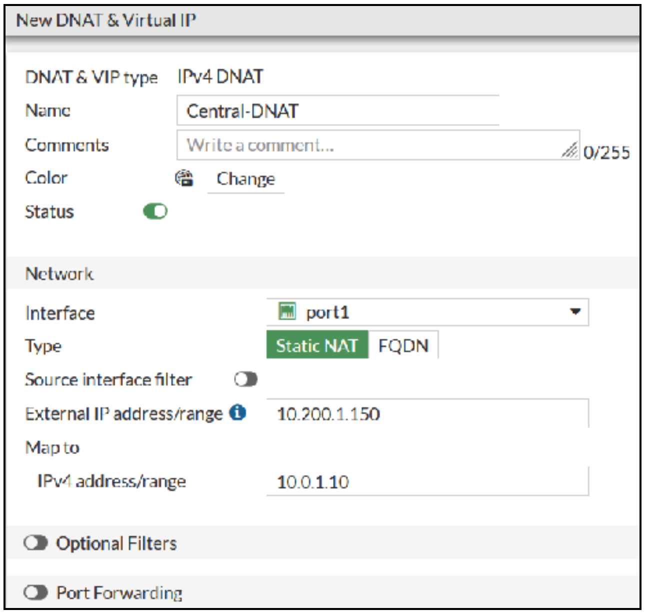
Create DNAT and VIPs

You will configure DNAT and VIPs.

To create DNAT and VIPs

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **DNAT & Virtual IPs**.
3. Click **Create New**, and then select **DNAT & Virtual IP**.
4. Configure the following settings:

Field	Value
Name	Central-DNAT
Interface	port1
Type	Static NAT (default setting)
External IP address/range	10.200.1.150
Mapped IP address/range	10.0.1.10



New DNAT & Virtual IP

DNAT & VIP type IPv4 DNAT
Name Central-DNAT
Comments Write a comment... 0/255
Color Change
Status

Network

Interface port1
Type Static NAT FQDN
Source interface filter
External IP address/range 10.200.1.150
Map to
IPv4 address/range 10.0.1.10

Optional Filters

Port Forwarding

5. Click **OK**.

Verify the Firewall Policy Settings

You will verify the firewall policy settings for the egress-to-ingress firewall policy.

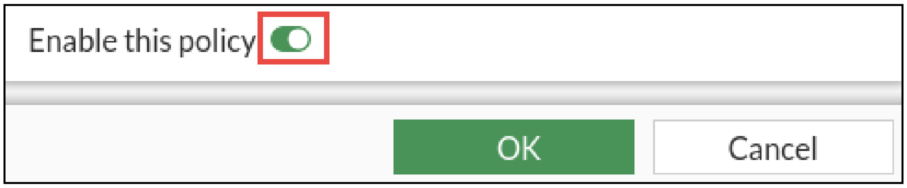
To verify the firewall policy settings

1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Right-click the **Web-Server-Access** firewall policy, and then click **Edit**.
3. Review the settings of the firewall policy.
4. Try to select the **Central-DNAT** object in the firewall **Destination** address.

   You will not be able to do so because the **Central-DNAT** object is not in the list.

In central NAT mode, you don't reference VIPs in firewall policies. As soon as you create the VIP object, FortiGate automatically creates a rule in the kernel for DNAT to occur.

5. Scroll to the bottom of the page, and then ensure that **Enable this policy** is enabled.



Enable this policy

6. Click **OK**.

Test DNAT and VIPs

You will test DNAT and VIPs by accessing the Local-Client VM.

To test DNAT and VIPs

1. On the Remote-Client VM, open a browser, and then access the following URL:

   `http://10.200.1.150`

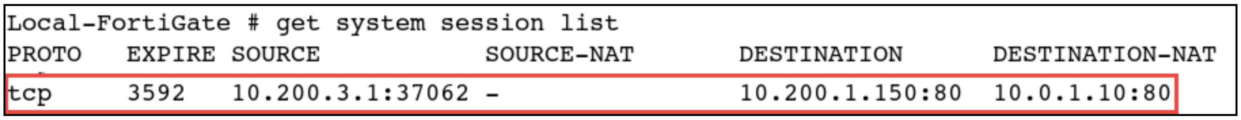
   If the VIP operation is successful, a simple web page opens.

2. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.

3. Enter the following command to check the destination NAT entries in the session table:

   ```
   get system session list
   ```

   The following example shows a sample output:



```
Local-FortiGate # get system session list
PROTO    EXPIRE  SOURCE            SOURCE-NAT        DESTINATION       DESTINATION-NAT
tcp      3592    10.200.3.1:37062  -                 10.200.1.150:80   10.0.1.10:80
```

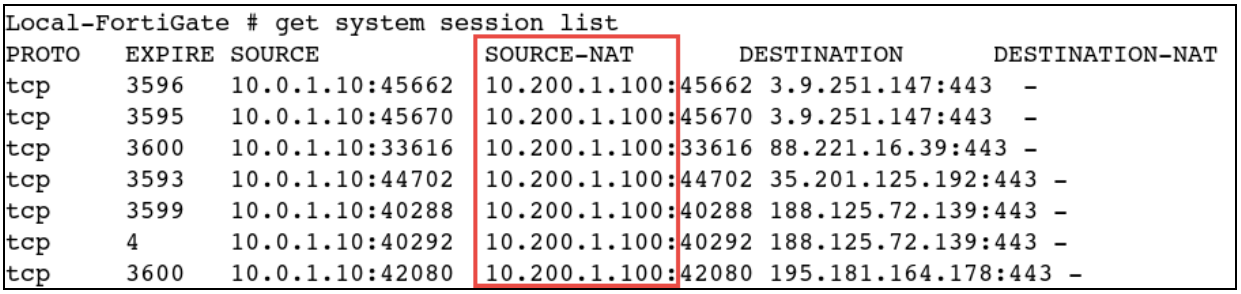
The HTTP session may have been deleted by the time you run the `get system session list` command. You can repeat steps 1–3 to generate a new HTTP connection and, therefore, another HTTP session through Local-FortiGate.

4. On the Local-Client VM, open a few browser tabs, and connect to a few websites, such as:
   - www.fortinet.com
   - www.yahoo.com
   - www.bbc.com

5. Return to the Local-FortiGate CLI session, and then verify the SNAT IP address that those sessions are using:

   ```
   get system session list
   ```

   The following example shows a sample output:



```
Local-FortiGate # get system session list
PROTO    EXPIRE  SOURCE            SOURCE-NAT          DESTINATION          DESTINATION-NAT
tcp      3596    10.0.1.10:45662   10.200.1.100:45662 3.9.251.147:443     -
tcp      3595    10.0.1.10:45670   10.200.1.100:45670 3.9.251.147:443     -
tcp      3600    10.0.1.10:33616   10.200.1.100:33616 88.221.16.39:443    -
tcp      3593    10.0.1.10:44702   10.200.1.100:44702 35.201.125.192:443  -
tcp      3599    10.0.1.10:40288   10.200.1.100:40288 188.125.72.139:443  -
tcp      4       10.0.1.10:40292   10.200.1.100:40292 188.125.72.139:443  -
tcp      3600    10.0.1.10:42080   10.200.1.100:42080 195.181.164.178:443 -
```

Notice that the SNAT address is still `10.200.1.100`, as configured in the central SNAT policy using IP pool. That is, the DNAT and VIP object you created did not override the central SNAT policy. This behavior is similar to firewall policy NAT configured with IP pool.

If both the central SNAT policy and DNAT and VIP object are defined, FortiGate uses the NAT address configured in the central SNAT policy to perform SNAT.

To summarize, when you configure a VIP for a host, the following occurs in firewall policy NAT mode:

- If the outgoing policy has NAT enabled, FortiGate uses the external address defined in the VIP as the NAT IP.
- If the outgoing policy references an IP pool, FortiGate uses the external address defined in the IP pool as the NAT IP.

In central NAT mode, FortiGate uses the address configured in the SNAT policy as the NAT IP. This address can be the egress interface address or the IP pool external address.

6. Close the Local-FortiGate CLI window.

7. Close all browser tabs except the Local-FortiGate GUI.

Lab 4: Firewall Authentication

In this lab, you will examine how to configure FortiGate to communicate with a remote LDAP server for server-based password authentication.

You will also configure a captive portal, so that users who connect to the network are prompted for their login credentials (active authentication).

Objectives

- Configure server-based password authentication with an LDAP server

Time to Complete

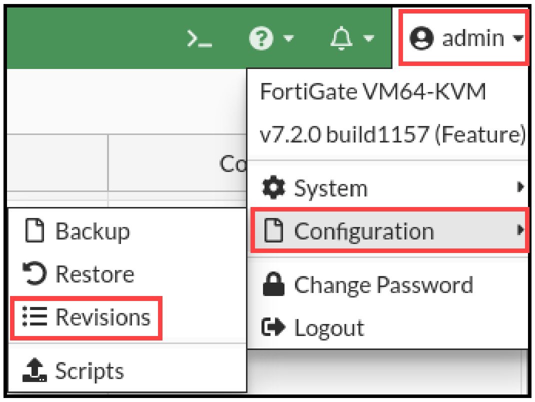
Estimated: 20 minutes

Prerequisites

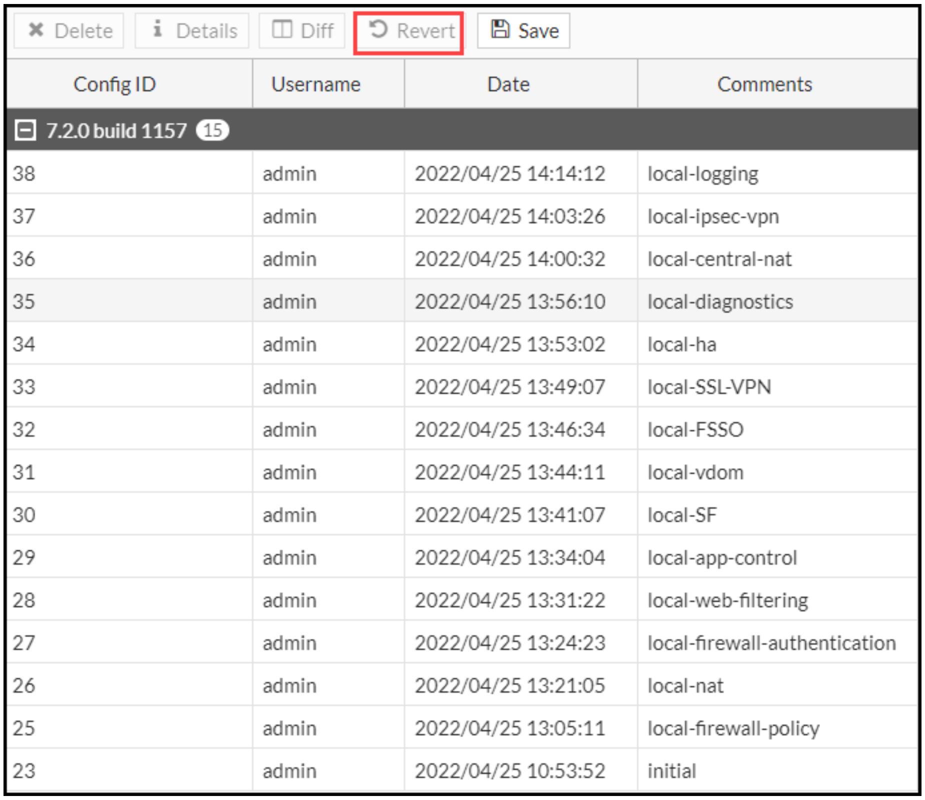
Before beginning this lab, you must restore a configuration file to Local-FortiGate.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click **+** to expand the list.
4. Select the configuration with the comment **local-firewall-authentication**, and then click **Revert**.



Config ID	Username	Date	Comments
7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

Exercise 1: Configuring Remote Authentication

In this exercise, you will examine how to configure an LDAP server on FortiGate for remote authentication, create a remote authentication group for remote users, and then add that group as a source in a firewall policy. Finally, you will authenticate as one of the remote users, and then monitor the login as the administrator.

Configure an LDAP Server on FortiGate

You can configure FortiGate to point to a preconfigured FortiAuthenticator acting as an LDAP server for server-based password authentication.

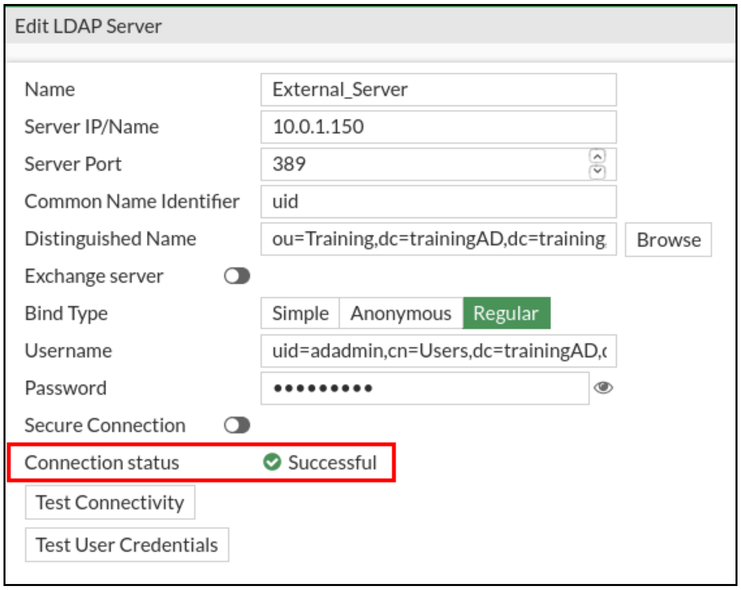
To configure an LDAP server on FortiGate

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **User & Authentication** > **LDAP Servers**, and then click **Create New**.
3. Configure a server using the following settings:

Field	Value
Name	External_Server
Server IP/Name	10.0.1.150 This is the IP address of the FortiAuthenticator acting as the LDAP server. For more information, see Network Topology on page 8.
Server Port	389 This is the default port for LDAP.
Common Name Identifier	uid This is the attribute name used to find the username on the preconfigured LDAP server.
Distinguished Name	ou=Training,dc=trainingAD,dc=training,dc=lab This is the domain name for the LDAP directory on FortiAuthenticator, with all users located under the **Training** organizational unit (ou).
Bind Type	Regular
Username	uid=adadmin,cn=Users,dc=trainingAD,dc=training,dc=lab You are using the credentials of an LDAP user called adadmin to authenticate to the LDAP server.

Field	Value
Password	Training! This is the password preconfigured for the adadmin user. You must use it to be able to bind.

4. Click **Test Connectivity**.



Edit LDAP Server

Name	External_Server
Server IP/Name	10.0.1.150
Server Port	389
Common Name Identifier	uid
Distinguished Name	ou=Training,dc=trainingAD,dc=training
Exchange server	○
Bind Type	Simple / Anonymous / **Regular**
Username	uid=adadmin,cn=Users,dc=trainingAD,(
Password	•••••••••
Secure Connection	○
Connection status	✓ Successful

You should see a message indicating that the connection was successful.

5. Click **OK**.

Assign an LDAP User Group to a Firewall Group

You will assign an LDAP user group (**AD_users**) that includes two users (**aduser1** and **aduser2**) to a firewall user group, called **Remote-users**, on FortiGate. By doing this, you will be able to configure firewall policies to act on the firewall user group.

Usually, groups are used to more effectively manage individuals who have a shared relationship.

The **Remote-users** firewall group is preconfigured for you. However, you must modify it to add the users from the remote LDAP server you configured in the previous procedure.

Take the Expert Challenge!

On Local-FortiGate (`10.0.1.254`), assign the Active Directory user group called **AD_users** to the FortiGate firewall user group called **Remote-users**.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

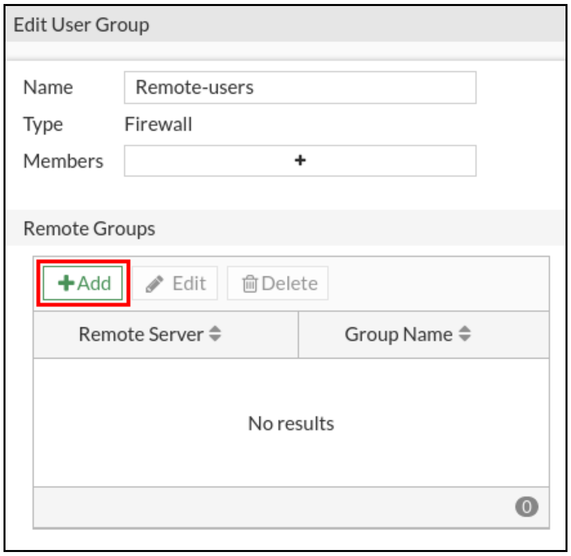
After you have completed this exercise, see Configuring Remote Authentication on page 64.

To assign a user to a user group

1. On the Local-FortiGate GUI, click **User & Authentication** > **User Groups**, and then edit the **Remote-users** group.

   Notice that it's currently configured as a firewall group.

2. To add users from the remote LDAP server, in the **Remote Groups** table, click **Add**.



Edit User Group

Name: Remote-users

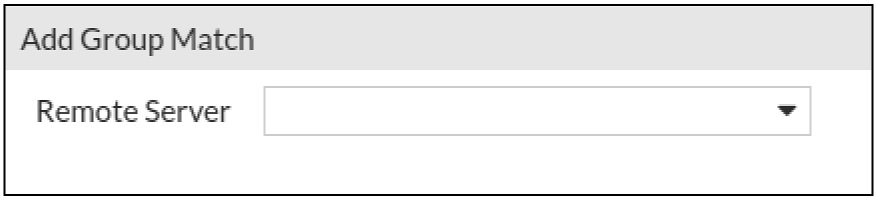
Type: Firewall

Members: +

Remote Groups

Remote Server	Group Name
No results	

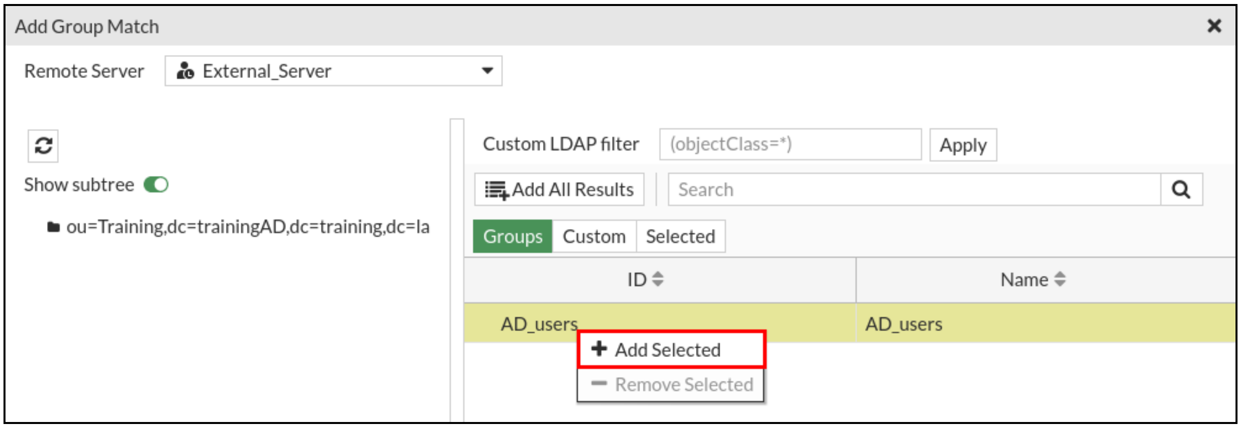
The **Add Group Match** dialog box opens.



Add Group Match

Remote Server:

3. In the **Remote Server** drop-down list, select **External_Server**.
4. On the **Groups** tab, right-click **AD_users**, and then click **Add Selected**.



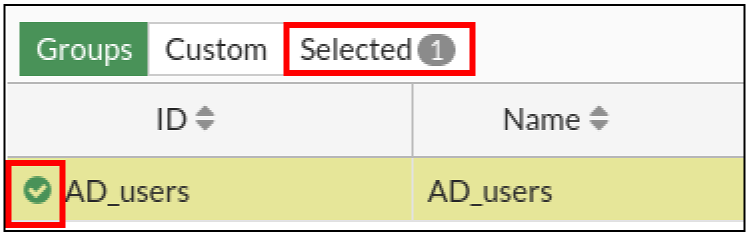
Remote Server: External_Server

Custom LDAP filter: (objectClass=*)

ou=Training,dc=trainingAD,dc=training,dc=la

ID	Name
AD_users	AD_users

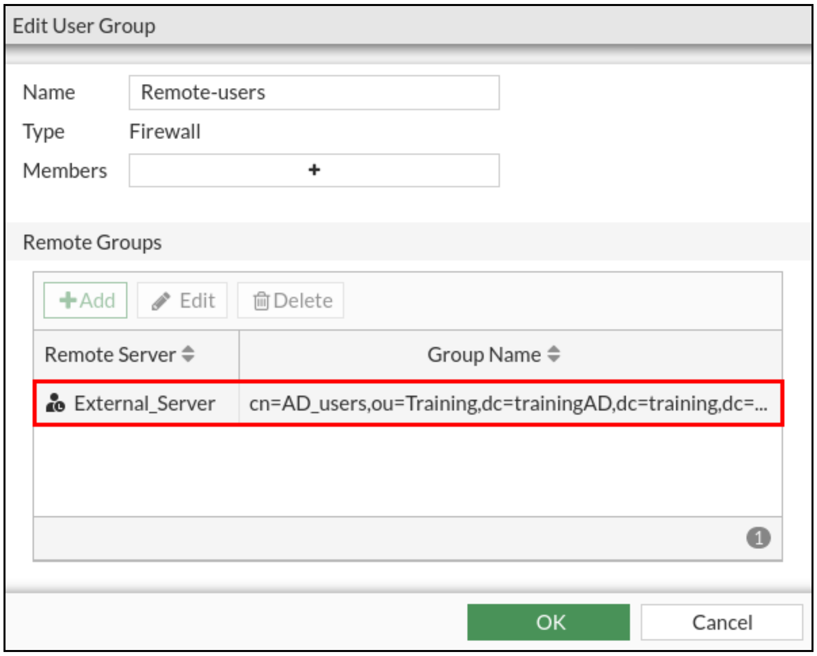
AD_users has a green check mark beside it, which indicates that it was added.



ID	Name
✓ AD_users	AD_users

5. Click **OK**.

   The users in this Active Directory group are now included in the FortiGate **Remote-users** firewall user group. Only users from the remote LDAP server that match this user group entry can authenticate.



Name	Remote-users
Type	Firewall
Members	+

Remote Server	Group Name
External_Server	cn=AD_users,ou=Training,dc=trainingAD,dc=training,dc=...

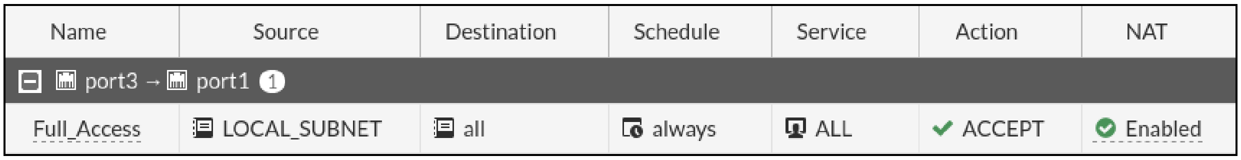
6. Click **OK**.

Add the Remote User Group to the Firewall Policy

Now that you have added the LDAP server to the **Remote-users** firewall user group, you can add the group to a firewall policy. This allows you to control access to network resources, because policy decisions are made for the group as a whole.

To add the remote user group to the firewall policy

1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**, and then double-click the existing port3 to port1 firewall policy.



Name	Source	Destination	Schedule	Service	Action	NAT
⊟ port3 → port1 1						
Full_Access	LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	✓ Enabled

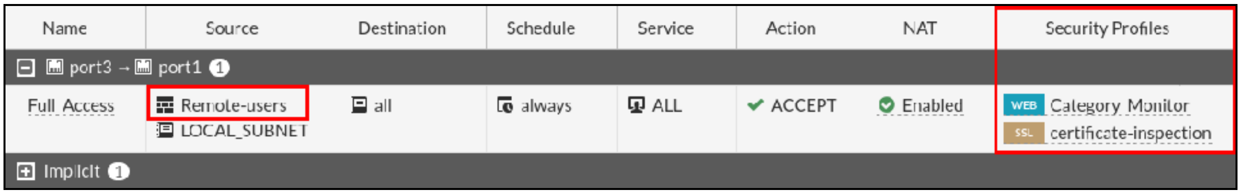
2. Configure the following setting:

Field	Value
Source	Click **+**, and then select **Remote-users** (located under **User**).

3. In the **Security Profiles** section, enable **Web Filter**, and then select **Category_Monitor**.

   This web filter was preconfigured and is set to block the following categories: **Potentially Liable**, **Adult/Mature Content**, and **Security Risk**.

4. In the **Logging Options** section, ensure **Log Allowed Traffic** is enabled, and then select **All Sessions**.
5. Click **OK**.



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
⊟ port3 → port1 1							
Full_Access	Remote-users LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	✓ Enabled	WEB Category_Monitor SSL certificate-inspection
⊞ Implicit 1							

To test whether aduser1 can successfully authenticate

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following command:

```
diagnose test authserver ldap <LDAP server name> <LDAP user name> <password>
```

   Where:

- `<LDAP server name>` is `External_Server` (case-sensitive)
- `<LDAP user name>` is `aduser1`
- `<password>` is `Training!`

A message like the following example should appear to indicate that authentication was successful:

```
Local-FortiGate # diagnose test authserver ldap External_Server aduser1 Training!
authenticate 'aduser1' against 'External_Server' succeeded!
Group membership(s) - cn=AD_users,ou=Training,dc=trainingAD,dc=training,dc=lab
```

3. Close the Local-FortiGate CLI window.

Authenticate and Monitor the Authentication

You will authenticate through the firewall policy as `aduser1`. This user is a member of the **Remote-users** group on FortiGate. Then, you will monitor the authentication.

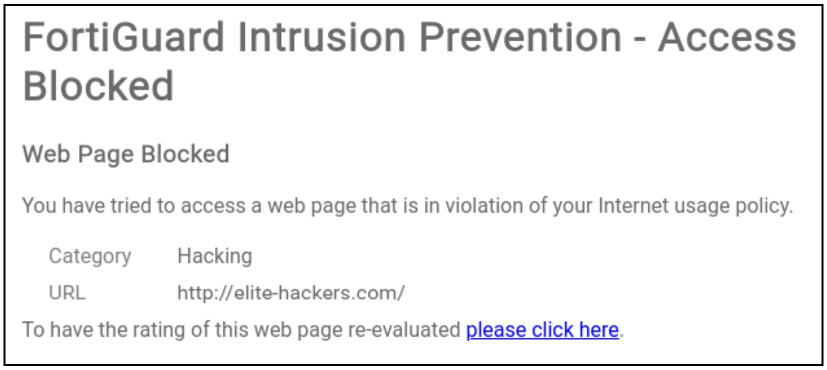
To authenticate as a remote user

1. On the Local-Client VM, open a new browser tab, and then go to `elite-hackers.com`.

   You are asked to log in to the network.

2. Log in as `aduser1` with the password `Training!`.

   This URL is set to be blocked by the web filter security profile you enabled in the firewall policy.



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page that is in violation of your Internet usage policy.

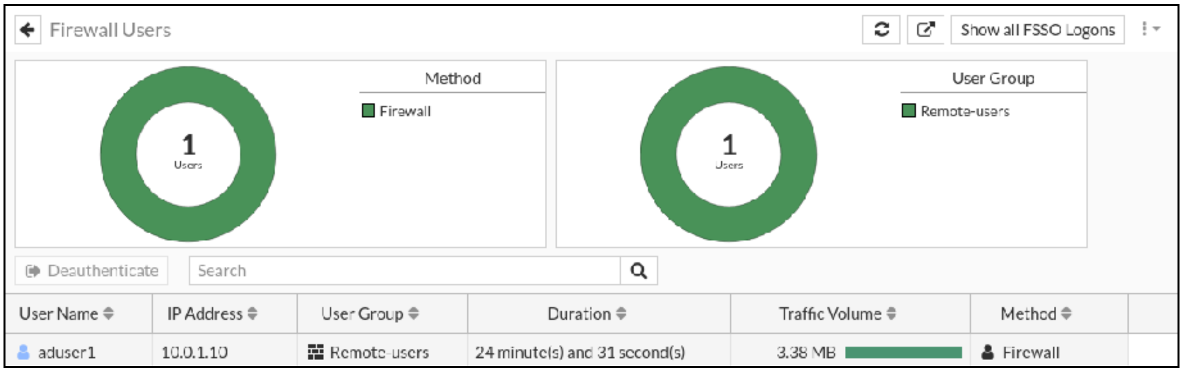
Category	Hacking
URL	http://elite-hackers.com/

To have the rating of this web page re-evaluated please click here.

Notice that the blocked page displays a replacement message that includes useful information, such as the **URL** and **Category**.

To monitor active captive portal authentications

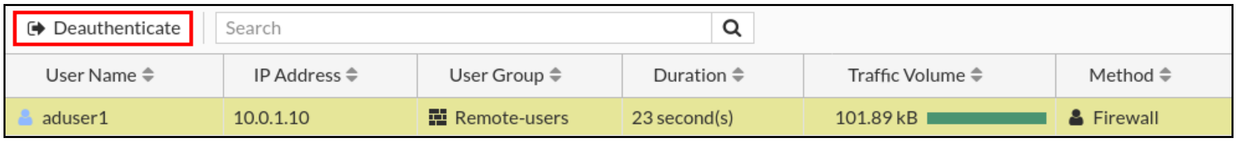
1. Return to the browser tab where you are logged in to the Local-FortiGate GUI as `admin`.
2. Monitor the firewall authenticated user. To view this login authentication, click **Dashboard** > **Users & Devices**, and then click **Firewall Users** to expand it to full screen.



User Name	IP Address	User Group	Duration	Traffic Volume	Method
aduser1	10.0.1.10	Remote-users	24 minute(s) and 31 second(s)	3.38 MB	Firewall

You will see **aduser1** listed along with other information, such as **User Group** and **IP Address**.

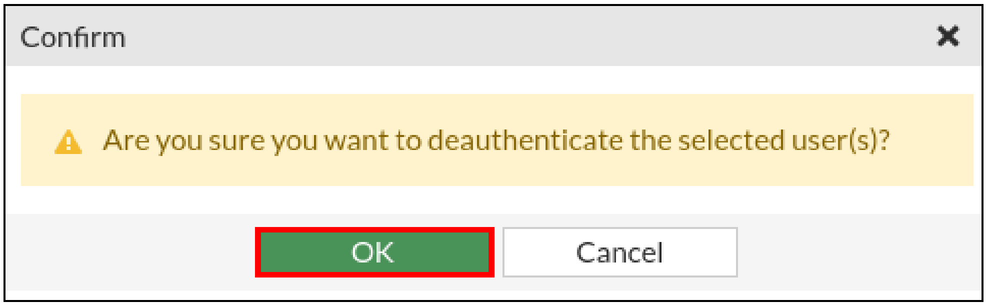
3. Click **aduser1**, and then click **Deauthenticate**.



User Name	IP Address	User Group	Duration	Traffic Volume	Method
aduser1	10.0.1.10	Remote-users	23 second(s)	101.89 kB	Firewall

While the `config user setting` CLI command determines how long a user authenticating through the captive portal can remain authenticated, you can choose to manually revoke a captive portal user authentication by selecting the user in the **Firewall User Monitor** list, and then clicking **Deauthenticate**. After the user is deauthenticated, the user disappears from the list, because it is reserved for active users only.

4. In the **Confirm** window, click **OK**.



Confirm

Are you sure you want to deauthenticate the selected user(s)?

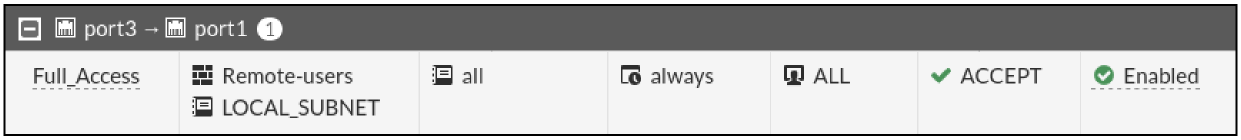
This deauthenticates the user. The user must log in again to access the resources protected by the firewall policy.

Remove the User Group From the Firewall Policy

You will remove the user group assigned to the firewall policy for authentication.

To remove the remote user group from the firewall policy

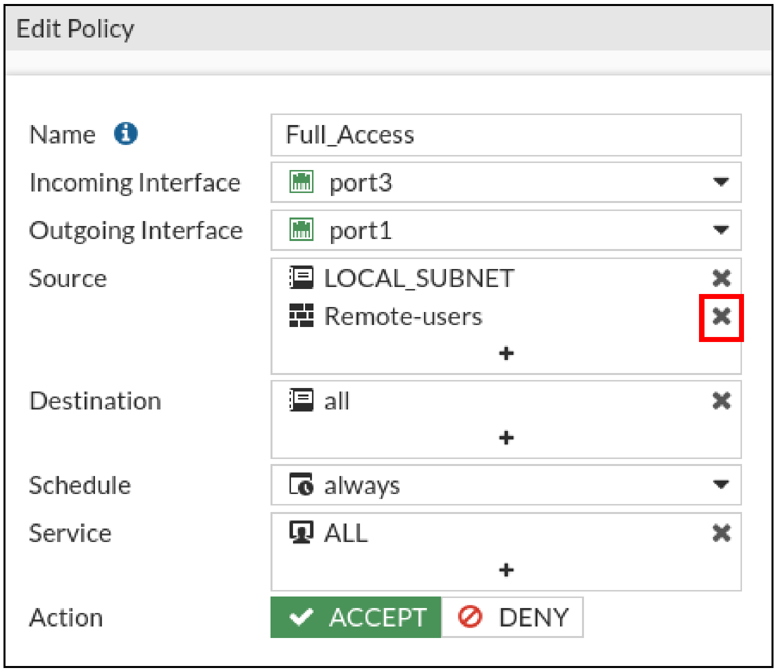
1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**, and then double-click the existing port3 to port1 firewall policy.



port3 → port1 1

Full_Access	Remote-users LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	Enabled

2. In the **Source** field, remove the **Remote-users** user group.



Edit Policy

Name: Full_Access

Incoming Interface: port3

Outgoing Interface: port1

Source: LOCAL_SUBNET ✖
Remote-users ✖
+

Destination: all ✖
+

Schedule: always

Service: ALL ✖
+

Action: ✓ ACCEPT ⊘ DENY

3. Click **Close**, and then click **OK**to save the changes.

Lab 5: Log Configuration and Monitoring

In this lab, you will configure log settings on Local-FortiGate, configure alert emails, and view logs.

Objectives

- Configure logging on FortiGate
- Configure threat weight
- Monitor logs through alert emails
- View logs on the Local-FortiGate GUI

Time to Complete

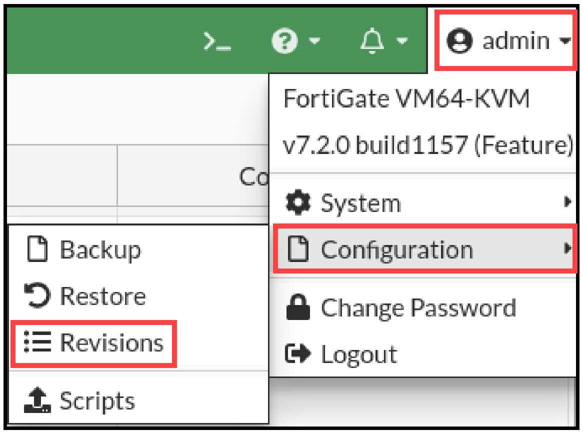
Estimated: 35 minutes

Prerequisites

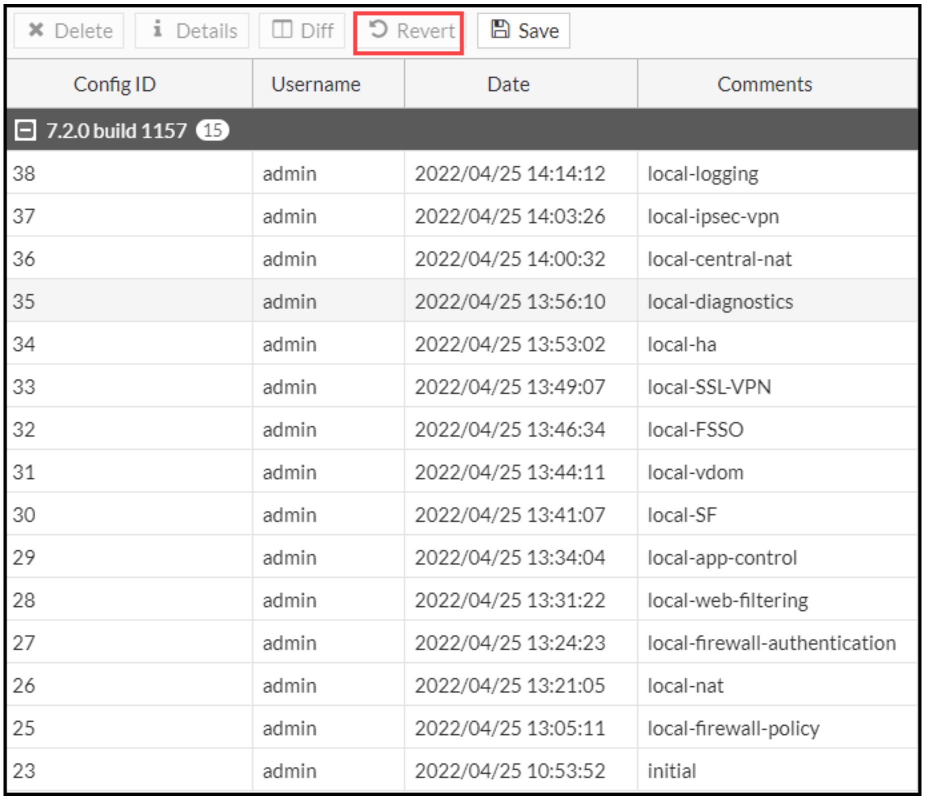
Before beginning this lab, you must restore a configuration file to Local-FortiGate. After Local-FortiGate reboots, you must check the status of your web filter license because you will use web filtering in this lab, and it must appear as licensed.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **local-logging**, and then click **Revert**.

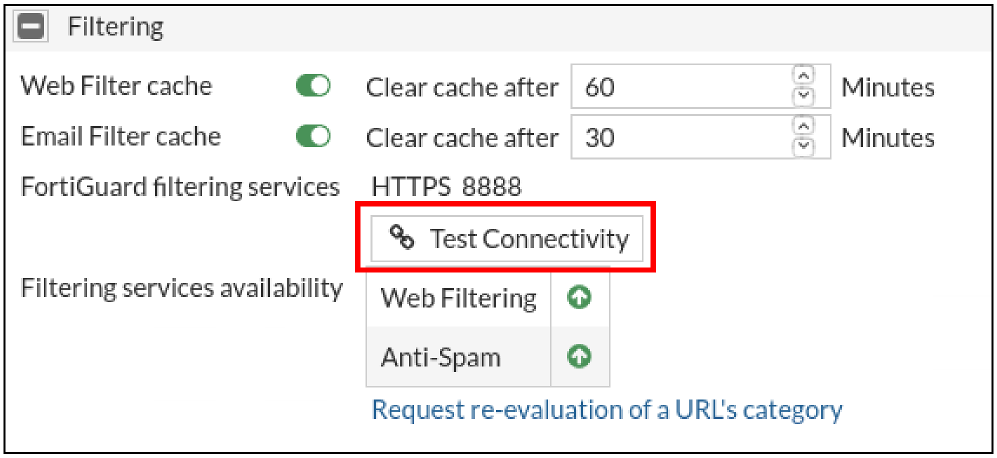


Config ID	Username	Date	Comments
⊟ 7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

To check the web filter license status after Local-FortiGate reboots

1. Continuing on the Local-FortiGate GUI with the username `admin` and password `password`.
2. Select **Dashboard** > **Status**, and then in the **Licenses** widget, verify that there is a green check mark beside **Web Filtering**, which indicates that the service is licensed and active.
3. Click **System** > **FortiGuard**.
4. Scroll to the bottom of the page, and then in the **Filtering** section, beside **FortiGuard filtering services**, click **Test Connectivity** to confirm connectivity.



Filtering

Web Filter cache ● Clear cache after 60 Minutes

Email Filter cache ● Clear cache after 30 Minutes

FortiGuard filtering services HTTPS 8888

Test Connectivity

Filtering services availability

Web Filtering	⬆
Anti-Spam	⬆

Request re-evaluation of a URL's category

5. Click **Apply** to confirm.

You should see a green up arrow beside the web filtering service, which confirms FortiGuard connectivity.

Exercise 1: Configuring Log Settings

To record network activity, you must configure logging on FortiGate. In this exercise, you will configure the log settings.

Configure Log Settings

Configuring log settings does not generate logs directly on FortiGate. Instead, log settings define if, where, and how a log is stored.

The objective of this exercise is to prepare the log settings on Local-FortiGate. For the purposes of this lab, this includes:

- Enabling disk logging, so that logs are stored locally on FortiGate
- Enabling historical FortiView, so that more than only real-time information is captured in the FortiView dashboards
- Configuring event logging for all activity, to track and monitor events that occur on FortiGate
- Disabling local traffic logging, to prevent filling up the disk too quickly with traffic going directly to and from FortiGate
- Configuring FortiGate to resolve host names, so that FortiGate performs reverse DNS lookups for all IP addresses, and makes it easier to search logs

Take the Expert Challenge!

Configure the log settings on Local-FortiGate (`10.0.1.254` | `admin` / `password`) according to the objective stated above.

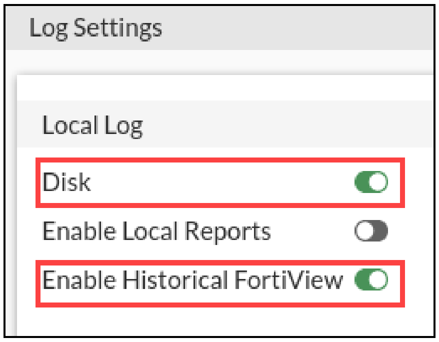
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configuring Log Settings on page 75.

To configure log settings

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Log & Report** > **Log Settings**.
3. In the **Local Log** section, enable the following settings:

Field	Value
Disk	<enable>
Enable Historical FortiView	<enable>



Log Settings

Local Log

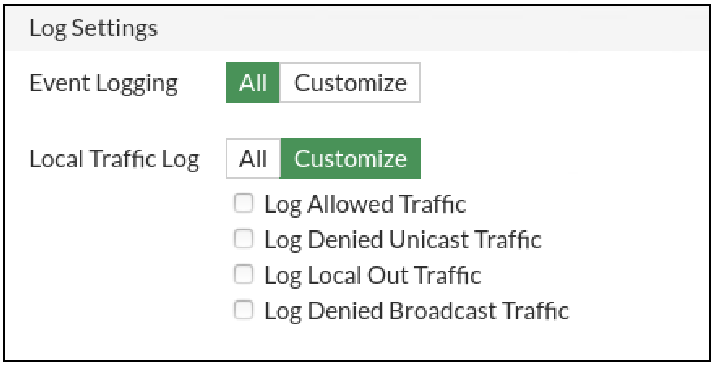
Disk ●

Enable Local Reports ○

Enable Historical FortiView ●

4. In the **Log Settings** section, make sure the following settings are configured:

Field	Value
Event Logging	All Event logs provide all the system information that FortiGate generates (they are not caused by traffic passing through firewall policies). However, it is a good practice to track and monitor events that occur on FortiGate.
Local Traffic Log	Customize—with all traffic logging checkboxes cleared These logs record traffic directly to and from FortiGate, and can fill up your disk quickly if not properly managed and monitored. For the purposes of this lab, leave all checkboxes associated with local traffic log options cleared.



Log Settings

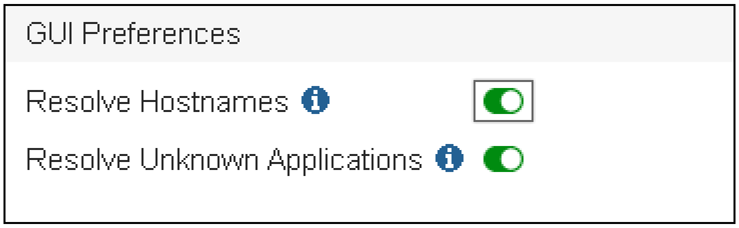
Event Logging [✓ All] Customize

Local Traffic Log All [✓ Customize]

□ Log Allowed Traffic
□ Log Denied Unicast Traffic
□ Log Local Out Traffic
□ Log Denied Broadcast Traffic

5. In the **GUI Preferences** section, configure the following settings:

Field	Value
Resolve Hostnames	<enable> Resolving hostnames requires FortiGate to perform reverse DNS lookups for all IP addresses, and makes it easier to search the logs.



GUI Preferences

Resolve Hostnames ● On

Resolve Unknown Applications ● On

6. Click **Apply**.

Configure Threat Weight

To prioritize solving the most relevant issues easily, you can configure severity levels for IPS signatures, web categories, and applications that are associated with a threat weight (or score). Threat weight allows you to set the risk values for low, medium, high, and critical levels, and then apply a threat weight to specific categories.

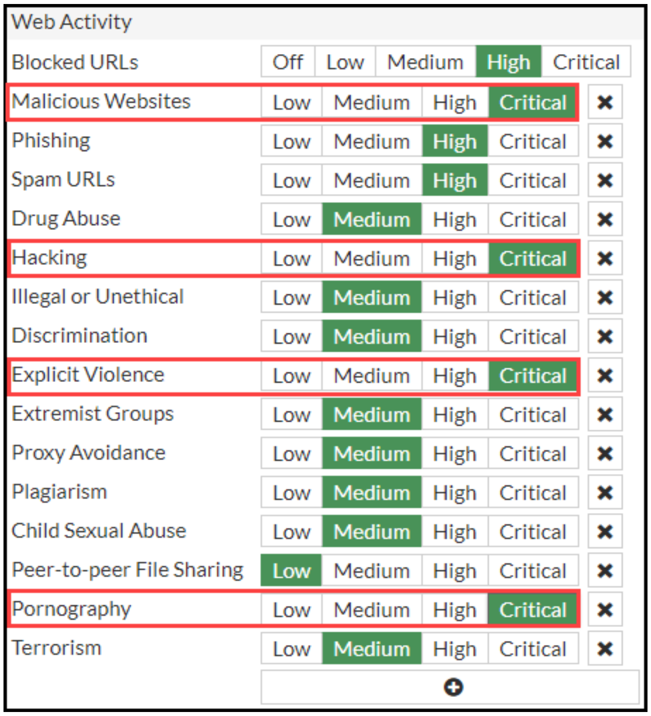
The objective of this task is to set the following categories to a critical status:

- **Malicious Websites**
- **Hacking**
- **Explicit Violence**
- **Pornography**

You will use threat weight later, when you search for logs at a specific threat weight.

To configure threat weight

1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Threat Weight**.
2. In the **Web Activity** section, select the **Critical** option for the following categories:



Web Activity

Blocked URLs	Off	Low	Medium	[✓ High]	Critical	
Malicious Websites		Low	Medium	High	[✓ Critical]	✖
Phishing		Low	Medium	[✓ High]	Critical	✖
Spam URLs		Low	Medium	[✓ High]	Critical	✖
Drug Abuse		Low	[✓ Medium]	High	Critical	✖
Hacking		Low	Medium	High	[✓ Critical]	✖
Illegal or Unethical		Low	[✓ Medium]	High	Critical	✖
Discrimination		Low	[✓ Medium]	High	Critical	✖
Explicit Violence		Low	Medium	High	[✓ Critical]	✖
Extremist Groups		Low	[✓ Medium]	High	Critical	✖
Proxy Avoidance		Low	[✓ Medium]	High	Critical	✖
Plagiarism		Low	[✓ Medium]	High	Critical	✖
Child Sexual Abuse		Low	[✓ Medium]	High	Critical	✖
Peer-to-peer File Sharing		[✓ Low]	Medium	High	Critical	✖
Pornography		Low	Medium	High	[✓ Critical]	✖
Terrorism		Low	[✓ Medium]	High	Critical	✖

3. In the **Risk Level Values** section, record the value associated with the **Critical** risk level.

   You will use this information later to search for logs, using the risk level value as a filter.

Risk level	Value
Critical	

4. Click **Apply**.

Exercise 2: Enabling Logging on Firewall Policies

Now that you defined if, where, and how a log is stored using the FortiGate log settings, you must define whether logs are generated. To accomplish this, you must enable logging on your firewall policy. A log message can generate only when logging is enabled on a firewall policy.

Enable Logging on a Firewall Policy

For the purposes of this lab, two firewall policies were created for you. However, you must now configure these firewall policies for logging.

The two firewall policies are:

- **IPS**: You will use this firewall policy to capture IPS traffic.
- **Full Access**: You will use this firewall policy to capture antivirus, web filter, DNS, and application control traffic.

Take the Expert Challenge!

On the Local-FortiGate GUI (`10.0.1.254` | `admin`/`password`), configure logging for *all sessions* on both the **IPS** and **Full Access** firewall policies. Enable the following security profiles:

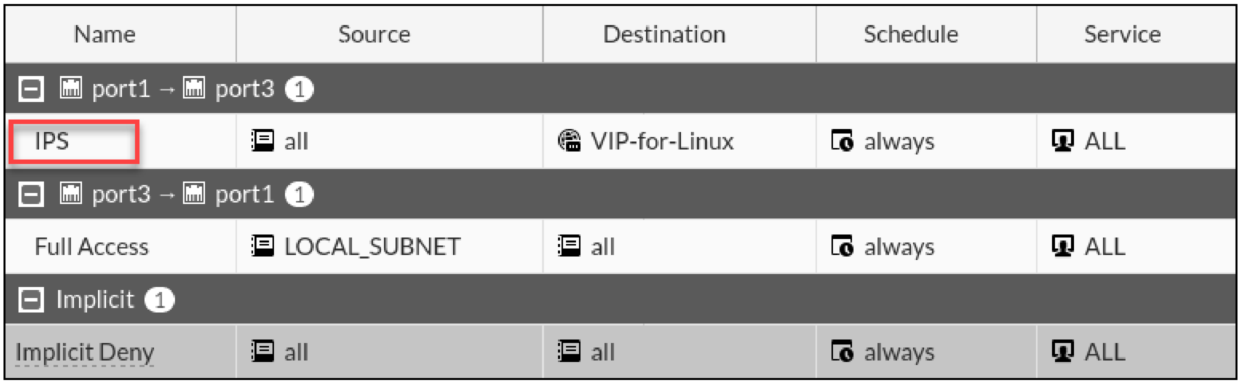
- IPS
    - IPS | default
    - SSL Inspection | certificate-inspection
- Full Access
    - AntiVirus | default
    - Web Filter | Category-block-and-warning
    - DNS Filter | default
    - Application Control | block-high-risk
    - SSL Inspection | certificate-inspection

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Monitoring Logs Through Email Alerts on page 82.

To enable logging on the IPS firewall policy

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Firewall Policy**, and then edit the **IPS** firewall policy.



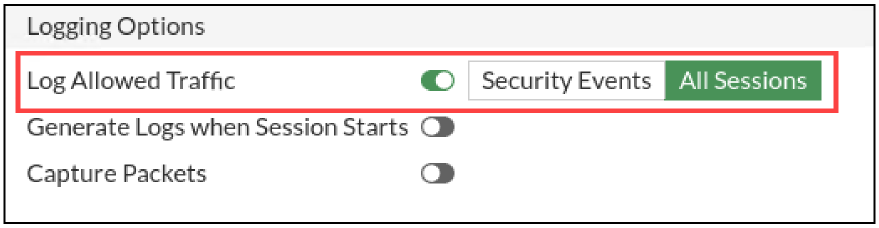
Name	Source	Destination	Schedule	Service
⊟ port1 → port3 1				
IPS	all	VIP-for-Linux	always	ALL
⊟ port3 → port1 1				
Full Access	LOCAL_SUBNET	all	always	ALL
⊟ Implicit 1				
Implicit Deny	all	all	always	ALL

3. In the **Security Profiles** section, configure the following settings:

Security profiles	Profile
IPS	default
SSL Inspection	certificate-inspection

4. In the **Logging Options** section, enable **Log Allowed Traffic**, and then select **All Sessions**.

   Remember, you will not receive any logs if **Log Allowed Traffic** is not enabled.



Logging Options

Log Allowed Traffic ● Security Events [✓ All Sessions]

Generate Logs when Session Starts ○

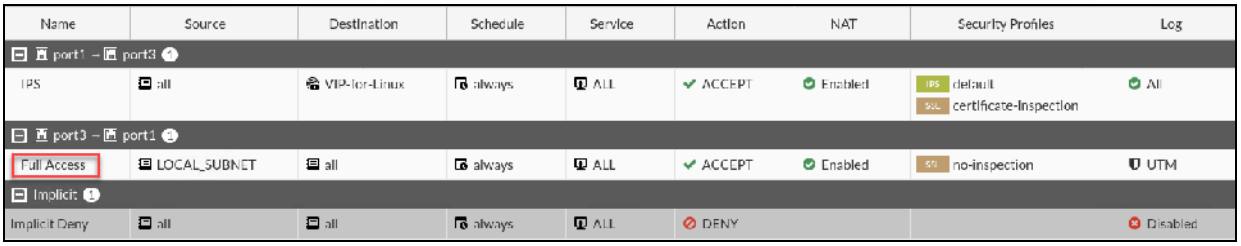
Capture Packets ○

5. Click **OK**.

   You successfully enabled logging on your firewall policy. Later in this lab, you will test these log settings.

To enable logging on the Full Access firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**, and then edit the **Full Access** firewall policy.



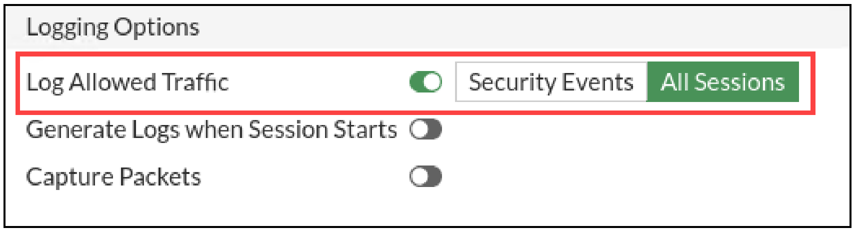
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
⊟ port1 → port3 1								
IPS	all	VIP-for-Linux	always	ALL	✓ ACCEPT	Enabled	IPS default SSL certificate-inspection	All
⊟ port3 → port1 1								
Full Access	LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM
⊟ Implicit 1								
Implicit Deny	all	all	always	ALL	⊘ DENY			Disabled

2. In the **Security Profiles** section, configure the following settings:

Security profiles	Profile
AntiVirus	default
Web Filter	Category-block-and-warning
DNS Filter	default
Application Control	block-high-risk
SSL Inspection	certificate-inspection

3. In the **Logging Options** section, enable **Log Allowed Traffic**, and then select **All Sessions**.

   Remember, you will not receive any logs if **Log Allowed Traffic** is not enabled.



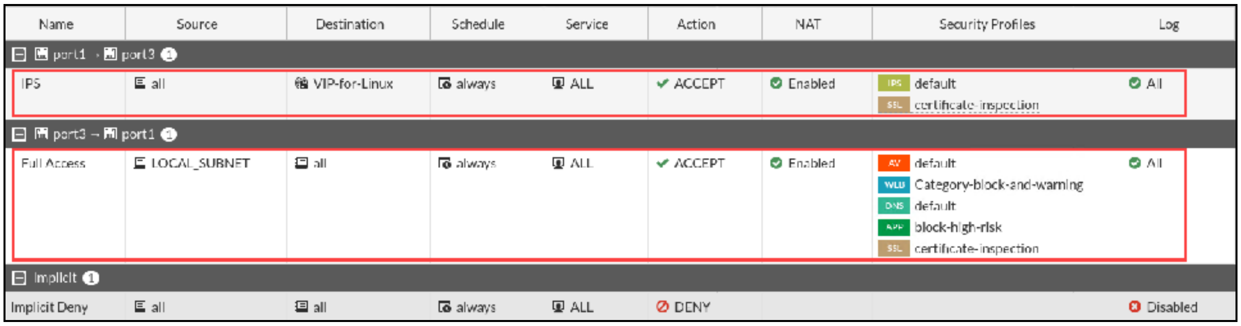
Logging Options

Log Allowed Traffic: enabled — Security Events | **All Sessions**

Generate Logs when Session Starts: disabled

Capture Packets: disabled

4. Click **OK**.



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
port1 → port3 ❶								
IPS	all	VIP-for-Linux	always	ALL	✓ ACCEPT	Enabled	IPS default SSL certificate-inspection	All
port3 → port1 ❶								
Full Access	LOCAL_SUBNET	all	always	ALL	✓ ACCEPT	Enabled	AV default WEB Category-block-and-warning DNS default APP block-high-risk SSL certificate-inspection	All
Implicit ❶								
Implicit Deny	all	all	always	ALL	DENY			Disabled

You successfully enabled logging on your firewall policy. Later in this lab, you will test these log settings.

Exercise 3: Monitoring Logs Through Email Alerts

In this exercise, you will configure email alerts, run some traffic through Local-FortiGate, and then view the email alerts.

Configure Email Alerts

Because you can't always be physically at the FortiGate, you can monitor events by setting up email alerts. Email alerts provide an efficient and direct method of notifying an administrator of events.

An SMTP mail server is required for email alerts to operate. Because configuring a mail server is out of scope for this lab, one was configured for you. You can view the email service configuration on the Local-FortiGate GUI by clicking **System** > **Settings**, and then scrolling down to the **Email Service** configuration.

To configure email alerts

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following CLI commands:

```
config alertemail setting
   set username FortiGate@training.lab
   set mailto1 admin@training.lab
   set email-interval 1
   set IPS-logs enable
   set webfilter-logs enable
end
```

3. Close the Local-FortiGate CLI window.

Generate Traffic

For the purposes of this lab, you must generate traffic so you can see the logs that FortiGate collects.

The traffic you generate will go through Local-FortiGate. You already enabled the security policy on the IPS firewall policy and logging for all sessions.

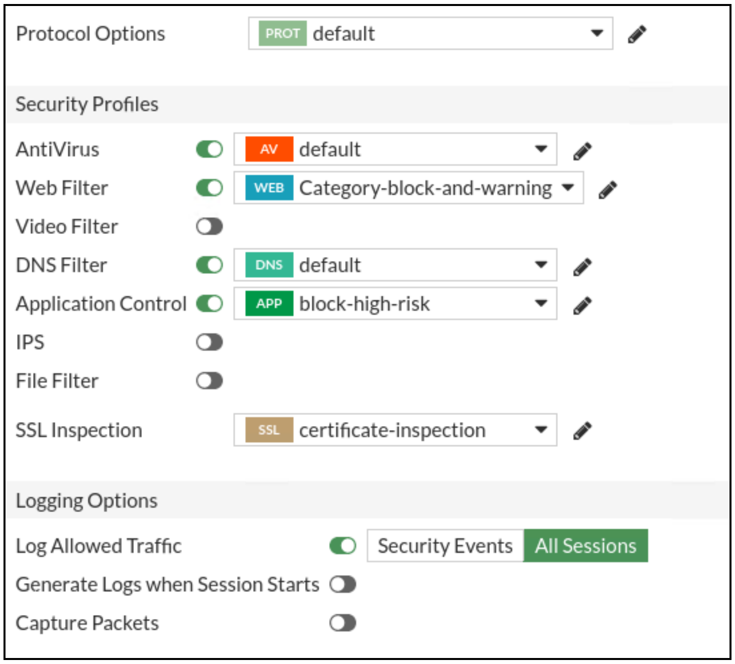
You will use two different tools to create different types of traffic.

Generate Traffic Through FIT

The firewall inspection tester (FIT) program on the FIT VM generates web browsing traffic, application control, botnet IP hits, malware URLs, and malware downloads.

In this lab, you will direct the traffic that FIT generates through Local-FortiGate. The FIT is behind port3 on Local-FortiGate. The traffic from FIT will go through the **Full Access** firewall policy. For more information, see Network Topology on page 8.

You configured the **Full Access** firewall policy to include the following security policies and logging options:



Protocol Options: PROT default

Security Profiles

AntiVirus: on, AV default

Web Filter: on, WEB Category-block-and-warning

Video Filter: off

DNS Filter: on, DNS default

Application Control: on, APP block-high-risk

IPS: off

File Filter: off

SSL Inspection: SSL certificate-inspection

Logging Options

Log Allowed Traffic: on, Security Events | All Sessions (All Sessions selected)

Generate Logs when Session Starts: off

Capture Packets: off

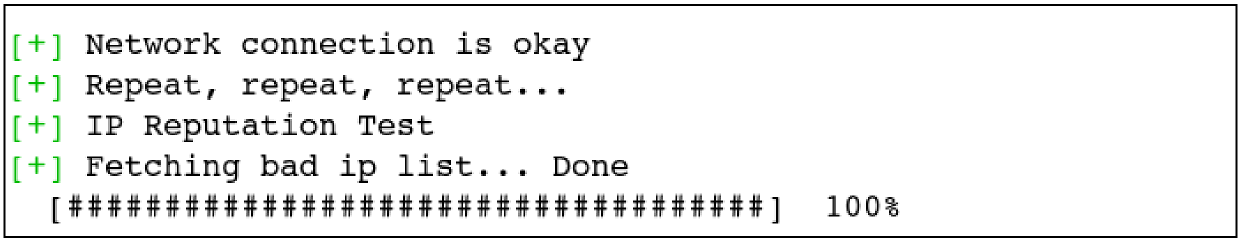
Because the traffic that FIT generates originates from the IP address of the FIT VM (`10.0.1.20`), all these logs show the same source IP address. This is a limitation of the lab environment. In a real-world scenario, there will likely be many different source IP addresses for your traffic.

To generate traffic through FIT

1. Continuing on the Local-Client VM, open PuTTY, and then connect over SSH to the FIT saved session.
2. Log in with the username `student` and password `password`.
3. Enter the following commands:

```
cd FIT
./fit.py all --repeat
```

   Traffic begins to generate and repeats the script each time it completes.



```
[+] Network connection is okay
[+] Repeat, repeat, repeat...
[+] IP Reputation Test
[+] Fetching bad ip list... Done
  [#####################################]  100%
```

4. Leave the PuTTY session open (you can minimize it) so traffic continues to generate.

This will run for the remainder of this lab.

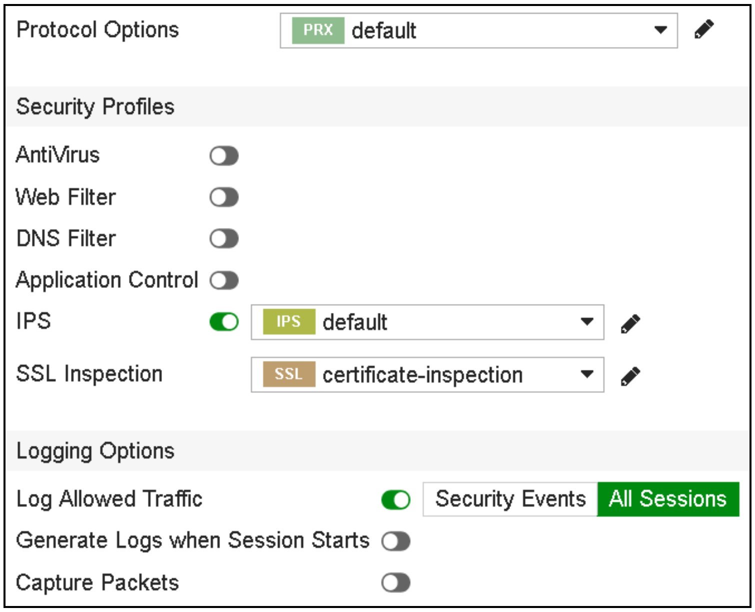
Do not close the FIT PuTTY session or traffic will stop generating.

Generate Traffic Through Nikto

Nikto generates intrusion prevention system (IPS) traffic.

You will direct the traffic that Nikto generates through Local-FortiGate. Nitko is running on the Linux VM, and the traffic will go through the egress-to-ingress firewall policy named **IPS**. For more information, see Network Topology on page 8.

You configured the **IPS** firewall policy to include the following security policy and logging options:



Protocol Options: PRX default

Security Profiles

AntiVirus ○

Web Filter ○

DNS Filter ○

Application Control ○

IPS ● IPS default

SSL Inspection: SSL certificate-inspection

Logging Options

Log Allowed Traffic ● Security Events [✓ All Sessions]

Generate Logs when Session Starts ○

Capture Packets ○

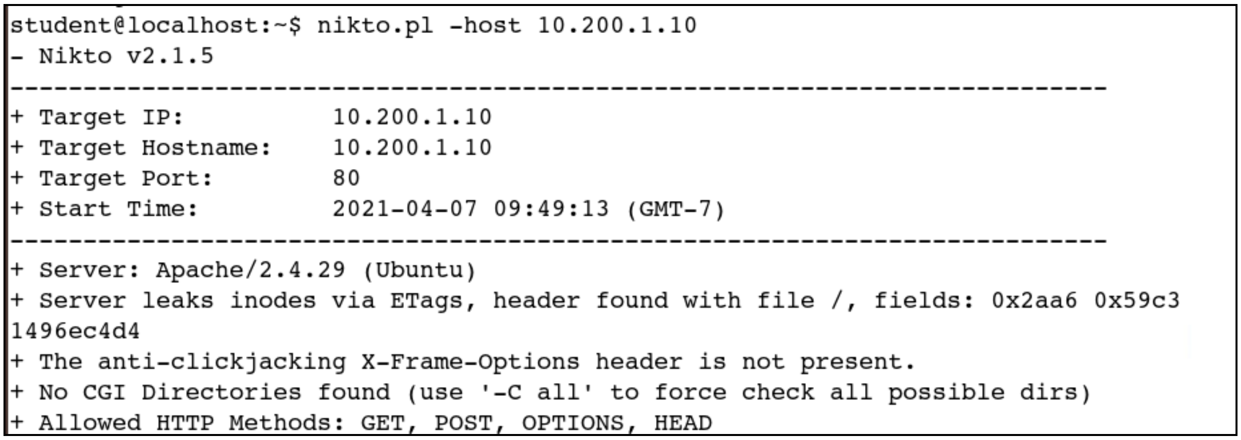
Because the traffic that Nikto generates originates from the IP address of the Linux VM where Nikto is installed (`10.200.1.254`), all these logs show the same source IP address. This is a limitation of the lab environment. In a real-world scenario, there will likely be many different source IP addresses for your traffic.

To generate traffic through Nikto

1. Continuing on the Local-Client VM, open a second PuTTY session, and then connect over SSH to the LINUX saved session.
2. Log in with the username `student` and password `password`.
3. Enter the following command:

   ```
   nikto.pl -host 10.200.1.10
   ```

   The vulnerability scanning results in traffic beginning to generate.



```
student@localhost:~$ nikto.pl -host 10.200.1.10
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.200.1.10
+ Target Hostname:    10.200.1.10
+ Target Port:        80
+ Start Time:         2021-04-07 09:49:13 (GMT-7)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x2aa6 0x59c3
1496ec4d4
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
```

The scan will continue for a while.

4. Leave the PuTTY session open (you can minimize it) so traffic continues to generate.

   This will run for the remainder of the lab.

Do not close the LINUX PuTTY session or traffic will stop generating.

View Email Alerts

Now that traffic is being sent through FortiGate, you can check the admin@training.lab email to see if any alerts were generated based on that traffic. You configured the email alert to generate an alert every minute when an intrusion is detected by the IPS security profile on the **IPS** firewall policy, and when the web filter security profile blocks traffic on the **Full Access** firewall policy.

The log message that accompanies an alert provides more details about the traffic that caused the alert.

To view email alerts

1. Continuing on Local-Client, on the desktop, open Mozilla Thunderbird.

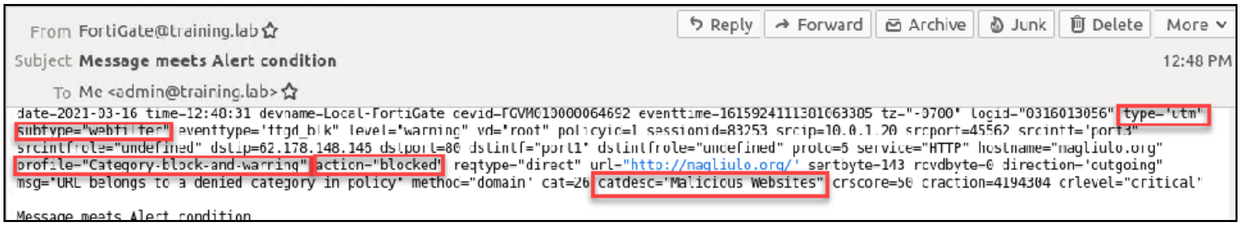
2. Select the inbox of the admin@training.lab email account, and then click **Get Messages**.

   You should see a message in the admin inbox with a subject of "Message meets Alert condition". If no email appears in the inbox, wait 30 seconds, and then click **Get Messages** again.

3. Open any email alert, and then review the log message.

   As you can see, the log message is in raw format. In the web filter example below (you may receive a different log message), the log message header provides the `type` (`utm`) and `subtype` (`webfilter`). The log message body provides information about the web filter security profile that was applied to the traffic

(`Category-block-and-warning`), the action it took (`blocked`), and the category description of the traffic (`Malicious Websites`).



From ForliGate@training.lab ☆
Subject **Message meets Alert condition**
To Me <admin@training.lab> ☆
12:48 PM

```
date-2021-03-16 time-12:40:31 devname-Local-FortiGate cevid-FGVM010000064692 eventtime-1615924111301063305 tz-"-0700" logid-"0316013056" type-'utm'
subtype="webfilter" eventtype='ftgd_blk" level='warning" vd='root" policyid=1 sessionid=83253 srcip=10.0.1.20 srcport=45562 srcintf='port3"
srcintfrole="undefined" dstip=62.178.148.145 dstport=80 dstintf="port1' dstintfrole="undefined" proto=6 service="HTTP" hostname="nagliulo.org"
profile-"Category-block-and-warning" action-"blocked" reqtype-"direct" url-"http://nagliulo.org/' sentbyte-143 rcvdbyte-0 direction-'outgoing"
msg='URL belongs to a denied category in policy' method="domain' cat=26 catdesc='Malicious Websites" crscore=50 craction=4194304 crlevel="critical'

Message meets Alert condition
```

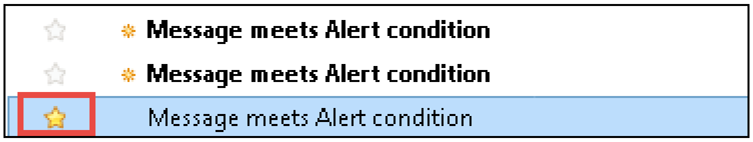
4. Open another email alert, and then record the following information from a single *web filter* log:

Field	Value
date	
time	
logid	
subtype	
level	
sessionid	
profile	
catdesc	
crscore	

You will locate this log on the Local-FortiGate GUI in the next exercise.

5. Select the email of the log you recorded by clicking the star icon to the left of the email subject.

The star icon turns yellow.



☆ ✱ **Message meets Alert condition**
☆ ✱ **Message meets Alert condition**
★ Message meets Alert condition

If you want to review more email alerts, click **Get Messages** in your admin inbox again. You configured your email alert to send messages that meet the alert condition every one minute.

6. When you are finished, close the Thunderbird email client.

Exercise 4: Viewing Logs on the FortiGate GUI

In this exercise, you will view logs using both the **Log & Report** and **FortiView** menus on the Local-FortiGate GUI. You will also configure filter options to locate specific logs.

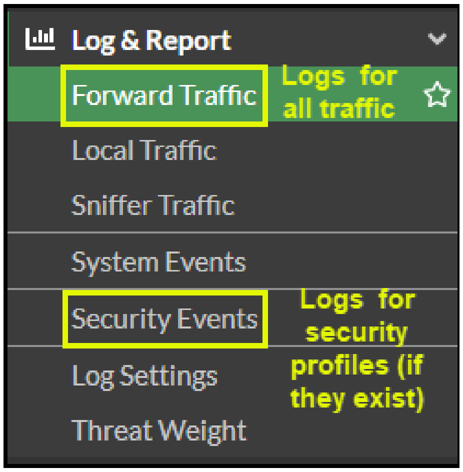
View Logs From the Log & Report Menu

You will examine the logs, on the Local-FortiGate GUI, that are based on the traffic you generated from the FIT VM and Nikto.

View Forward Traffic Logs

The first place you will examine logs is on the **Forward Traffic** page.

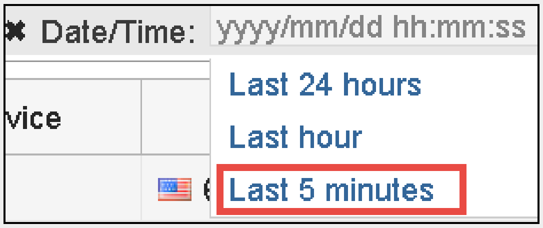
All logs that are related to security profiles are tracked in the forward traffic logs, so you can search all forward traffic in one place. This is helpful if you are looking to see all activity from a specific address, security feature, or traffic. Security profile logs are still tracked separately in the GUI, but only appear when logs exist.



To view and filter forward traffic logs

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Log & Report** > **Forward Traffic**.
3. To narrow down the logs (results), on the search bar, click **Add Filter**, and then add some filters.

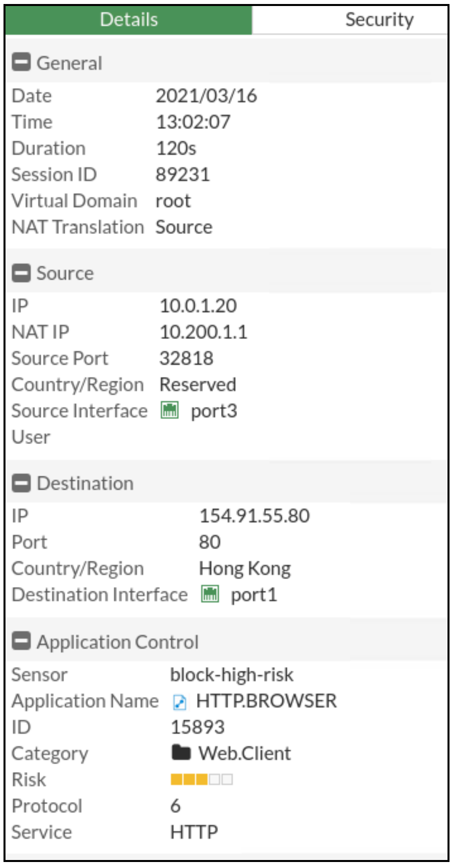
   The following table shows some example filters:

Filter	Value
Date/Time	Last 5 minutes This filters on all logs from the last 5 minutes.  ✖ Date/Time: yyyy/mm/dd hh:mm:ss vice Last 24 hours Last hour Last 5 minutes
Result	Deny (all) This filters on all blocked traffic.
Threat Score	>=50 This filters on all web activity greater than or equal to the critical (50) risk level. Remember, you set **Malicious Websites**, **Hacking**, **Explicit Violence**, and **Pornography** to the critical risk level.

If the information that you are filtering on does not appear in the table, you may need to add the related column to the table. To do so, right-click any column in the table, and then select the column you want to add. For example, to view the **Threat Score** column, add **Threat Score**. At the bottom of the list, click **Apply** to refresh the table with the new column.

4. Double-click the log you want to view.

   The **Log Details** pane appears on the right side of the page.



Details	Security
General	
Date	2021/03/16
Time	13:02:07
Duration	120s
Session ID	89231
Virtual Domain	root
NAT Translation	Source
Source	
IP	10.0.1.20
NAT IP	10.200.1.1
Source Port	32818
Country/Region	Reserved
Source Interface	port3
User	
Destination	
IP	154.91.55.80
Port	80
Country/Region	Hong Kong
Destination Interface	port1
Application Control	
Sensor	block-high-risk
Application Name	HTTP.BROWSER
ID	15893
Category	Web.Client
Risk	■■■□□
Protocol	6
Service	HTTP

5. View both the **Details** and **Security** tabs to see the information that is available.

View Security Profile Logs

You will examine the security profile logs, which are tracked separately on the GUI. The menu item for the specific security profile only appears on the GUI if logs of that type exist.

To view web filter logs

1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Security Events** > **Web Filter**.

If this menu item does not display, you can refresh the page, or log out of the Local-FortiGate GUI and log in again.

2. Use log filters to locate the log in the email alert that you recorded in Monitoring Logs Through Email Alerts on page 82.

Stop and think!

Which filter would best return the specific log you are seeking? For example, filters based on log subtype or crscore will most likely return too many logs, which makes the search inefficient.

Answer: **Session ID**.

3. After you locate the log, double-click the entry to view the log details.

   As you can see, the log details in the alert email are the same as the log details on the GUI. The only difference is the format—alert emails provide the log detail information in raw format, while the GUI provides the log detail information in a formatted view.

View and Filter IPS Logs

You will view and filter IPS logs.

Take the Expert Challenge!

On the Local-FortiGate GUI (`10.0.1.254`), complete the following:

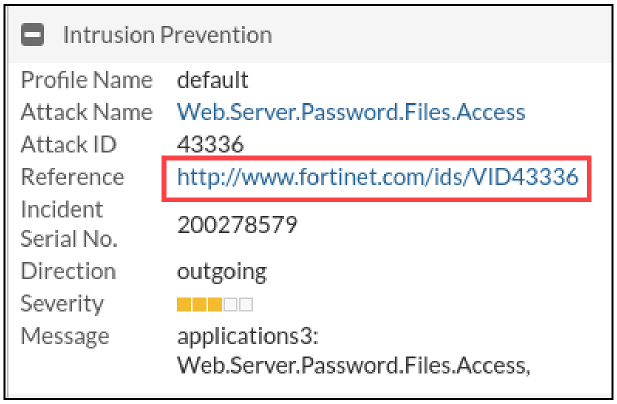
- View the GUI page that shows intrusion prevention logs only.
- Double-click any IPS log to view more information about an attack.
- View the attack information on FortiGuard.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Viewing Logs on the FortiGate GUI on page 87.

To view and filter IPS logs

1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Security Events** > **Intrusion Prevention**.
2. Double-click any IPS log to view more information about an attack.
3. In the **Log Details** pane, under **Intrusion Prevention**, click the reference link.



Intrusion Prevention

Profile Name	default
Attack Name	Web.Server.Password.Files.Access
Attack ID	43336
Reference	http://www.fortinet.com/ids/VID43336
Incident Serial No.	200278579
Direction	outgoing
Severity	■■■□□
Message	applications3: Web.Server.Password.Files.Access,

   This takes you to the FortiGuard website, where you can gather more information about the specific attack, such as the description of the attack, affected products, impact, and recommended actions.

4. After you finish, close the FortiGuard tab.

View Logs in FortiView

FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view on FortiGate.

You will view the logs in FortiView.

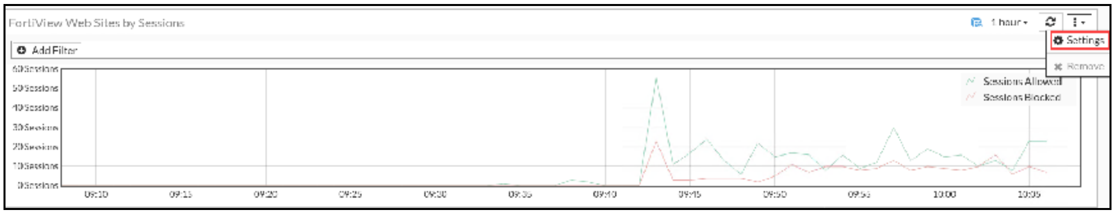
To view logs in FortiView

1. Continuing on the Local-FortiGate GUI, click **Dashboard** > **FortiView Web Sites**.

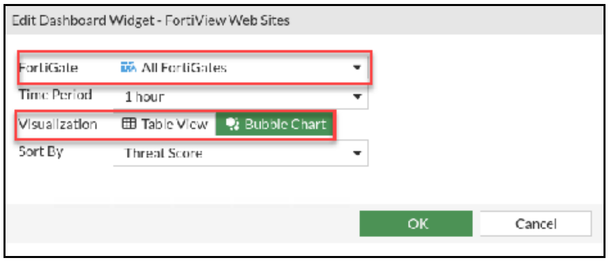
   By default, the search settings are set to display logs that are currently being created. If no logs are being created currently, the page is blank—this is expected.

2. Use the search settings to display the web activity in a different way, for example, you can do the following:

   - Click **Settings**.



   - In the **FortiGate** field, select **All FortiGates**, and then in the **Visualization** field, click **Bubble Chart**.



Edit Dashboard Widget - FortiView Web Sites

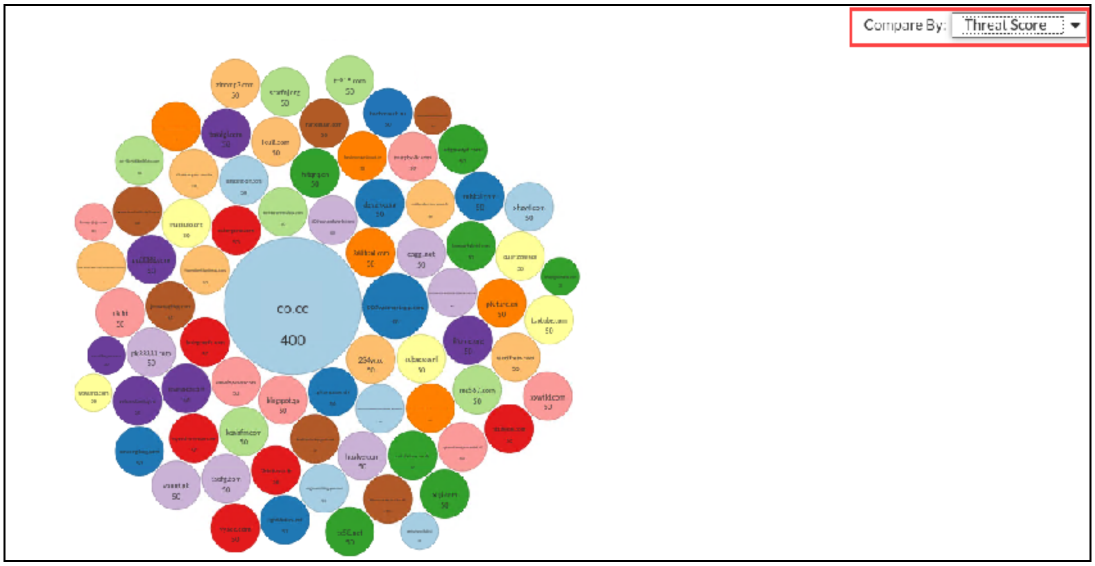
FortiGate: All FortiGates

Time Period: 1 hour

Visualization: Table View | Bubble Chart

Sort By: Threat Score

   - Use the **Sort By** drop-down menu to display the information by **Threat Score**, **Sessions**, **Browsing Time**, or **Bytes**.



Close both the FIT and LINUX PuTTY sessions to stop log generation.

Lab 6: Certificate Operations

In this lab, you will configure full SSL inspection using a self-signed SSL certificate on FortiGate to inspect outbound traffic. You will also import a web server certificate on FortiGate and configure inbound SSL inspection.

Objectives

- Configure and enable full SSL inspection on outbound traffic
- Import an external web server certificate
- Configure and enable full SSL inspection on inbound traffic

Time to Complete

Estimated: 40 minutes

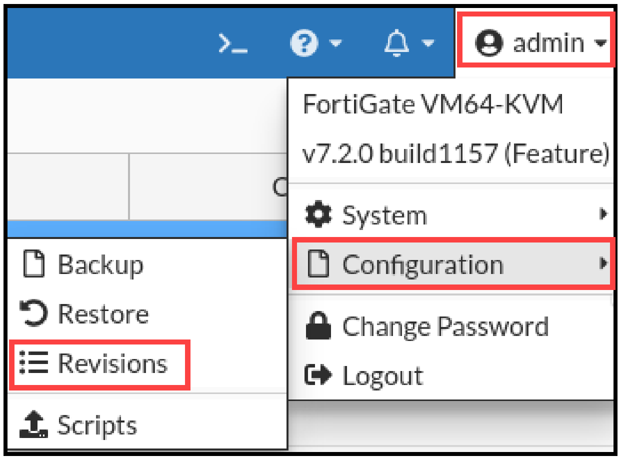
Prerequisites

Before beginning this lab, you must restore a configuration file on each FortiGate.

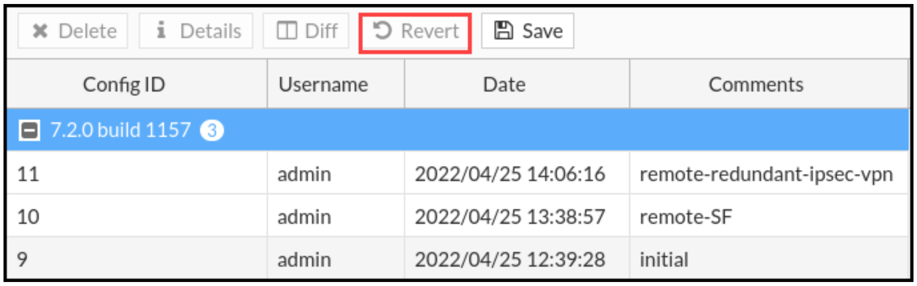
Make sure that you restore the correct configuration on each FortiGate, using the following steps. Failure to restore the correct configuration on each FortiGate will prevent you from doing the lab exercises.

To restore the Remote-FortiGate configuration file

1. Connect to the Remote-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.

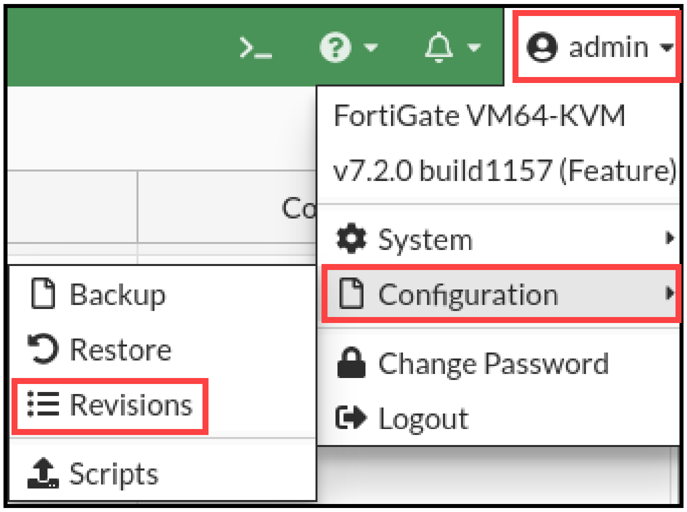


Config ID	Username	Date	Comments
7.2.0 build 1157 3			
11	admin	2022/04/25 14:06:16	remote-redundant-ipsec-vpn
10	admin	2022/04/25 13:38:57	remote-SF
9	admin	2022/04/25 12:39:28	initial

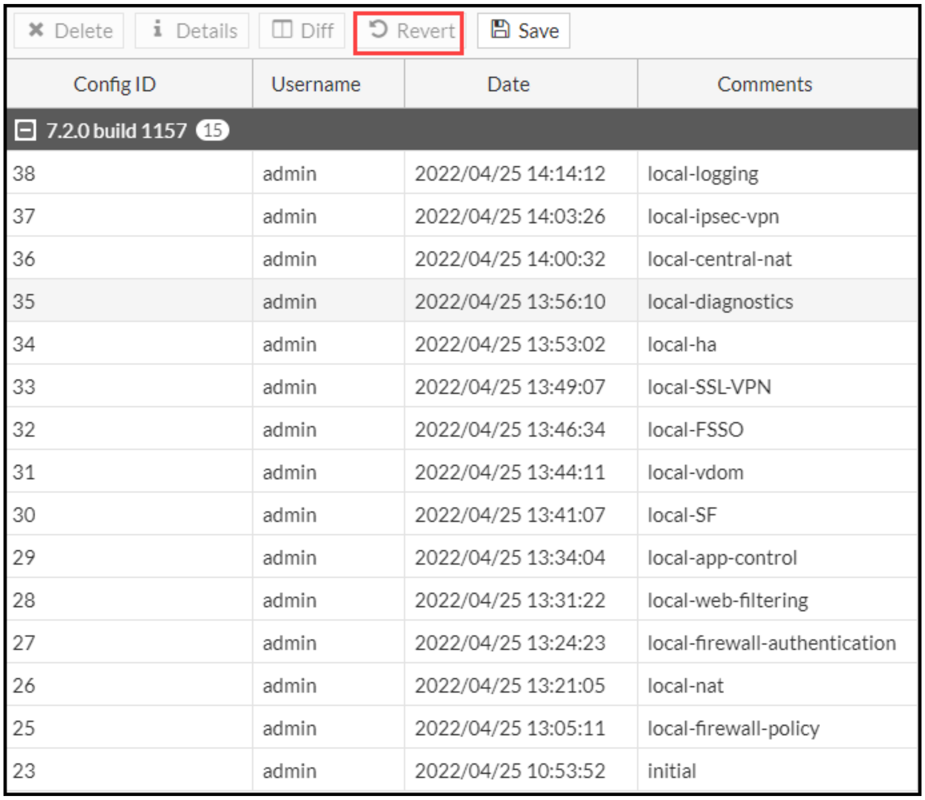
5. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.



Config ID	Username	Date	Comments
⊟ 7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

Exercise 1: Configuring Full SSL Inspection on Outbound Traffic

Full SSL inspection on outbound traffic allows FortiGate to inspect encrypted internet-bound traffic and apply security profiles to that traffic to protect your network and end users. FortiGate employs a man-in-the-middle (MITM) attack to inspect the traffic and apply security profiles, such as antivirus, web filter, and application control.

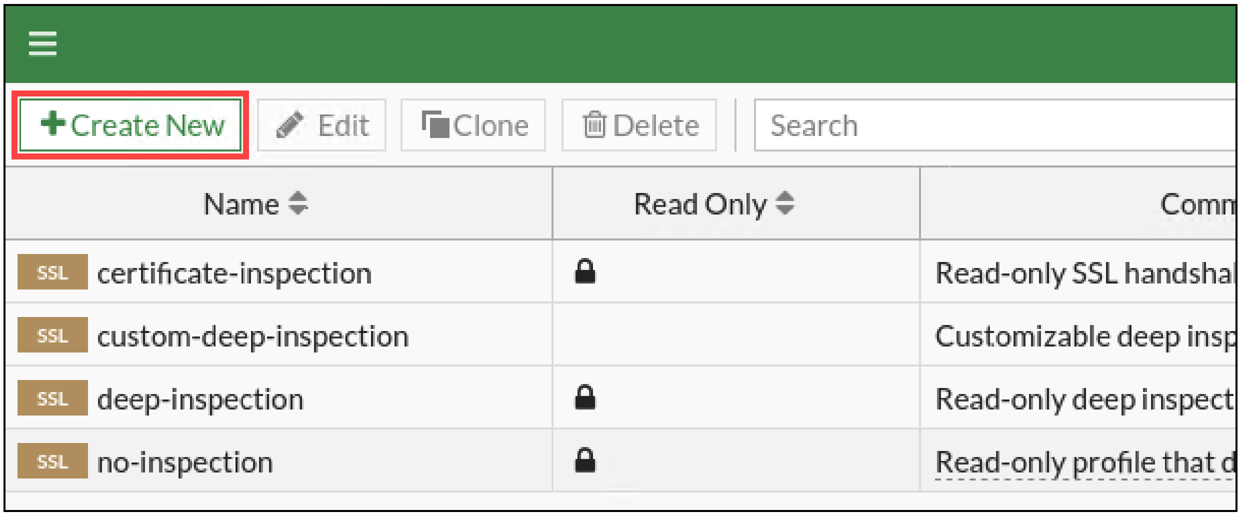
In this exercise, you will configure and enable full SSL inspection on all outbound traffic.

Configure SSL Inspection

By default, FortiGate includes four security profiles for SSL/SSH inspection: **certificate-inspection**, **custom-deep-inspection**, **deep-inspection**, and **no-inspection**. You can modify the settings for the **custom-deep-inspection** profile only. The other profiles are read-only. Because this exercise involves configuring full SSL inspection on FortiGate, you will configure a new SSL/SSH inspection profile for this purpose.

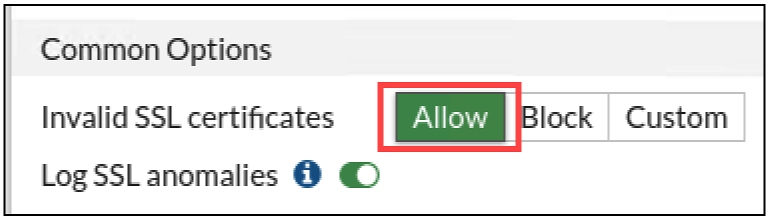
To configure SSL inspection

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Security Profiles** > **SSL/SSH Inspection**.
3. In the upper-left corner, click **Create New** to create a new profile.



Name	Read Only	Comm
SSL certificate-inspection	🔒	Read-only SSL handshal
SSL custom-deep-inspection		Customizable deep insp
SSL deep-inspection	🔒	Read-only deep inspect
SSL no-inspection	🔒	Read-only profile that d

4. In the **Name** field, type `Custom_Full_Inspection`.
5. At the bottom of the page, in the **Common Options** section, in the **Invalid SSL certificates** field, click **Allow**.



Common Options

Invalid SSL certificates: Allow | Block | Custom

Log SSL anomalies

6. Click **OK**.

Enable SSL Inspection on a Firewall Policy

You must enable SSL inspection on a firewall policy to start inspecting SSL traffic. However, you cannot enable SSL inspection by itself. You must enable one or more additional security profiles in the firewall policy. When you enable SSL inspection, this configures how you want FortiGate to handle encrypted traffic, and then you must configure which traffic you want FortiGate to inspect. For the purposes of this lab, you will enable the default web filter security profile.

To enable SSL inspection on a firewall policy

1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Double-click the **Full_Access** firewall policy to edit it.
3. In the **Security Profiles** section, enable the following security profiles:

Security Profile	Value
Web Filter	default
SSL Inspection	Custom_Full_Inspection This is the profile you created previously.

4. In the **Logging Options** section, enable **Log Allowed Traffic**, and then select **All Sessions**.
5. Click **OK**.

Install the Fortinet_CA_SSL Certificate

FortiGate includes an SSL certificate, named Fortinet_CA_SSL, that you can use for full SSL inspection. It is signed by a certificate authority (CA) named FortiGate CA, which is not public. Because the CA is not public, each time a user connects to an HTTPS site, the browser displays a certificate warning. This is because the browser receives certificates signed by FortiGate, which is a CA it does not know and trust. You can avoid this warning by downloading the Fortinet_CA_SSL certificate and installing it on all workstations as a public authority.

In this procedure, you will first test access to an HTTPS site *without* the Fortinet_CA_SSL certificate installed. Then, you will install the Fortinet_CA_SSL certificate and test access to the HTTPS site again.

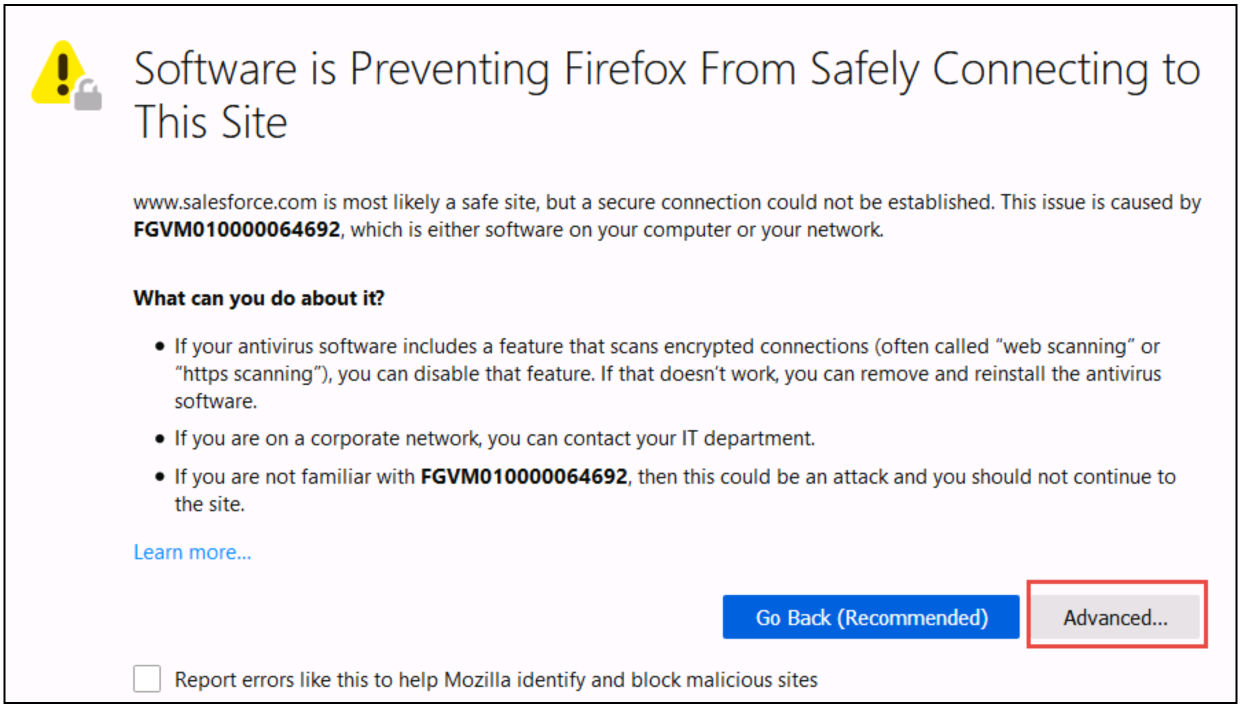
To test full SSL inspection without a trusted CA

1. On the Local-Client VM, open a new browser tab, and then go to an HTTPS site, such as:

`https://salesforce.com`

2. Click **Advanced**.

   Notice the certificate warning. This appears because the browser receives certificates signed by the FortiGate CA private key, and the corresponding CA certificate is not in the Local-Client certificate store.



Software is Preventing Firefox From Safely Connecting to This Site

www.salesforce.com is most likely a safe site, but a secure connection could not be established. This issue is caused by **FGVM010000064692**, which is either software on your computer or your network.

What can you do about it?

- If your antivirus software includes a feature that scans encrypted connections (often called "web scanning" or "https scanning"), you can disable that feature. If that doesn't work, you can remove and reinstall the antivirus software.
- If you are on a corporate network, you can contact your IT department.
- If you are not familiar with **FGVM010000064692**, then this could be an attack and you should not continue to the site.

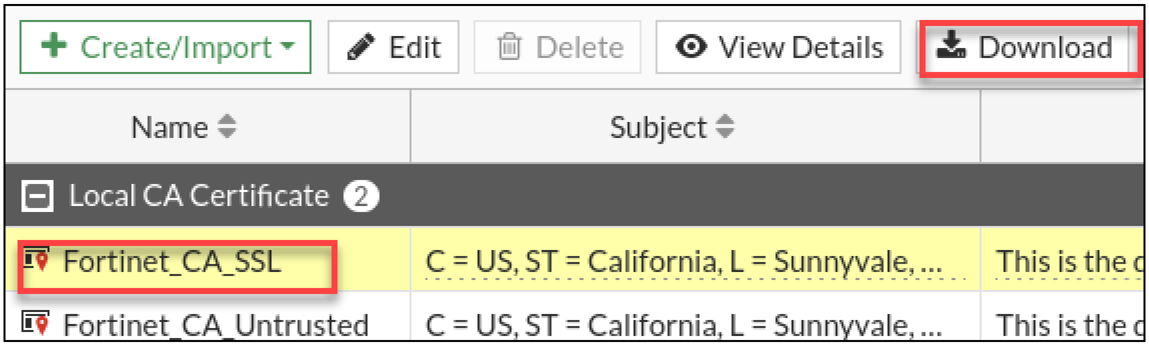
Learn more...

□ Report errors like this to help Mozilla identify and block malicious sites

3. Leave the browser tab open, and then continue to the next procedure. *Do not click* **Accept the Risk and Continue**.

To install the Fortinet_CA_SSL certificate in the browser

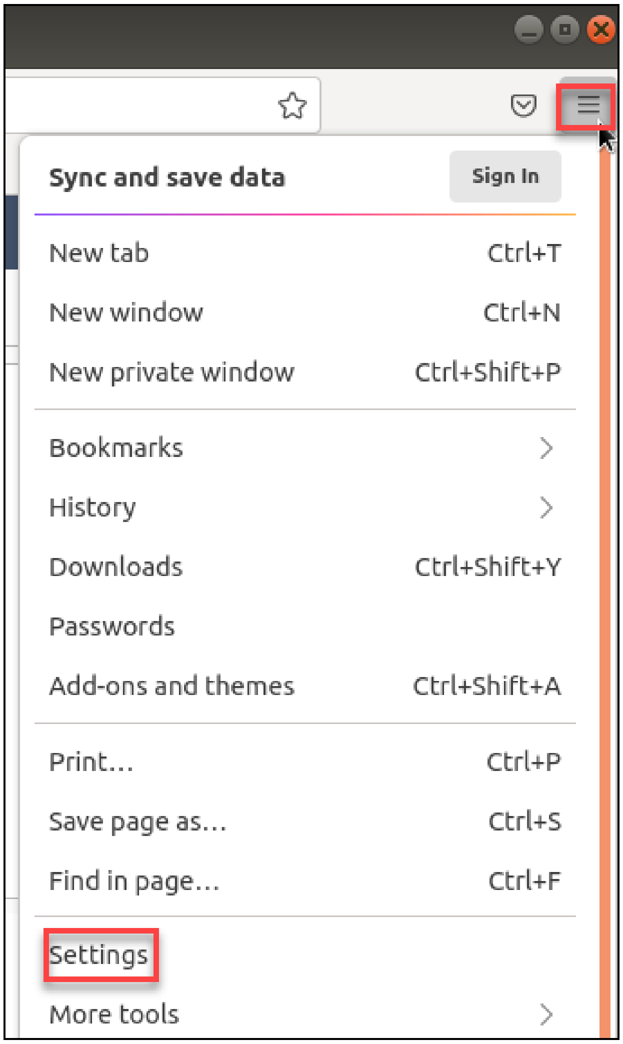
1. On the Local-Client VM, open a new browser, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.
2. Click **System** > **Certificates**.
3. In the **Local CA Certificate** section, click **Fortinet_CA_SSL**, and then click **Download**.



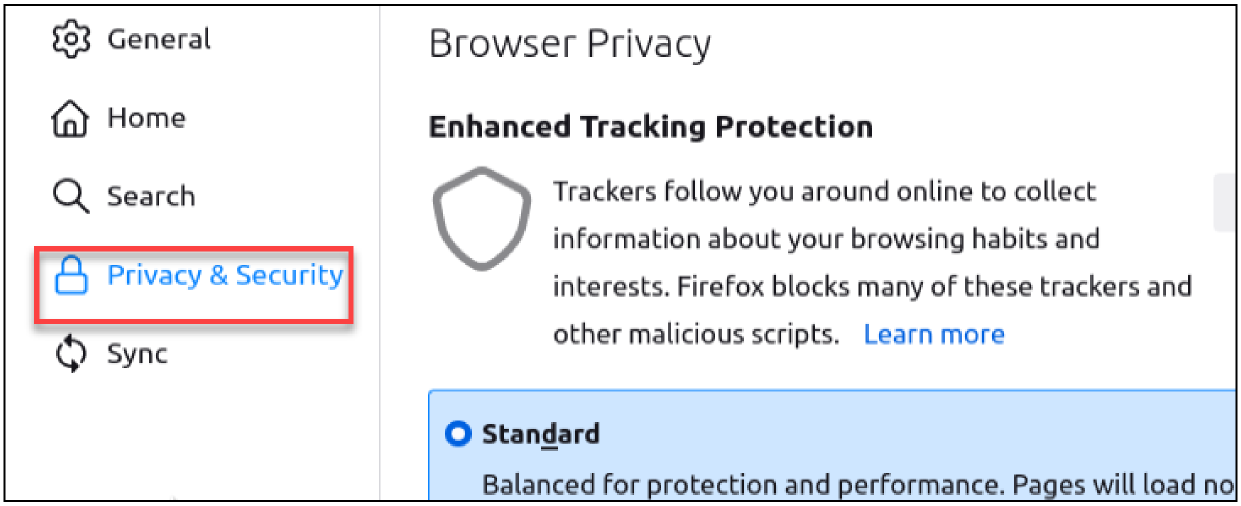
Name	Subject	
Local CA Certificate 2		
Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, ...	This is the c
Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, ...	This is the c

The certificate downloads to your **Downloads** folder.

4. In Firefox, in the upper-right corner, click the **Open menu** icon, and then click **Settings**.



5. Click **Privacy & Security**.



Browser Privacy

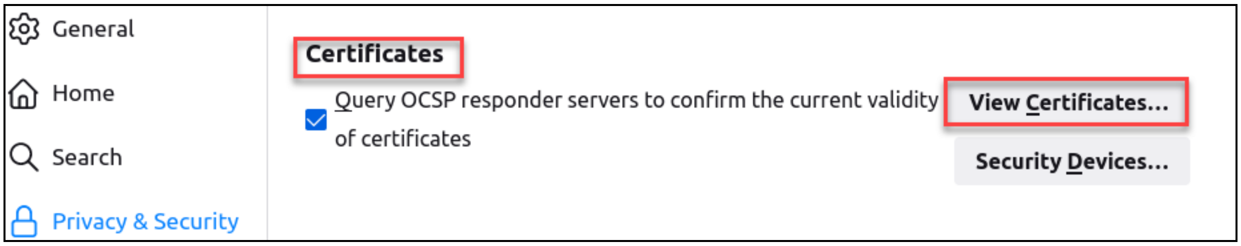
Enhanced Tracking Protection

Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts. Learn more

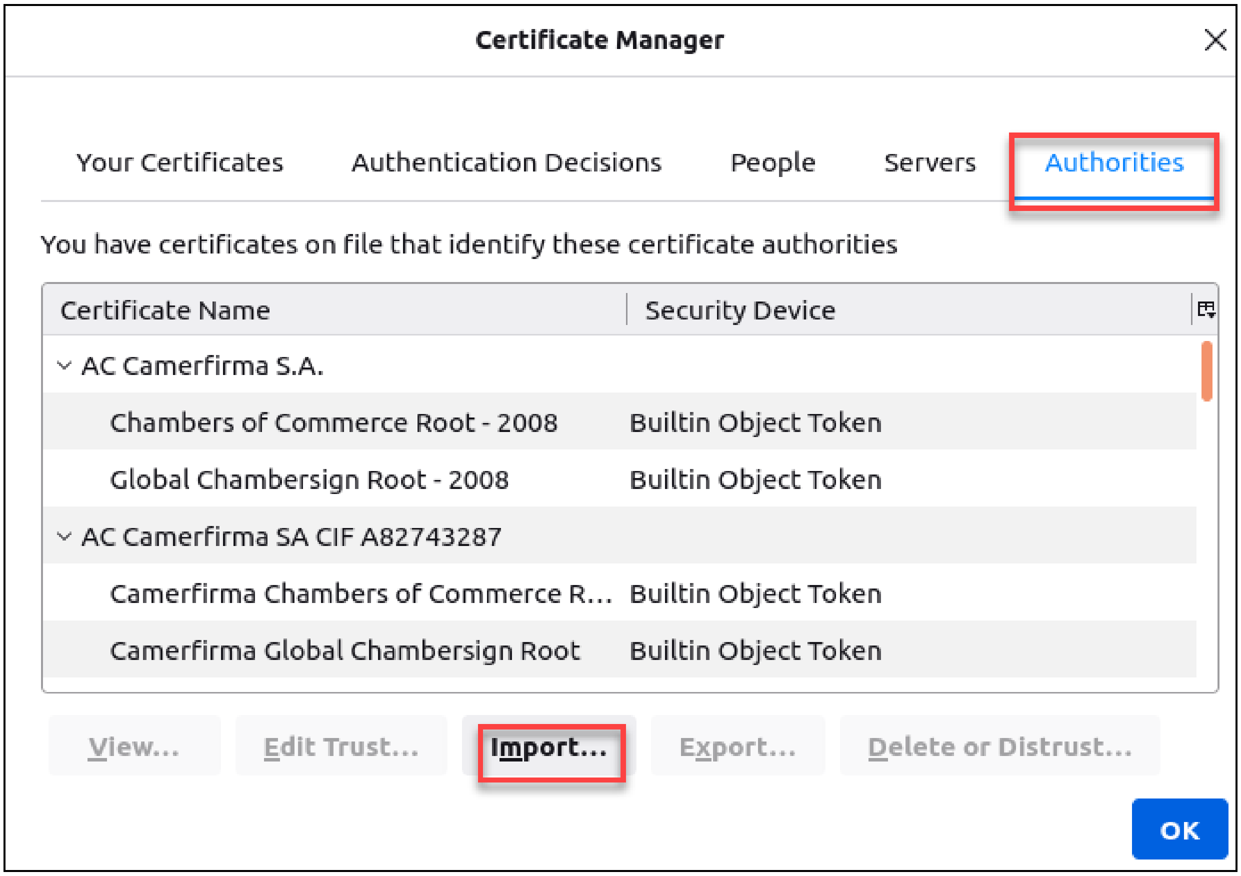
● Standard

Balanced for protection and performance. Pages will load no

6. In the **Certificates** section, click **View Certificates**.



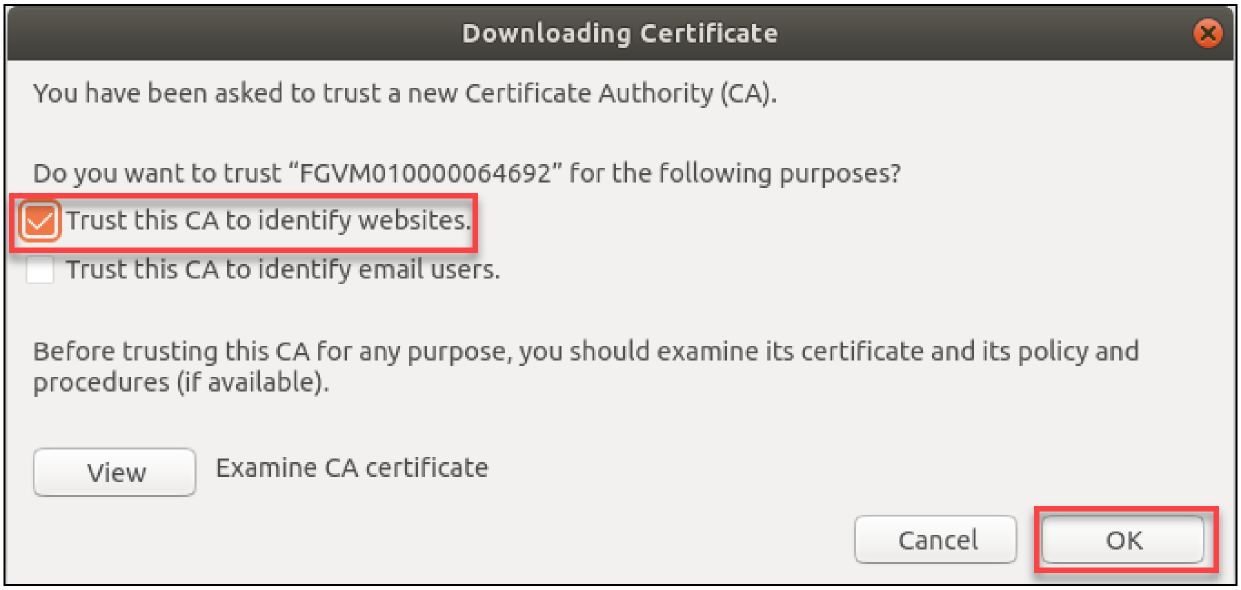
7. In the **Certificate Manager** window, click the **Authorities** tab, and then click **Import**.



You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce R...	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token

8. Click **Downloads** > `Fortinet_CA_SSL.cer`, and then click **Select**.
9. In the **Downloading Certificate** window, select **Trust this CA to identify websites**, and then click **OK**.



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "FGVM010000064692" for the following purposes?

☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

The **Fortinet_CA_SSL** certificate is added to the Firefox **Authorities** certificate store.

10. Click **OK**.
11. Restart Firefox.

Test Full SSL Inspection

Now that you added the Fortinet_CA_SSL certificate to your browser, you will not receive certificate warnings when you access a secure site.

The CA that signed this certificate is not public, but the browser does not issue a certificate warning for it because you added it as a trusted authority in the previous exercise.

To test SSL full inspection

1. On the Local-Client VM, open a new browser, and then go to a secure site, such as:

   ```
   https://salesforce.com
   ```

   This time, you are passed through to the site without certificate warnings.

2. Close the browser.

Exercise 2: Configuring Full SSL Inspection on Inbound Traffic

You can use full SSL inspection on inbound traffic to protect internal resources, such as web servers that users can access on the internet. Implementing inbound full SSL inspection allows you to apply antivirus, IPS, and web application firewall (WAF) on encrypted traffic destined for your web servers to protect them from malicious files and traffic.

In this exercise, you will import an external web server certificate to Local-FortiGate, and then configure full SSL inspection to protect a web server with an antivirus profile.

Configure a Virtual IP and Firewall Policy

First, you will configure a virtual IP to map an external IP address to the internal IP address of the web server. Then, you will configure a firewall policy to allow access to the virtual IP.

Take the Expert Challenge!

- On the Local-FortiGate GUI, configure a new virtual IP to map the external IP, `10.200.1.200`, to the internal IP, `10.0.1.10`, using **port1** as the external interface. Use `VIP-WEB-SERVER` as the name of your virtual IP.
- Create a new firewall policy to allow all inbound traffic to the virtual IP. Use `Web_Server_Access` as the name of the firewall policy.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Install the Training CA Certificate on page 103.

To configure a virtual IP

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **Virtual IPs**.
3. Click **Create New**, and then select **Virtual IP**.
4. Configure the following settings:

Field	Value
Name	VIP-WEB-SERVER
Interface	port1

Field	Value
External IP address/range	10.200.1.200
Map to IPv4 address/range	10.0.1.10

5. Click **OK**.

To configure a firewall policy

1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Create New**, and then create a new firewall policy using the following settings:

Field	Value
Name	Web_Server_Access
Incoming Interface	port1
Outgoing Interface	port3
Source	all
Destination	VIP-WEB-SERVER
Service	ALL
NAT	<disabled>

3. Click **OK**.

Install the Training CA Certificate

You will verify access to the web server URL, and then install the CA certificate on Firefox to eliminate certificate errors.

Take the Expert Challenge!

- On the Remote-Client VM, verify that you have access to the web server using `https://lab.webserver`.
- Using Firefox, review the web server certificate details and identify the certificate issuer.
- Install the CA certificate in the Firefox **Authorities** certificate store. The certificate file is located in **Desktop** > **Resources** > **FortiGate-Security** > **Certificate-Operations** > `CA.crt`.
- Make sure certificate-related warning messages no longer appear before proceeding to the next section.

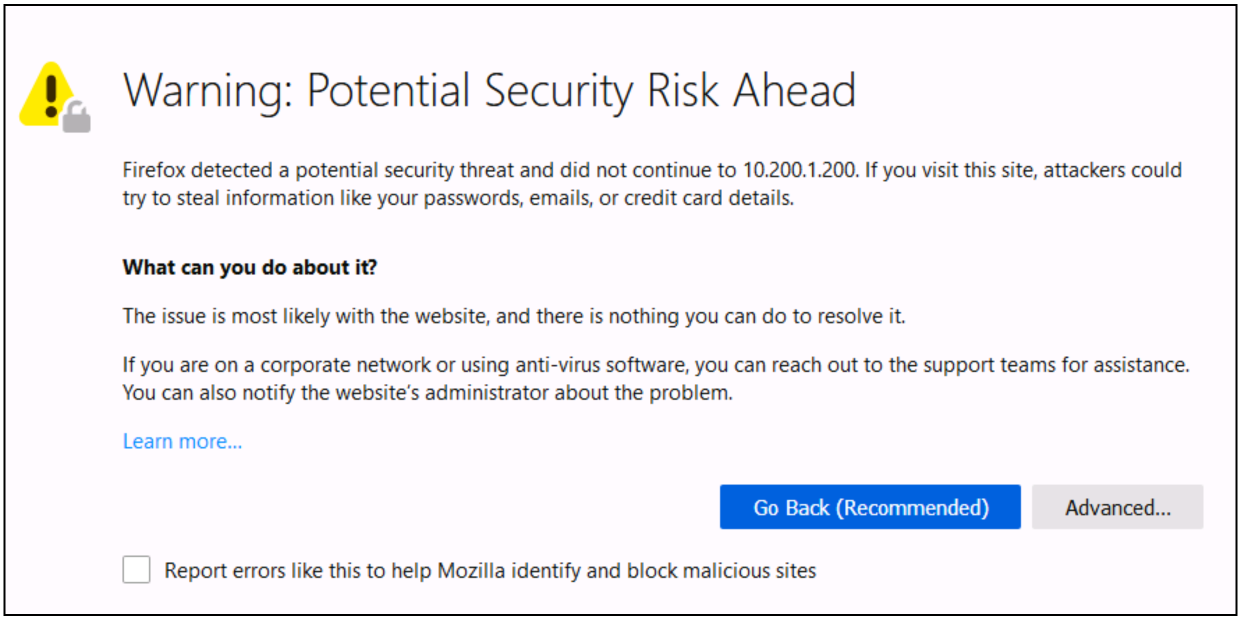
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure Inbound Full SSL Inspection on page 109.

To verify access

1. On the Remote-Client VM, open a new browser tab, and then access the web server using `https://lab.webserver`.

   A security warning appears.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to 10.200.1.200. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

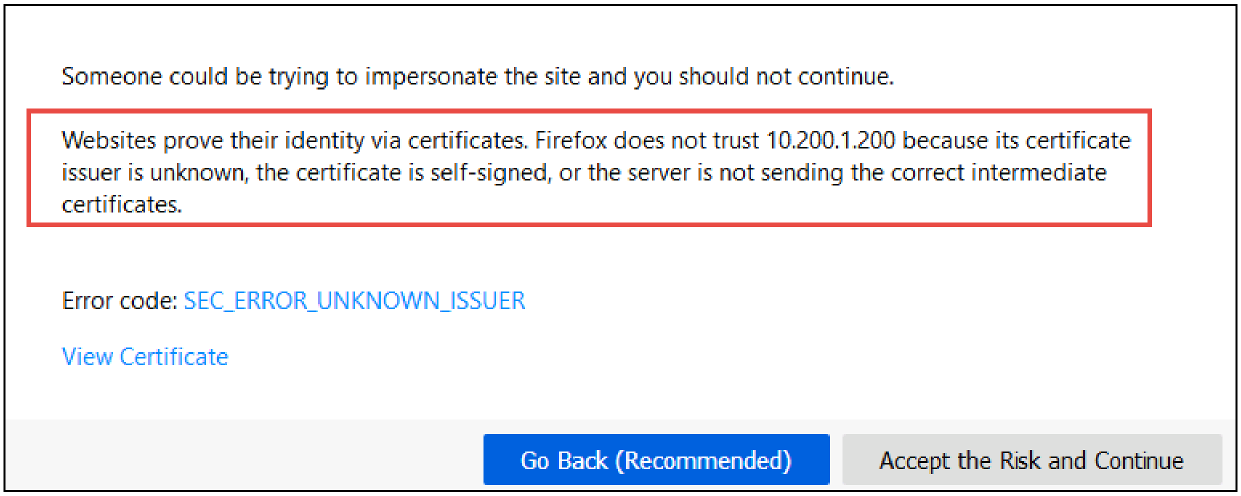
What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more...
Go Back (Recommended)
Advanced...
□ Report errors like this to help Mozilla identify and block malicious sites

2. Click **Advanced**, and then review the warning message.



Someone could be trying to impersonate the site and you should not continue.

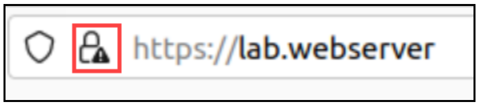
Websites prove their identity via certificates. Firefox does not trust 10.200.1.200 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

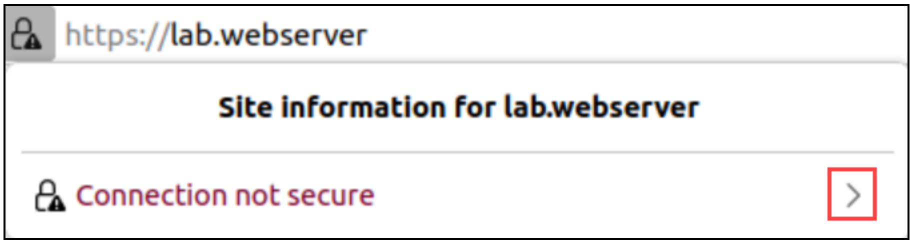
3. Click **Accept the Risk and Continue**.

   The Apache2 Ubuntu default page loads.

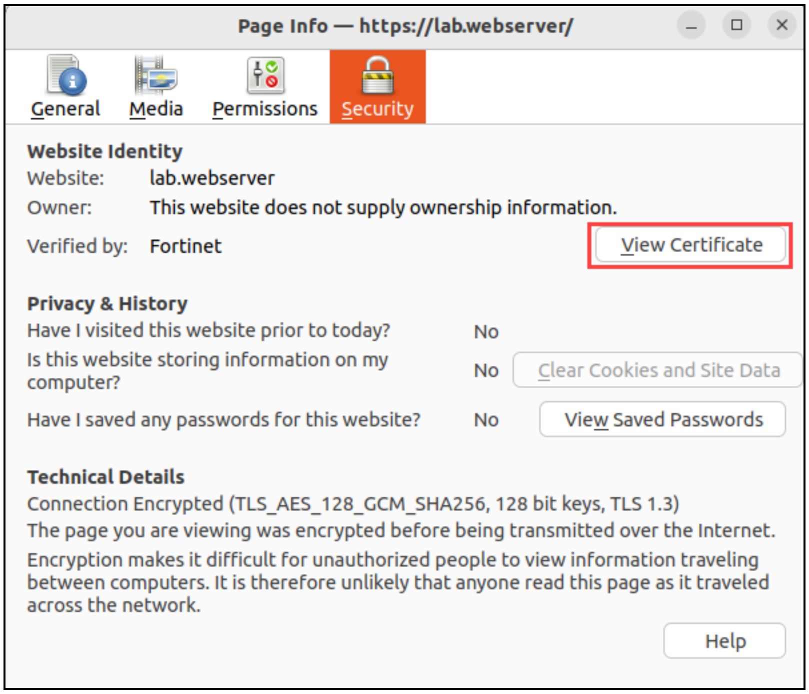
4. Click the **security exception** icon.



5. Click the **Show connection details** icon.



6. Click **More Information**.
7. Click **View Certificate**.


Page Info — https://lab.webserver/

Website Identity

Website: lab.webserver

Owner: This website does not supply ownership information.

Verified by: Fortinet

Privacy & History

Have I visited this website prior to today? No

Is this website storing information on my computer? No

Have I saved any passwords for this website? No

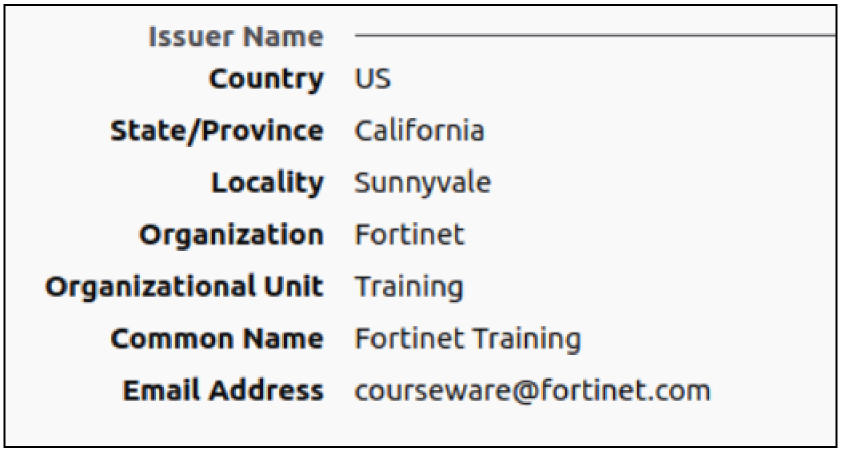
Technical Details

Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

8. In the **Issuer Name** section, review the information.

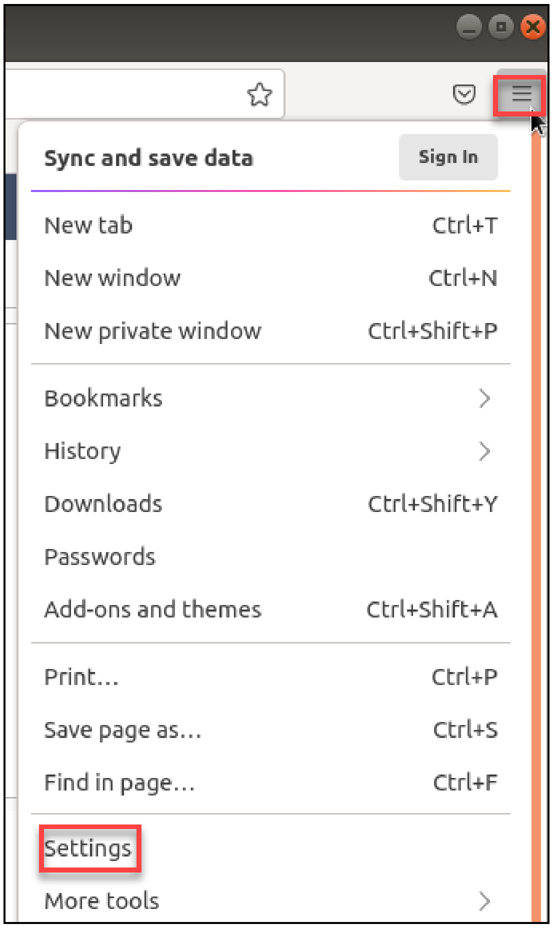

Issuer Name

Country	US
State/Province	California
Locality	Sunnyvale
Organization	Fortinet
Organizational Unit	Training
Common Name	Fortinet Training
Email Address	courseware@fortinet.com

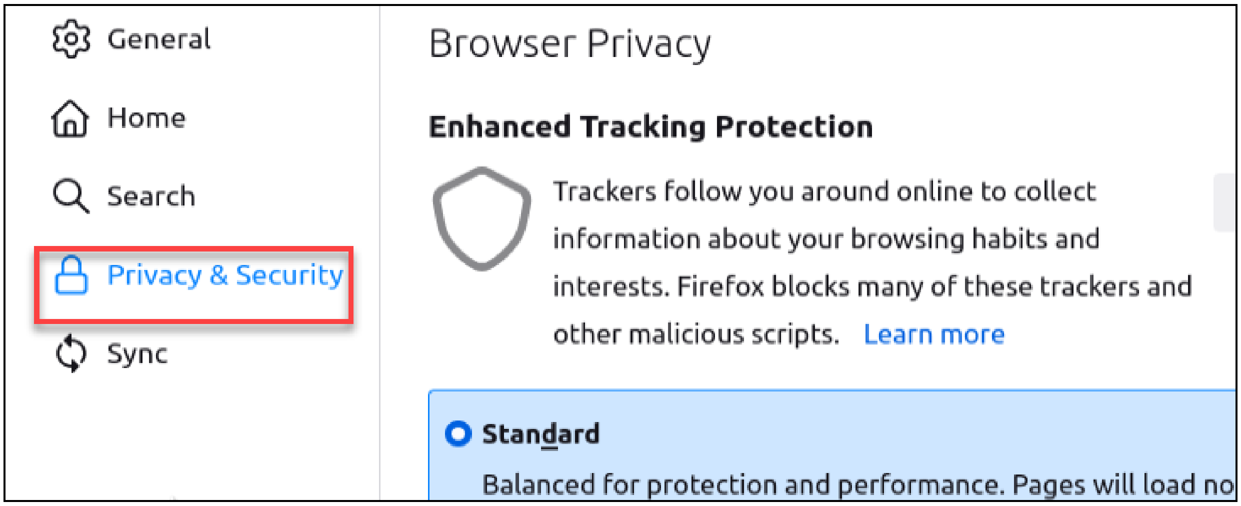
9. Close the certificate details window.

To install the Training CA certificate

1. On the Remote-Client VM, in the upper-right corner of the Firefox browser, click the **Open menu** icon, and then click **Settings**.



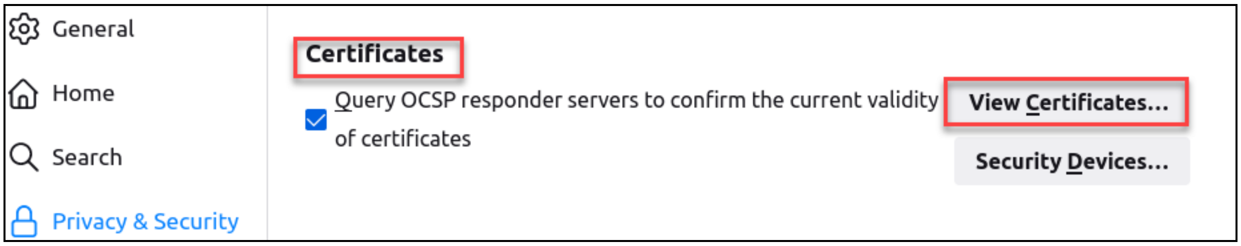
2. Click **Privacy & Security**.



Trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts. Learn more

Balanced for protection and performance. Pages will load no

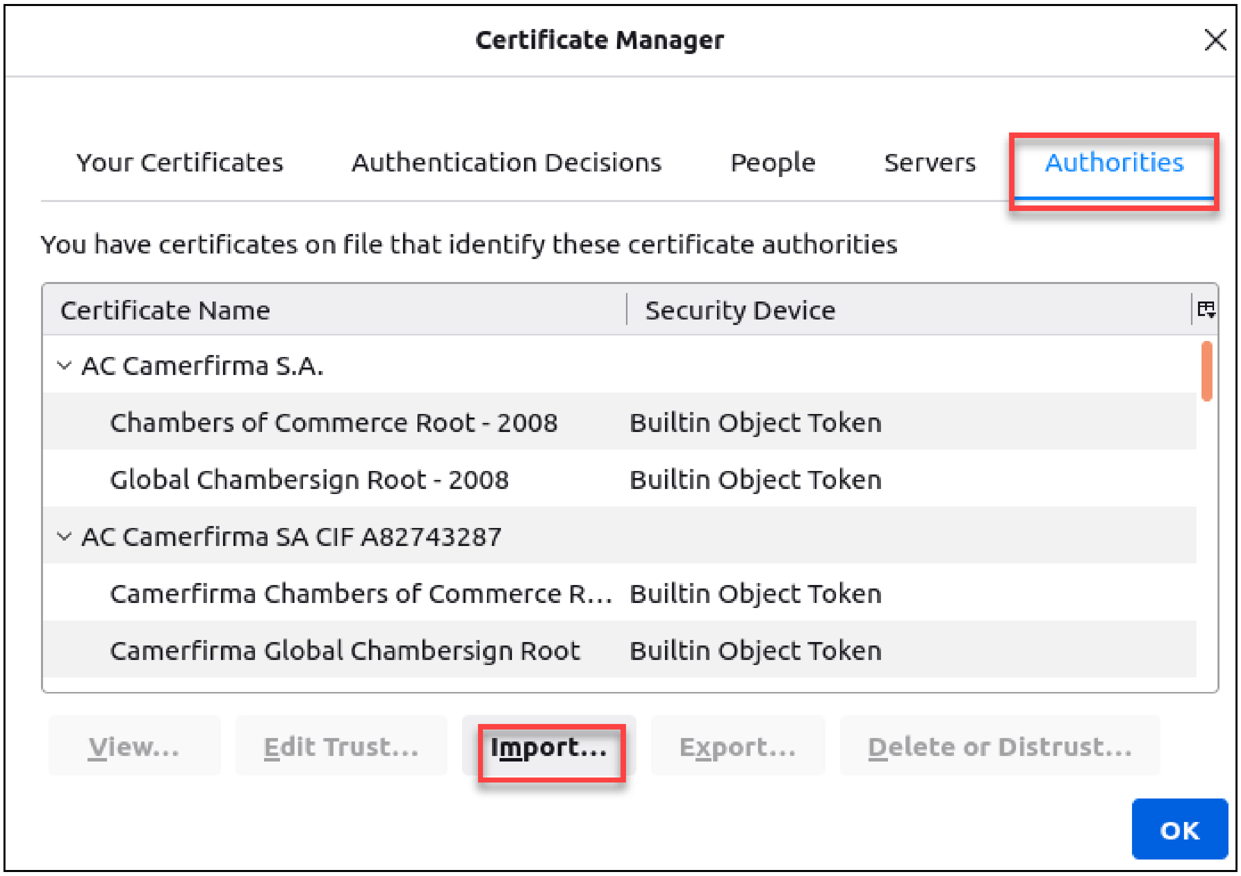
3. In the **Certificates** section, click **View Certificates**.



Certificates

☑ Query OCSP responder servers to confirm the current validity of certificates

4. In the **Certificate Manager** window, click the **Authorities** tab, and then click **Import**.



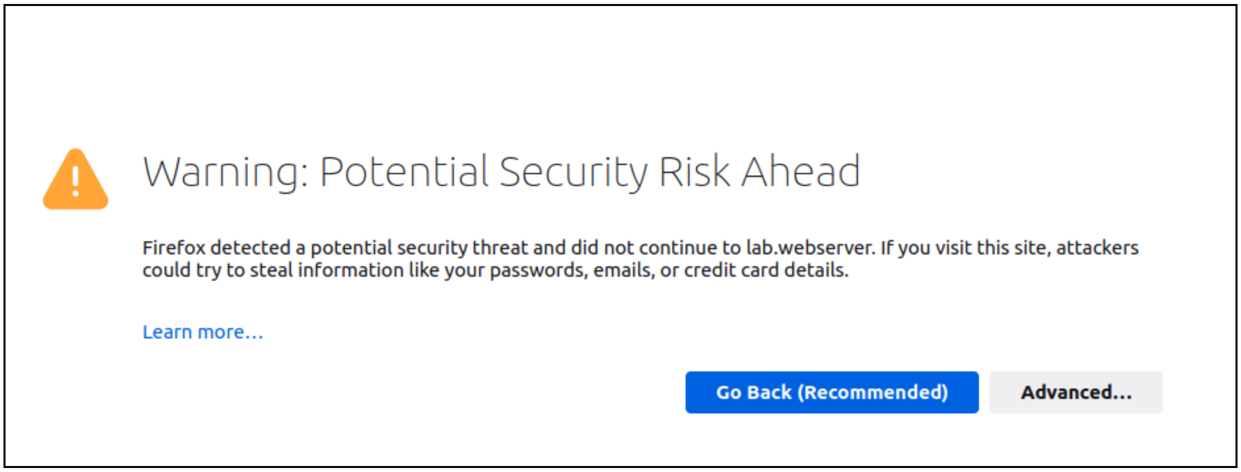
Certificate Manager

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce R...	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token

5. Click **Desktop** > **Resources** > **FortiGate-Security** > **Certificate-Operations** > **CA.crt**, and then click **Select**. The **Downloading Certificate** window opens.

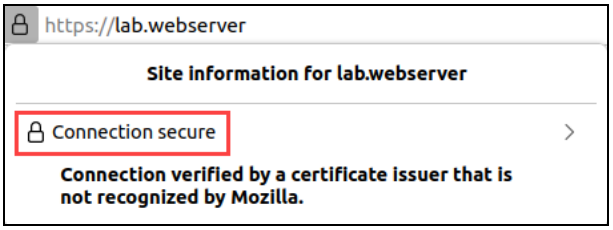
6. Click **Trust this CA to identify websites**, and then click **OK**.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to lab.webserver. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

7. Click **OK**.
8. Restart Firefox.
9. Go to `https://lab.webserver`, and then verify that the security warning is no longer displayed.



Site information for lab.webserver

Connection secure

Connection verified by a certificate issuer that is not recognized by Mozilla.

10. Close the browser.

Configure Inbound Full SSL Inspection

On Local-FortiGate, you will configure and enable full SSL inspection on all inbound traffic destined to the web server, using the default certificate. You will also observe the changes to the end-user browser session on Remote-Client. Then, you will import the external web server certificate on Local-FortiGate, and use it to perform full SSL inspection to eliminate security errors.

To configure inbound full SSL inspection

1. Return to the Local-FortiGate GUI, click **Security Profiles** > **SSL/SSH Inspection**.
2. In the upper-left corner, click **Create New** to create a new profile.
3. Configure the following settings:

Field	Value
Name	Inbound_SSL_Inspection
Enable SSL inspection of	Protecting SSL Server
Server certificate	Fortinet_SSL

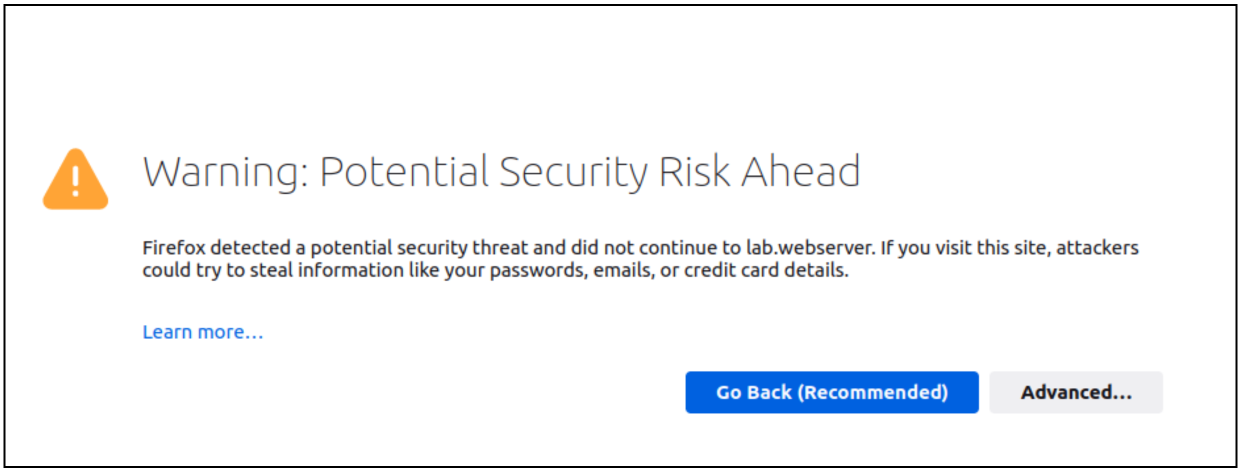
4. Click **OK**.
5. Click **Policy & Objects** > **Firewall Policy**.
6. Edit the **Web_Server_Access** policy.
7. In the **Inspection Mode** field, select **Proxy-based**.
8. In the **Security Profiles** section, enable the following security profiles:

Security profile	Value
AntiVirus	default
SSL Inspection	Inbound_SSL_Inspection

9. Click **OK**.

To verify inbound full SSL inspection

1. On the Remote-Client VM, close any existing instances of Firefox.
2. Open Firefox again, and then go to `https://lab.webserver`.

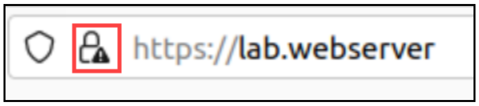


Warning: Potential Security Risk Ahead

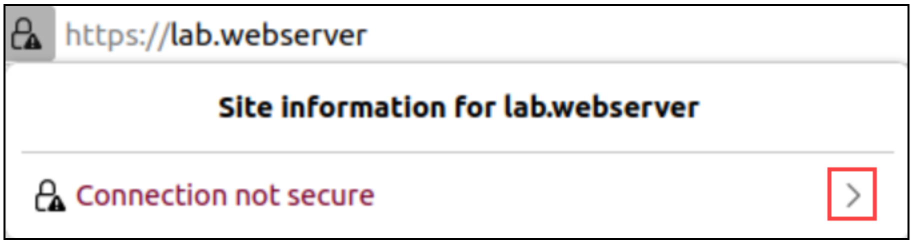
Firefox detected a potential security threat and did not continue to lab.webserver. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

A security warning is displayed. If you do not receive a security warning, refresh the page (`F5`). This forces Firefox to update its local cache.

3. Click **Advanced**, and then review the error message.
4. Click **Accept the Risk and Continue**.
5. Click the **security exception** icon.



6. Click the **Show connection details** icon.

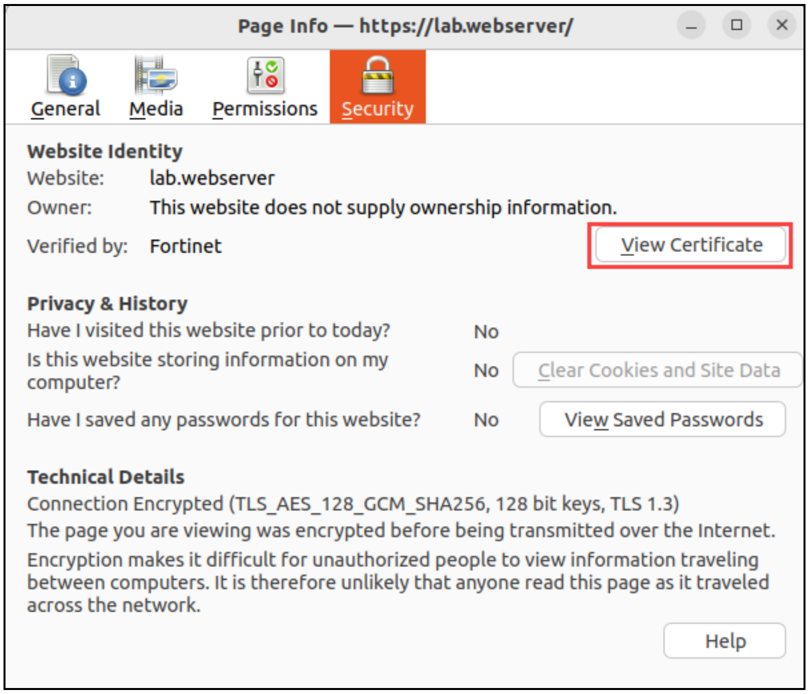


https://lab.webserver

Site information for lab.webserver

Connection not secure

7. Click **More Information**.
8. Click **View Certificate**.



Page Info — https://lab.webserver/

Website Identity

Website: lab.webserver

Owner: This website does not supply ownership information.

Verified by: Fortinet

Privacy & History

Have I visited this website prior to today? No

Is this website storing information on my computer? No

Have I saved any passwords for this website? No

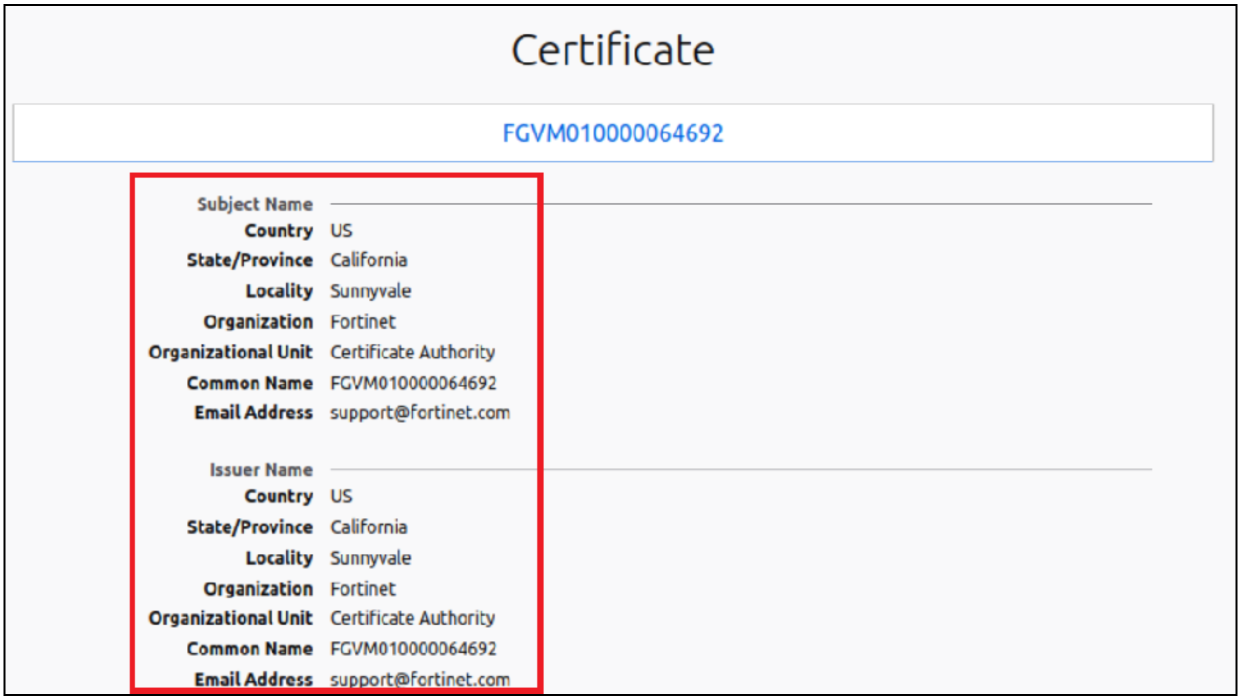
Technical Details

Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

9. Review the certificate information.



Certificate

FGVM010000064692

Subject Name
Country US
State/Province California
Locality Sunnyvale
Organization Fortinet
Organizational Unit Certificate Authority
Common Name FGVM010000064692
Email Address support@fortinet.com

Issuer Name
Country US
State/Province California
Locality Sunnyvale
Organization Fortinet
Organizational Unit Certificate Authority
Common Name FGVM010000064692
Email Address support@fortinet.com

Stop and think!

To inspect the encrypted traffic, Local-FortiGate must proxy the connection between Remote-Client and the web server. To do this, FortiGate must use its own certificate (FortiGate_SSL), which is *not* a trusted certificate. It is also not issued for the host name you are using in the URL to access the secure website. While this does verify that Local-FortiGate is inspecting the encrypted traffic, you must perform a few more configuration steps to make sure the correct certificate is being used, to eliminate any security errors on the end-user side.

10. Close the certificate details window.

To import the web server certificate and private key on Local-FortiGate

1. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.
2. On the Local-FortiGate GUI, click **System** > **Certificates**.
3. Click **Create/Import**, and then select **Certificate**.
4. Click **Import Certificate**.
5. In the **Type** field, select **PKCS # 12 Certificate**.
6. Click **Upload**.
7. Browse to **Desktop** > **Resources** > **FortiGate-Security** > **Certificate-Operations** > `Webserver.p12`, and then click **Open**.

   The **Certificate Name** field is auto-populated from the certificate filename.

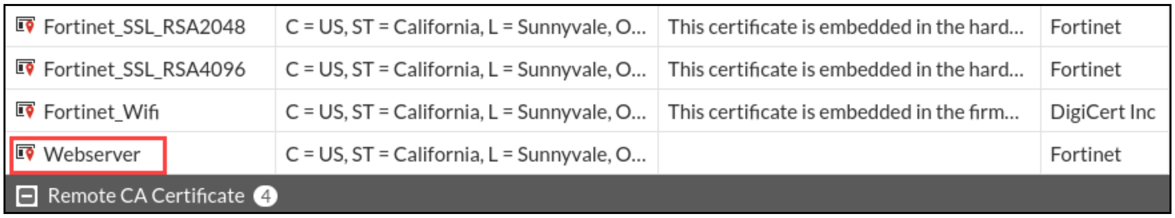
PKCS#12 (.p12 file extension) is an archive file format used to bundle a certificate with its private key. It is usually protected using a password.

The `Webserver.p12` file contains the web server certificate and private key.

8. In the **Password** field, type `fortinet`, and then type the same password in the **Confirm Password** field.
9. Click **Create**.

   The certificate and key are imported.

10. Click **OK**.



Fortinet_SSL_RSA2048	C = US, ST = California, L = Sunnyvale, O...	This certificate is embedded in the hard...	Fortinet
Fortinet_SSL_RSA4096	C = US, ST = California, L = Sunnyvale, O...	This certificate is embedded in the hard...	Fortinet
Fortinet_Wifi	C = US, ST = California, L = Sunnyvale, O...	This certificate is embedded in the firm...	DigiCert Inc
Webserver	C = US, ST = California, L = Sunnyvale, O...		Fortinet

To modify the inbound SSL inspection profile

1. Continuing on the Local-FortiGate GUI, click **Security Profiles** > **SSL/SSH Inspection**.
2. Edit **Inbound_SSL_Inspection**.
3. In the **Server certificate** field, remove **Fortinet_SSL**, and then select **Webserver**.
4. Click **OK**.

To verify the SSL inspection profile change

1. Return to the Remote-Client VM, and then close any existing instances of Firefox.
2. Open Firefox again, and then go to `https://lab.webserver`.

   Verify that there are no more security errors. If you still receive errors, refresh the page (`F5`). This forces Firefox to update its local cache.

Lab 7: Web Filtering

In this lab, you will configure one of the most used security profiles on FortiGate: web filter. This includes configuring a FortiGuard category-based filter, applying the web filter profile on a firewall policy, testing the configuration, and basic troubleshooting.

Objectives

- Configure web filtering on FortiGate
- Apply the FortiGuard category-based option for web filtering
- Troubleshoot the web filter
- Read and interpret web filter log entries

Time to Complete

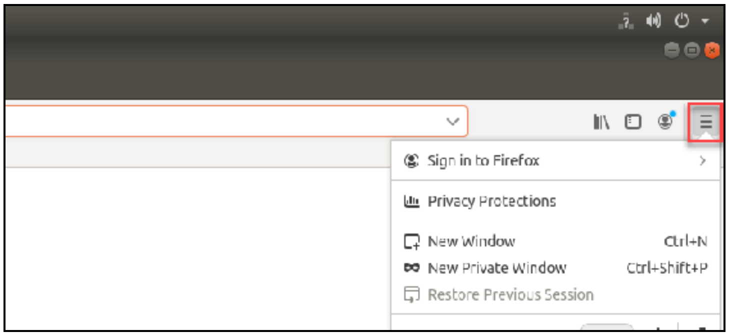
Estimated: 25 minutes

Prerequisites

Before beginning this lab, you must clear the browser history, and then restore a configuration file to Local-FortiGate.

To clear the browser history

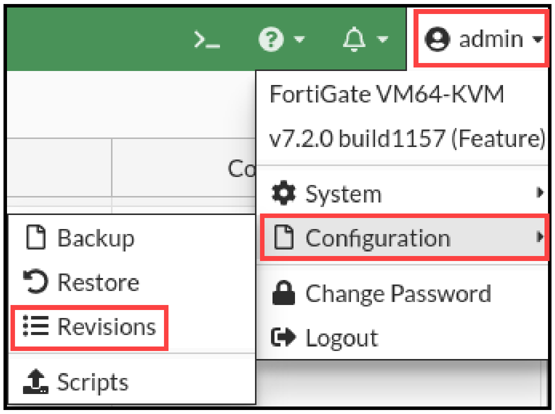
1. On the Local-Client VM, open the browser, and then click the menu icon in the upper-right corner.



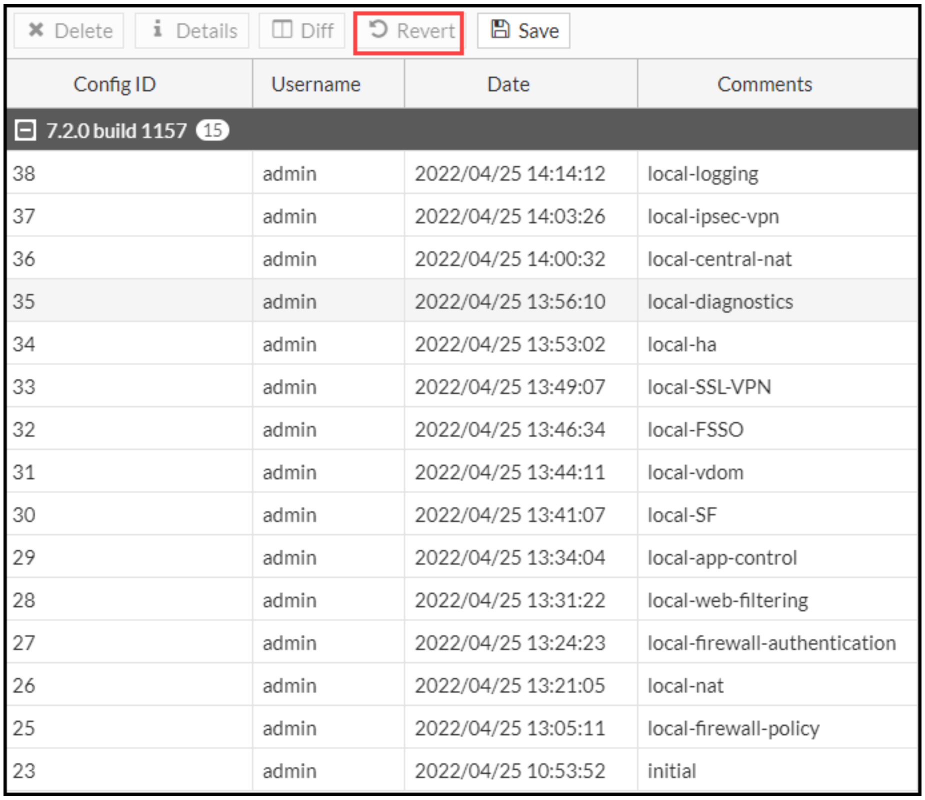
2. Click **Settings** > **Privacy & Security**.
3. Scroll to **History**, click **Clear History**, and then ensure the time range to clear is set to **Everything**.
4. Click **OK**.

To restore the FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **local-web-filtering**, and then click **Revert**.



Config ID	Username	Date	Comments
7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

Exercise 1: Configuring FortiGuard Web Filtering

To configure FortiGate for web filtering based on FortiGuard categories, you must make sure that FortiGate has a valid FortiGuard security subscription license. The license provides the web filtering capabilities necessary to protect against inappropriate websites.

Then, you must configure a category-based web filter security profile on FortiGate, and apply the security profile on a firewall policy to inspect the HTTP traffic.

Finally, you can test different actions taken by FortiGate according to the website rating.

Review the FortiGate Settings

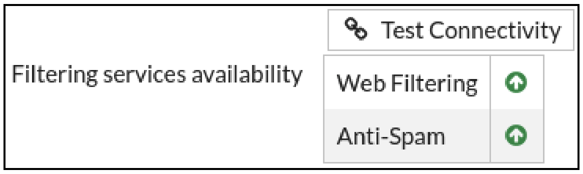
You will review the inspection mode and license status according to the uploaded settings. You will also list the FortiGuard Distribution Servers (FDS) that your FortiGate uses to send the web filtering requests.

To review the restored settings on FortiGate

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. On the **Dashboard**, locate the **Licenses** widget, and then confirm that the **Web Filtering** service is licensed and active.

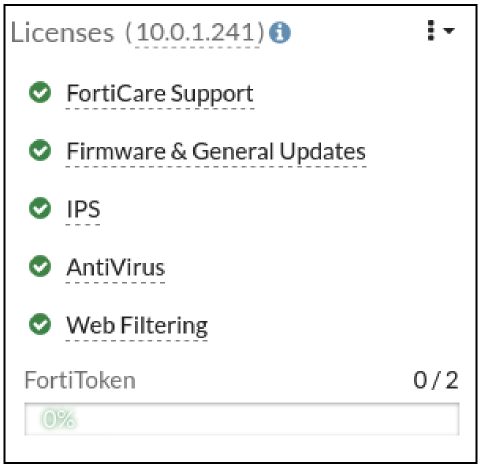
   A green check mark should appear beside **Web Filtering**.

Because of the reboot following the restoration of the configuration file, the web filter license status may be **Unavailable**. In this case, navigate to **System** > **FortiGuard**, in the **Filtering** section, click **Test Connectivity** to force an update, and then click **OK** to confirm.



Test Connectivity

Filtering services availability		
	Web Filtering	●
	Anti-Spam	●



Licenses (10.0.1.241)

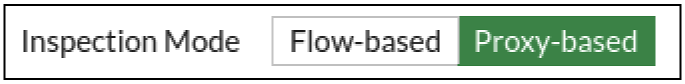
- ✓ FortiCare Support
- ✓ Firmware & General Updates
- ✓ IPS
- ✓ AntiVirus
- ✓ Web Filtering

FortiToken 0 / 2

0%

3. Click **Policy & Objects** > **Firewall Policy**.
4. Double-click the **Full_Access** policy to edit it.
5. Verify the **Inspection Mode** setting.

   Notice that the default inspection mode is set to **Flow-based**.
6. Under **Inspection Mode**, select **Proxy-based**.
7. Click **OK**.
8. Click **Policy & Objects** > **Firewall Policy**.
9. Double-click the **Full_Access** policy to edit it, and then verify that **Inspection Mode** is now set to **Proxy-based**.



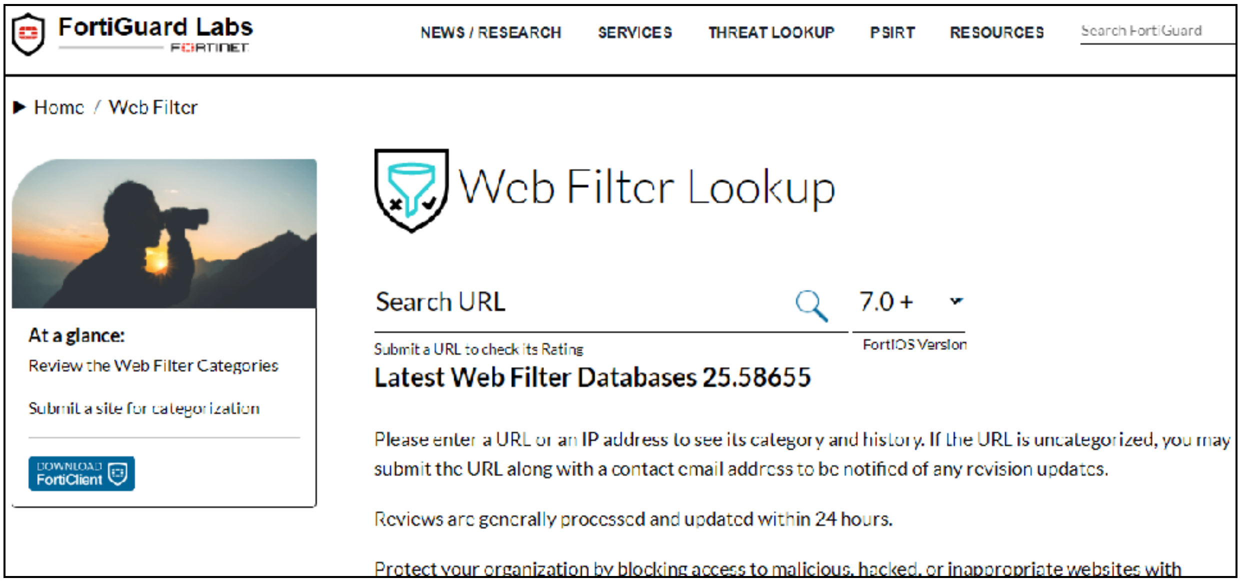
Inspection Mode: Flow-based [✓ Proxy-based]

Determine Web Filter Categories

To configure web filter categories, you must first identify how specific websites are categorized by the FortiGuard service.

To determine web filter categories

1. On the Local-Client VM, open a new browser tab, and then go to `https://www.fortiguard.com/webfilter`.



At a glance:
Review the Web Filter Categories
Submit a site for categorization

Web Filter Lookup

Search URL 7.0 +
Submit a URL to check its Rating FortiOS Version

Latest Web Filter Databases 25.58655

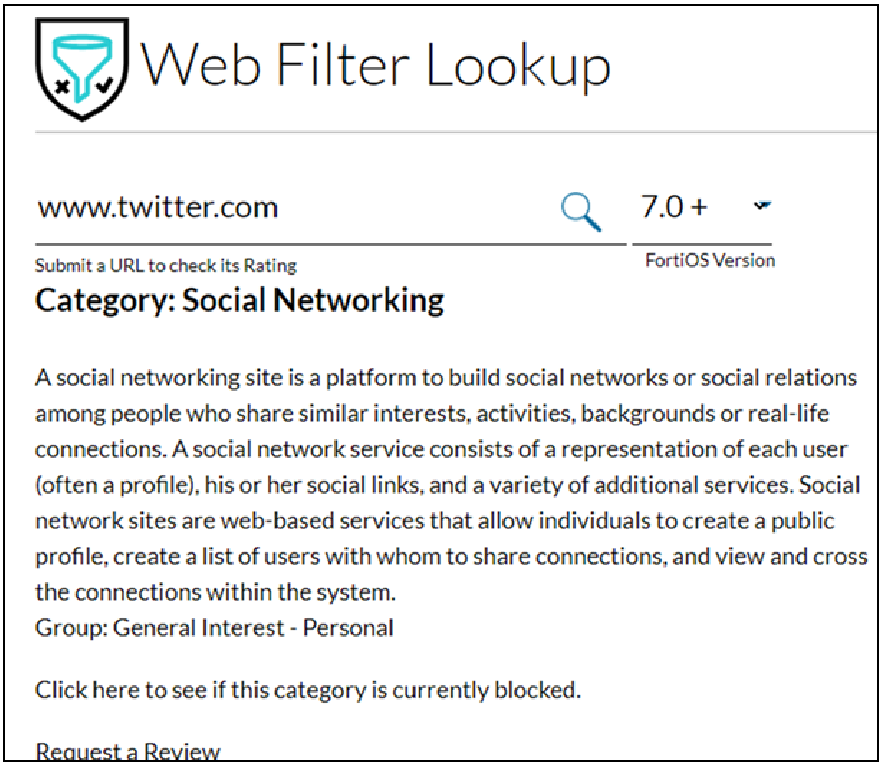
Please enter a URL or an IP address to see its category and history. If the URL is uncategorized, you may submit the URL along with a contact email address to be notified of any revision updates.

Reviews are generally processed and updated within 24 hours.

Protect your organization by blocking access to malicious, hacked, or inappropriate websites with

2. Use the **Web Filter Lookup** tool to search for the following URL:

```
www.twitter.com
```



Web Filter Lookup

www.twitter.com 7.0 +
Submit a URL to check its Rating FortiOS Version

Category: Social Networking

A social networking site is a platform to build social networks or social relations among people who share similar interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), his or her social links, and a variety of additional services. Social network sites are web-based services that allow individuals to create a public profile, create a list of users with whom to share connections, and view and cross the connections within the system.
Group: General Interest - Personal

Click here to see if this category is currently blocked.

Request a Review

This is one of the websites you will use later to test your web filter.

As you can see, Twitter is listed in the **Social Networking** category.

3. Use the **Web Filter Lookup** tool again to find the web filter category for the following websites:

- `www.skype.com`
- `www.ask.com`
- `www.bing.com`

You will test your web filter using these websites also.

The following table shows the category assigned to each URL, as well as the action you will configure your FortiGate to take based on your web filter security profile:

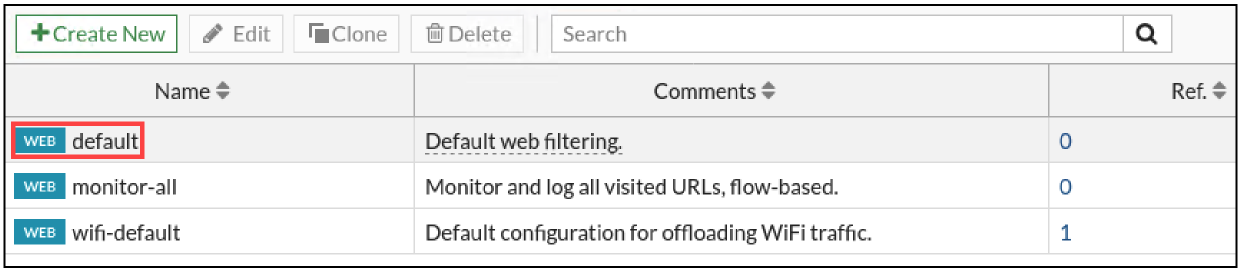
Website	Category	Action
www.twitter.com	Social Networking	Block
www.skype.com	Internet Telephony	Warning
www.bing.com	Search Engines and Portals	Allow
www.ask.com	Search Engines and Portals	Allow

Configure a FortiGuard Category-Based Web Filter

You will review the default web filtering profile, and then configure the FortiGuard category-based filter.

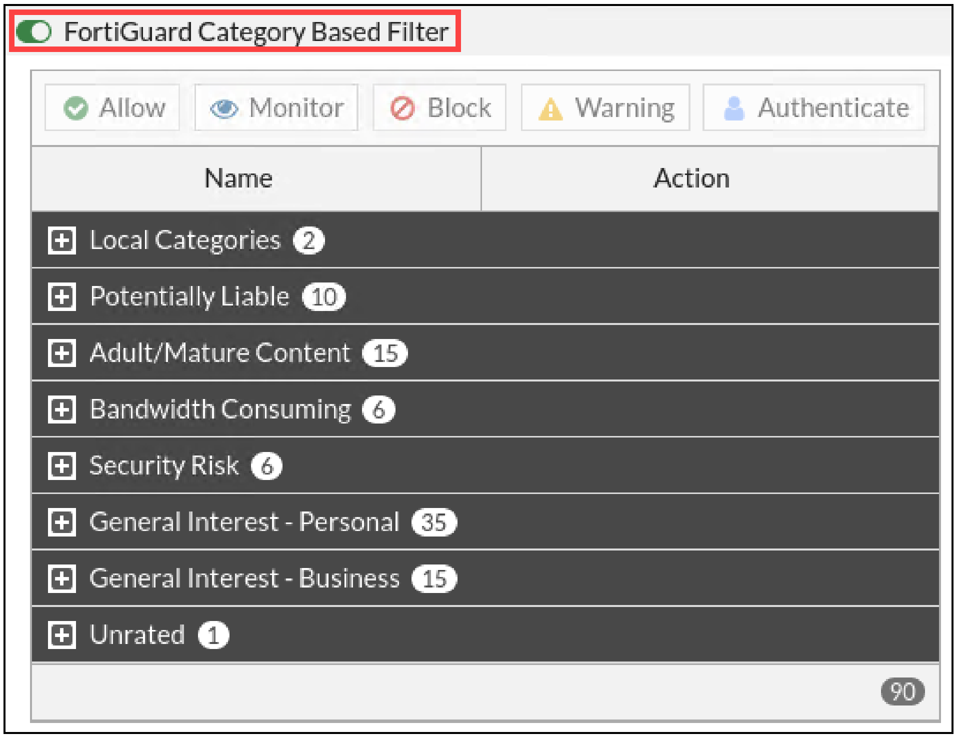
To configure the web filter security profile

1. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and then click **Security Profiles** > **Web Filter**.
2. Double-click the **default** web filter profile to edit it.



Name	Comments	Ref.
WEB default	Default web filtering.	0
WEB monitor-all	Monitor and log all visited URLs, flow-based.	0
WEB wifi-default	Default configuration for offloading WiFi traffic.	1

3. Verify that **FortiGuard Category Based Filter** is enabled.



FortiGuard Category Based Filter

Name	Action
⊞ Local Categories 2	
⊞ Potentially Liable 10	
⊞ Adult/Mature Content 15	
⊞ Bandwidth Consuming 6	
⊞ Security Risk 6	
⊞ General Interest - Personal 35	
⊞ General Interest - Business 15	
⊞ Unrated 1	

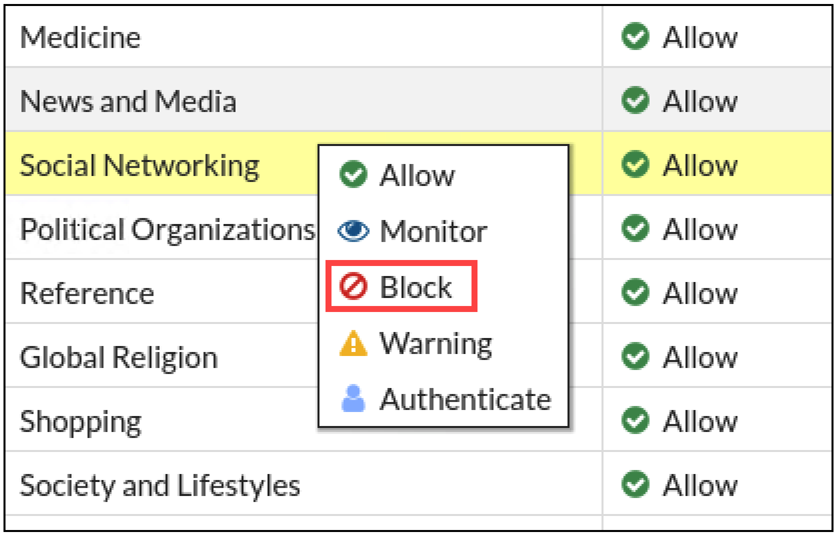
90

4. Review the default actions for each category.

Category	Action
Local Categories	Disable
Potentially Liable	Block: **Extremist Group** Allow: all other subcategories **Tip**: Expand **Potentially Liable** to view the subcategories.
Adult/Mature Content	Block
Bandwidth Consuming	Allow
Security Risk	Block
General Interest - Personal	Allow
General Interest - Business	Allow
Unrated	Block

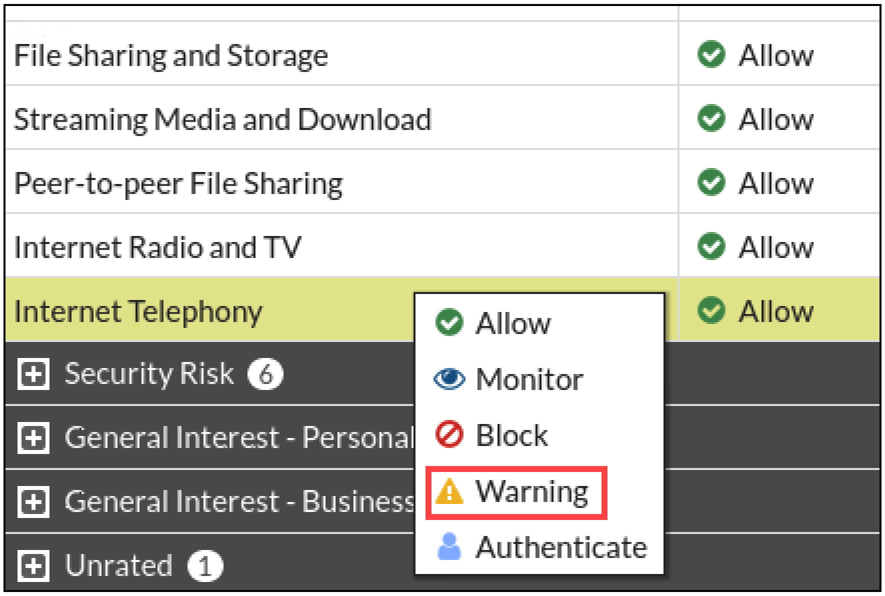
5. Expand **General Interest - Personal** to view the subcategories.

6. Right-click **Social Networking**, and then select **Block**.



Medicine	✓ Allow
News and Media	✓ Allow
Social Networking	✓ Allow
Political Organizations	✓ Allow
Reference	✓ Allow
Global Religion	✓ Allow
Shopping	✓ Allow
Society and Lifestyles	✓ Allow

7. Expand **Bandwidth Consuming** to view the subcategories.
8. Right-click **Internet Telephony**, and then select **Warning**.



File Sharing and Storage	✓ Allow
Streaming Media and Download	✓ Allow
Peer-to-peer File Sharing	✓ Allow
Internet Radio and TV	✓ Allow
Internet Telephony	✓ Allow
⊞ Security Risk 6	
⊞ General Interest - Personal	
⊞ General Interest - Business	
⊞ Unrated 1	

The **Edit Filter** dialog box opens, which allows you to modify the warning interval.

9. Keep the default setting of five minutes, and then click **OK**.
10. Click **OK**.

Apply the Web Filter Profile to a Firewall Policy

Now that you configured the web filter profile, you must apply this security profile to a firewall policy in order to start inspecting web traffic.

You will also enable the logs to store and analyze the security events that the web traffic generates.

Take the Expert Challenge!

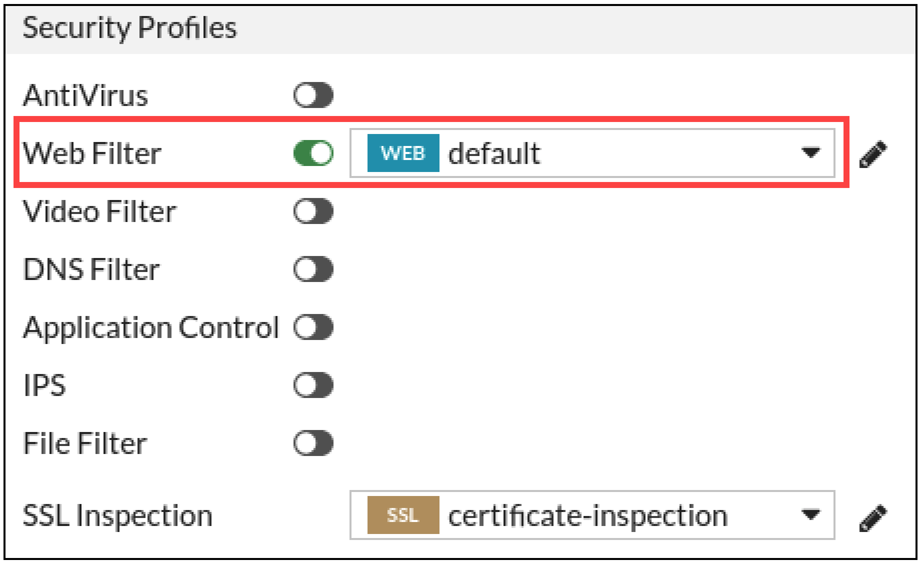
On the Local-FortiGate GUI, apply the web filter profile to the existing **Full_Access** firewall policy. Make sure that logging is also enabled and set to **Security Events**.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Test the Web Filter on page 123.

To apply a security profile on a firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Double-click the **Full_Access** policy to edit it.
3. In the **Security Profiles** section, enable **Web Filter**, and then in the drop-down menu, select **default**.



Security Profiles

AntiVirus: off

Web Filter: on — WEB default

Video Filter: off

DNS Filter: off

Application Control: off

IPS: off

File Filter: off

SSL Inspection: SSL certificate-inspection

4. Under **Log Allowed Traffic**, make sure **Security Events** is selected.
5. Keep all other default settings, and then click **OK**.

Test the Web Filter

For the purposes of this lab, you will test the web filter security profile you configured for each category.

To test the web filter

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following command to verify the web filter status:

```
get webfilter status
```

The `get webfilter status` and `diagnose debug rating` commands show the list of FDSs that your FortiGate uses to send web filtering requests. In normal operations, FortiGate sends the rating requests only to the server at the top of the list. Each server is probed for round-trip time (RTT) every two minutes.

Stop and think!

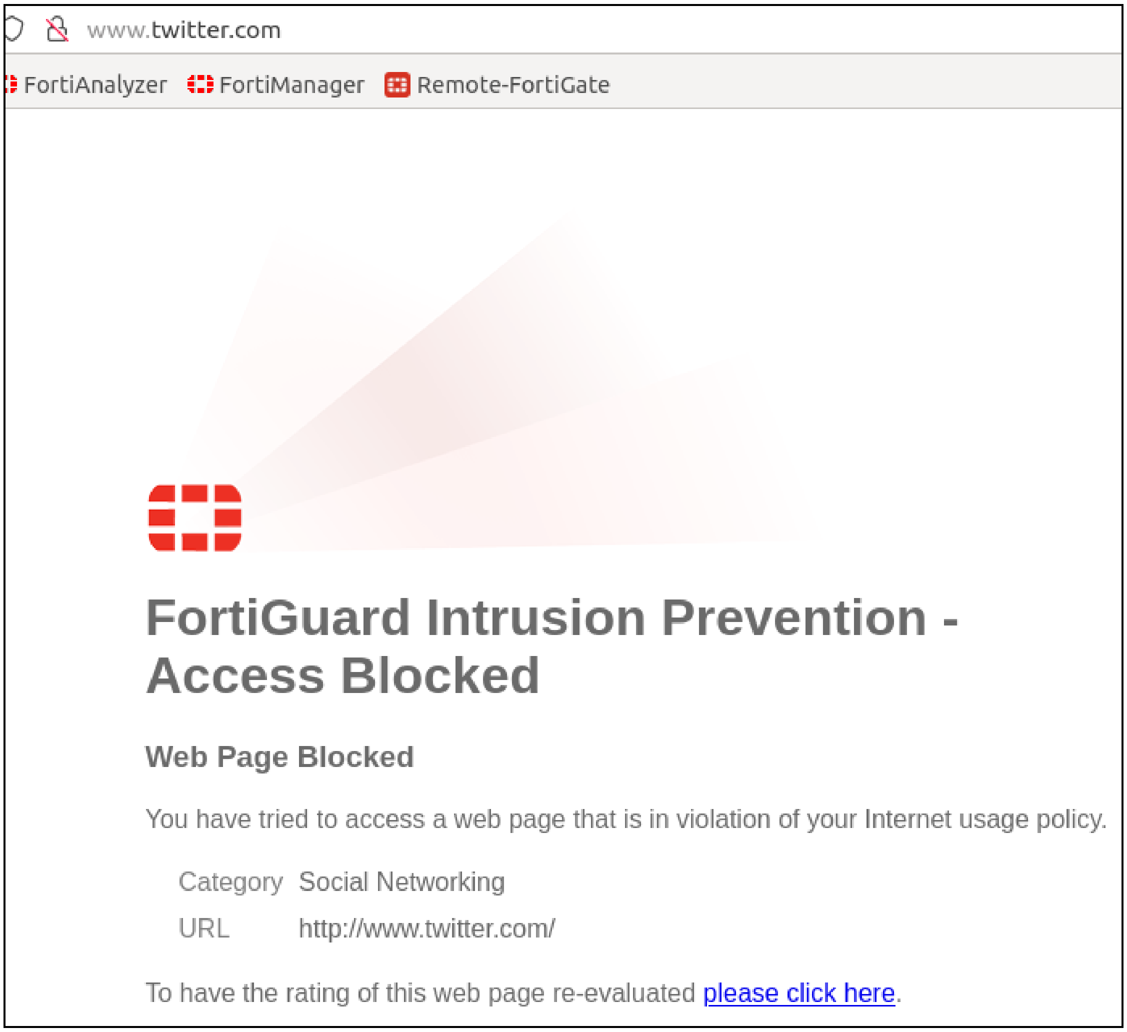
Why does only one IP address from your network appear in the server list?

Your lab environment uses a FortiManager at `10.0.1.241`, which is configured as a local FDS. It contains a local copy of the FDS web rating database.

FortiGate sends the rating requests to FortiManager instead of the public FDS. For this reason, the output of the command above lists the FortiManager IP address only.

3. On the Local-Client VM, open a new browser tab, and then go to `www.twitter.com`.

   A warning appears, according to the predefined action for this website category.



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

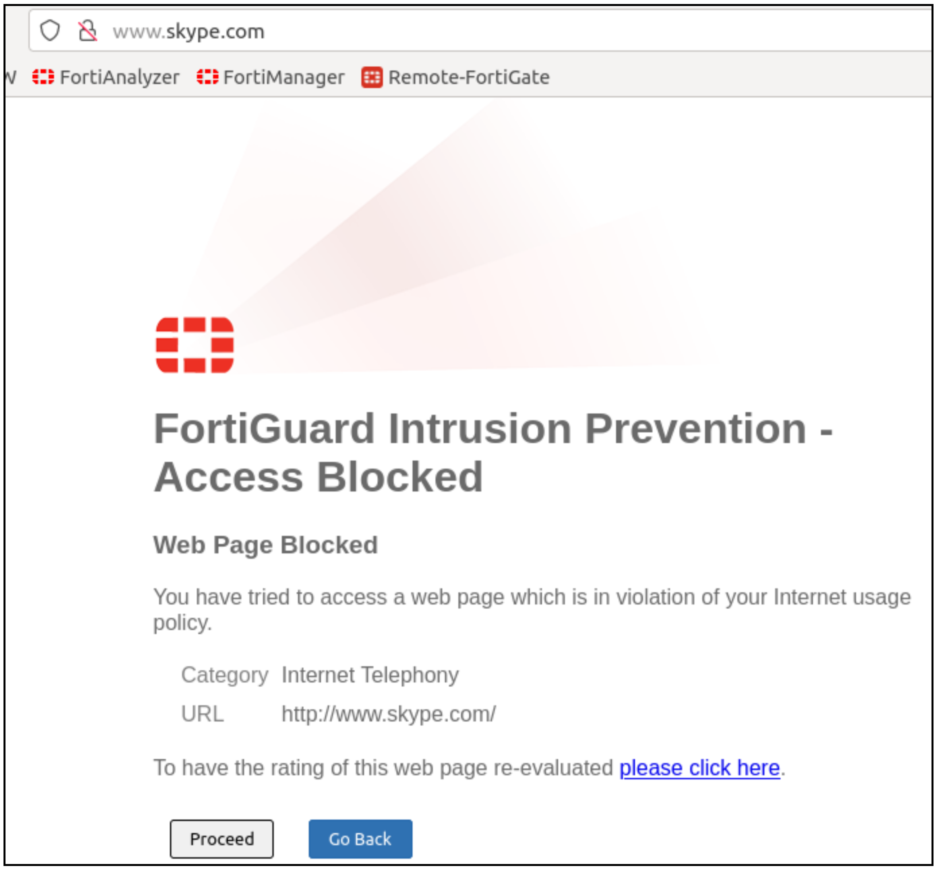
You have tried to access a web page that is in violation of your Internet usage policy.

Category	Social Networking
URL	http://www.twitter.com/

To have the rating of this web page re-evaluated please click here.

4. Open a new browser tab, and then go to `www.skype.com`.

   A warning appears, according to the predefined action for this website category.



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page which is in violation of your Internet usage policy.

Category Internet Telephony

URL http://www.skype.com/

To have the rating of this web page re-evaluated please click here.

5. Click **Proceed** to accept the warning and access the website.
6. Open a new browser tab, and then go to `www.bing.com`.

   This website appears because it belongs to the **Search Engines and Portals** category, which is set to **Allow**.

Create a Web Rating Override

You will override the category for `www.bing.com`.

To create a web rating override

1. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and then click **Security Profiles** > **Web Rating Overrides.**
2. Click **Create New**, and then configure the following settings:

Field	Value
URL	www.bing.com
Category	Security Risk
Sub-Category	Malicious Websites

3. Click **OK**.

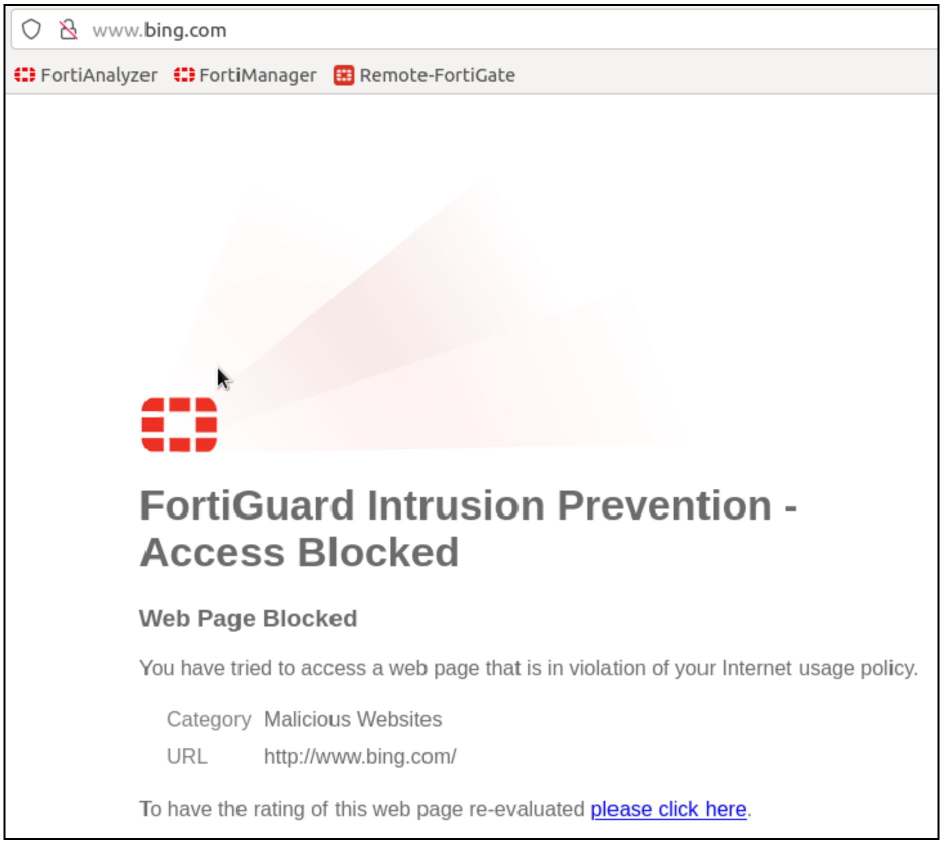
Test the Web Rating Override

You will test the web rating override you created in the previous procedure.

To test the web rating override

1. On the Local-Client VM, open a new browser tab, and then try to access the `www.bing.com` website again.

   The website is blocked, and it matches a local rating instead of a FortiGuard rating.



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page that is in violation of your Internet usage policy.

Category	Malicious Websites
URL	http://www.bing.com/

To have the rating of this web page re-evaluated please click here.

Exercise 2: Setting Up Web Filtering Authentication

In this exercise, you will configure and test the authenticate action for web filtering categories.

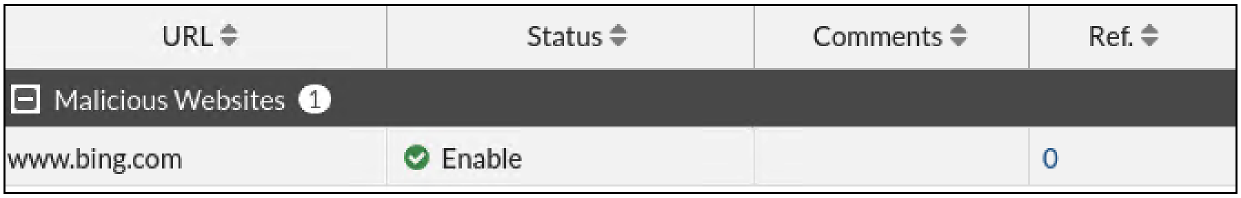
Set Up the Authenticate Action

First, you will confirm that the override category for `www.bing.com` is set to **Malicious Websites**. Then, you will set the action for this FortiGuard category to **Authenticate**.

To override the category

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Security Profiles** > **Web Rating Overrides**.

   There is an entry for `www.bing.com`. The override category is set to **Malicious Websites**, which you should have created in the previous exercises.



URL	Status	Comments	Ref.
Malicious Websites 1			
www.bing.com	✓ Enable		0

3. Double-click `www.bing.com` to verify the rating override, and confirm the category and subcategory.

Field	Value
Category	Security Risk
Sub-Category	Malicious Websites

By default, the **Security Risk** category is set to **Block** on your FortiGate.

4. Click **Cancel**.

To set up the authenticate action

1. Continuing on the Local-FortiGate GUI, click **Security Profiles** > **Web Filter**.
2. Double-click the **default** web filter profile to edit it.
3. Under **FortiGuard Category Based Filter**, expand **Security Risk**, right-click **Malicious Websites**, and then select **Authenticate**.

   The **Edit Filter** dialog box opens, which allows you to modify the warning interval.
4. Configure the following settings:

Field	Value
Warning Interval	5 minutes
Selected User Groups	Override_Permissions

5. Click **OK**.
6. Click **OK**.

For the purpose of this lab, **Override_Permissions** is a predefined user group. To review the user groups, click **User & Authentication** > **User Groups**.

Define Users and Groups

You will define a user in order to test the authenticate action.

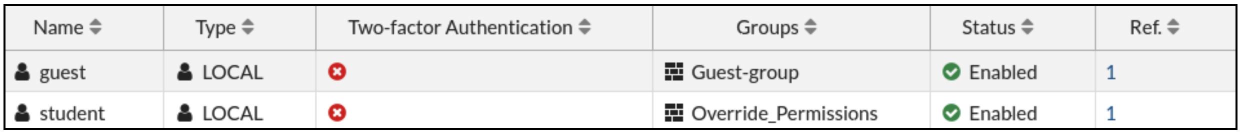
To create a user

1. Continuing on the Local-FortiGate GUI, click **User & Authentication** > **User Definition**.
2. Click **Create New**.
3. In the **User Type** field, select **Local User**.
4. Click **Next**, and then configure the following settings:

Field	Value
Username	student
Password	fortinet

5. Click **Next**.
6. Click **Next**.
7. Enable **User Group**, and then in the drop-down list, select **Override_Permissions**.
8. Click **Submit**.

   The **student** user is created.



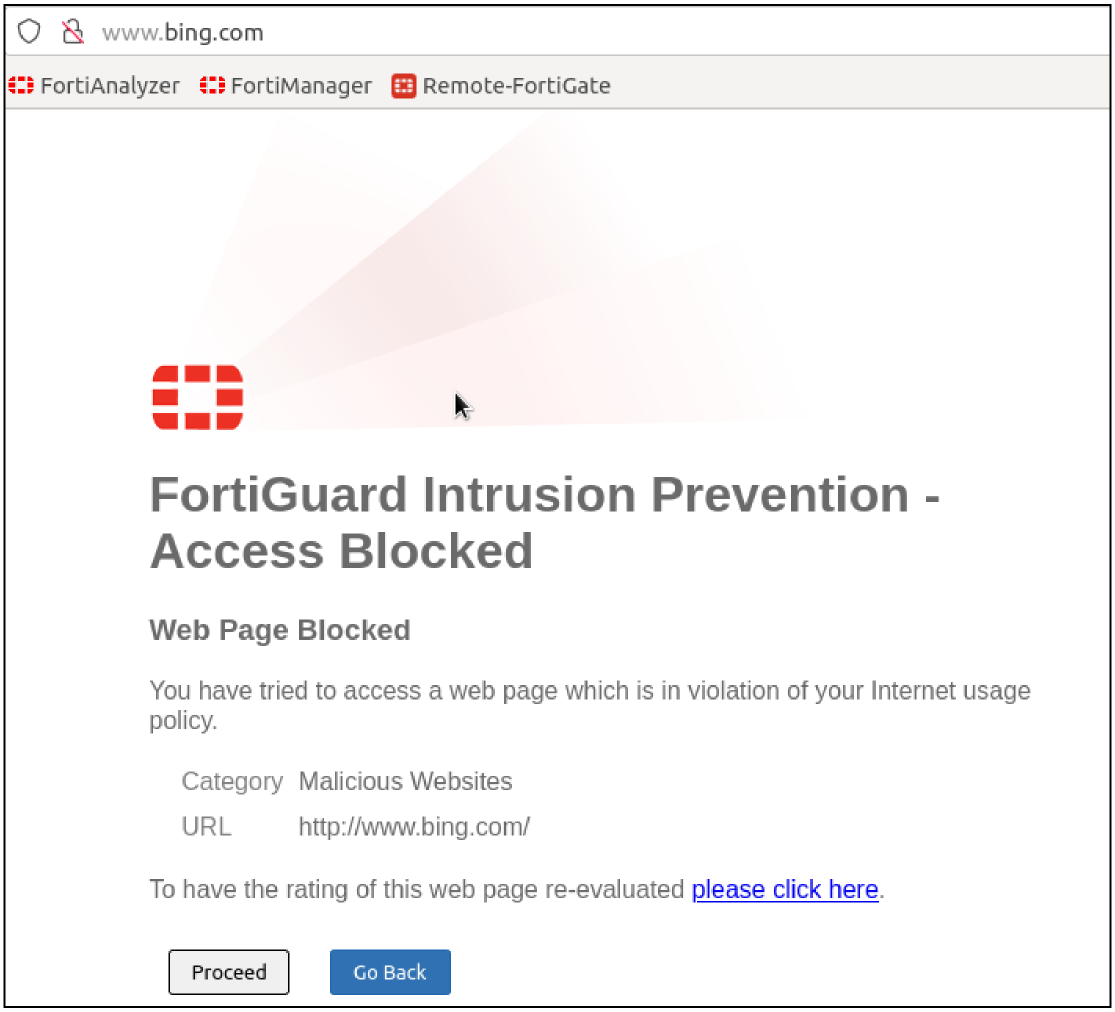
Name	Type	Two-factor Authentication	Groups	Status	Ref.
guest	LOCAL	✗	Guest-group	✓ Enabled	1
student	LOCAL	✗	Override_Permissions	✓ Enabled	1

Test the Authenticate Action

You will test access to a website using the authenticate action, and then analyze the logs that the security events create.

To test the web rating override

1. On the Local-Client VM, open a new browser tab, and then try to access `www.bing.com`.
   A warning appears. Note that it is a different message from the one that appeared before.



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page which is in violation of your Internet usage policy.

Category	Malicious Websites
URL	http://www.bing.com/

To have the rating of this web page re-evaluated please click here.

2. Click **Proceed**.

You might receive a certificate warning at this stage. This is normal and is the result of using a self-signed certificate. Accept the warning message to proceed with the remainder of the procedure (click **Advanced**, and then click **Accept the Risk and Continue**).

3. Enter the following credentials:

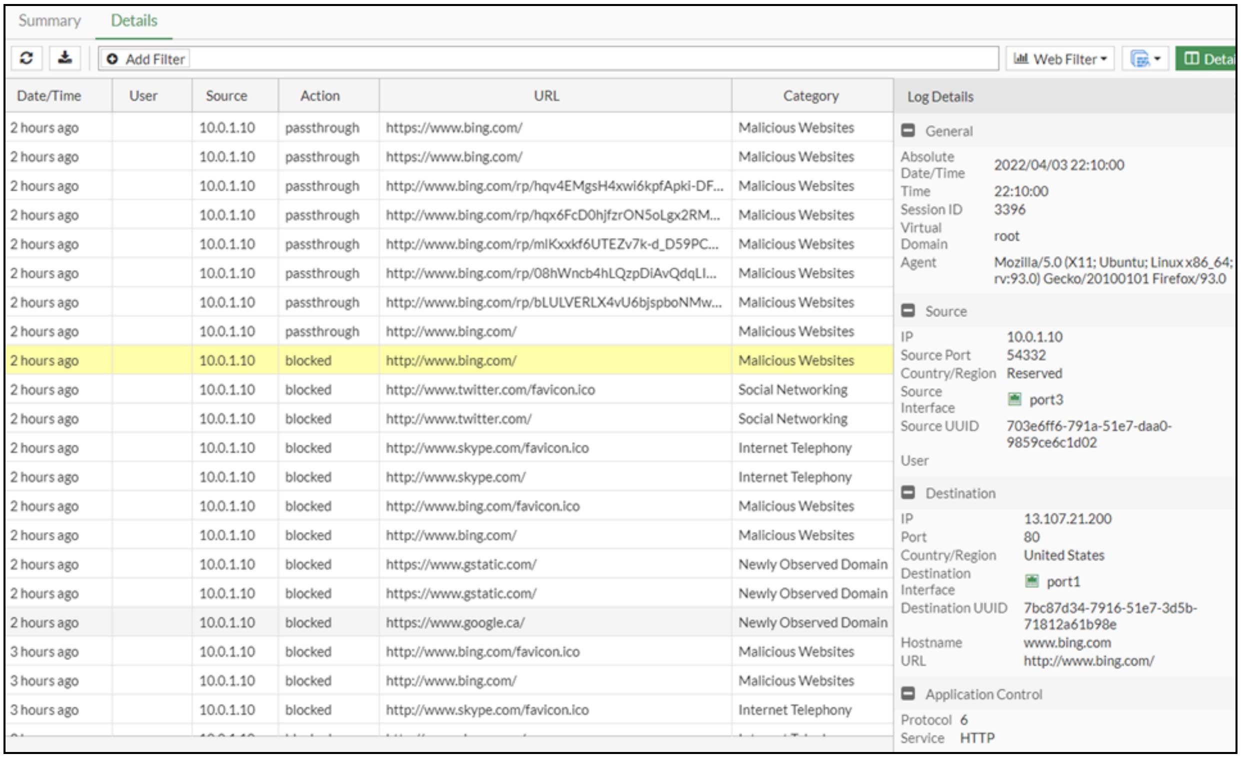
Field	Value
Username	student
Password	fortinet

4. Click **Continue**.

   This website now displays correctly.

To review the web filter logs for web rating overrides

1. Return to your browser tab where you are logged in to the Local-FortiGate GUI, and then click **Log & Report** > **Security Events**.
2. Under **Summary**, click **Web Filter**.



Date/Time	User	Source	Action	URL	Category
2 hours ago		10.0.1.10	passthrough	https://www.bing.com/	Malicious Websites
2 hours ago		10.0.1.10	passthrough	https://www.bing.com/	Malicious Websites
2 hours ago		10.0.1.10	passthrough	http://www.bing.com/rp/hqv4EMgsH4xwi6kpfApki-DF...	Malicious Websites
2 hours ago		10.0.1.10	passthrough	http://www.bing.com/rp/hqx6FcD0hjfzrON5oLgx2RM...	Malicious Websites
2 hours ago		10.0.1.10	passthrough	http://www.bing.com/rp/mlKxxkf6UTEZv7k-d_D59PC...	Malicious Websites
2 hours ago		10.0.1.10	passthrough	http://www.bing.com/rp/08hWncb4hLQzpDiAvQdqLl...	Malicious Websites
2 hours ago		10.0.1.10	passthrough	http://www.bing.com/rp/bLULVERLX4vU6bjspboNMw...	Malicious Websites
2 hours ago		10.0.1.10	passthrough	http://www.bing.com/	Malicious Websites
2 hours ago		10.0.1.10	blocked	http://www.bing.com/	Malicious Websites
2 hours ago		10.0.1.10	blocked	http://www.twitter.com/favicon.ico	Social Networking
2 hours ago		10.0.1.10	blocked	http://www.twitter.com/	Social Networking
2 hours ago		10.0.1.10	blocked	http://www.skype.com/favicon.ico	Internet Telephony
2 hours ago		10.0.1.10	blocked	http://www.skype.com/	Internet Telephony
2 hours ago		10.0.1.10	blocked	http://www.bing.com/favicon.ico	Malicious Websites
2 hours ago		10.0.1.10	blocked	http://www.bing.com/	Malicious Websites
2 hours ago		10.0.1.10	blocked	https://www.gstatic.com/	Newly Observed Domain
2 hours ago		10.0.1.10	blocked	https://www.gstatic.com/	Newly Observed Domain
2 hours ago		10.0.1.10	blocked	https://www.google.ca/	Newly Observed Domain
3 hours ago		10.0.1.10	blocked	http://www.bing.com/favicon.ico	Malicious Websites
3 hours ago		10.0.1.10	blocked	http://www.bing.com/	Malicious Websites
3 hours ago		10.0.1.10	blocked	http://www.skype.com/favicon.ico	Internet Telephony

Log Details

General

Absolute Date/Time	2022/04/03 22:10:00
Time	22:10:00
Session ID	3396
Virtual Domain	root
Agent	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:93.0) Gecko/20100101 Firefox/93.0

Source

IP	10.0.1.10
Source Port	54332
Country/Region	Reserved
Source Interface	port3
Source UUID	703e6ff6-791a-51e7-daa0-9859ce6c1d02
User	

Destination

IP	13.107.21.200
Port	80
Country/Region	United States
Destination Interface	port1
Destination UUID	7bc87d34-7916-51e7-3d5b-71812a61b98e
Hostname	www.bing.com
URL	http://www.bing.com/

Application Control

Protocol	6
Service	HTTP

According to the logs, `http://www.bing.com` was initially blocked, but after you clicked **Proceed** and authenticated, the logs show a different action: **passthrough**.

Remember, `http://www.bing.com` is rated by FortiGuard as belonging to the **Search Engines and Portals** category, where the action, by default, is set to **Allow**.

However, for this website, you changed the subcategory to **Malicious Websites**.

Lab 8: Application Control

In this lab, you will configure and use application control in profile-based mode and policy-based mode to apply an appropriate action to specific application traffic. You will then view the generated logs.

Objectives

- Configure and test application control in NGFW profile mode
- Configure and test application control in NGFW policy mode
- Read and understand application control logs

Time to Complete

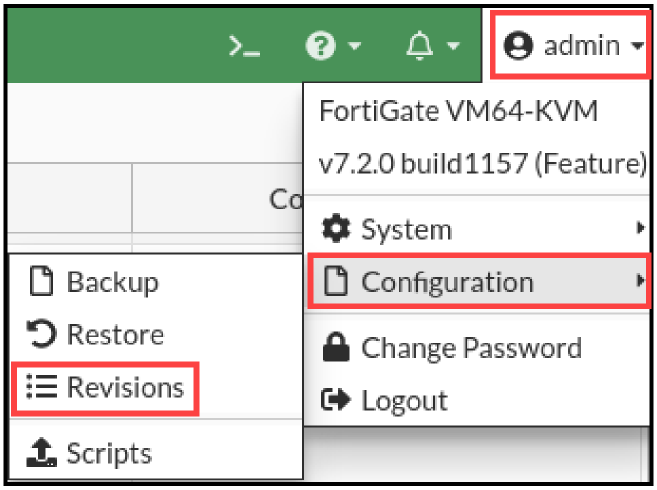
Estimated: 30 minutes

Prerequisites

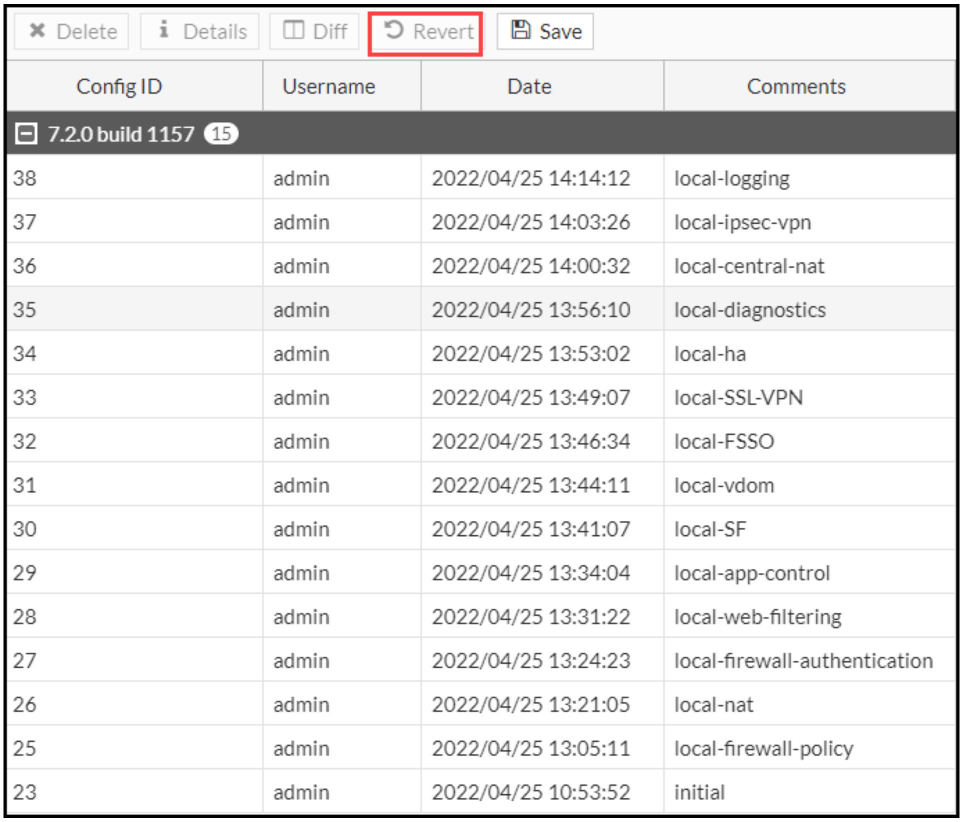
Before beginning this lab, you must restore a configuration file to Local-FortiGate.

To restore the FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **local-app-control**, and then click **Revert**.



Config ID	Username	Date	Comments
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

Exercise 1: Controlling Application Traffic

In this exercise, you will create a profile-based application control profile in flow-based inspection mode. Flow-based and proxy-based inspection modes share identical configuration steps for application control. FortiGate matches the traffic in the following order:

1. Application and filter overrides
2. Categories

You will also view the application control logs to confirm that FortiGate identifies applications and takes the configured actions on them.

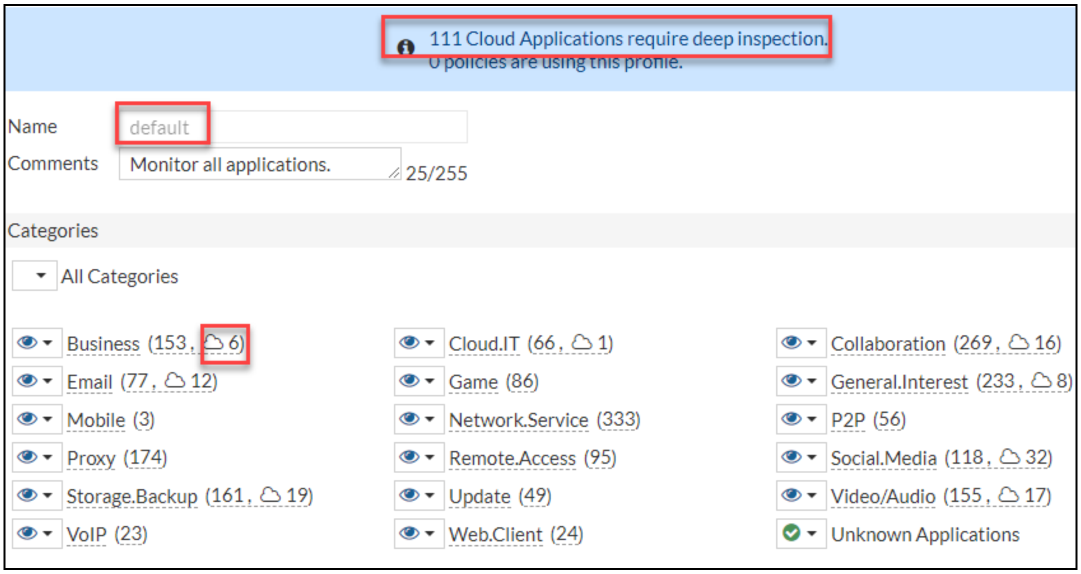
Configure Filter Overrides

The configuration file for this exercise has the application control categories set to **Monitor** (except for **Unknown Applications**). This allows the applications to pass, but also records a log message.

You will configure filter overrides.

To configure filter overrides

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Security Profiles** > **Application Control**.
3. Double-click the **default** application control profile to edit it.



111 Cloud Applications require deep inspection.
0 policies are using this profile.

Name: default
Comments: Monitor all applications. 25/255

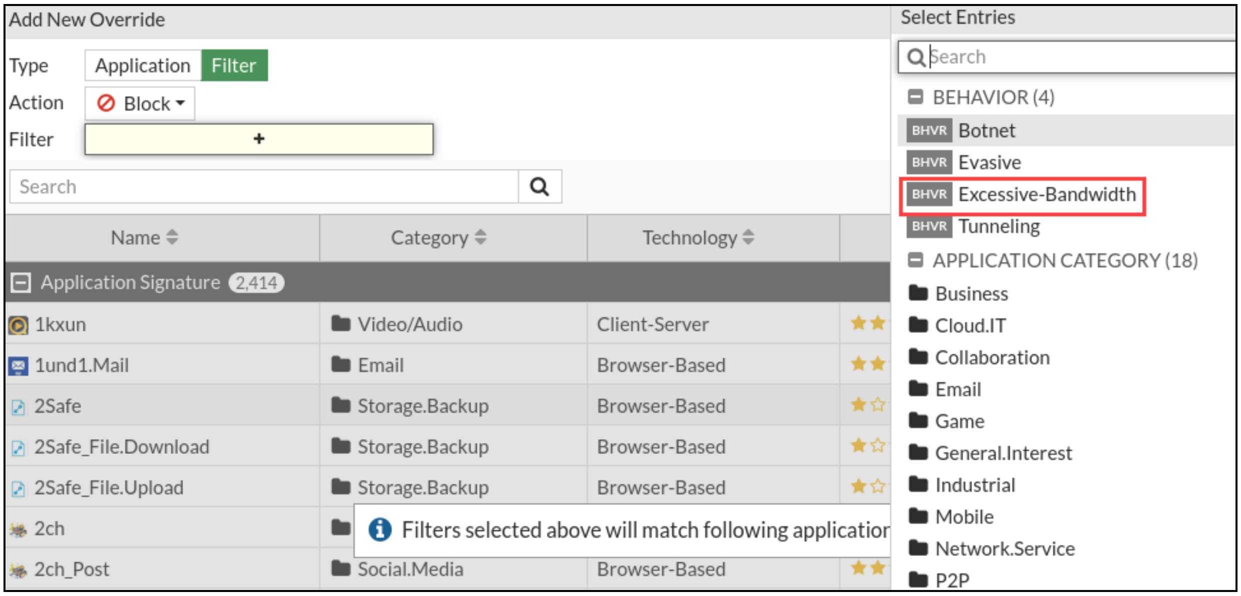
Categories

All Categories

Business (153, ☁ 6)	Cloud.IT (66, ☁ 1)	Collaboration (269, ☁ 16)
Email (77, ☁ 12)	Game (86)	General.Interest (233, ☁ 8)
Mobile (3)	Network.Service (333)	P2P (56)
Proxy (174)	Remote.Access (95)	Social.Media (118, ☁ 32)
Storage.Backup (161, ☁ 19)	Update (49)	Video/Audio (155, ☁ 17)
VoIP (23)	Web.Client (24)	✓ Unknown Applications

There are 111 cloud-based application signatures available in the application control signatures database that require deep inspection. The number beside the cloud icon in each category represents the number of cloud application signatures in a specific category. The number of cloud applications increases as new applications are added to this list.

4. In the **Application and Filter Overrides** section, click **Create New** to add a filter override.
5. On the **Add New Override** page, in the **Type** field, select **Filter**.
6. Click **+** to add a filter.
7. Under **BEHAVIOR**, click **Excessive-Bandwidth**.



Add New Override

Type: Application | **Filter**

Action: ⊘ Block ▾

Filter: +

Search

Name	Category	Technology	
Application Signature 2,414			
1kxun	Video/Audio	Client-Server	★★
1und1.Mail	Email	Browser-Based	★★
2Safe	Storage.Backup	Browser-Based	★☆
2Safe_File.Download	Storage.Backup	Browser-Based	★☆
2Safe_File.Upload	Storage.Backup	Browser-Based	★☆
2ch			
2ch_Post	Social.Media	Browser-Based	★★

ℹ Filters selected above will match following application

Select Entries

Search

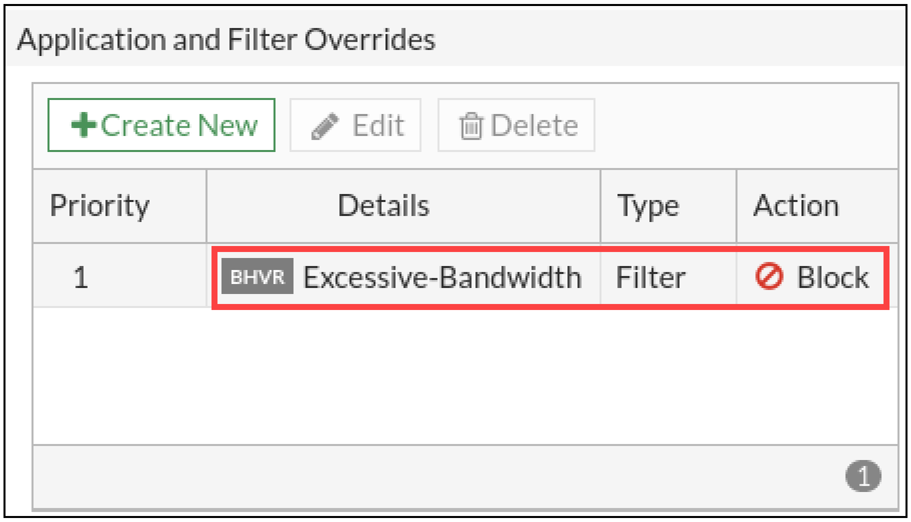
BEHAVIOR (4)
- BHVR Botnet
- BHVR Evasive
- BHVR Excessive-Bandwidth
- BHVR Tunneling

APPLICATION CATEGORY (18)
- Business
- Cloud.IT
- Collaboration
- Email
- Game
- General.Interest
- Industrial
- Mobile
- Network.Service
- P2P

The **Excessive-Bandwidth** setting blocks many applications that are known to be bandwidth intensive. Applications can belong to different categories, but they may be part of this behavior filter if they are bandwidth intensive.

8. Click **OK**.

Your configuration should look similar to the following image. The **Action** should be set to **Block**.



Application and Filter Overrides

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	⊘ Block

9. Click **OK**.

Apply the Application Control Profile to the Firewall Policy

Now that you configured the application control profile, you will apply it to the firewall policy.

Take the Expert Challenge!

On the Local-FortiGate GUI, edit the existing **Application_Control** firewall policy and do the following:

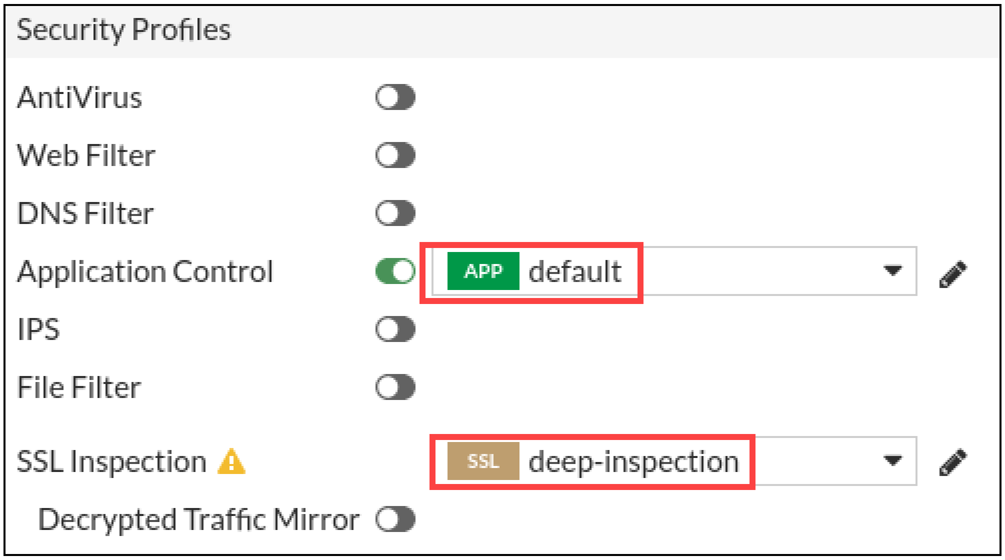
- Enable the **default** application control profile.
- Enable **deep-inspection** in the SSL/SSH inspection profile.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Test the Application Control Profile on page 137.

To apply the application control profile to the firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **+** to expand the policy list.
3. Double-click the **Application_Control** firewall policy to edit it.
4. In the **Security Profiles** section, enable **Application Control**, and then select **default** in the drop-down list.
5. In the **SSL Inspection** field, select the **deep-inspection** profile in the drop-down list.



Security Profiles

AntiVirus ○

Web Filter ○

DNS Filter ○

Application Control ● APP default

IPS ○

File Filter ○

SSL Inspection ⚠ SSL deep-inspection

Decrypted Traffic Mirror ○

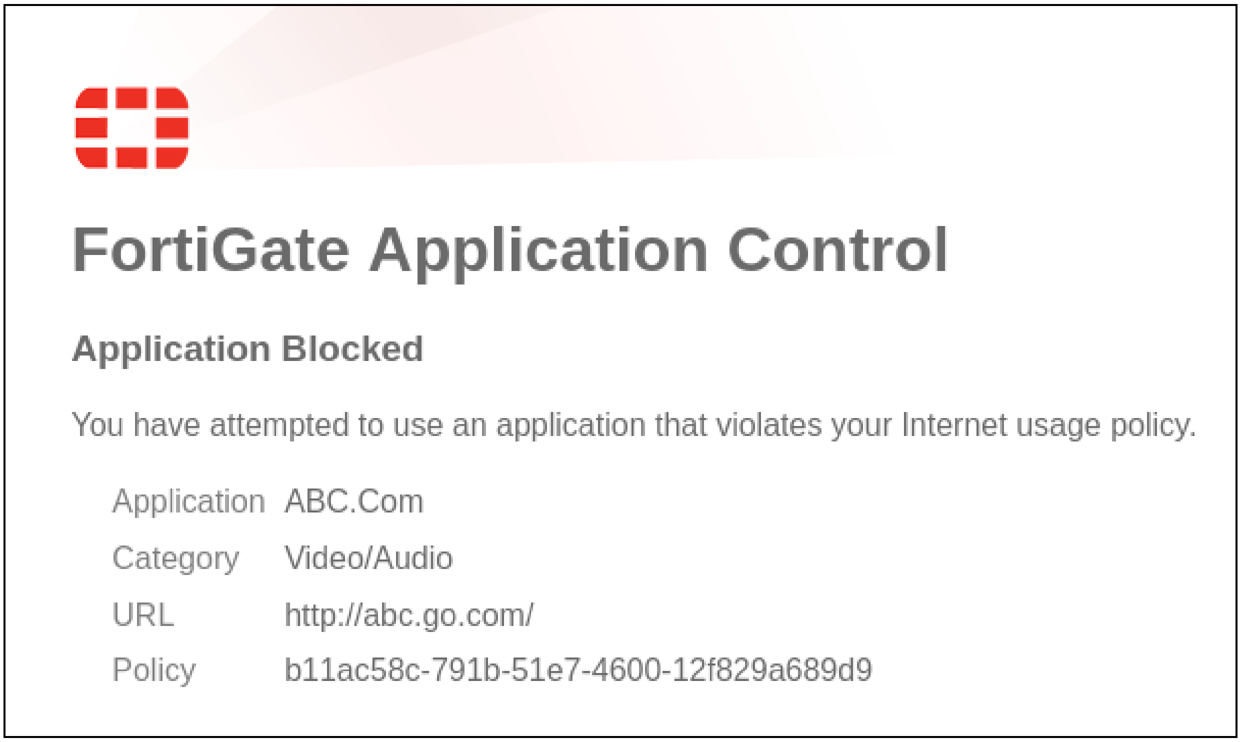
6. Click **OK** to save the changes.

Test the Application Control Profile

You will test the application control profile by going to the application that you blocked in the application override configuration.

To test the application control profile

1. On the Local-Client VM, open a new browser tab, and then go to the following URL: http://abc.go.com.
   You should see that you cannot connect to this site—it times out.
2. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and then click **Security Profiles** > **Application Control**.
3. Edit the **default** application sensor again.
4. In the **Options** section at the bottom of the page, enable **Replacement Messages for HTTP-based Applications**.
5. Click **OK**.
6. Open a new browser tab, and then go to the following URL: http://abc.go.com.
   FortiGate should display a block message—it can take up to two minutes for the block page to appear because of the change in configuration.



FortiGate Application Control

Application Blocked

You have attempted to use an application that violates your Internet usage policy.

Application	ABC.Com
Category	Video/Audio
URL	http://abc.go.com/
Policy	b11ac58c-791b-51e7-4600-12f829a689d9

If the FortiGate self-signed, full-inspection certificate is not installed on the browser, end users see a certificate warning message. In this lab environment, the FortiGate self-signed SSL inspection certificate is installed on the browser. If the block page does not appear after two minutes, close all browser tabs, and then restart the browser.

Configure Application Overrides

You will configure application overrides. The application overrides take precedence over filter overrides and application categories.

Take the Expert Challenge!

On the Local-FortiGate GUI, complete the following:

- Modify the **default** application control profile.
- Add **Application Overrides** for the **ABC.Com** application signature, and set the action to **Allow**.

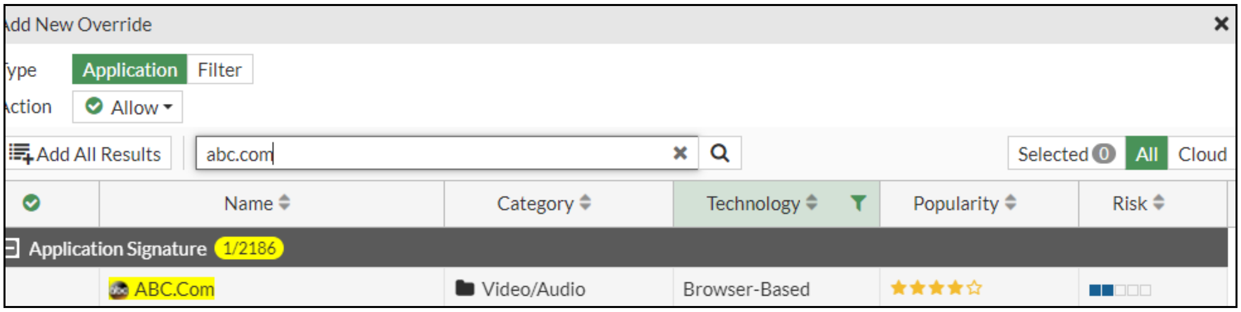
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Test Application Overrides on page 139.

To configure application overrides

1. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and then click **Security Profiles** > **Application Control**.
2. Edit the **default** application sensor again.
3. In the **Application and Filter Overrides** section, click **Create New**.
4. On the **Add New Override** page, in the **Type** field, select **Application**.
5. In the **Action** field, select **Allow**.
6. In the search field, type `abc.com`, and then press `Enter`.

   A signature is returned.



dd New Override

ype: Application | Filter

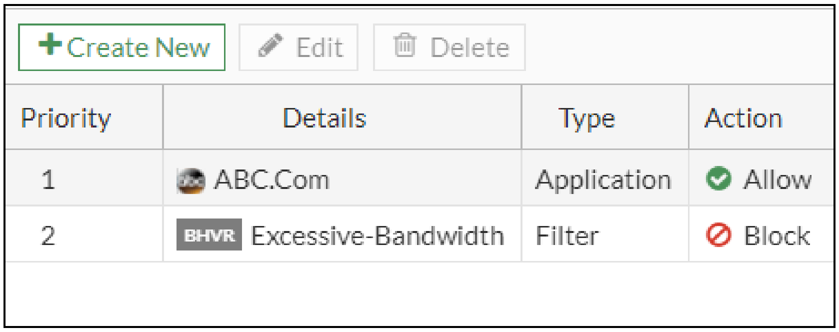
ction: Allow

Add All Results | abc.com | Selected 0 | All | Cloud

	Name	Category	Technology	Popularity	Risk
Application Signature 1/2186					
	ABC.Com	Video/Audio	Browser-Based	★★★★☆	■■□□□

7. Right-click **ABC.Com**, and then click **Add Selected.**
8. Click **OK**.
9. Drag the **ABC.Com** application filter and place it above the **Excessive-Bandwidth** filter.

   Your configuration should look like the following image:



Priority	Details	Type	Action
1	ABC.Com	Application	✓ Allow
2	BHVR Excessive-Bandwidth	Filter	⊘ Block

10. Click **OK**.

This application control profile is already applied to a firewall policy that is scanning all outbound traffic. You do not need to reapply the application control profile for the changes to take effect.

Test Application Overrides

You will test the application control profile by going to the application that you allowed.

To test the application control profile

1. On the Local-Client VM, open a new browser tab, and then go to the following URL: http://abc.go.com.

   FortiGate allows the website to load properly.

View Logs

You will view the logs for the test you just performed.

To view logs

1. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and then click **Log & Report** > **Security Events**.
2. Under **Summary**, click **Application Control**.
3. Use the **Application Name** log filter, and then search for **ABC.Com**.

   You will see log messages with the action set to **block**.

4. Double-click a log to view more details.

   The details include application sensor name, application name, category, policy ID, and the action taken by FortiGate.

5. Click **Log & Report** > **Forward Traffic**, and then search and view the log information for **ABC.Com**.

   You can see more details about the log, including translated IP, bytes sent, bytes received, action, and application.

Exercise 2: Controlling Application Bandwidth Usage

You can limit the bandwidth consumption of an application category or a specific application by configuring a traffic shaping policy. You must ensure that the matching criteria aligns with the firewall policy or policies that you want to apply shaping to.

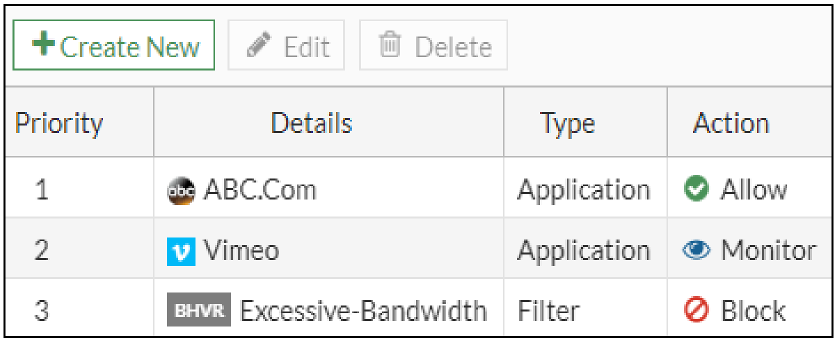
In this exercise, you will configure and apply traffic shaping to an application to limit its bandwidth consumption.

Modify the Application Override Action

You will add the application override for the Vimeo application to the application control profile. Then, you will apply traffic shaping in the next procedure.

To add the application override action

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Security Profiles** > **Application Control**.
3. Edit the **default** application sensor.
4. In the **Application and Filter Overrides** section, click **Create New**.
5. On the **Add New Override** page, in the **Type** field, select **Application**.
6. In the **Action** field, select **Monitor**.
7. In the search field, type `Vimeo`, and then press `Enter`.
8. Right-click **Vimeo**, and then click **Add Selected**.
9. Click **OK**.
10. Drag the **Vimeo** application filter and place it above the **Excessive-Bandwidth** filter.
    Your configuration should look like the following image:



Priority	Details	Type	Action
1	ABC.Com	Application	✓ Allow
2	Vimeo	Application	Monitor
3	BHVR Excessive-Bandwidth	Filter	⊘ Block

11. Click **OK**.

For the purposes of this lab, setting the action to **Monitor** ensures all application control events are logged.

Configure a Traffic Shaping Policy

You will configure a traffic shaping policy using the preconfigured traffic shaper to limit the bandwidth usage of the Vimeo application.

Take the Expert Challenge!

On the Local-FortiGate GUI, complete the following:

- Create a traffic shaping policy for the Vimeo application only from port1.
- Apply the **VIMEO_SHAPER** as the **Reverse Shaper**.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

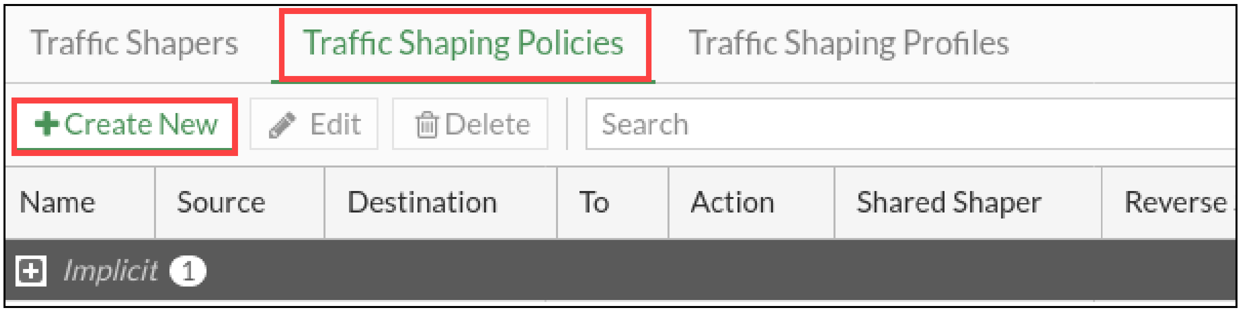
After you complete the challenge, see Test Traffic Shaping on page 144.

To configure a traffic shaping policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Traffic Shaping** > **Traffic Shapers**.
2. For the **VIMEO_SHAPER**, examine the **Max Bandwidth** column.

   You will notice that the maximum amount of allowed bandwidth is very low.

3. Click **Policy & Objects** > **Traffic Shaping**, and then click **Traffic Shaping Policies**.
4. Click **Create New**.

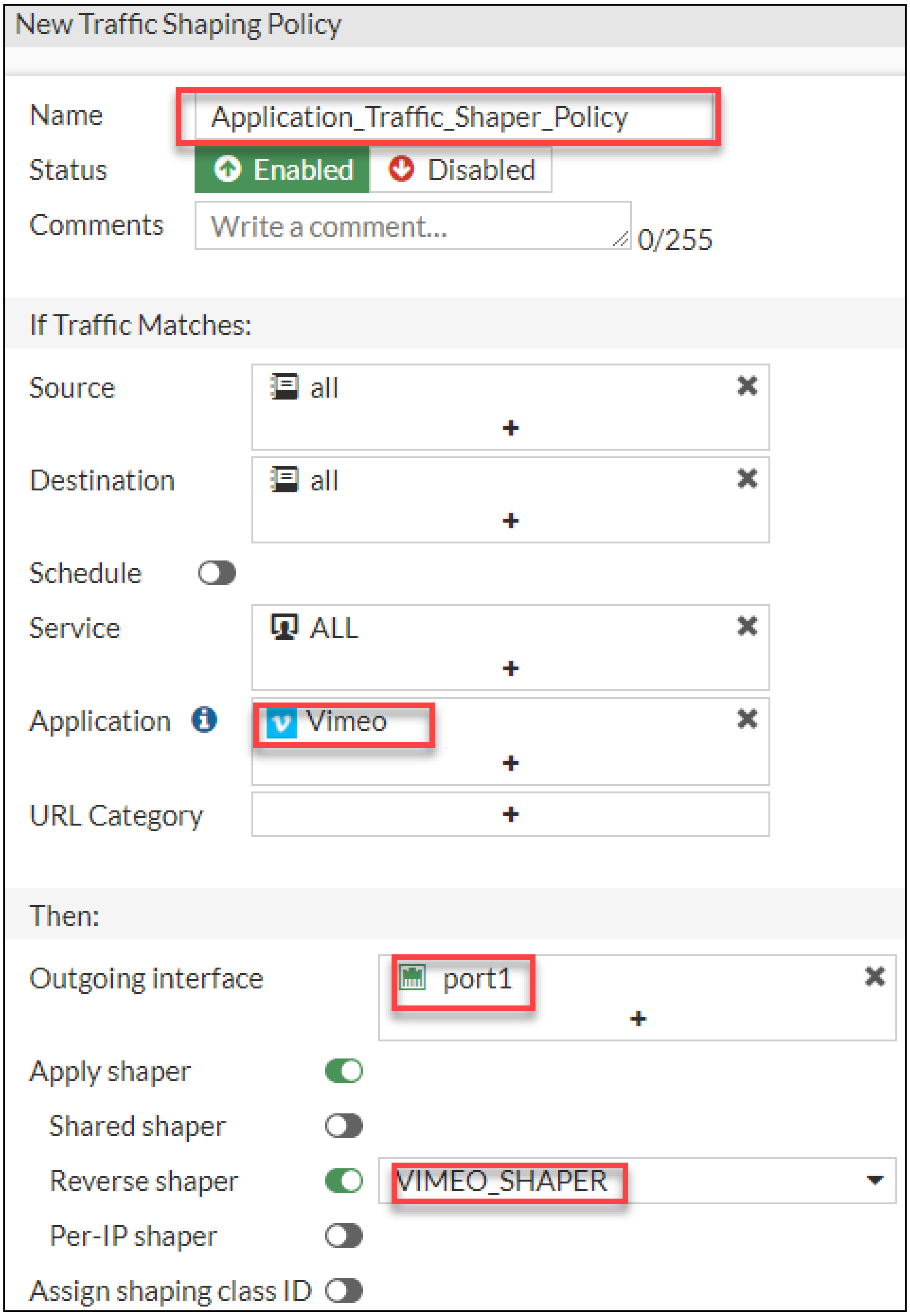


5. Configure the following settings:

Field	Value
Name	Application_Traffic_Shaper_Policy
Source	all
Destination	all
Service	ALL

Field	Value
Application	Vimeo **Tip**: Type `Vimeo` in the search box in the right pane to locate it easily.
Outgoing interface	port1 This is the FortiGate egress interface.
Apply shaper	<enable>
Reverse shaper	<enable> and apply **VIMEO_SHAPER**

Your configuration should look like the following image:



New Traffic Shaping Policy

Name: Application_Traffic_Shaper_Policy

Status: Enabled | Disabled

Comments: Write a comment... 0/255

If Traffic Matches:

Source: all

Destination: all

Schedule: ○

Service: ALL

Application: Vimeo

URL Category:

Then:

Outgoing interface: port1

Apply shaper: ●

Shared shaper: ○

Reverse shaper: ● VIMEO_SHAPER

Per-IP shaper: ○

Assign shaping class ID: ○

6. Click **OK**.

The **Shared Shaper** option limits the bandwidth from ingress-to-egress. It is useful for limiting uploading bandwidth. The **Reverse Shaper** limits the bandwidth from egress-to-ingress. It is useful for limiting downloading or streaming bandwidth.

You must ensure that the matching criteria aligns with the firewall policy or policies that you want to apply traffic shaping to.

Test Traffic Shaping

You will test traffic shaping by playing a video on Vimeo.

To test traffic shaping

1. On the Local-Client VM, open a new browser tab, and then go to the following URL: `http://vimeo.com/watch`.
2. Try to play any video.

   You will notice that access to this site is slow and the video is taking a long time to buffer and play.

If your classroom uses a virtual lab, the underlying hardware is shared, so the amount of available bandwidth for internet access varies according to other simultaneous use. The traffic shaper is set to a very low value to make sure that the difference in behavior is easily noticeable. In real networks, this setting would be set to a higher value.

3. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and then click **Policy & Objects** > **Traffic Shaping** > **Traffic Shapers**.
4. Review the **Bandwidth Utilization** and **Dropped Bytes** columns for the **VIMEO_SHAPER**.

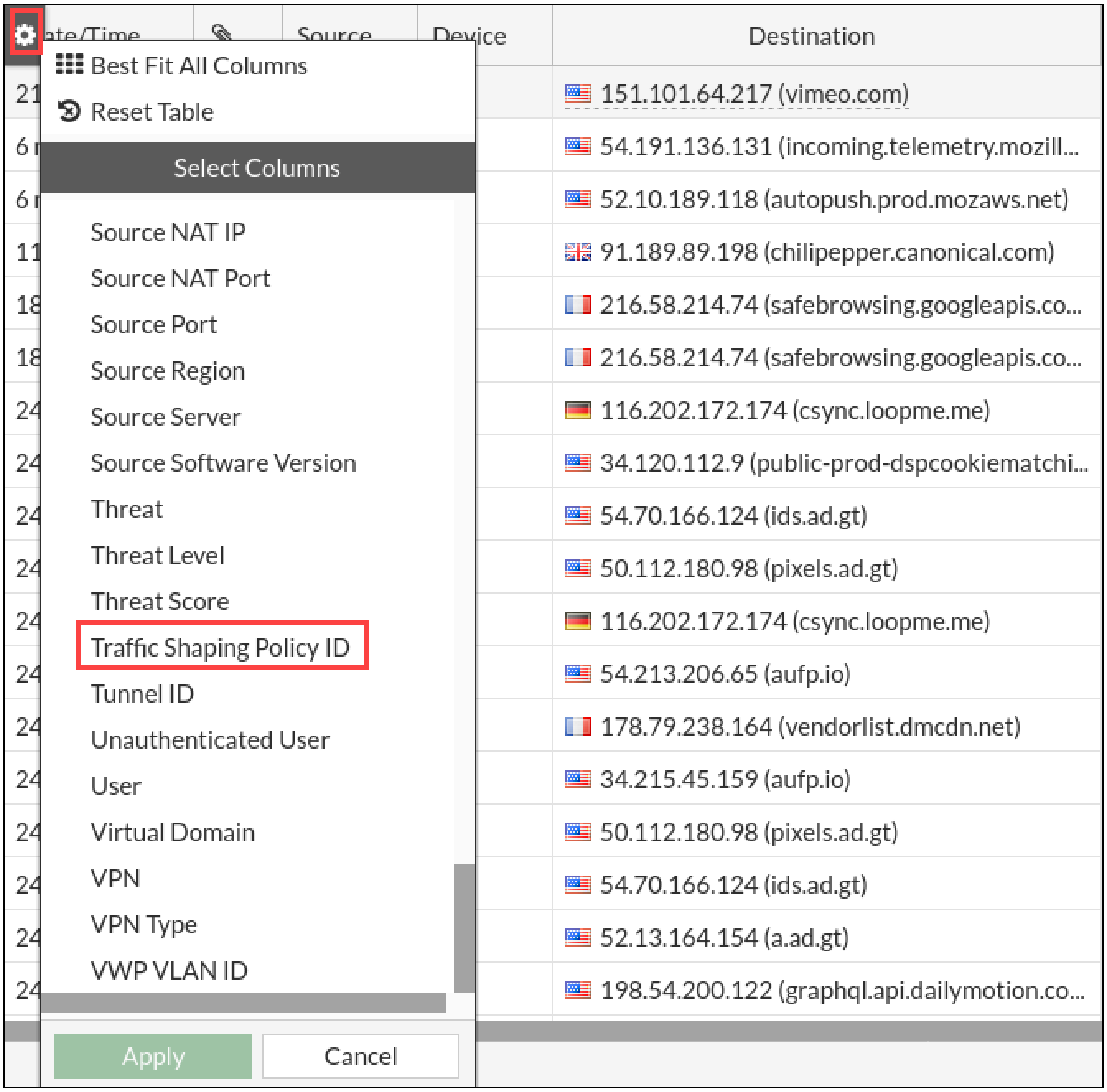
   You might need to refresh the FortiGate GUI to view the statistics on **Traffic Shapers**.

   You will notice the bandwidth used by the Vimeo application, and that FortiGate is dropping the packets that exceed the configured bandwidth in the traffic shaper.

Monitor statistics are current as of the time that you requested the GUI page, so make sure to view them while a video is downloading. Also, refresh the page a few times to get the results.

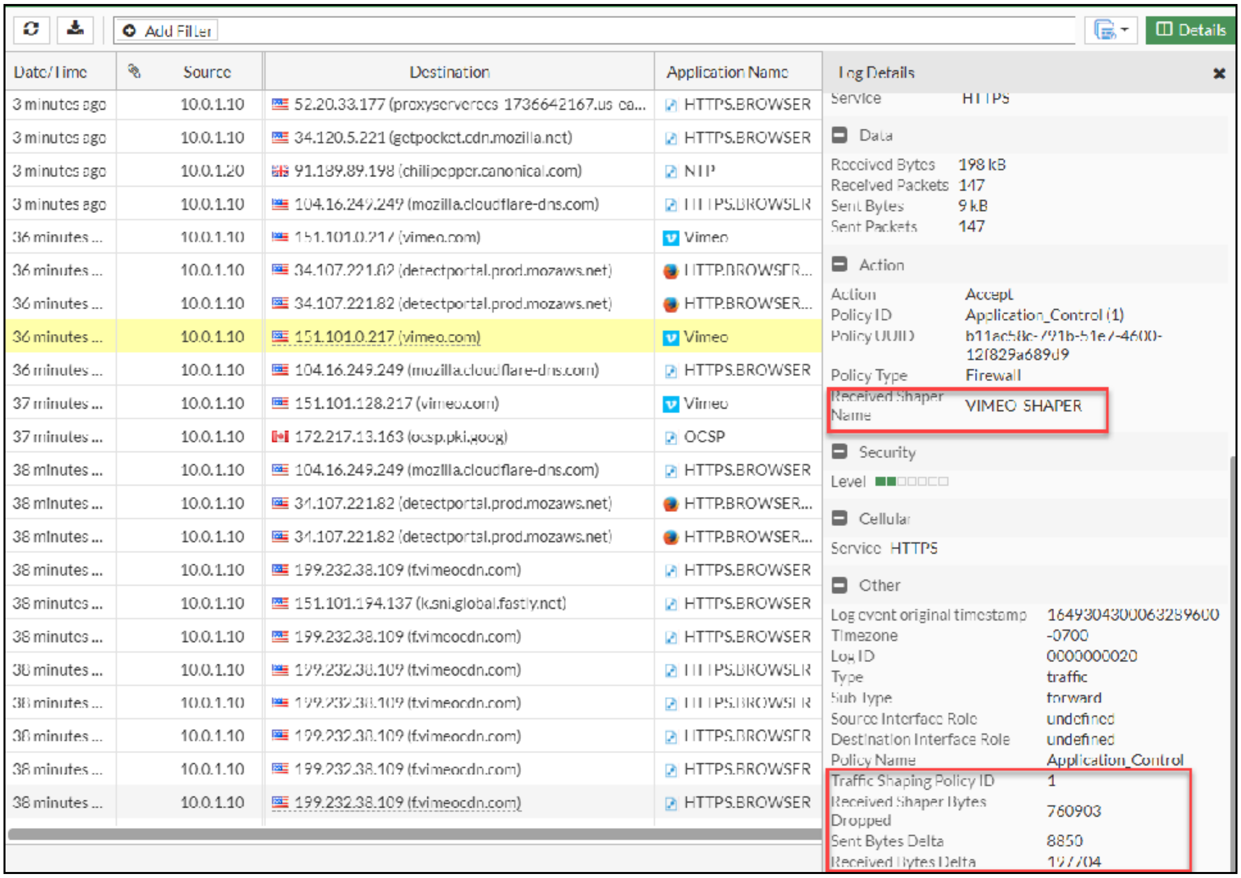
5. Click **Log & Report** > **Forward Traffic**.
6. Click **Configure Table**.
7. Scroll down, and then click **Traffic Shaping Policy ID** to enable it.

   The following image shows the details:



Destination
151.101.64.217 (vimeo.com)
54.191.136.131 (incoming.telemetry.mozill...
52.10.189.118 (autopush.prod.mozaws.net)
91.189.89.198 (chilipepper.canonical.com)
216.58.214.74 (safebrowsing.googleapis.co...
216.58.214.74 (safebrowsing.googleapis.co...
116.202.172.174 (csync.loopme.me)
34.120.112.9 (public-prod-dspcookiematchi...
54.70.166.124 (ids.ad.gt)
50.112.180.98 (pixels.ad.gt)
116.202.172.174 (csync.loopme.me)
54.213.206.65 (aufp.io)
178.79.238.164 (vendorlist.dmcdn.net)
34.215.45.159 (aufp.io)
50.112.180.98 (pixels.ad.gt)
54.70.166.124 (ids.ad.gt)
52.13.164.154 (a.ad.gt)
198.54.200.122 (graphql.api.dailymotion.co...

8. Click **Apply**.
9. Review the logs to display basic information about the **Traffic Shaper** policy.



Date/Time	Source	Destination	Application Name
3 minutes ago	10.0.1.10	52.20.33.177 (proxyserverces 1736642167.us ca...	HTTPS.BROWSER
3 minutes ago	10.0.1.10	34.120.5.221 (getpocket.cdn.mozilla.net)	HTTPS.BROWSER
3 minutes ago	10.0.1.20	91.189.89.198 (chilipepper.canonical.com)	NTP
3 minutes ago	10.0.1.10	104.16.249.249 (mozilla.cloudflare-dns.com)	HTTPS.BROWSER
36 minutes ...	10.0.1.10	151.101.0.217 (vimeo.com)	Vimeo
36 minutes ...	10.0.1.10	34.107.221.82 (detectportal.prod.mozaws.net)	HTTP.BROWSER...
36 minutes ...	10.0.1.10	34.107.221.82 (detectportal.prod.mozaws.net)	HTTP.BROWSER...
36 minutes ...	10.0.1.10	151.101.0.217 (vimeo.com)	Vimeo
36 minutes ...	10.0.1.10	104.16.249.249 (mozilla.cloudflare-dns.com)	HTTPS.BROWSER
37 minutes ...	10.0.1.10	151.101.128.217 (vimeo.com)	Vimeo
37 minutes ...	10.0.1.10	172.217.13.163 (ocsp.pki.goog)	OCSP
38 minutes ...	10.0.1.10	104.16.249.249 (mozilla.cloudflare-dns.com)	HTTPS.BROWSER
38 minutes ...	10.0.1.10	34.107.221.82 (detectportal.prod.mozaws.net)	HTTP.BROWSER...
38 minutes ...	10.0.1.10	34.107.221.82 (detectportal.prod.mozaws.net)	HTTP.BROWSER...
38 minutes ...	10.0.1.10	199.232.38.109 (f.vimeocdn.com)	HTTPS.BROWSER
38 minutes ...	10.0.1.10	151.101.194.137 (k.sni.global.fastly.net)	HTTPS.BROWSER
38 minutes ...	10.0.1.10	199.232.38.109 (f.vimeocdn.com)	HTTPS.BROWSER
38 minutes ...	10.0.1.10	199.232.38.109 (f.vimeocdn.com)	HTTPS.BROWSER
38 minutes ...	10.0.1.10	199.232.38.109 (f.vimeocdn.com)	HTTPS.BROWSER
38 minutes ...	10.0.1.10	199.232.38.109 (f.vimeocdn.com)	HTTPS.BROWSER
38 minutes ...	10.0.1.10	199.232.38.109 (f.vimeocdn.com)	HTTPS.BROWSER
38 minutes ...	10.0.1.10	199.232.38.109 (f.vimeocdn.com)	HTTPS.BROWSER

Service	HTTPS
Data	
Received Bytes	198 kB
Received Packets	147
Sent Bytes	9 kB
Sent Packets	147
Action	
Action	Accept
Policy ID	Application_Control (1)
Policy UUID	b11ac58c-791b-51e7-4600-12f829a689d9
Policy Type	Firewall
Received Shaper Name	VIMEO_SHAPER
Security	
Level	■■□□□□□
Cellular	
Service	HTTPS
Other	
Log event original timestamp	1649304300063289600
Timezone	-0700
Log ID	0000000020
Type	traffic
Sub Type	forward
Source Interface Role	undefined
Destination Interface Role	undefined
Policy Name	Application_Control
Traffic Shaping Policy ID	1
Received Shaper Bytes Dropped	760903
Sent Bytes Delta	8850
Received Bytes Delta	197704

Exercise 3: Implementing Application Control in NGFW Policy-Based Mode

In an NGFW firewall, there are two modes that you can use to implement application control in security policies: policy-based mode and profile-based mode. In policy-based NGFW mode, you can implement application control directly in security policies without using application control profiles.

In this exercise, you will enable policy-based NGFW mode on FortiGate, and then implement application control in the security policy to explicitly allow access to only the LinkedIn web application and block access to all other web applications.

Enable Policy-Based NGFW Mode

You will change the NGFW mode on Local-FortiGate from profile-based to policy-based.

To enable policy-based NGFW mode

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **System** > **Settings**.
3. In the **View Settings** section, change **NGFW Mode** to **Policy-based**.
4. Click **Apply**, and then click **OK** to confirm the change.

Changing NGFW modes removes the existing firewall policies and central SNAT. To pass traffic in policy-based NGFW mode, FortiGate requires three types of policies to be configured. This is unlike a profile-based NGFW mode setup, where only one policy is required.

Configure SSL Inspection and Central SNAT Policies

You will modify the default SSL inspection policy to use the deep-inspection SSL inspection profile, and then create a central SNAT policy.

To modify the SSL inspection policy

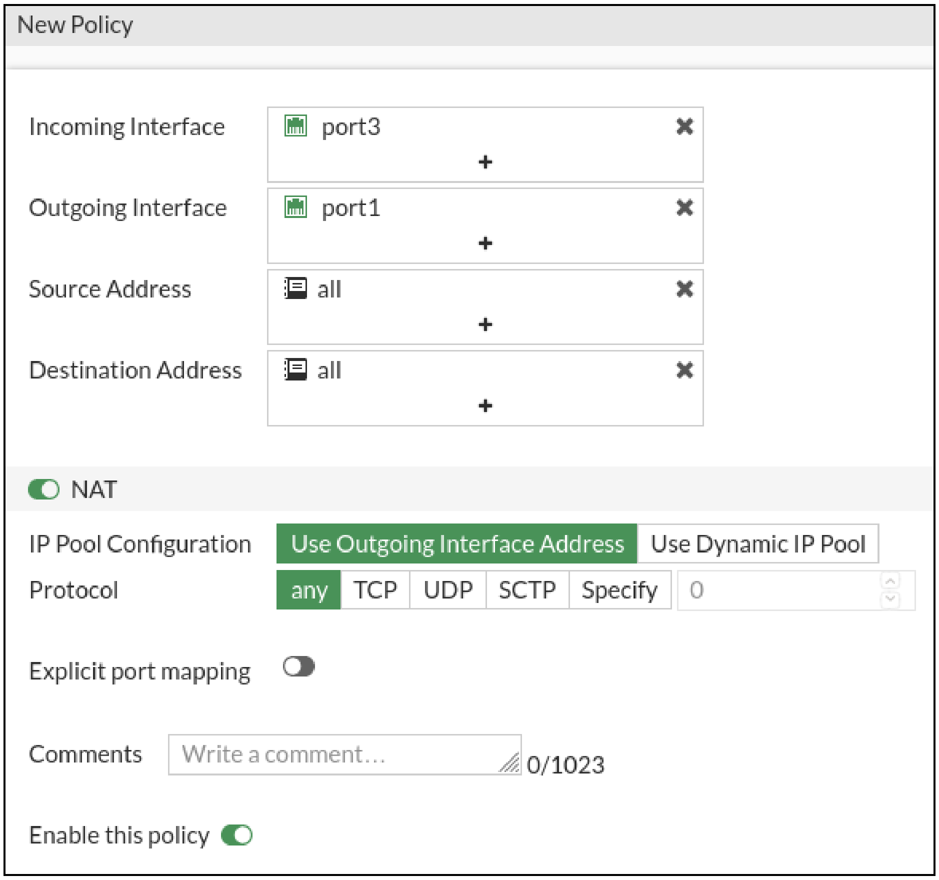
1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **SSL Inspection & Authentication**.
2. Double-click the **Default** policy to edit it.
3. In the **Security Profiles** section, in the **SSL Inspection** field, select the **deep-inspection** profile in the drop-down list.
4. Click **OK**.

To create the central SNAT policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Central SNAT**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Incoming Interface	port3
Outgoing Interface	port1
Source Address	all
Destination Address	all

Your configuration should look like the following image:



New Policy

Incoming Interface: port3

Outgoing Interface: port1

Source Address: all

Destination Address: all

NAT: enabled

IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool

Protocol: any | TCP | UDP | SCTP | Specify | 0

Explicit port mapping: disabled

Comments: Write a comment... 0/1023

Enable this policy: enabled

4. Click **OK**.

Configure the Security Policy and Test Application Control

You will create a security policy to apply the application signature required to allow access to the LinkedIn web application and block access to all other web applications.

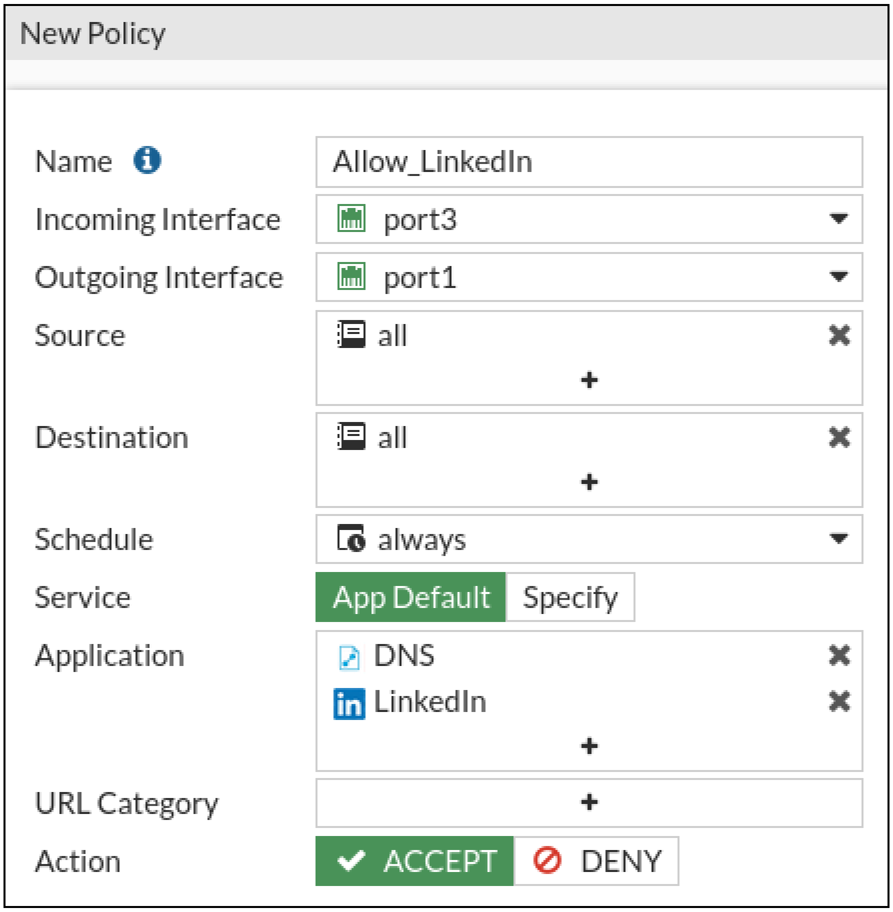
To create a security policy to allow the LinkedIn web application

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Security Policy**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	Allow_LinkedIn
Incoming Interface	port3
Outgoing Interface	port1
Source	all
Destination	all
Application	LinkedIn DNS **Tip**: Type `LinkedIn` in the search box in the right pane to locate it easily.

4. Verify **Action** is set to **ACCEPT**.

Your configuration should look like the following image:



New Policy

Name	Allow_LinkedIn
Incoming Interface	port3
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	App Default | Specify
Application	DNS LinkedIn
URL Category	
Action	✓ ACCEPT | DENY

5. Click **OK**.

FortiGate policy-based NGFW follows the concept of precedence to evaluate security policies. If traffic does not match the created security policy, it is processed by the implicit security policy, which denies access to all other web application traffic.

To test policy-based NGFW mode application control

1. On the Local-Client VM, open a new browser tab, and then go to the following URL:

   ```
   http://linkedin.com
   ```

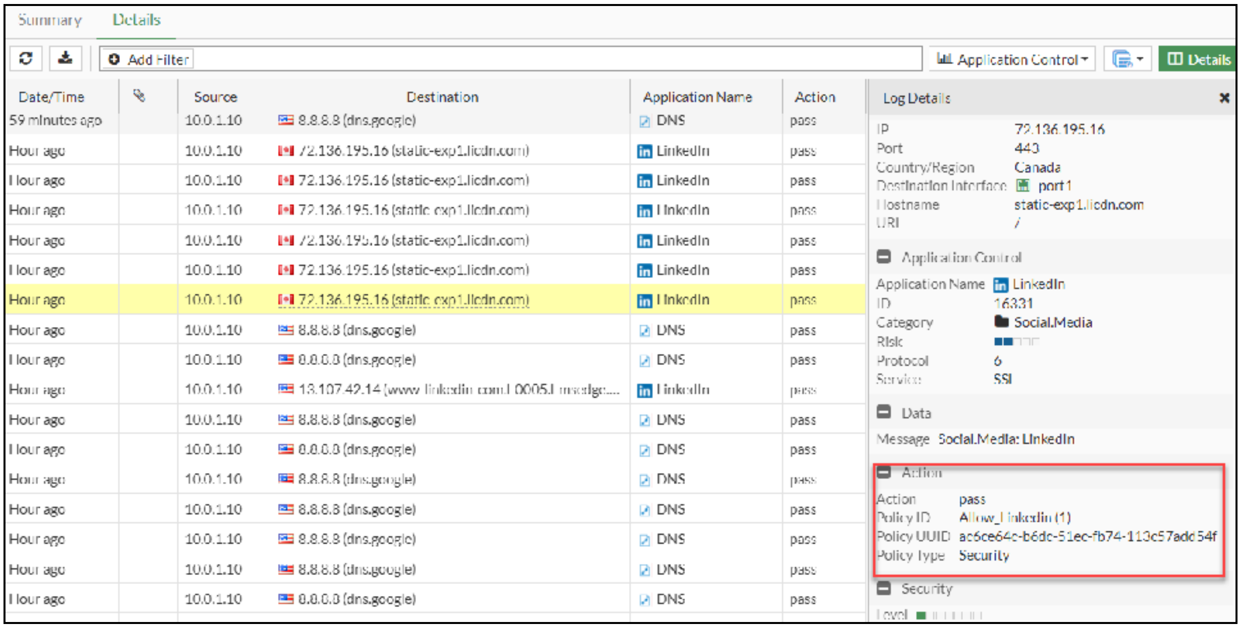
   FortiGate allows the website to load properly.

2. Open a new tab, and then go to the following URL:

   ```
   http://facebook.com
   ```

   FortiGate blocks access to the Facebook web application according to the implicit security policy.

3. Return to your browser tab where you are logged in to the Local-FortiGate GUI.
4. Click **Log & Report** > **Security Events**.
5. Under **Summary**, click **Application Control**.
6. Review the logs that allowed access to the LinkedIn web application.



Date/Time		Source	Destination	Application Name	Action
59 minutes ago		10.0.1.10	8.8.8.8 (dns.google)	DNS	pass
Hour ago		10.0.1.10	72.136.195.16 (static-exp1.licdn.com)	LinkedIn	pass
Hour ago		10.0.1.10	72.136.195.16 (static-exp1.licdn.com)	LinkedIn	pass
Hour ago		10.0.1.10	72.136.195.16 (static-exp1.licdn.com)	LinkedIn	pass
Hour ago		10.0.1.10	72.136.195.16 (static-exp1.licdn.com)	LinkedIn	pass
Hour ago		10.0.1.10	72.136.195.16 (static-exp1.licdn.com)	LinkedIn	pass
Hour ago		10.0.1.10	72.136.195.16 (static-exp1.licdn.com)	LinkedIn	pass
Hour ago		10.0.1.10	8.8.8.8 (dns.google)	DNS	pass
Hour ago		10.0.1.10	8.8.8.8 (dns.google)	DNS	pass
Hour ago		10.0.1.10	13.107.42.14 (www.linkedin.com.l-0005.l-msedge....	LinkedIn	pass
Hour ago		10.0.1.10	8.8.8.8 (dns.google)	DNS	pass
Hour ago		10.0.1.10	8.8.8.8 (dns.google)	DNS	pass
Hour ago		10.0.1.10	8.8.8.8 (dns.google)	DNS	pass
Hour ago		10.0.1.10	8.8.8.8 (dns.google)	DNS	pass
Hour ago		10.0.1.10	8.8.8.8 (dns.google)	DNS	pass
Hour ago		10.0.1.10	8.8.8.8 (dns.google)	DNS	pass
Hour ago		10.0.1.10	8.8.8.8 (dns.google)	DNS	pass

Log Details

IP	72.136.195.16
Port	443
Country/Region	Canada
Destination Interface	port1
Hostname	static-exp1.licdn.com
URI	/

Application Control

Application Name	LinkedIn
ID	16331
Category	Social.Media
Risk	■■□□□
Protocol	6
Service	SSL

Data

Message Social.Media: LinkedIn

Action

Action	pass
Policy ID	Allow_Linkedin (1)
Policy UUID	ac6ce64c-b6dc-51ec-fb74-113c57add54f
Policy Type	Security

Security

Level ■□□□□□□□

Lab 9: Antivirus

In this lab, you will examine how to configure, use, and monitor antivirus scanning on Local-FortiGate in both flow-based and proxy-based inspection modes.

Objectives

- Configure antivirus scanning in both flow-based and proxy-based inspection modes
- Understand FortiGate antivirus scanning behavior
- Scan multiple protocols
- Read and understand antivirus logs
- Understand machine learning (AI) scan

Time to Complete

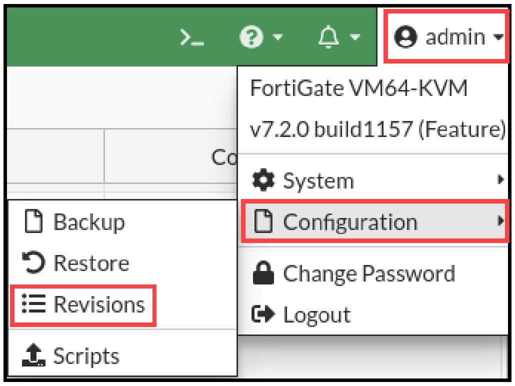
Estimated: 25 minutes

Prerequisites

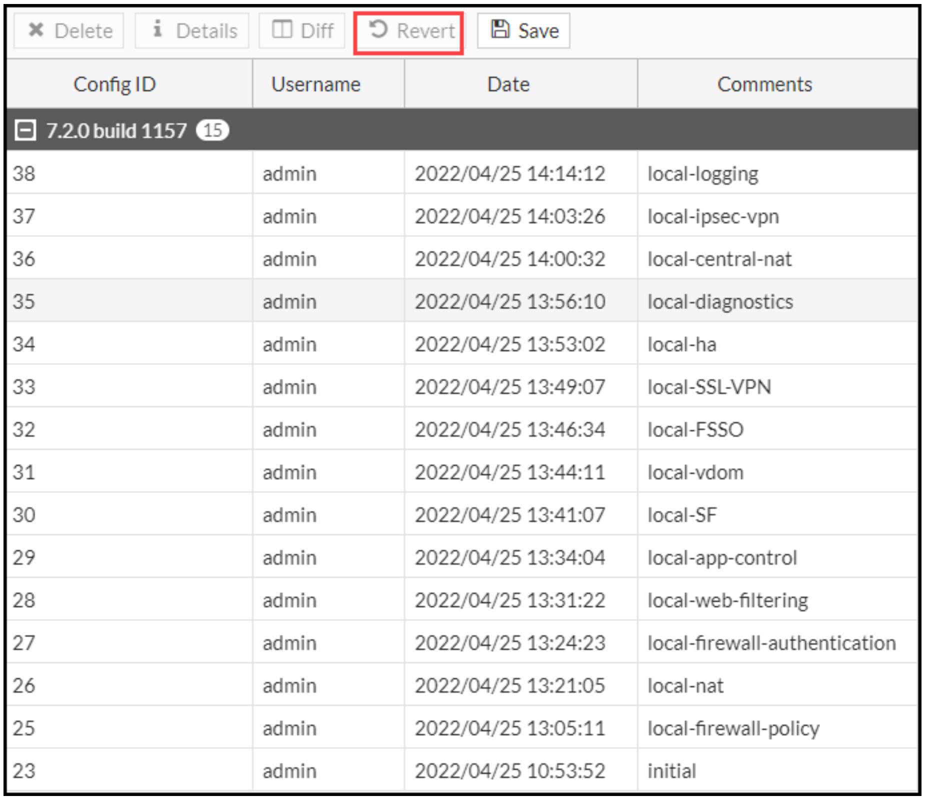
Before beginning this lab, you must restore a configuration file to Local-FortiGate.

To restore the FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click **+** to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.



Config ID	Username	Date	Comments
7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

Exercise 1: Using Antivirus Scanning in Proxy-Based Inspection Mode

In proxy-based inspection mode, the proxy for each protocol buffers the entire file (or waits for oversize limit) and then scans it. The client must wait for the scan to finish.

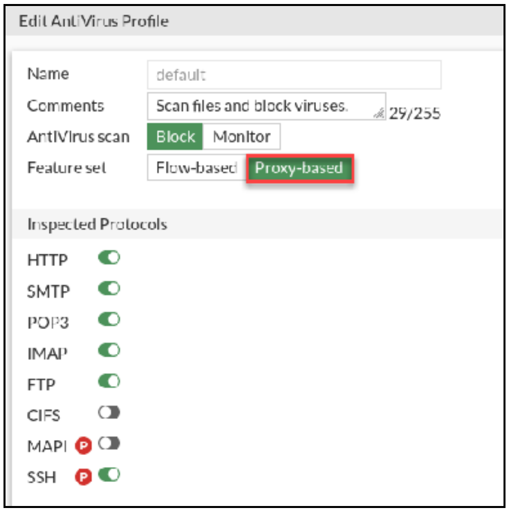
In this exercise, you will examine how to use antivirus in proxy-based inspection mode to understand how FortiGate performs antivirus scanning. You will observe the behavior of antivirus scanning, with and without deep inspection, to understand the importance of performing full-content inspection.

Change the Antivirus Profile Inspection Mode

You will change the inspection mode in the default antivirus profile, which is applied on the firewall policy, to inspect traffic.

To change the antivirus profile inspection mode

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Security Profiles** > **AntiVirus**.
3. Right-click the **default** antivirus profile, and then click **Edit**.
4. In the **Feature set** field, select **Proxy-based**.
5. On the **SSH** protocol, toggle to enable.



Edit AntiVirus Profile

Name: default
Comments: Scan files and block viruses. 29/255
AntiVirus scan: [✓ Block] Monitor
Feature set: Flow-based [✓ Proxy-based]

Inspected Protocols

HTTP ●
SMTP ●
POP3 ●
IMAP ●
FTP ●
CIFS ○
MAPI P ○
SSH P ●

6. Click **OK**.

Feature set is an option to specify the type of antivirus profile applied to a firewall policy. Flow-based antivirus profiles offer higher throughput performance, while proxy-based profiles are useful to mitigate stealthy malicious code.

Enable the Antivirus Profile on a Firewall Policy

By default, flow-based inspection mode is enabled on the FortiGate firewall policy. You will change the inspection mode from flow-based to proxy-based.

Take the Expert Challenge!

On the Local-FortiGate GUI, complete the following:

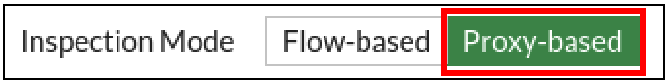
- Edit the **Full_Access** firewall policy, and change the **Inspection Mode** to **Proxy-based**.
- Enable the **default** antivirus profile.
- Use the **certificate-inspection** profile for SSL inspection.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Test the Antivirus Configuration on page 155.

To change the firewall policy inspection mode

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Double-click the **Full_Access** policy to edit it.
3. In the **Inspection Mode** field, select **Proxy-based**.



Inspection Mode Flow-based [✓ Proxy-based]

4. In the **Protocol Options** field, verify the **default** profile is selected.
5. In the **Security Profiles** section, enable **AntiVirus**, and then select **default** from the drop-down list.
6. In the **SSL Inspection** drop-down list, keep the default **certificate-inspection** profile.

The **Protocol Options** profile provides the required settings to hold traffic in proxy while the inspection process is carried out. The default profile is preconfigured to follow the standardized parameters for the common protocols used in networking.

SSL Inspection selects the **certificate-inspection** profile by default. You can select any preconfigured SSL inspection profile in the associated drop-down list.

7. Keep the default values for the remaining settings, and click **OK** to save the changes..

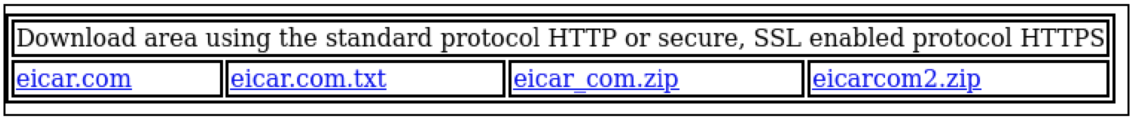
Test the Antivirus Configuration

You will download the EICAR test file to your Local-Client VM. The EICAR test file is an industry-standard virus used to test antivirus detection without causing damage. The file contains the following characters:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

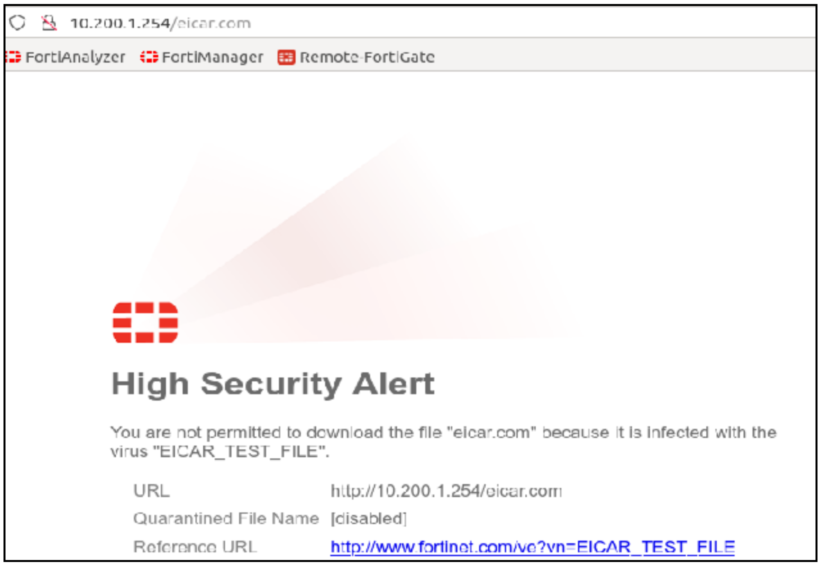
To test the antivirus configuration

1. On the Local-Client VM, open a new web browser tab, and then access the following website:
   `http://10.200.1.254/test_av.html`
2. In the **Download area** section, download any EICAR sample file.



Download area using the standard protocol HTTP or secure, SSL enabled protocol HTTPS			
eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip

FortiGate should block the download attempt, and insert a replacement message similar to the following example:



High Security Alert

You are not permitted to download the file "eicar.com" because it is infected with the virus "EICAR_TEST_FILE".

URL	http://10.200.1.254/eicar.com
Quarantined File Name	[disabled]
Reference URL	http://www.fortinet.com/ve?vn=EICAR_TEST_FILE

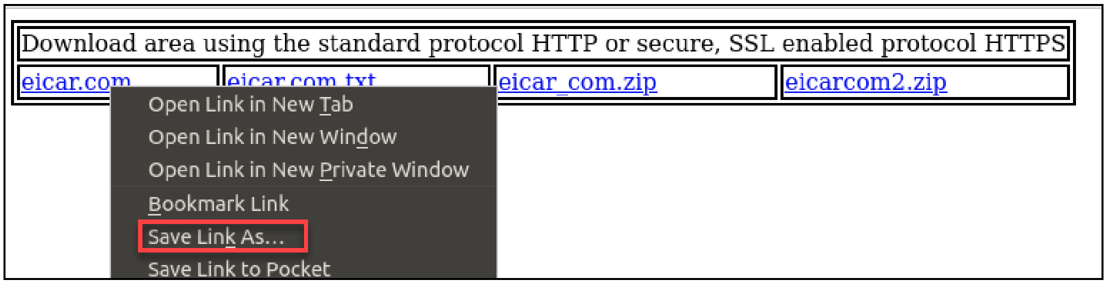
FortiGate shows the HTTP virus message when it blocks or quarantines infected files.

Test an Alternate Download Method

You will test the proxy-based antivirus configuration using the **Save Link As** method to download the EICAR text file.

To test the antivirus configuration

1. On the Local-Client VM, open a new web browser tab, and then go to the following website:
   `http://10.200.1.254/test_av.html`
2. In the **Download area** section, right-click **eicar.com.txt**, and then select **Save Link As**.



Download area using the standard protocol HTTP or secure, SSL enabled protocol HTTPS

eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip

3. Change the download location to **Desktop**, and then click **Save**.

   You should see the file you downloaded on the desktop. Why was the download allowed?

4. On your desktop, right-click the `eicar.com.txt` downloaded file, click **Open With Other Application**, click **Notepad++**, and then click **Select** to open the file you downloaded.

   Is the content of the file what it's supposed to be?

Stop and think!

Remember, you are using proxy-based inspection mode. When a firewall policy inspection mode is set to proxy, traffic flowing through the policy is buffered by FortiGate for inspection. This means that FortiGate holds the packets for a file, email message, or web page until the entire payload is inspected for violations (virus, spam, or malicious web links). After FortiOS has finished the inspection, FortiGate either releases the payload to the destination (if traffic is clean) or drops and replaces it with a message (if the traffic contains violations). FortiGate injects the block message into the partially downloaded file. The client can use Notepad to open and view the file.

5. Close **Notepad++**.
6. Delete the downloaded `eicar.com.txt` file from the desktop.

View the Antivirus Logs

The purpose of logs is to help you monitor your network traffic, locate problems, establish baselines, and make adjustments to network security, if necessary.

To view the antivirus logs

1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**. You may need to remove any log filters you set.
2. Locate the antivirus log message, and then double-click it.

   The **Details** tab shows forward traffic log information, along with the action taken.

3. Select the **Security** tab to view security logs, which provide information more specific to security events, such as filename, virus or botnet, and reference.
4. To view antivirus security logs, click **Log & Report** > **Security Events** > **AntiVirus**.

Enable SSL Inspection on a Firewall Policy

So far, you have tested unencrypted traffic for antivirus scanning. In order for FortiGate to inspect the encrypted traffic, you must enable deep inspection on the firewall policy. After you enable this feature, FortiGate can inspect SSL traffic using a technique similar to a man-in-the-middle (MITM) attack.

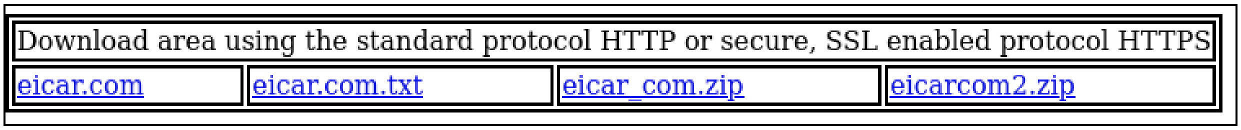
Take the Expert Challenge!

- On Local-Client, test the configuration by downloading the `eicar.com` file using HTTPS, without enabling the **deep-inspection** profile on the **Full Access** firewall policy.
- Configure Local-FortiGate to scan secure protocols by enabling **SSL Inspection**, using the **deep-inspection** profile on the **Full Access** firewall policy.
- Test the configuration by downloading the `eicar.com` file using HTTPS.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

To test antivirus scanning without SSL inspection enabled on the firewall policy

1. On the Local-Client VM, open a web browser, and then go to the following website:
   `https://10.200.1.254/test_av.html`
2. Click **Advanced**.
3. Click **Accept the Risk and Continue**.
4. In the **Download area**section, download the **eicar.com** sample file.



Download area using the standard protocol HTTP or secure, SSL enabled protocol HTTPS			
eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip

FortiGate should not block the file, because you did not enable full SSL inspection.

To enable and test the SSL inspection profile on a firewall policy

1. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and click **Policy & Objects** > **Firewall Policy**.
2. Double-click the **Full Access** firewall policy to edit it.
3. In the **Security Profiles** section, in the **SSL Inspection** drop-down list, select **deep-inspection**.
4. Keep the remaining default settings, and click **OK** to save the changes.
5. In the **Download area** section, try to download the same `eicar.com` file again.

If the FortiGate self-signed, full-inspection certificate is not installed on the browser, end users will see a certificate warning message. In this environment, the FortiGate self-signed SSL inspection certificate is installed on the browser. If the block page does not appear after two minutes, close all web browser tabs and restart the web browser.

FortiGate should block the download and replace it with a message. If it doesn't, you may need to clear your cache. In Firefox, click **Preferences** > **Privacy & Security**. Scroll to **History**, click **Clear History**, and ensure the time range to clear is set to **Everything**. Click **Clear Now**.

Exercise 2: Configuring Flow-Based Antivirus Scanning

When a firewall policy's inspection mode is set to flow, FortiGate does not buffer traffic flowing through the policy. Unlike proxy mode, FortiGate inspects the content payload passing through the policy packet by packet. FortiGate holds the very last packet until the scan returns a verdict. If FortiGate detects a violation in the traffic, it sends a reset packet to the receiver, which terminates the connection, and prevents the payload from being sent successfully.

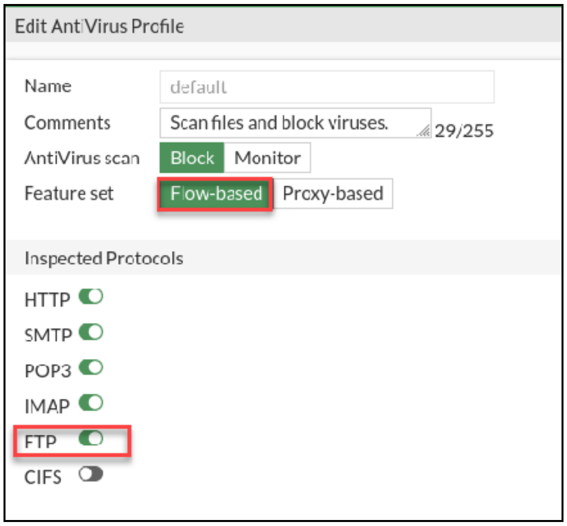
In this exercise, you will convert the inspection mode on the firewall policy and the antivirus profile to flow-based inspection mode. Then, you will perform a test to download a file located on an FTP server. You will view the logs and summary information related to the antivirus scanning. Finally, you will test the machine learning detection feature on Fortigate.

Change the Antivirus Profile Inspection Mode

You will change the inspection mode in the default antivirus profile, which is applied on the firewall policy, to inspect traffic including FTP.

To change the antivirus profile inspection mode

1. Continuing on the Local-FortiGate GUI, click **Security Profiles** > **AntiVirus**.
2. Right-click the **default** antivirus profile, and then click **Edit**.
3. In the **Feature set** field, select **Flow-based**.
4. In the **Inspected Protocols** section, verify that **FTP** is enabled.



Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

AntiVirus scan: [✓ Block] Monitor

Feature set: [✓ Flow-based] Proxy-based

Inspected Protocols

HTTP ●

SMTP ●

POP3 ●

IMAP ●

FTP ●

CIFS ○

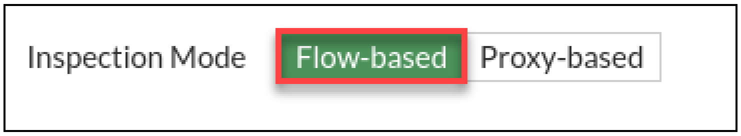
5. Click **OK**.

Change the FortiGate Inspection Mode

By default, flow-based inspection mode is enabled on the FortiGate firewall policy. In this exercise, you will change the inspection mode from proxy-based to flow-based.

To change the firewall policy inspection mode

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Policy & Objects** > **Firewall Policy**.
3. Double-click the **Full_Access** policy to edit it.
4. In the **Inspection Mode** field, select **Flow-based**.



5. In the **Protocol Options** field, verify that the **default** profile is selected.
6. In the **Security Profiles** section, verify that the **default AntiVirus profile** is selected.
7. Click **OK**.

Test the Flow-Based Antivirus Profile

You will test the flow-based antivirus profile using FTP.

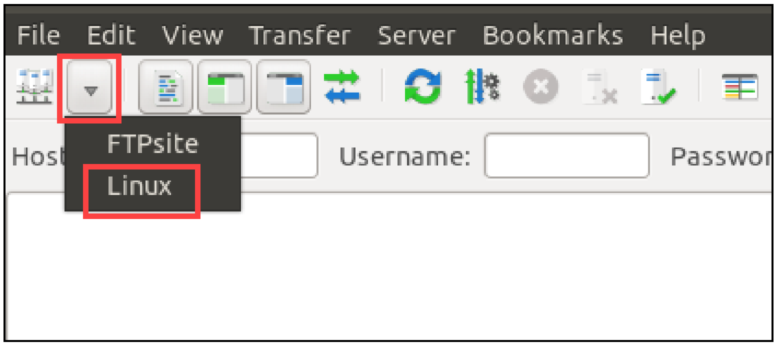
Take the Expert Challenge!

- On the Local-Client VM desktop, use the FileZilla FTP client to connect to the **Linux** preconfigured profile under **Site Manager**.
- Leave the username and password fields empty.
- Download the `eicar.com` file from the FTP server.
- View the relevant logs on the Local-FortiGate GUI, and identify the action taken as a result of the scanning.

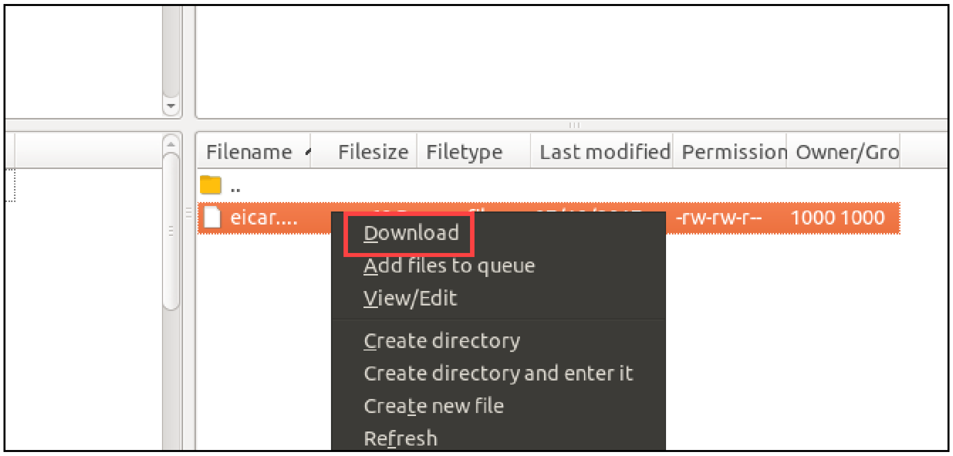
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

To test the antivirus configuration

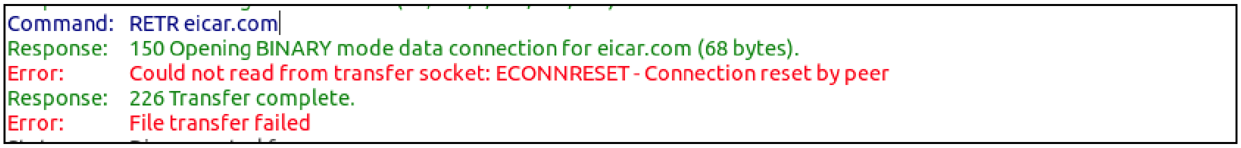
1. On the Local-Client VM, open the FileZilla FTP client software from the desktop.
2. Click the **Site Manager** icon in the upper-left corner, and then select **Linux**.



3. On the **Remote site** side of the application (right), right-click the **eicar.com** file, and then select **Download**.



The client should display an error message that the server terminated the connection. FortiGate sends the replacement message as a server response.



```
Command:   RETR eicar.com
Response:  150 Opening BINARY mode data connection for eicar.com (68 bytes).
Error:     Could not read from transfer socket: ECONNRESET - Connection reset by peer
Response:  226 Transfer complete.
Error:     File transfer failed
```

In flow-based inspection mode, FortiGate does not buffer traffic flowing through the policy. If FortiGate detects a violation in the traffic, it sends a reset packet to the receiver, which terminates the connection, and prevents the payload from being sent successfully.

4. Close the FileZilla FTP client.

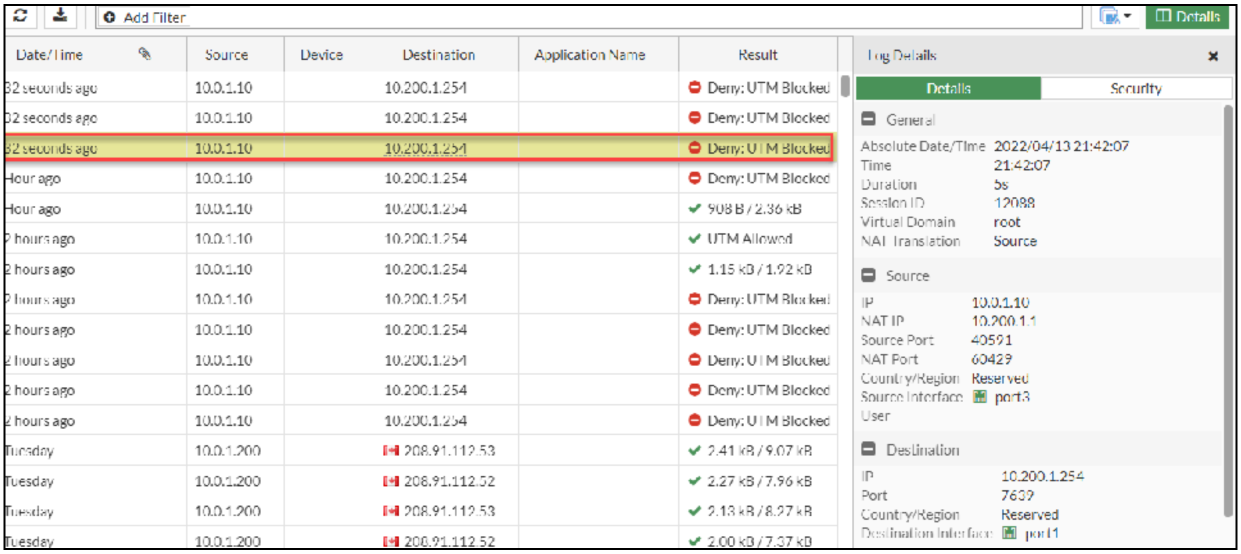
View the Antivirus Logs

You will check and confirm the logs for the test you just performed.

To view the antivirus logs

1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.
2. Locate the antivirus log message from when you tried to access the file using FTP, and double-click the log entry to view the details.

   The **Details** tab shows forward traffic log information, along with the action taken.



Date/Time	Source	Device	Destination	Application Name	Result
32 seconds ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked
32 seconds ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked
32 seconds ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked
Hour ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked
Hour ago	10.0.1.10		10.200.1.254		✓ 908 B / 2.36 kB
2 hours ago	10.0.1.10		10.200.1.254		✓ UTM Allowed
2 hours ago	10.0.1.10		10.200.1.254		✓ 1.15 kB / 1.92 kB
2 hours ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked
2 hours ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked
2 hours ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked
2 hours ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked
2 hours ago	10.0.1.10		10.200.1.254		Deny: UTM Blocked
Tuesday	10.0.1.200		208.91.112.53		✓ 2.41 kB / 9.07 kB
Tuesday	10.0.1.200		208.91.112.52		✓ 2.27 kB / 7.96 kB
Tuesday	10.0.1.200		208.91.112.53		✓ 2.13 kB / 8.27 kB
Tuesday	10.0.1.200		208.91.112.52		✓ 2.00 kB / 7.37 kB

Log Details

Details | Security

General

Absolute Date/Time	2022/04/13 21:42:07
Time	21:42:07
Duration	5s
Session ID	12088
Virtual Domain	root
NAT Translation	Source

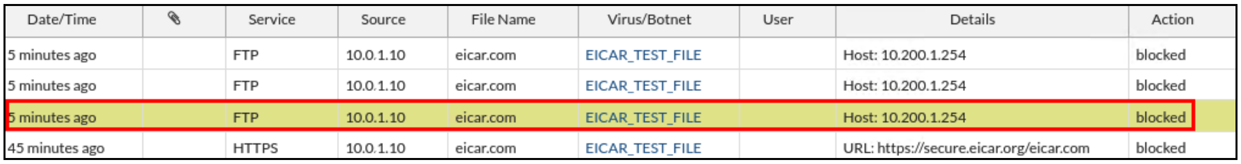
Source

IP	10.0.1.10
NAT IP	10.200.1.1
Source Port	40591
NAT Port	60429
Country/Region	Reserved
Source Interface	port3
User	

Destination

IP	10.200.1.254
Port	7639
Country/Region	Reserved
Destination Interface	port1

3. To view security log information, do one of the following:
   - Select the **Security** tab. This includes information more specific to the security event, such as filename, virus or botnet, reference, and so on.
   - Click **Log & Report** > **Security Events** > **AntiVirus**.



Date/Time		Service	Source	File Name	Virus/Botnet	User	Details	Action
5 minutes ago		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	blocked
5 minutes ago		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	blocked
5 minutes ago		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	blocked
45 minutes ago		HTTPS	10.0.1.10	eicar.com	EICAR_TEST_FILE		URL: https://secure.eicar.org/eicar.com	blocked

Test the Machine learning (AI) scan

By default, machine learning detection is enabled on FortiGate and it detects zero-day attacks. In this exercise, you will disable machine learning detection and then download an unknown malware from the FTP server. Then you will enable machine learning detection and download the same file again to test the machine learning detection scan.

To disable machine learning detection

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following commands to disable machine learning detection:

```
config antivirus settings
set machine-learning-detection disable
end
```

3. On the Local-Client VM, open the FileZilla FTP client software from the desktop.
4. Click the **Site Manager** icon in the upper-left corner, and then select **Linux**.
5. On the **Remote site** side of the application (right), right-click the **1132999808** file, and then select **Download**.

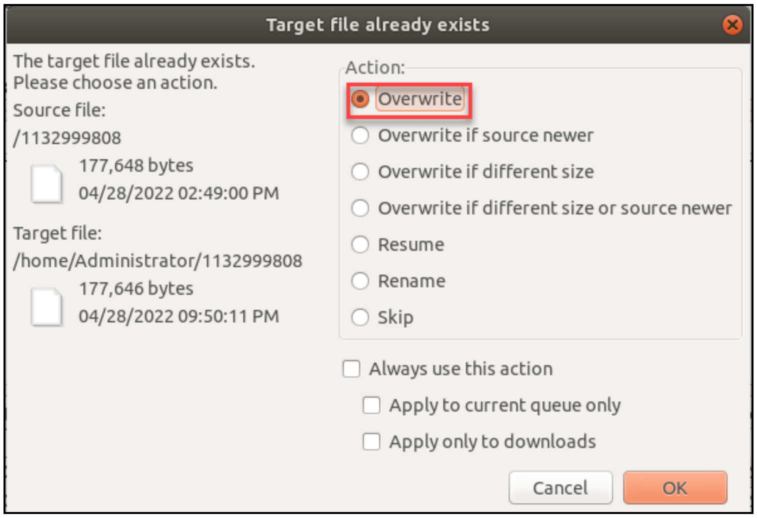
You will see that the download completed successfully.

Block the unknown malware using machine learning scan

1. Return to the Local-FortiGate CLI and enter the following commands to enable machine learning detection:

```
config antivirus settings
set machine-learning-detection enable
end
```

2. Open the FileZilla FTP client software again, right-click the **1132999808** file, and then select **Download**.
3. In the **Target file already exists** window, select **Overwrite**, and then click **OK**.



Target file already exists

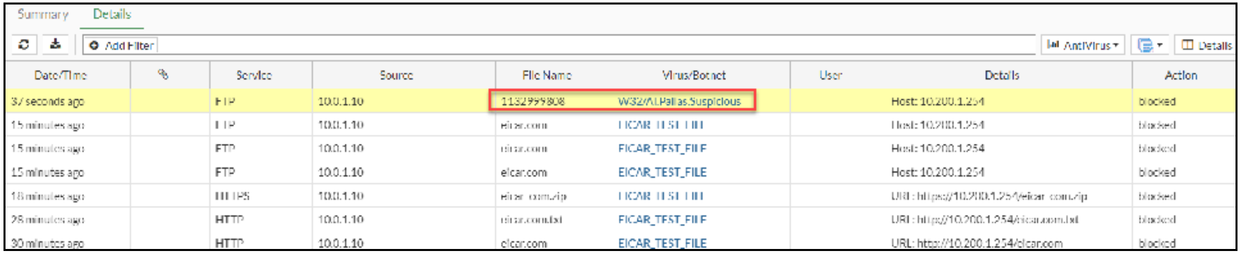
The target file already exists.
Please choose an action.
Source file:
/1132999808
177,648 bytes
04/28/2022 02:49:00 PM
Target file:
/home/Administrator/1132999808
177,646 bytes
04/28/2022 09:50:11 PM

Action:
● Overwrite
○ Overwrite if source newer
○ Overwrite if different size
○ Overwrite if different size or source newer
○ Resume
○ Rename
○ Skip

□ Always use this action
□ Apply to current queue only
□ Apply only to downloads

You will see that the download failed this time because the AI engine terminated the file transfer.

4. In the **Target file already exists** window,click **Cancel**.
5. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Security Events** > **AntiVirus**.



Date/Time	%	Service	Source	File Name	Virus/Botnet	User	Details	Action
37 seconds ago		FTP	10.0.1.10	1132999808	W32/AI.Pallas.Suspicious		Host: 10.200.1.254	blocked
15 minutes ago		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	blocked
15 minutes ago		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	blocked
15 minutes ago		FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		Host: 10.200.1.254	blocked
18 minutes ago		HTTPS	10.0.1.10	eicar_com.zip	EICAR_TEST_FILE		URL: https://10.200.1.254/eicar_com.zip	blocked
28 minutes ago		HTTP	10.0.1.10	eicar.com.txt	EICAR_TEST_FILE		URL: http://10.200.1.254/eicar.com.txt	blocked
30 minutes ago		HTTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		URL: http://10.200.1.254/eicar.com	blocked

A zero-day attack is malware that is new, unknown, and therefore, does not have an existing associated signature. Files detected by a machine learning scan are identified with the W32/AI.Pallas.Suspicious signature.

Lab 10: IPS and DoS

In this lab, you will set up intrusion prevention system (IPS) profiles and denial of service (DoS) policies. You will also use a vulnerability scanner and a custom script to generate attacks on Local-FortiGate.

Objectives

- Protect your network against known attacks using IPS signatures
- Use rate-based signatures to block brute force attacks
- Mitigate and block DoS attacks

Time to Complete

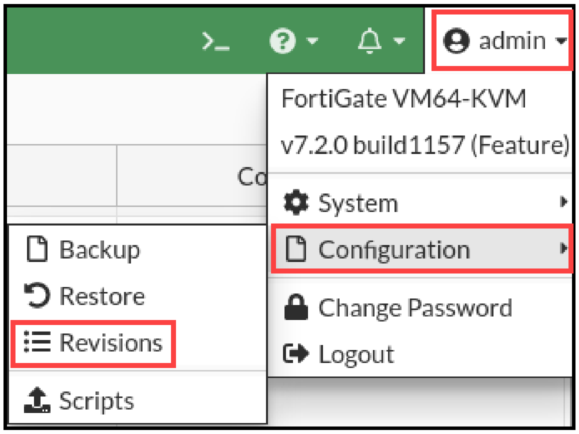
Estimated: 40 minutes

Prerequisites

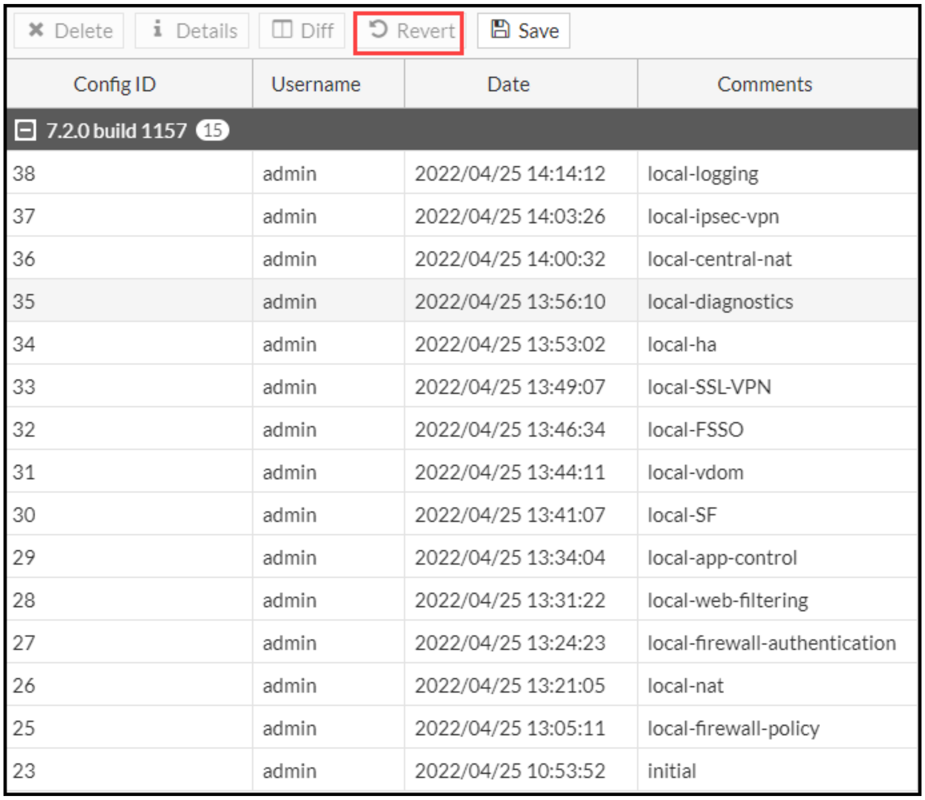
Before beginning this lab, you must restore a configuration file to the Local-FortiGate.

To restore the Local-FortiGate configuration file

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **initial**, and then click **Revert**.



Config ID	Username	Date	Comments
7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click **OK** to reboot.

Exercise 1: Blocking Known Exploits

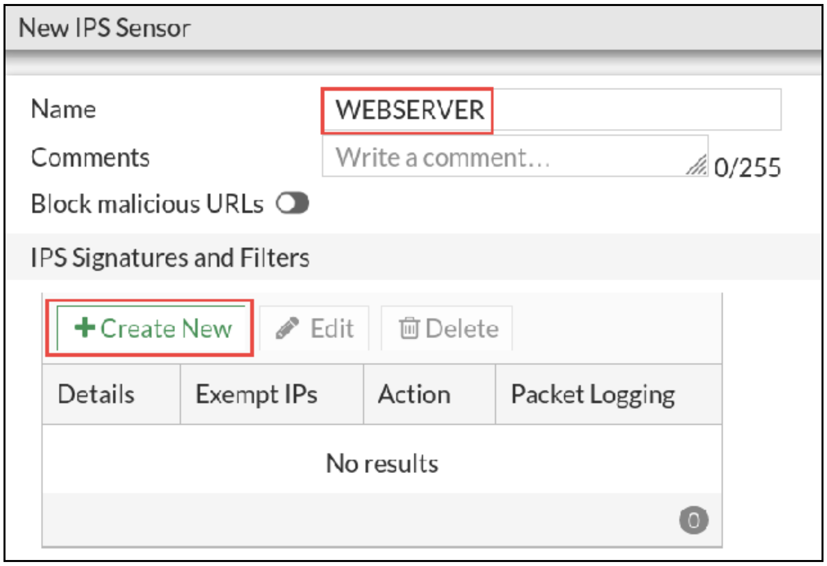
In this exercise, you will configure IPS inspection on the Local-FortiGate.

Configure IPS Inspection

You will configure an IPS sensor that includes the signatures for known attacks based on different severity levels.

To configure IPS inspection

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Security Profiles** > **Intrusion Prevention**.
3. Click **Create New**.
4. In the **Name** field, type `WEBSERVER` for the new sensor name.
5. In the **IPS Signatures and Filters** section, click **Create New**.



New IPS Sensor

Name: WEBSERVER

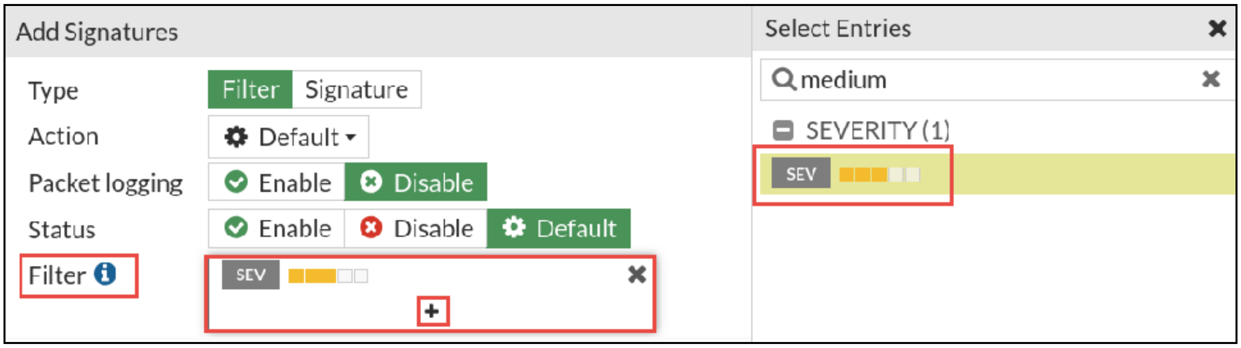
Comments: Write a comment... 0/255

Block malicious URLs

IPS Signatures and Filters

Details	Exempt IPs	Action	Packet Logging
No results			

6. In the **Add Signatures** window, click **+** to add a **Filter**.
7. In the search bar, type `medium`, and then click the **SEV** object to select the medium severity filter.



Add Signatures

Type: Filter | Signature

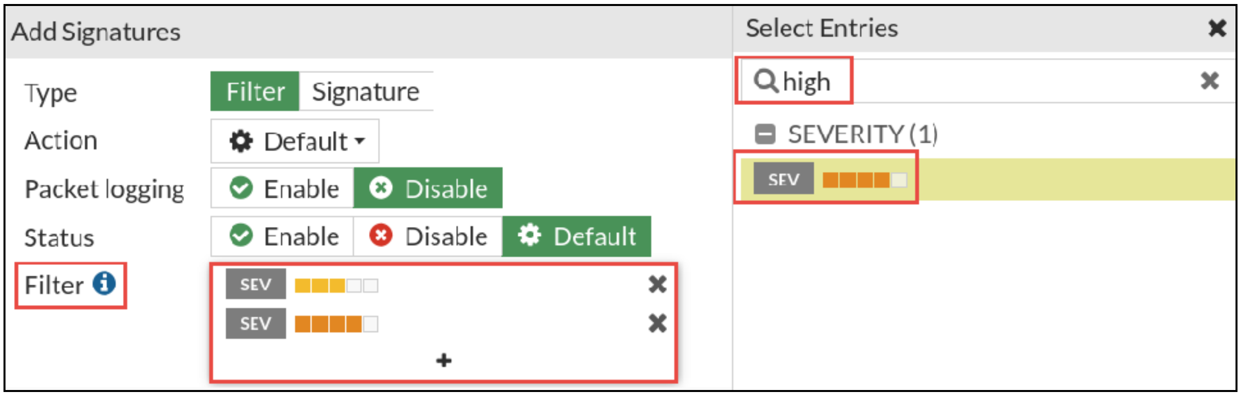
Action: Default

Packet logging: Enable | Disable

Status: Enable | Disable | Default

Filter: SEV

8. In the search bar, delete `medium`, and then type `high`.
9. Click the **SEV** object to select the high severity filter.



Add Signatures

Type: Filter | Signature
Action: Default
Packet logging: Enable | Disable
Status: Enable | Disable | Default
Filter: SEV, SEV

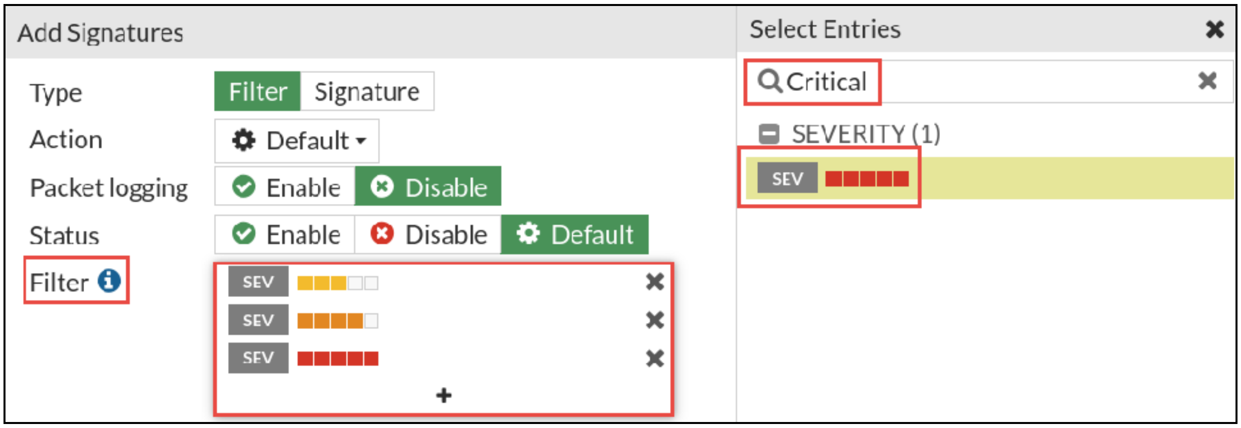
Select Entries

high

SEVERITY (1)

SEV

10. In the search bar, delete `high`, and then type `critical`.
11. Click the **SEV** object to select the critical severity filter.



Add Signatures

Type: Filter | Signature
Action: Default
Packet logging: Enable | Disable
Status: Enable | Disable | Default
Filter: SEV, SEV, SEV

Select Entries

Critical

SEVERITY (1)

SEV

12. Click **OK** to add the selected filters.

    All signatures that match the filters are added to the IPS sensor, and FortiGate takes the default action for these signatures.

13. Click **OK**.

Apply an IPS Sensor to a VIP Firewall Policy

You will apply the new IPS sensor to a firewall policy that allows external access to the web server running on the Local-Client.

Take the Expert Challenge!

On the Local-FortiGate GUI, do the following:

- Configure a new virtual IP to map the external IP `10.200.1.200` to the internal IP `10.0.1.10`, using port1 as the external interface. Name the virtual IP `VIP-WEB-SERVER`.
- Create a new firewall policy to allow all inbound traffic to the virtual IP, and enable the **WEBSERVER** IPS sensor. Name the firewall policy `Web_Server_Access_IPS`.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Generate Attacks From the Linux Server on page 172

To create a virtual IP

1. Continuing on the Local-Fortigate GUI, click **Policy & Objects** > **Virtual IPs**.
2. Click **Create New** > **Virtual IP**.
3. Configure the following settings:

Field	Value
Name	VIP-WEB-SERVER
Interface	port1
External IP address/range	10.200.1.200
Map to IPv4 address/range	10.0.1.10

4. Click **OK**.

To configure a firewall policy

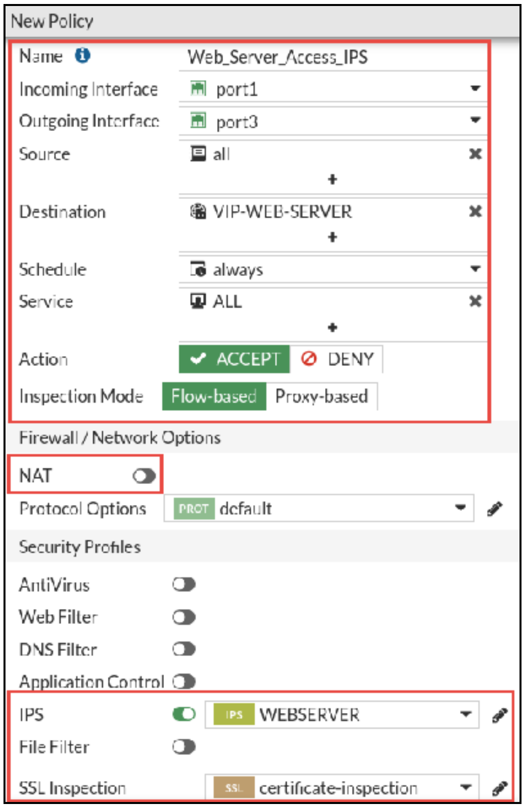
1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Create New**, and create a new firewall policy using the following settings:

Field	Value
Name	Web_Server_Access_IPS
Incoming Interface	port1
Outgoing Interface	port3
Source	all
Destination	VIP-WEB-SERVER

Field	Value
Schedule	always
Service	ALL
Action	ACCEPT
Inspection Mode	Flow-based
NAT	disabled

3. In the **Security Profiles** section, enable **IPS** and, in the drop-down list, select **WEBSERVER**.

   The policy should look like the following example:



New Policy

Name	Web_Server_Access_IPS
Incoming Interface	port1
Outgoing Interface	port3
Source	all
Destination	VIP-WEB-SERVER
Schedule	always
Service	ALL
Action	✓ ACCEPT / DENY
Inspection Mode	Flow-based / Proxy-based

Firewall / Network Options

NAT	○
Protocol Options	PROT default

Security Profiles

AntiVirus	○
Web Filter	○
DNS Filter	○
Application Control	○
IPS	● IPS WEBSERVER
File Filter	○
SSL Inspection	SSL certificate-inspection

Configuring full SSL inspection would significantly increase the time required to complete this lab. Therefore, for the purposes of this exercise, you will not configure full SSL inspection.

4. Click **OK**.

Generate Attacks From the Linux Server

You will run a Perl script to generate attacks from the Linux server located in front of the Local-FortiGate.

To generate attacks from the Linux server

1. On the Local-Client VM, open PuTTY, and then connect over SSH to the LINUX saved session.
2. Log in with the username `student` and password `password`.
3. Run the following script to start the attacks:

```
nikto.pl -host 10.200.1.200
```

4. Leave the PuTTY session open (you can minimize it) so traffic continues to generate.

Do not close the LINUX PuTTY session or traffic will stop generating.

Monitor the IPS

You will check the IPS logs to monitor for known attacks being detected and dropped by the Local-FortiGate.

Take the Expert Challenge!

On the Local-FortiGate GUI, complete the following:

- Review the IPS logs for all detected and dropped attacks.
- Review the FortiGuard encyclopedia pages.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

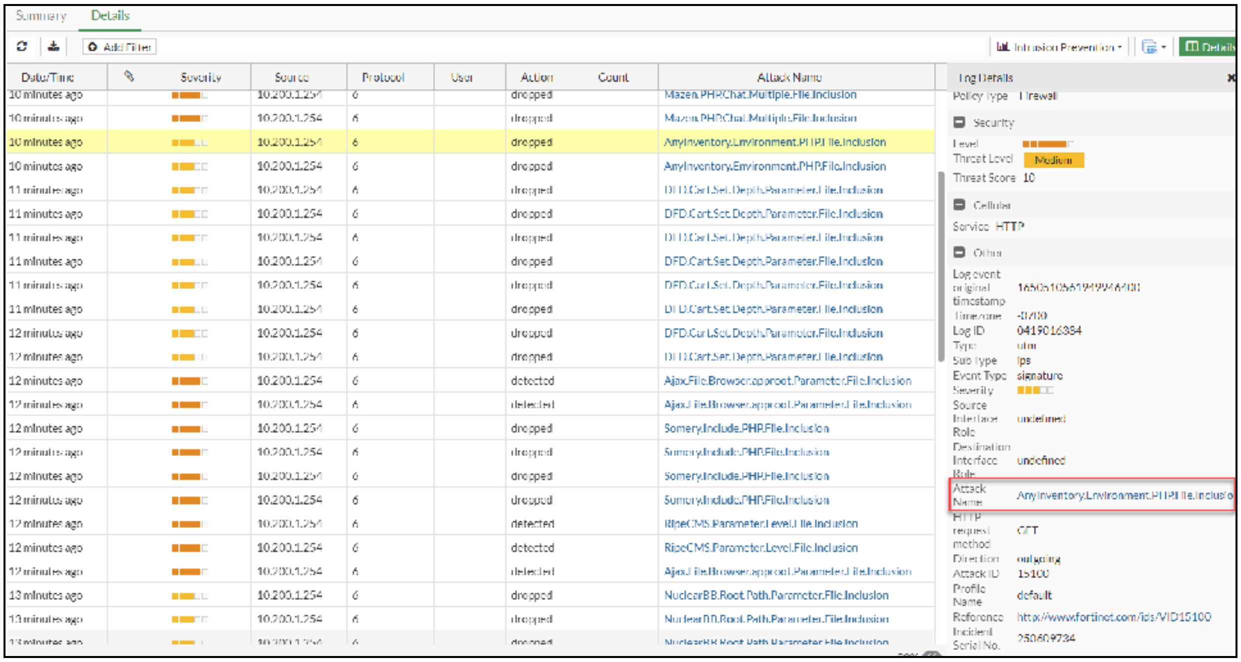
To monitor the IPS

1. Return to your browser tab where you are logged in to the Local-FortiGate GUI, and click **Log & Report** > **Security Events** > **Intrusion Prevention**.
2. Locate and review the relevant log entries for the detected and dropped attacks.

FortiGate creates an intrusion prevention log entry for the following:

- Detected attack without blocking it
- Dropped attack with blocking it

3. Click a log entry, and then click **Details**.
4. Click the **Attack Name** link.



Date/Time		Severity	Source	Protocol	User	Action	Count	Attack Name
10 minutes ago			10.200.1.254	6		dropped		Mazen.PHPChat.Multiple.File.Inclusion
10 minutes ago			10.200.1.254	6		dropped		Mazen.PHPChat.Multiple.File.Inclusion
10 minutes ago			10.200.1.254	6		dropped		AnyInventory.Environment.PHP.File.Inclusion
10 minutes ago			10.200.1.254	6		dropped		AnyInventory.Environment.PHP.File.Inclusion
11 minutes ago			10.200.1.254	6		dropped		DFD.Cart.Set.Depth.Parameter.File.Inclusion
11 minutes ago			10.200.1.254	6		dropped		DFD.Cart.Set.Depth.Parameter.File.Inclusion
11 minutes ago			10.200.1.254	6		dropped		DFD.Cart.Set.Depth.Parameter.File.Inclusion
11 minutes ago			10.200.1.254	6		dropped		DFD.Cart.Set.Depth.Parameter.File.Inclusion
11 minutes ago			10.200.1.254	6		dropped		DFD.Cart.Set.Depth.Parameter.File.Inclusion
11 minutes ago			10.200.1.254	6		dropped		DFD.Cart.Set.Depth.Parameter.File.Inclusion
12 minutes ago			10.200.1.254	6		dropped		DFD.Cart.Set.Depth.Parameter.File.Inclusion
12 minutes ago			10.200.1.254	6		dropped		DFD.Cart.Set.Depth.Parameter.File.Inclusion
12 minutes ago			10.200.1.254	6		detected		Ajax.File.Browser.approot.Parameter.File.Inclusion
12 minutes ago			10.200.1.254	6		detected		Ajax.File.Browser.approot.Parameter.File.Inclusion
12 minutes ago			10.200.1.254	6		dropped		Somery.Include.PHP.File.Inclusion
12 minutes ago			10.200.1.254	6		dropped		Somery.Include.PHP.File.Inclusion
12 minutes ago			10.200.1.254	6		dropped		Somery.Include.PHP.File.Inclusion
12 minutes ago			10.200.1.254	6		dropped		Somery.Include.PHP.File.Inclusion
12 minutes ago			10.200.1.254	6		detected		RipeCMS.Parameter.Level.File.Inclusion
12 minutes ago			10.200.1.254	6		detected		RipeCMS.Parameter.Level.File.Inclusion
12 minutes ago			10.200.1.254	6		detected		Ajax.File.Browser.approot.Parameter.File.Inclusion
13 minutes ago			10.200.1.254	6		dropped		NuclearBB.Root.Path.Parameter.File.Inclusion
13 minutes ago			10.200.1.254	6		dropped		NuclearBB.Root.Path.Parameter.File.Inclusion
13 minutes ago			10.200.1.254	6		dropped		NuclearBB.Root.Path.Parameter.File.Inclusion

Log Details

Policy Type Firewall

Security

Level
Threat Level Medium
Threat Score 10

Cellular

Service HTTP

Other

Log event original timestamp 1650510561949946400
Timezone -0700
Log ID 0419016384
Type utm
Sub Type ips
Event Type signature
Severity
Source Interface Role undefined
Destination Interface Role undefined
Attack Name AnyInventory.Environment.PHP.File.Inclusio
HTTP request method GET
Direction outgoing
Attack ID 15100
Profile Name default
Reference http://www.fortinet.com/ids/VID15100
Incident Serial No. 250609734

5. Review the FortiGuard encyclopedia pages for the signatures.

   The FortiGuard encyclopedia provides information about signatures, such as severity, coverage, affected products, impact, and recommended actions that you can take.

None of the affected products are currently installed on the Local-Client. This information is important to make a note of before you tune the **WEBSERVER** IPS sensor. If the affected products aren't installed, is it really necessary to inspect those packets?

6. Close the LINUX PuTTY session.

Exercise 2: Using Rate-Based IPS Signatures

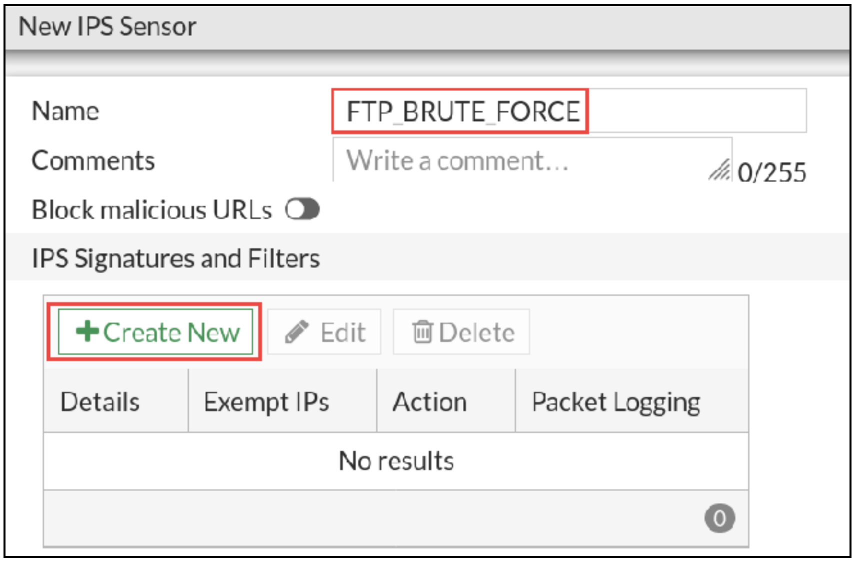
In this exercise, you will configure a rate-based signature to detect and block a brute force FTP attack.

Apply Rate-Based Signatures

You will create a new IPS sensor, and enable and configure the appropriate signature to detect and block FTP brute force attacks. You will then apply the IPS sensor to all outbound traffic on Local-FortiGate.

To create an IPS sensor

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Security Profiles** > **Intrusion Prevention**.
3. Click **Create New**.
4. In the **Name** field, type `FTP_BRUTE_FORCE`.
5. In the **IPS Signatures and Filters** section, click **Create New**.



New IPS Sensor

Name: FTP_BRUTE_FORCE

Comments: Write a comment... 0/255

Block malicious URLs

IPS Signatures and Filters

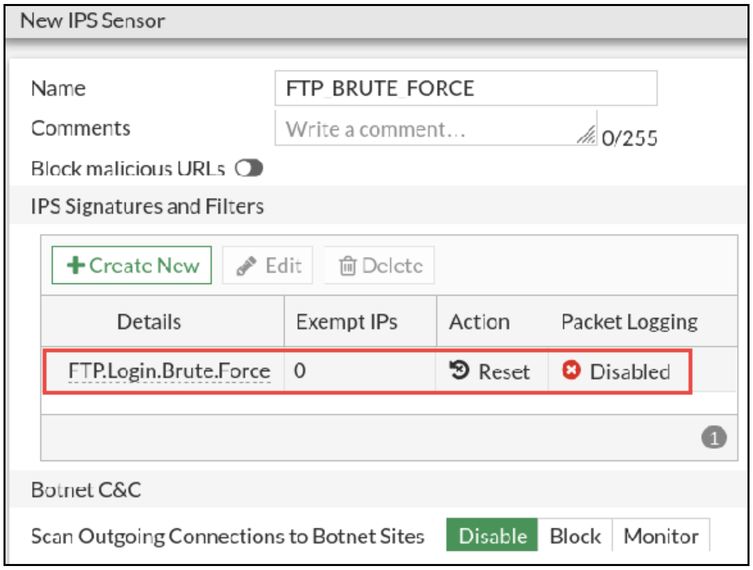
6. On the **Add Signatures** page, in the **Type** field, select **Signature**.
7. In the **Action** field, select **Reset** in the drop-down menu.
8. In the **Status** field, select **Enable**.
9. In the **Rate-based settings** field, select **Specify**.
10. Configure the following settings:

Field	Value
Threshold	5

Field	Value
Duration (seconds)	30
Track By	Source IP

11. Type `FTP.Login.Brute.Force` in the search field, and then press `Enter`.
12. Right-click **FTP.Login.Brute.Force**, and then click **Add Selected**.
13. Click **OK**.

    The configuration should look like the following image:



New IPS Sensor

Name: FTP_BRUTE_FORCE

Comments: Write a comment... 0/255

Block malicious URLs

IPS Signatures and Filters

Details	Exempt IPs	Action	Packet Logging
FTP.Login.Brute.Force	0	Reset	Disabled

Botnet C&C

Scan Outgoing Connections to Botnet Sites: Disable | Block | Monitor

14. Click **OK**.

To apply IPS on outbound traffic

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Double-click the existing **Full_Access** policy to edit it.
3. In the **Security Profiles** section, enable **IPS** and, in the drop-down list, select **FTP_BRUTE_FORCE**.
4. Click **OK**.

Test the Rate-Based Signature

You will use a custom bash script to generate invalid login attempts to the FTP server located on the Linux VM. You will then verify your configuration using the IPS logs.

A typical brute force attack uses a dictionary of usernames and passwords. In this scenario, the script uses an incorrect username and password to flood the FTP server with invalid login attempts. The `530 Login incorrect` responses from the FTP server should be enough to trigger the signature.

To run the bash script

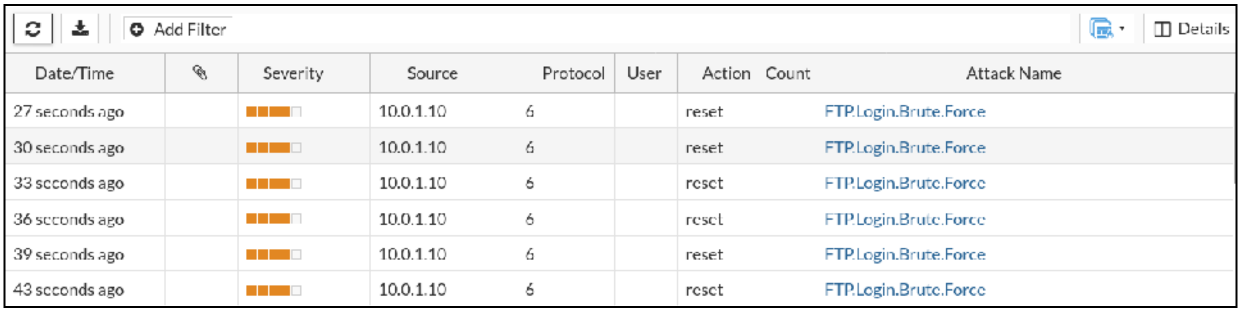
1. On the Local-Client VM, open a terminal window.
2. Change the working directory to `cd Desktop/Resources/FortiGate-Security/Intrusion-Prevention-System`.
3. Execute the bash script.

   ```
   bash bruteFTP.sh
   ```

4. Wait for the script to finish, and then leave the terminal window open in the background.

To view the IPS logs

1. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and click**Log & Report** > **Security Events** > **Intrusion Prevention**.
2. Locate the logs for the FTP brute force attacks.



Date/Time		Severity	Source	Protocol	User	Action	Count	Attack Name
27 seconds ago		■■■■□	10.0.1.10	6		reset		FTP.Login.Brute.Force
30 seconds ago		■■■■□	10.0.1.10	6		reset		FTP.Login.Brute.Force
33 seconds ago		■■■■□	10.0.1.10	6		reset		FTP.Login.Brute.Force
36 seconds ago		■■■■□	10.0.1.10	6		reset		FTP.Login.Brute.Force
39 seconds ago		■■■■□	10.0.1.10	6		reset		FTP.Login.Brute.Force
43 seconds ago		■■■■□	10.0.1.10	6		reset		FTP.Login.Brute.Force

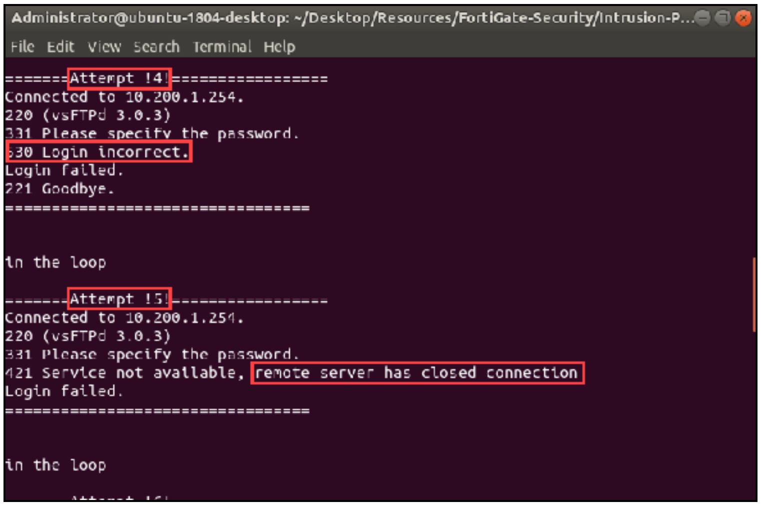
Why are there only six log entries, when the script generated 10 login attempts?

Stop and think!

You configured the **FTP.Login.Brute.Force** rate-based signature with a threshold of `5`. The IPS signature action was triggered only after this threshold was met.

To verify the IPS signature action

1. On the Local-Client VM, return to the terminal window.
2. Scroll up, and locate `Attempt 4` and `Attempt 5`.


Administrator@ubuntu-1804-desktop: ~/Desktop/Resources/FortiGate-Security/Intrusion-P...
File Edit View Search Terminal Help

```
=======Attempt !4!=================
Connected to 10.200.1.254.
220 (vsFTPd 3.0.3)
331 Please specify the password.
530 Login incorrect.
Login failed.
221 Goodbye.
==================================


in the loop

=======Attempt !5!=================
Connected to 10.200.1.254.
220 (vsFTPd 3.0.3)
331 Please specify the password.
421 Service not available, remote server has closed connection
Login failed.
==================================


in the loop

       Attempt !6!
```

Note that for `Attempt 4`, the server response is `530 Login incorrect`. However, for `Attempt 5`, the error message is `421 Service not available, remote server has closed connection`. This is where the rate-based signature action triggers, and the FTP client connections are reset. The same error message repeats until the script ends with `Attempt 10`.

3. Close the terminal window.

Exercise 3: Mitigating a DoS Attack

In this exercise, you will configure the Local-FortiGate for DoS protection.

Create a DoS Policy

You will create a DoS policy to detect and block an ICMP flood attack.

Take the Expert Challenge!

On the Local-FortiGate GUI, do the following:

- Create a new IPv4 DoS policy for port1.
- Configure the policy to block ICMP floods with a threshold of 200.
- Enable logging.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

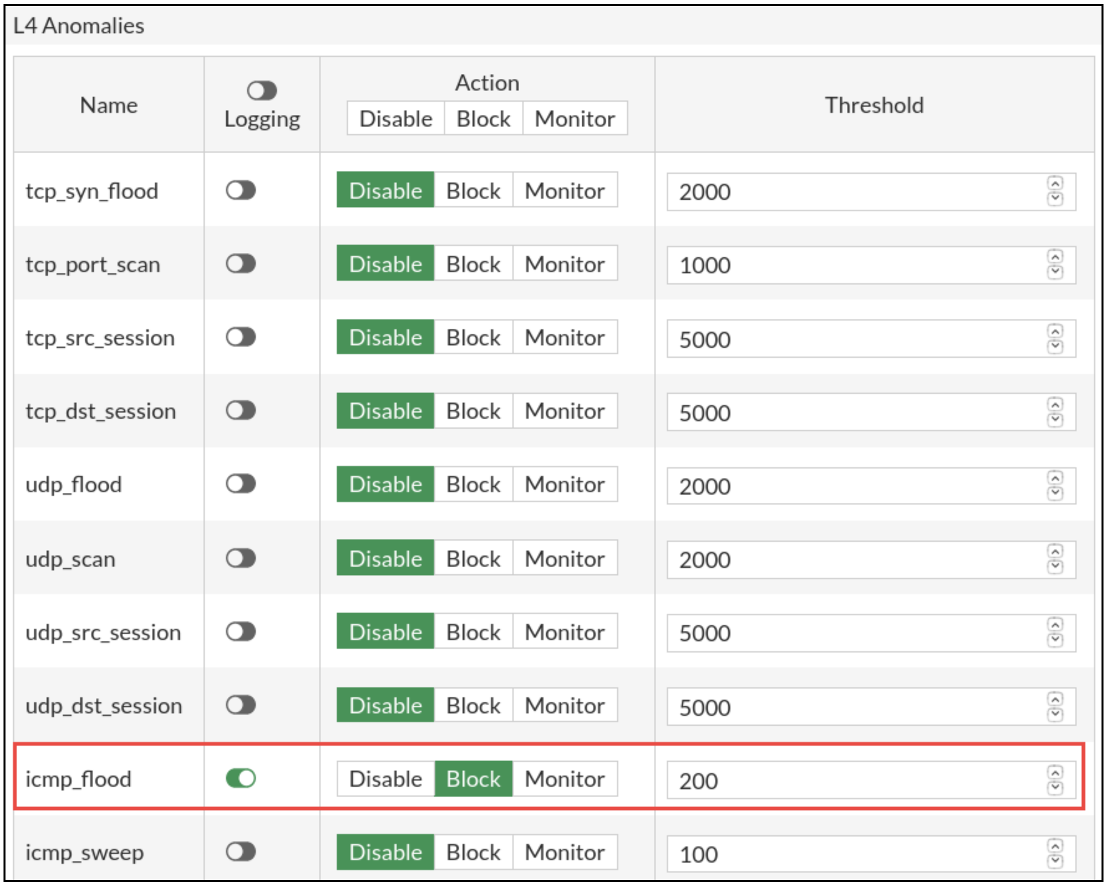
After you complete the challenge, see Test the DoS Policy on page 179.

To create a DoS policy

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Policy & Objects** > **IPv4 DoS Policy**.
3. Click **Create New**.
4. Configure the following settings:

Field	Value
Name	ICMP_Floods
Incoming Interface	port1
Source Address	all
Destination Address	all
Services	ALL

5. In the **L4 Anomalies** section, locate **icmp_flood**, and then enable **Logging**.
6. Set **Action** to **Block**, and then set **Threshold** to `200`.



L4 Anomalies

Name	Logging	Action	Threshold
tcp_syn_flood	○	[✓ Disable] Block Monitor	2000
tcp_port_scan	○	[✓ Disable] Block Monitor	1000
tcp_src_session	○	[✓ Disable] Block Monitor	5000
tcp_dst_session	○	[✓ Disable] Block Monitor	5000
udp_flood	○	[✓ Disable] Block Monitor	2000
udp_scan	○	[✓ Disable] Block Monitor	2000
udp_src_session	○	[✓ Disable] Block Monitor	5000
udp_dst_session	○	[✓ Disable] Block Monitor	5000
icmp_flood	●	Disable [✓ Block] Monitor	200
icmp_sweep	○	[✓ Disable] Block Monitor	100

7. Click **OK**.

Test the DoS Policy

You will generate an ICMP flood from the Linux VM. This will trigger the DoS policy on the Local-FortiGate.

To test the DoS policy

1. On the Local-Client VM, open PuTTY, and then connect over SSH to the **LINUX** saved session.
2. Log in with the username `student` and password `password`.
3. Enter the following command to generate an ICMP flood to the Local-FortiGate:

   ```
   sudo ping -f 10.200.1.1
   ```

   A password prompt for the `student` account is displayed.

The command option `-f` causes the ping utility to run continuously, and not wait for replies between ICMP echo requests. It also requires super-user privileges.

4. Enter `password`.

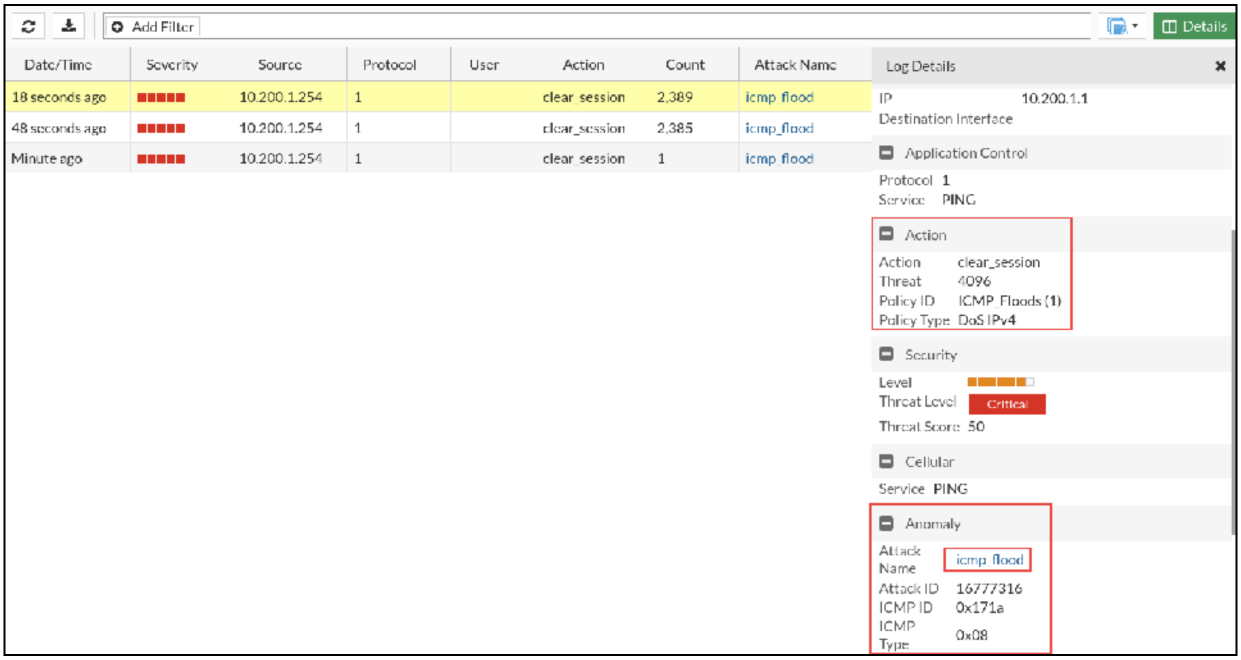
   For every ping sent, the SSH session displays a period.

5. Leave the SSH connection open with the ping running (you can minimize the window).

To view the anomaly logs

1. Return to the browser where you are logged in to the Local-FortiGate GUI, and press `F5` to refresh the browser (or log out and log in again).
2. Click **Log & Report** > **Security Events** > **Anamoly**.
3. Examine the logs.

   Note that the ICMP flood was blocked. This is indicated by the **clear_session** entry in the **Action** field.



Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
18 seconds ago	■■■■■	10.200.1.254	1		clear_session	2,389	icmp_flood
48 seconds ago	■■■■■	10.200.1.254	1		clear_session	2,385	icmp_flood
Minute ago	■■■■■	10.200.1.254	1		clear_session	1	icmp_flood

Log Details

IP 10.200.1.1
Destination Interface

Application Control
Protocol 1
Service PING

Action
Action clear_session
Threat 4096
Policy ID ICMP_Floods (1)
Policy Type DoS IPv4

Security
Level ■■■■□
Threat Level Critical
Threat Score 50

Cellular
Service PING

Anomaly
Attack Name icmp_flood
Attack ID 16777316
ICMP ID 0x171a
ICMP Type 0x08

4. Go back to the PuTTY window, and press `Ctrl+C` to stop the ping.
5. Close the PuTTY session.

Lab 11: Security Fabric

In this lab, you will learn to configure the Fortinet Security Fabric. After you configure the Security Fabric, you will access the physical and logical topology views.

Objectives

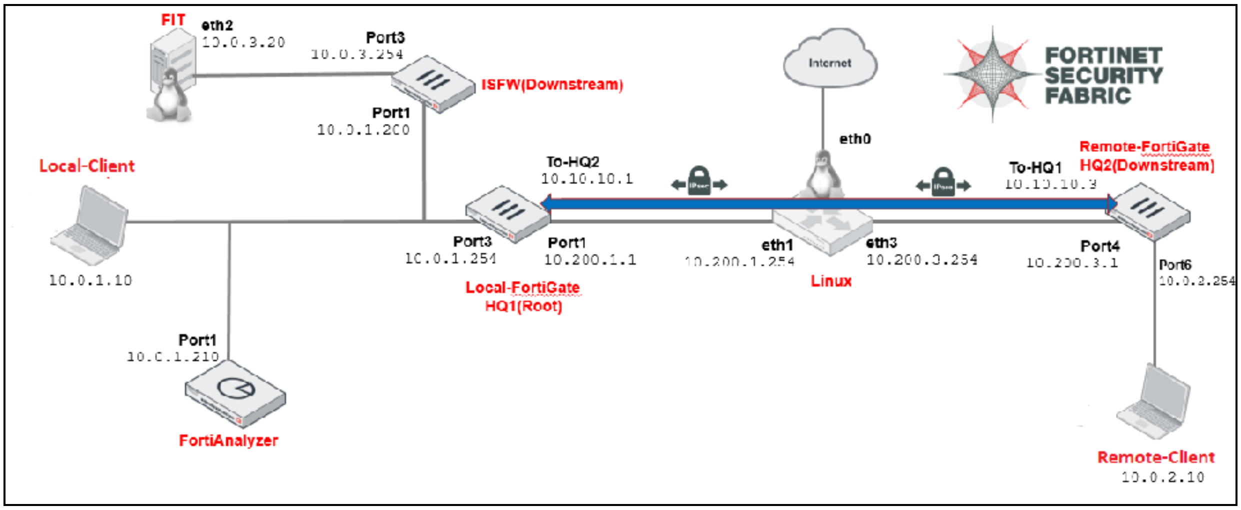
- Configure the Security Fabric on Local-FortiGate (root) and ISFW (downstream)
- Configure the Security Fabric on Local-FortiGate (root) and Remote-FortiGate (downstream)
- Use the Security Fabric topology views to examine the logical and physical views of your network topology
- Run the Security Fabric rating checks on the root FortiGate and apply a recommendation

Time to Complete

Estimated: 45 minutes

Topology

In this lab, you will learn how to configure the Security Fabric on all FortiGate devices in the topology. Local-FortiGate and Remote-FortiGate are connected through an IPsec tunnel. Local-FortiGate is the root FortiGate in the Security Fabric, and Remote-FortiGate and ISFW are downstream FortiGate devices. FortiAnalyzer is behind Local-FortiGate and will be used in the Security Fabric.



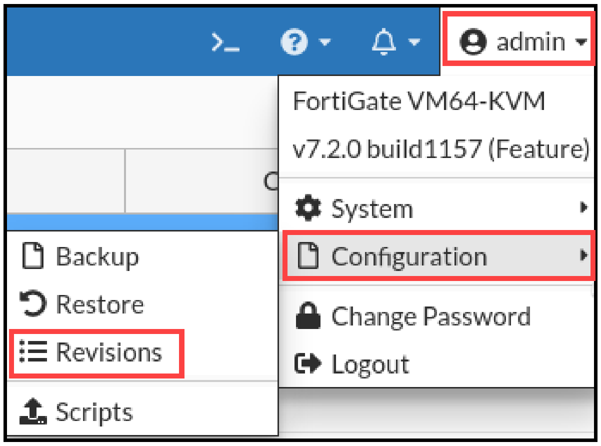
Prerequisites

Before beginning this lab, you must restore configuration files on Remote-FortiGate, Local-FortiGate, ISFW, and FortiAnalyzer.

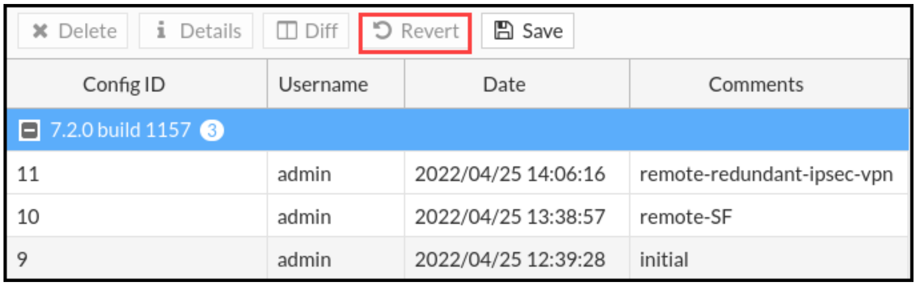
Make sure you restore the correct configuration on each FortiGate, using the following steps. Failure to restore the correct configuration on each FortiGate will prevent you from doing the lab exercise.

To restore the Remote-FortiGate configuration

1. Connect to the Remote-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **remote-SF**, and then click **Revert**.

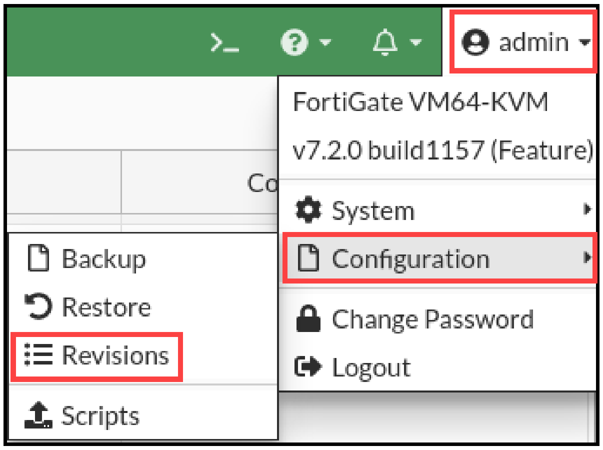


Config ID	Username	Date	Comments
7.2.0 build 1157 3			
11	admin	2022/04/25 14:06:16	remote-redundant-ipsec-vpn
10	admin	2022/04/25 13:38:57	remote-SF
9	admin	2022/04/25 12:39:28	initial

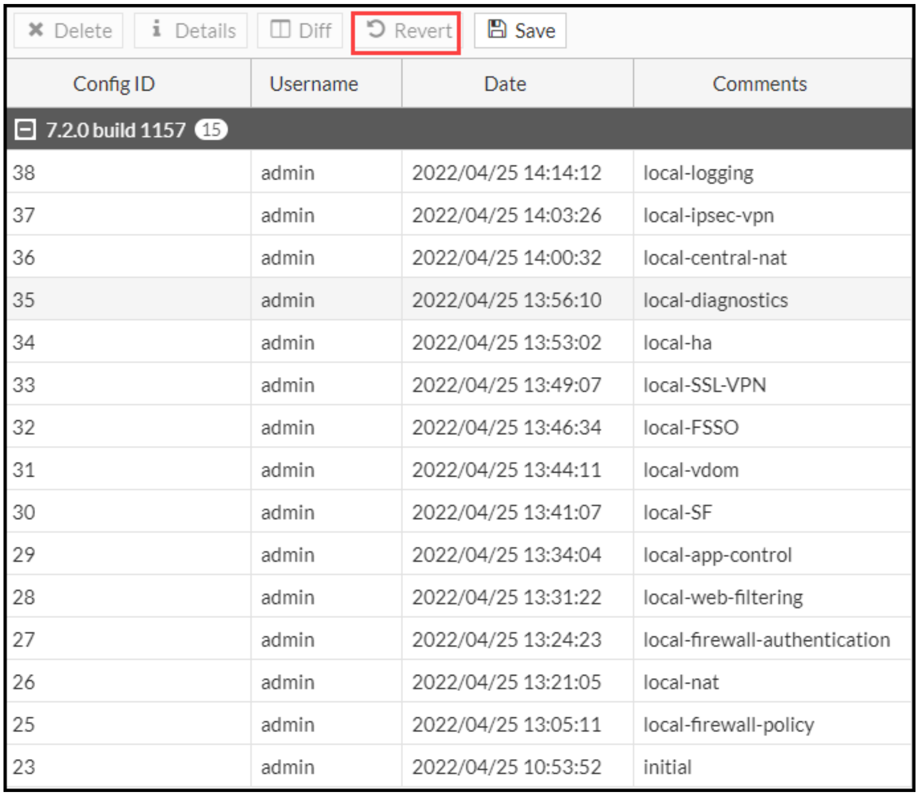
5. Click **OK** to reboot.

To restore the Local-FortiGate configuration

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **local-SF**, and then click **Revert**.

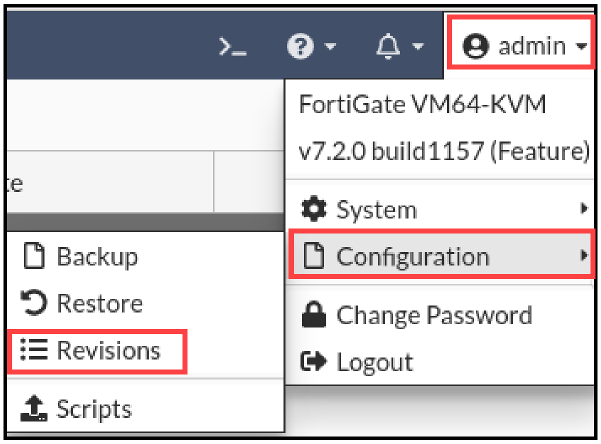


Config ID	Username	Date	Comments
7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

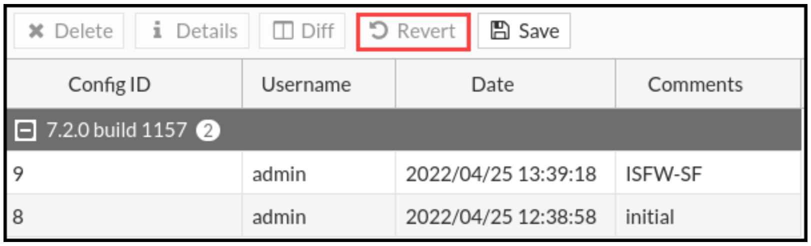
5. Click **OK** to reboot.

To restore the ISFW configuration

1. Connect to the ISFW GUI, and then log in with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.



3. Click the **+** sign to expand the list.
4. Select the configuration with the comment **ISFW-SF**, and then click **Revert**.

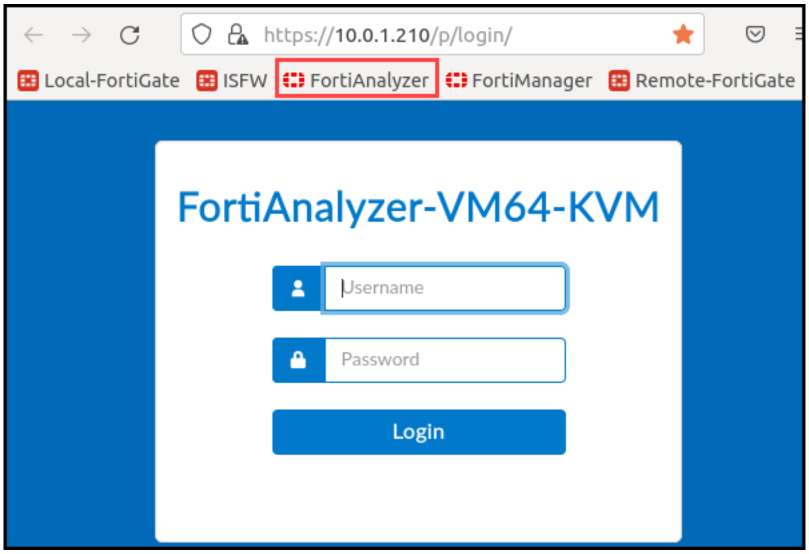


Config ID	Username	Date	Comments
7.2.0 build 1157 (2)			
9	admin	2022/04/25 13:39:18	ISFW-SF
8	admin	2022/04/25 12:38:58	initial

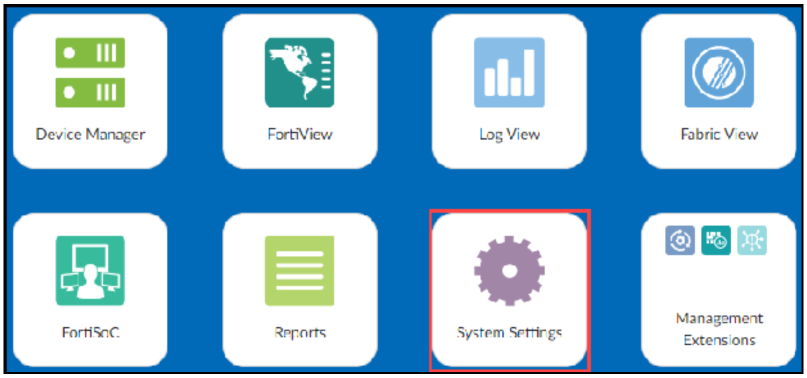
5. Click **OK** to reboot.

To restore the FortiAnalyzer configuration

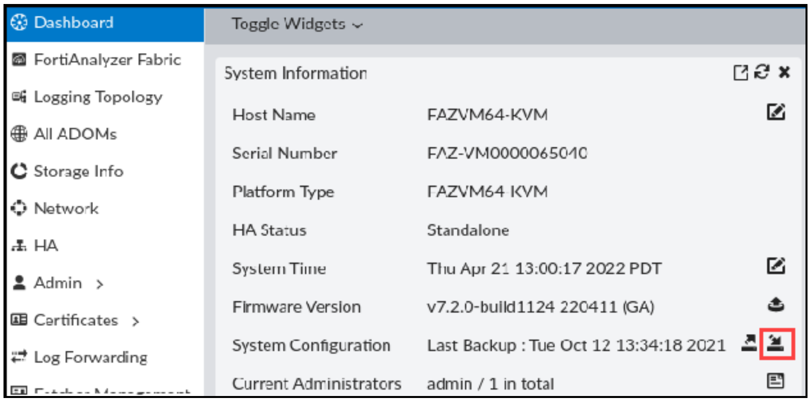
1. On the Local-Client VM, open a browser, and then connect to the FortiAnalyzer GUI at `http://10.0.1.210`.
2. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
   A link to FortiAnalyzer is added to the favorites bar in the browser on the Local-Client VM.



3. Click **System Settings**.

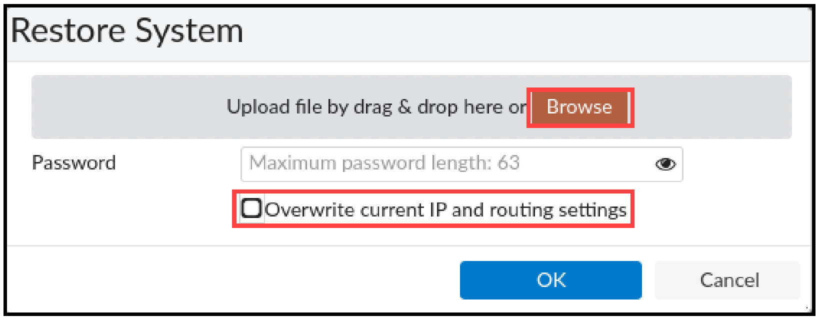


4. In the **System Information** section, click the icon to restore from an existing configuration.



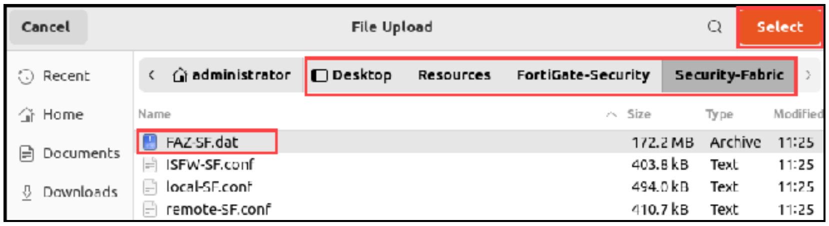
Host Name	FAZVM64-KVM
Serial Number	FAZ-VM0000065040
Platform Type	FAZVM64 KVM
HA Status	Standalone
System Time	Thu Apr 21 13:00:17 2022 PDT
Firmware Version	v7.2.0-build1124 220411 (GA)
System Configuration	Last Backup : Tue Oct 12 13:34:18 2021
Current Administrators	admin / 1 in total

5. Clear the **Overwrite current IP and routing settings** checkbox, and then click **Browse**.


Restore System
Upload file by drag & drop here or
Browse
Password
Maximum password length: 63
OK
Cancel

□ Overwrite current IP and routing settings

6. Browse to **Desktop** > **Resources** > **FortiGate-Security** > **Security-Fabric**, select `FAZ-SF.dat`, and then click **Select**.



Name	Size	Type	Modified
FAZ-SF.dat	172.2 MB	Archive	11:25
ISFW-SF.conf	403.8 kB	Text	11:25
local-SF.conf	494.0 kB	Text	11:25
remote-SF.conf	410.7 kB	Text	11:25

7. Click **OK**.

8. Wait until FortiAnalyzer restarts.

Exercise 1: Configuring the Security Fabric on Local-FortiGate and ISFW

In this exercise, you will configure the Security Fabric between Local-FortiGate (root) and ISFW (downstream).

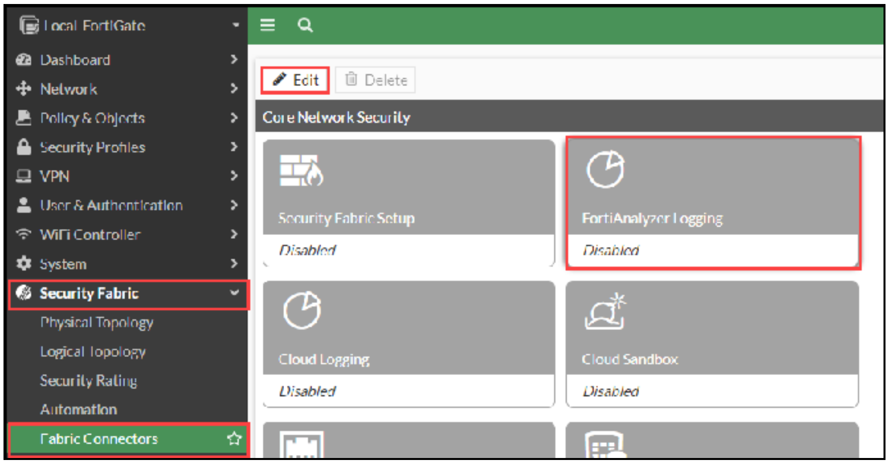
Configure FortiAnalyzer Logging on Local-FortiGate (Root)

You will configure the root of the Security Fabric to send all logs to FortiAnalyzer. These settings will be automatically replicated to all downstream devices when they become members of the Security Fabric.

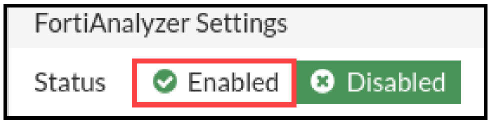
For this lab, FortiAnalyzer is already preconfigured to accept the registration requests that originate from all FortiGate devices in the topology.

To configure Local-FortiGate to send logs to FortiAnalyzer

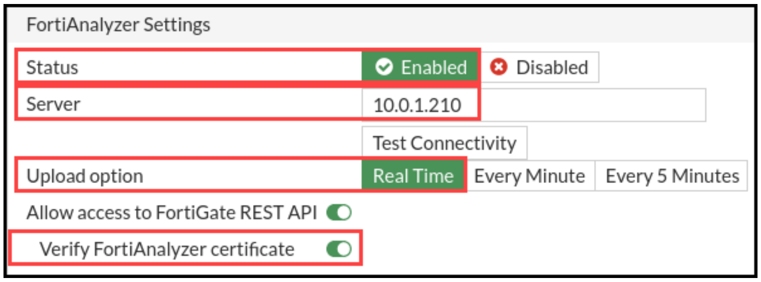
1. Log in to the Local-FortiGate GUI with the username `admin` and password `password`.
2. In the menu on the left, click **Security Fabric** > **Fabric Connectors**.
3. Select **FortiAnalyzer Logging**, and then click **Edit**.



4. Enable **FortiAnalyzer Logging**.



5. Edit the settings so they match the following image:



FortiAnalyzer Settings

Status: ● Enabled ○ Disabled

Server: 10.0.1.210

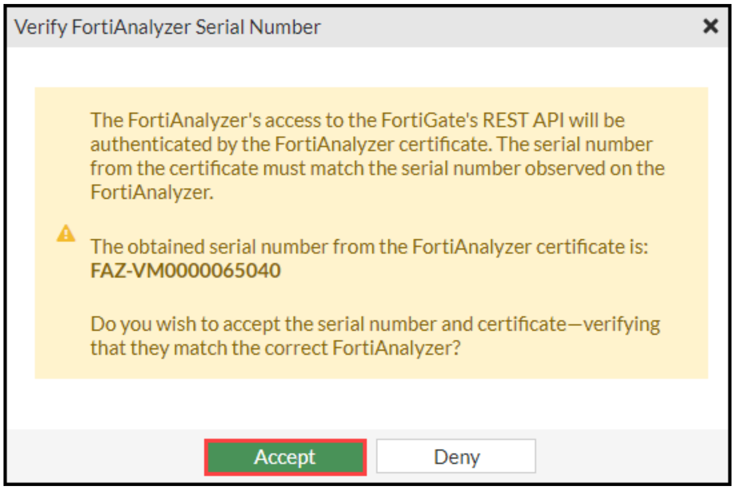
Upload option: [✓ Real Time] Every Minute Every 5 Minutes

Allow access to FortiGate REST API: enabled

Verify FortiAnalyzer certificate: enabled

6. Click **OK**.

7. In the verification window that appears, click **Accept**.



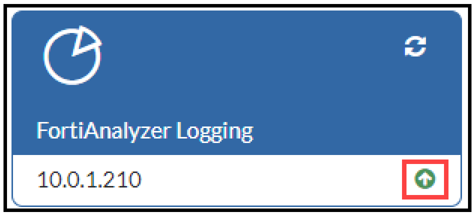
Verify FortiAnalyzer Serial Number

The FortiAnalyzer's access to the FortiGate's REST API will be authenticated by the FortiAnalyzer certificate. The serial number from the certificate must match the serial number observed on the FortiAnalyzer.

The obtained serial number from the FortiAnalyzer certificate is: **FAZ-VM0000065040**

Do you wish to accept the serial number and certificate—verifying that they match the correct FortiAnalyzer?

8. Verify that the status of **Security Fabric** > **Fabric Connectors** > **FortiAnalyzer Logging** is up.

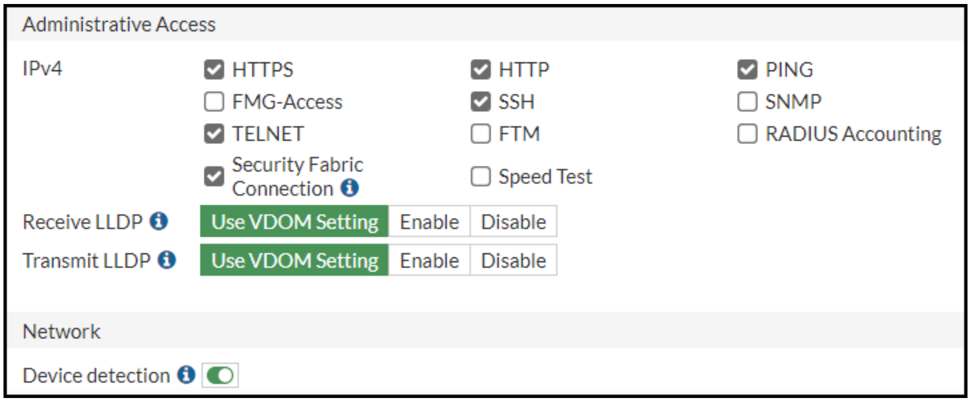


Configure the Security Fabric on Local-FortiGate (Root)

You will configure the root of the Security Fabric.

To enable the Security Fabric connection on Local-FortiGate interfaces

1. On the Local-FortiGate GUI, log in with the username `admin` and password `password`.
2. Click **Network** > **Interfaces**.
3. Click **port3**, and then click **Edit**.
4. In the **Administrative Access** section, select the **Security Fabric Connection** checkbox.
5. In the **Network** section, enable **Device detection**.
   Your configuration should look like the following example:



Administrative Access

IPv4
☑ HTTPS ☑ HTTP ☑ PING
□ FMG-Access ☑ SSH □ SNMP
☑ TELNET □ FTM □ RADIUS Accounting
☑ Security Fabric Connection □ Speed Test

Receive LLDP: [✓ Use VDOM Setting] Enable Disable

Transmit LLDP: [✓ Use VDOM Setting] Enable Disable

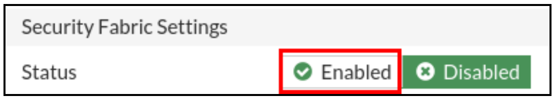
Network

Device detection: ● on

6. Click **OK**.
7. Click **Network** > **Interfaces**, and then expand **port1**.
8. Click the **To-Remote-HQ2** interface, and then click **Edit**.
9. In the **Administrative Access** section, select the **Security Fabric Connection** checkbox.
10. Click **OK**.

To enable the Security Fabric on Local-FortiGate

1. On the Local-FortiGate GUI, click **Security Fabric** > **Fabric Connectors**.
2. Click **Security Fabric Setup**, and then click **Edit**.
3. In the **Security Fabric Settings** section, click **Enabled**.



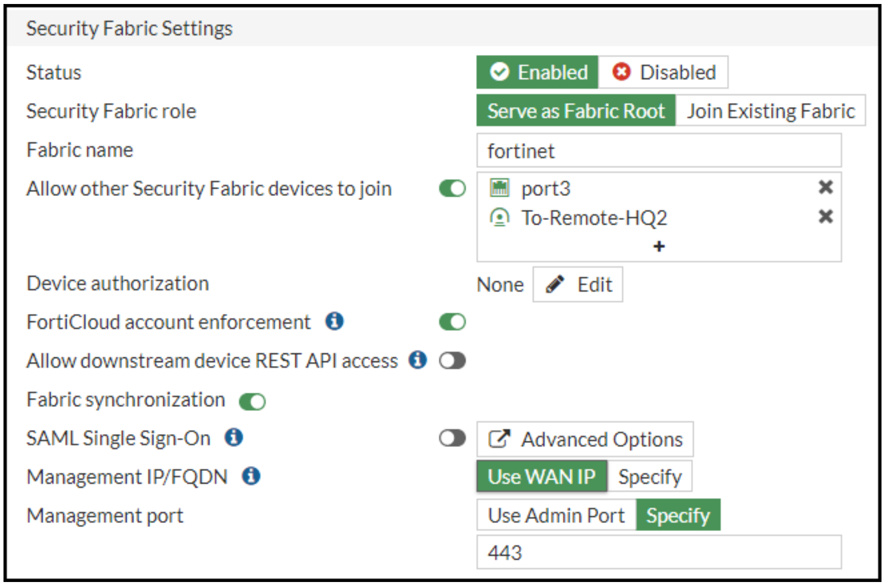
Security Fabric Settings

Status: [✓ Enabled] Disabled

4. Click **Serve as Fabric Root**.
5. Configure the following settings:

Field	Value
Fabric name	fortinet
Allow other Security Fabric devices to join	enable
(ensure both interfaces are selected)	port3, To-Remote-HQ2

Your configuration should look like the following example:



Security Fabric Settings

Status: Enabled (selected) | Disabled

Security Fabric role: Serve as Fabric Root (selected) | Join Existing Fabric

Fabric name: fortinet

Allow other Security Fabric devices to join: enabled — port3, To-Remote-HQ2

Device authorization: None | Edit

FortiCloud account enforcement: enabled

Allow downstream device REST API access: disabled

Fabric synchronization: enabled

SAML Single Sign-On: disabled — Advanced Options

Management IP/FQDN: Use WAN IP (selected) | Specify

Management port: Use Admin Port | Specify (selected)

443

6. Click **OK**.

Configure the Security Fabric on ISFW

You will configure ISFW to join the Security Fabric as a downstream FortiGate.

Take the Expert Challenge!

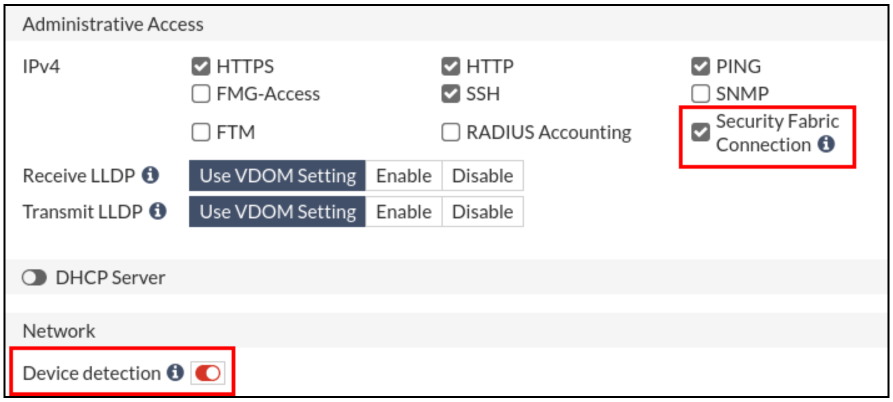
On the ISFW GUI, enable **Security Fabric Connection** on port1 and port3. Enable network device detection on both ports. After you enable **Security Fabric Connection**, connect ISFW to the Security Fabric that has Local-FortiGate as its root device.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see To enable the Security Fabric on ISFW (downstream) on page 190.

To enable the Security Fabric connection on ISFW interfaces

1. On the ISFW GUI, log in with the username `admin` and password `password`.
2. Click **Network** > **Interfaces**.
3. Click **port1**, and then click **Edit**.
4. In the **Administrative Access** section, confirm that the **Security Fabric Connection** checkbox is selected.
5. In the **Network** section, enable **Device detection**.



Administrative Access

IPv4
☑ HTTPS ☑ HTTP ☑ PING
□ FMG-Access ☑ SSH □ SNMP
□ FTM □ RADIUS Accounting ☑ Security Fabric Connection

Receive LLDP: Use VDOM Setting | Enable | Disable

Transmit LLDP: Use VDOM Setting | Enable | Disable

DHCP Server

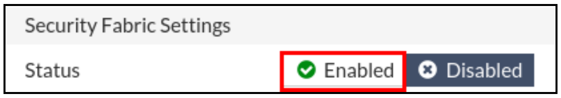
Network

Device detection: enabled

6. Click **OK**.
7. Click **Network** > **Interfaces**.
8. Click **port3**, and then click **Edit**.
9. In the **Administrative Access** section, select the **Security Fabric Connection** checkbox.
10. In the **Network** section, enable **Device detection**.
11. Click **OK** to save the changes.

To enable the Security Fabric on ISFW (downstream)

1. On the ISFW GUI, click **Security Fabric** > **Fabric Connectors**.
2. Click **Security Fabric Setup**, and then click **Edit**.
3. In the **Security Fabric Settings** section, click **Enabled**.

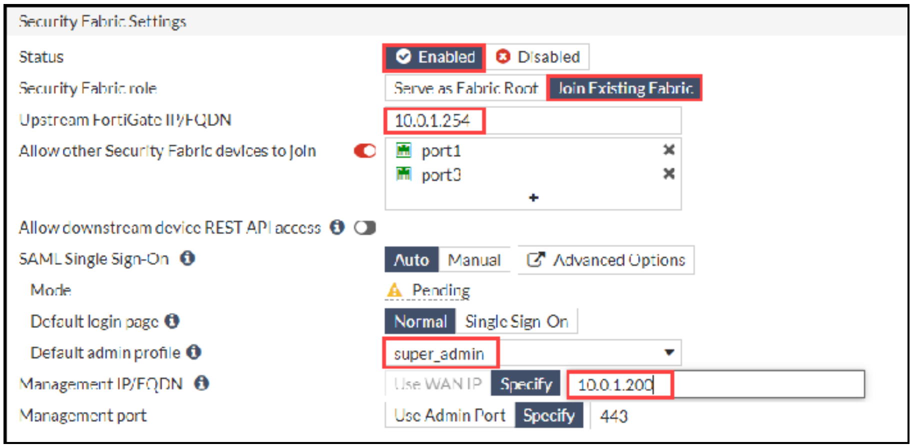


Security Fabric Settings

Status: Enabled | Disabled

4. In the **Security Fabric role** field, confirm that **Join Existing Fabric** is selected.
5. Verify that the **Upstream FortiGate IP** is set to `10.0.1.254`.
6. In the **Default admin profile** field, select `super_admin`.
7. In the **Management IP/FQDN** field, click **Specify**, and then type `10.0.1.200`.

   Your configuration should look like the following example:



Security Fabric Settings

Status: Enabled | Disabled

Security Fabric role: Serve as Fabric Root | Join Existing Fabric

Upstream FortiGate IP/FQDN: 10.0.1.254

Allow other Security Fabric devices to join: enabled — port1, port3

Allow downstream device REST API access: disabled

SAML Single Sign-On: Auto | Manual | Advanced Options

Mode: Pending

Default login page: Normal | Single Sign On

Default admin profile: super_admin

Management IP/FQDN: Use WAN IP | Specify — 10.0.1.200

Management port: Use Admin Port | Specify — 443

8. Click **OK**.
9. Click **OK** to confirm the settings.

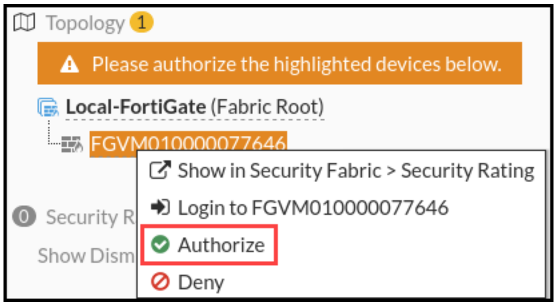
FortiAnalyzer logging is enabled on ISFW after the Security Fabric is enabled. Downstream FortiGate devices retrieve FortiAnalyzer settings from the root FortiGate when they join the Security Fabric.

Authorize ISFW (Downstream) on Local-FortiGate (Root)

You will authorize ISFW on Local-FortiGate to join the Security Fabric.

To authorize ISFW on Local-FortiGate

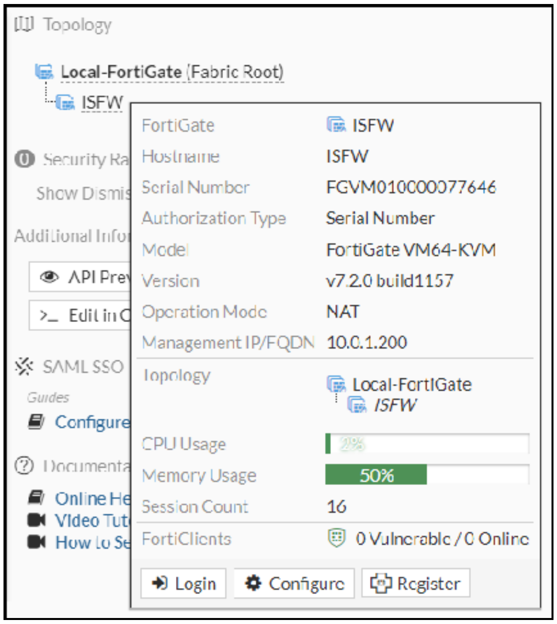
1. On the Local-FortiGate GUI, click **Security Fabric** > **Fabric Connectors**.
2. In the **Topology** section, click the highlighted FortiGate serial number, and then click **Authorize**.


Topology 1
Please authorize the highlighted devices below.
Local-FortiGate (Fabric Root)
FGVM010000077646
Show in Security Fabric > Security Rating
Login to FGVM010000077646
Authorize
Deny
0 Security R
Show Dism

3. In the **Device Registration** window, click **Authorize**, and then click **Close**.

After authorization, ISFW appears in the Security Fabric topology section, which means ISFW joined the Security Fabric successfully.

4. Hover over the **ISFW** icon to display a summary of the firewall settings, and then verify that it is correctly registered in the Security Fabric.



FortiGate	ISFW
Hostname	ISFW
Serial Number	FGVM010000077646
Authorization Type	Serial Number
Model	FortiGate VM64-KVM
Version	v7.2.0 build1157
Operation Mode	NAT
Management IP/FQDN	10.0.1.200
Topology	Local-FortiGate *ISFW*
CPU Usage	2%
Memory Usage	50%
Session Count	16
FortiClients	0 Vulnerable / 0 Online

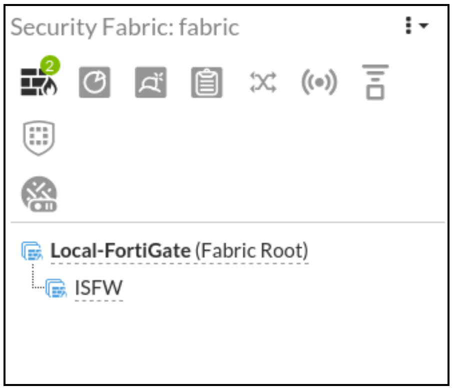
Check the Security Fabric Deployment Result

You will check the Security Fabric deployment result on Local-FortiGate (root).

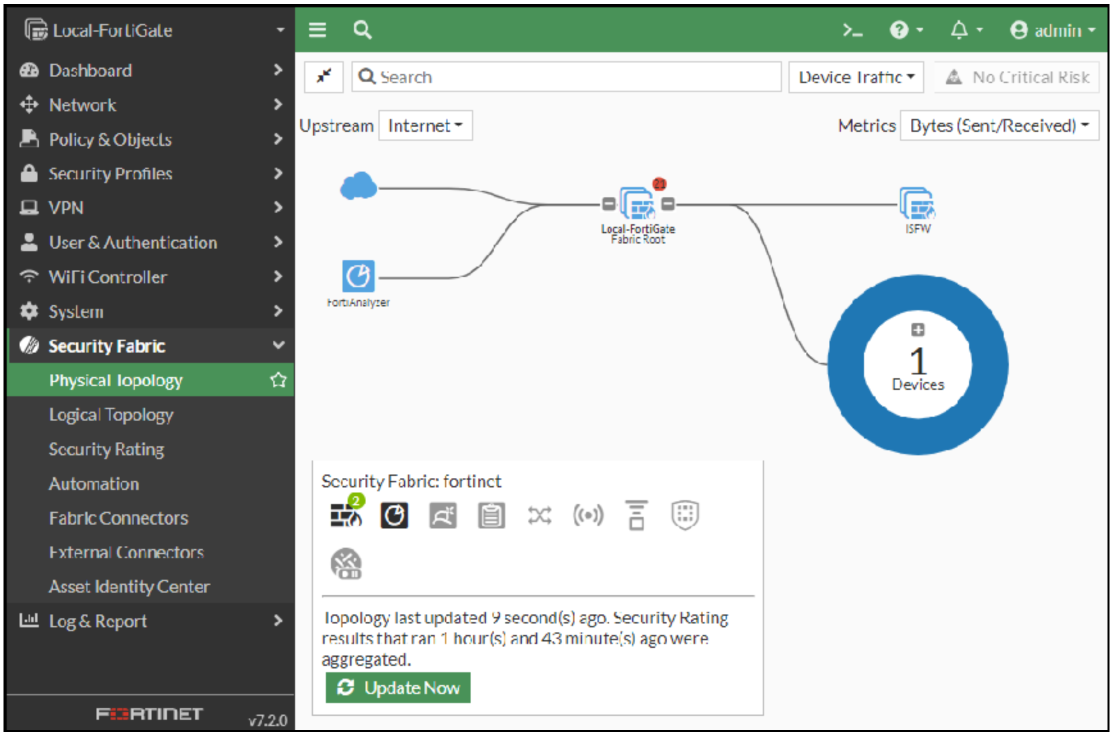
To check the Security Fabric on Local-FortiGate

1. On the Local-Client VM, open a new browser, and then go to https://www.fortinet.com.
   This is to generate some traffic from the Local-Client VM so it is included in the topology views.

2. On the Local-FortiGate GUI, click **Dashboard** > **Status**.
   The Security Fabric widget displays the FortiGate devices in the Security Fabric.



3. On the Local-FortiGate GUI, click **Security Fabric** > **Physical Topology**.
   This page shows a visualization of access layer devices in the Security Fabric.

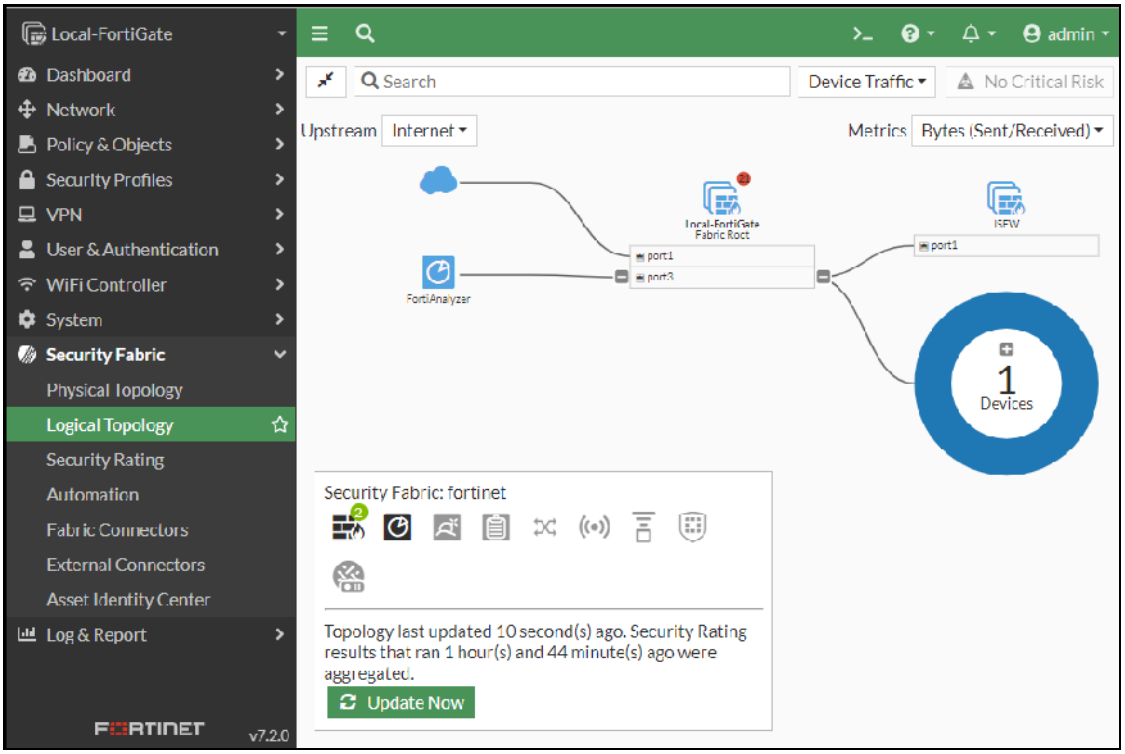


Topology last updated 9 second(s) ago. Security Rating results that ran 1 hour(s) and 43 minute(s) ago were aggregated.

Your topology view might not match exactly what is shown in this example.

4. On the Local-FortiGate GUI, click **Security Fabric** > **Logical Topology**.

This dashboard displays information about the interfaces that connect each device in the Security Fabric.



Topology last updated 10 second(s) ago. Security Rating results that ran 1 hour(s) and 44 minute(s) ago were aggregated.

Exercise 2: Configuring the Security Fabric on Local-FortiGate and Remote-FortiGate

In this exercise, you will add another FortiGate to the Security Fabric tree. In this topology, the downstream Remote-FortiGate connects to the root Local-FortiGate over IPsec VPN to join the Security Fabric.

Take the Expert Challenge!

On the Remote-FortiGate GUI, enable **Security Fabric Connection** on port6 and the **To-Local-HQ1** VPN interface. Enable network device detection on port6. After you enable **Security Fabric Connection**, connect Remote-FortiGate to the Security Fabric using the tunnel IP address `10.10.10.1` to connect to the root FortiGate.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Authorize Remote-FortiGate (Downstream) on Local-FortiGate (Root) on page 195.

Configure the Security Fabric on Remote-FortiGate (Downstream)

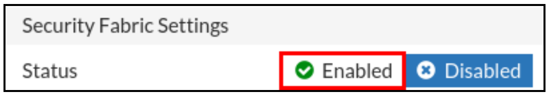
You will configure Remote-FortiGate to join the Security Fabric as a downstream FortiGate over the IPsec VPN.

To enable the Security Fabric connection on Remote-FortiGate interfaces

1. On the Remote-FortiGate GUI, log in with the username `admin` and password `password`.
2. Click **Network** > **Interfaces**.
3. Click **port6**, and then click **Edit**.
4. In the **Administrative Access** section, select the **Security Fabric Connection** checkbox.
5. In the **Network** section, ensure that **Device detection** is enabled.
6. Click **OK**.
7. Click **Network** > **Interfaces**, and then expand **port4**.
8. Click the **To-Local-HQ1** interface, and then click **Edit**.
9. In the **Administrative Access** section, select the **Security Fabric Connection** checkbox.
10. Click **OK** to save the changes.

To enable the Security Fabric on Remote-FortiGate

1. On the Remote-FortiGate GUI, click **Security Fabric** > **Fabric Connectors**.
2. Click **Security Fabric Setup**, and then click **Edit**.
3. In the **Security Fabric Settings** section, click **Enabled**.

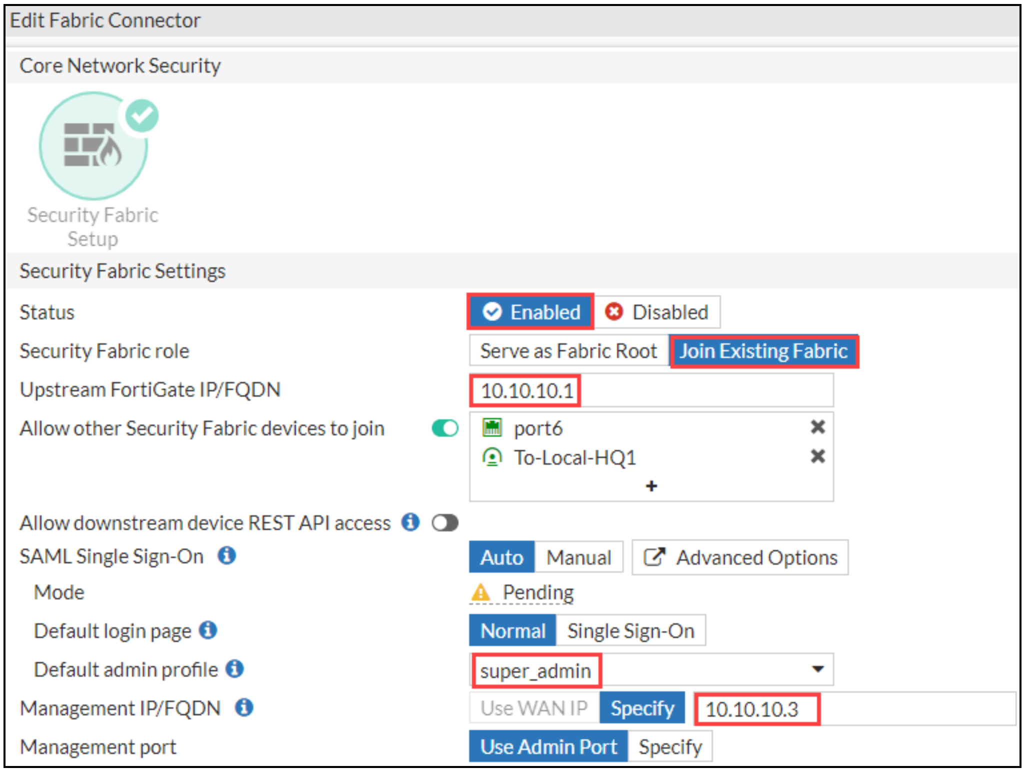


Security Fabric Settings

Status [✓ Enabled] Disabled

4. In the **Security Fabric role** field, ensure that **Join Existing Fabric** is selected.
5. In the **Upstream FortiGate IP** field, type `10.10.10.1`.
6. In the **Default admin profile** field, select `super_admin`.
7. In the **Management IP/FQDN** field, click **Specify**, and then type `10.10.10.3`.

   Your configuration should look like the following example:



Edit Fabric Connector

Core Network Security

Security Fabric Setup

Security Fabric Settings

Status: Enabled

Security Fabric role: Join Existing Fabric

Upstream FortiGate IP/FQDN: 10.10.10.1

Allow other Security Fabric devices to join: port6, To-Local-HQ1

Allow downstream device REST API access: off

SAML Single Sign-On: Auto

Mode: Pending

Default login page: Normal

Default admin profile: super_admin

Management IP/FQDN: Specify 10.10.10.3

Management port: Use Admin Port

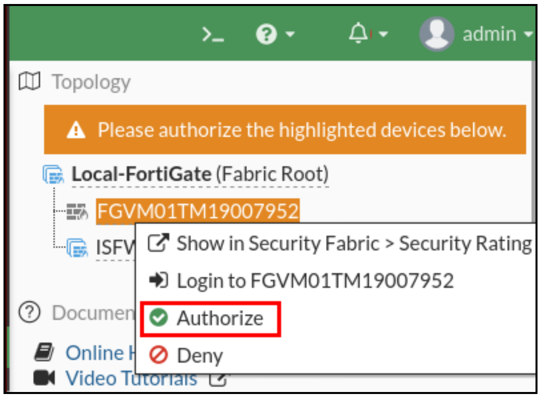
8. Click **OK**.
9. Click **OK** to confirm.

Authorize Remote-FortiGate (Downstream) on Local-FortiGate (Root)

You will authorize Remote-FortiGate on Local-FortiGate to join the Security Fabric.

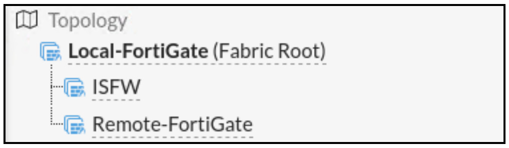
To authorize Remote-FortiGate on Local-FortiGate

1. On the Local-FortiGate GUI, log in with the username `admin` and password `password`.
2. Click **Security Fabric** > **Fabric Connectors**.
3. In the **Topology** section, click the highlighted FortiGate serial number, and then click **Authorize**.


admin
Topology
Please authorize the highlighted devices below.
Local-FortiGate (Fabric Root)
FGVM01TM19007952
ISFV
Show in Security Fabric > Security Rating
Login to FGVM01TM19007952
Authorize
Deny
Documen
Online H
Video Tutorials

4. In the **Device Registration** window, click **Authorize**, and then click **Close**.

After authorization, Remote-FortiGate appears in the topology. Now, both ISFW and Remote-FortiGate are shown as downstream devices of the root, Local-FortiGate. Your configuration should look like the following example:



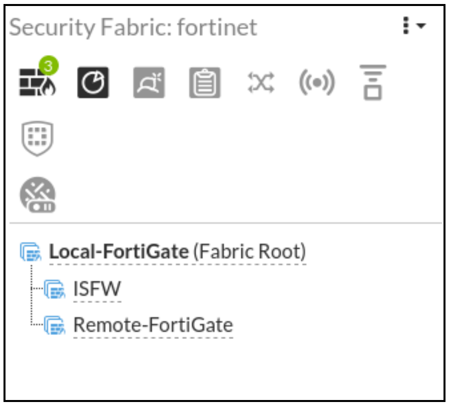
You may need to refresh the page to match the image above.

Check the Security Fabric Deployment Result

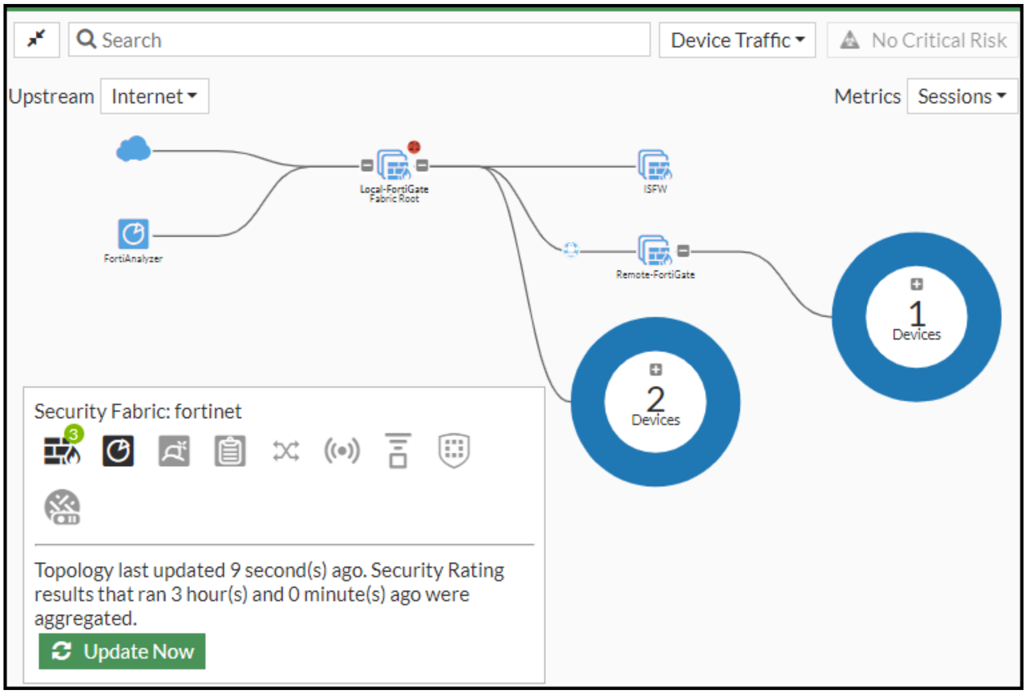
You will check the Security Fabric deployment result on the root, Local-FortiGate.

To check the Security Fabric on Local-FortiGate

1. On the Local-FortiGate GUI, click **Dashboard** > **Status**.
   The **Security Fabric** widget displays all FortiGate devices in the Security Fabric.



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



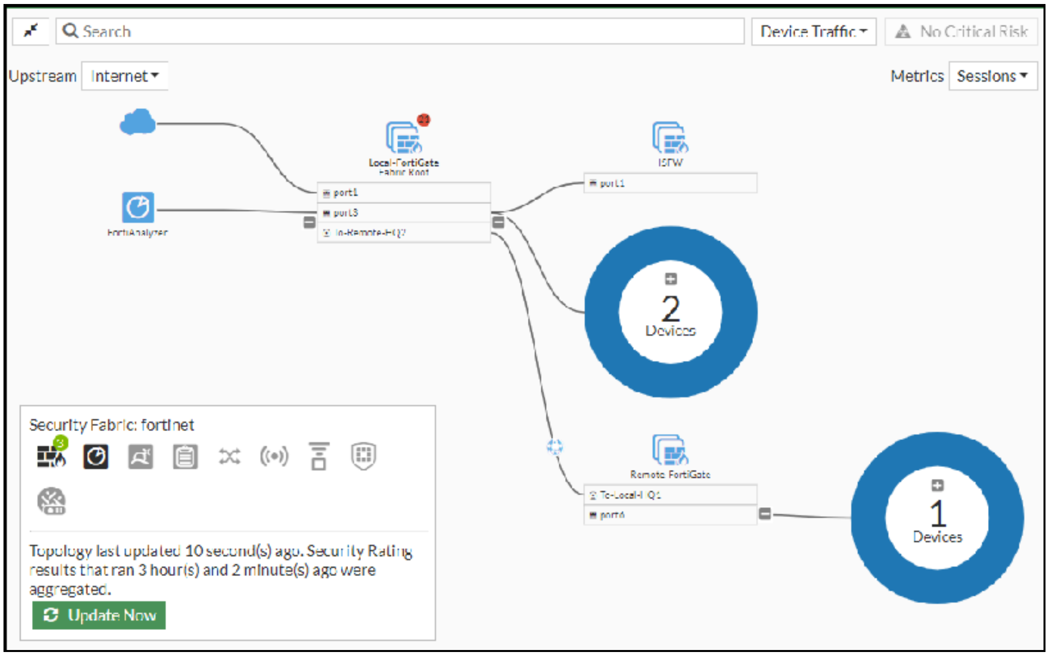
Security Fabric: fortinet

Topology last updated 9 second(s) ago. Security Rating results that ran 3 hour(s) and 0 minute(s) ago were aggregated.

You may need to click the **Update Now** button to refresh the topology. Your topology view might not match what is shown in this example.

3. Click **Security Fabric** > **Logical Topology**.

   This dashboard displays information about the interfaces that each device in the Security Fabric connects to.



Security Fabric: fortinet

Topology last updated 10 second(s) ago. Security Rating results that ran 3 hour(s) and 2 minute(s) ago were aggregated.

You may need to click the **Update Now** button to refresh the topology.

Your topology view might not match what is shown in this example. At a minimum, you should see Local-FortiGate, Remote-FortiGate, and ISFW in the topology view.

You can generate some traffic from the Linux VMs to have them shown in the topology.

Exercise 3: Running the Security Rating

The security rating feature includes three major score cards: **Security Posture**, **Fabric Coverage**, and **Optimization**. These can help you make improvements to your organization's network, such as enforcing password security, applying recommended login attempt thresholds, encouraging two-factor authentication, and more. In this exercise, you will run security ratings and apply some of the recommendations.

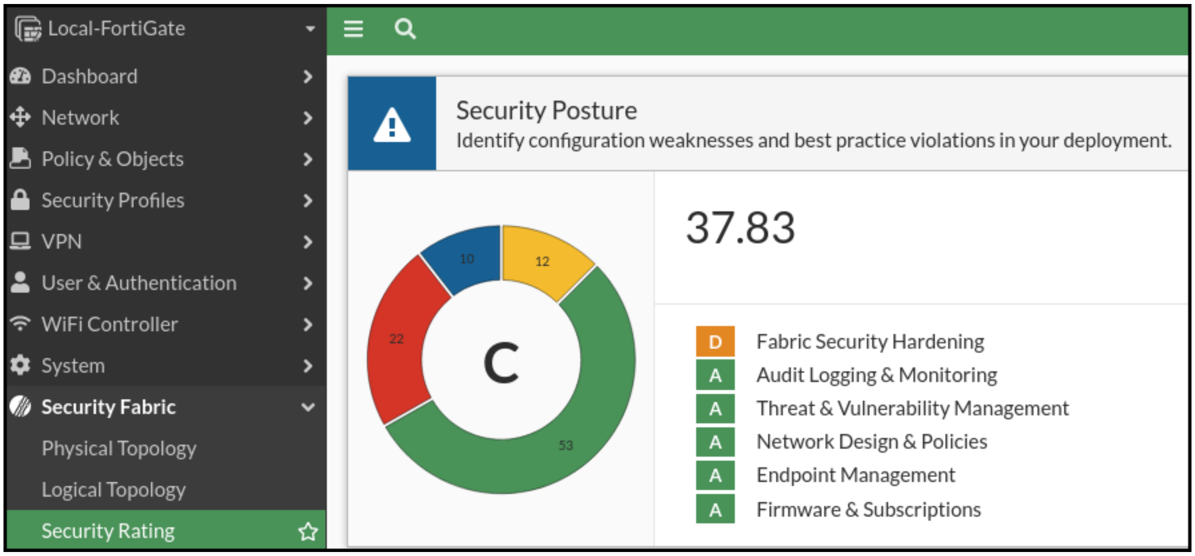
> When you make changes through the **Security Posture** page, FortiGate generates two configuration revisions for each change you make. Because FortiGate can store only a limited number of revisions, if you make multiple changes through the security rating, you may lose some of the revisions needed for other labs.
>
> If you lose any revisions that you make for the labs, contact the instructor for assistance.

Run the Security Rating on the Local-FortiGate (Root)

You will run a security rating check, which analyzes the Security Fabric deployment, and then identifies potential vulnerabilities and highlights best practices. You must run the Security Fabric rating on the root FortiGate in the Security Fabric.

To review the Security Posture widget

1. On the Local-FortiGate GUI, log in with the username `admin` and password `password`.
2. Click **Security Fabric** > **Security Rating**, and then check the **Security Posture** widget to see the score of your Security Fabric deployment.



Security Posture
Identify configuration weaknesses and best practice violations in your deployment.

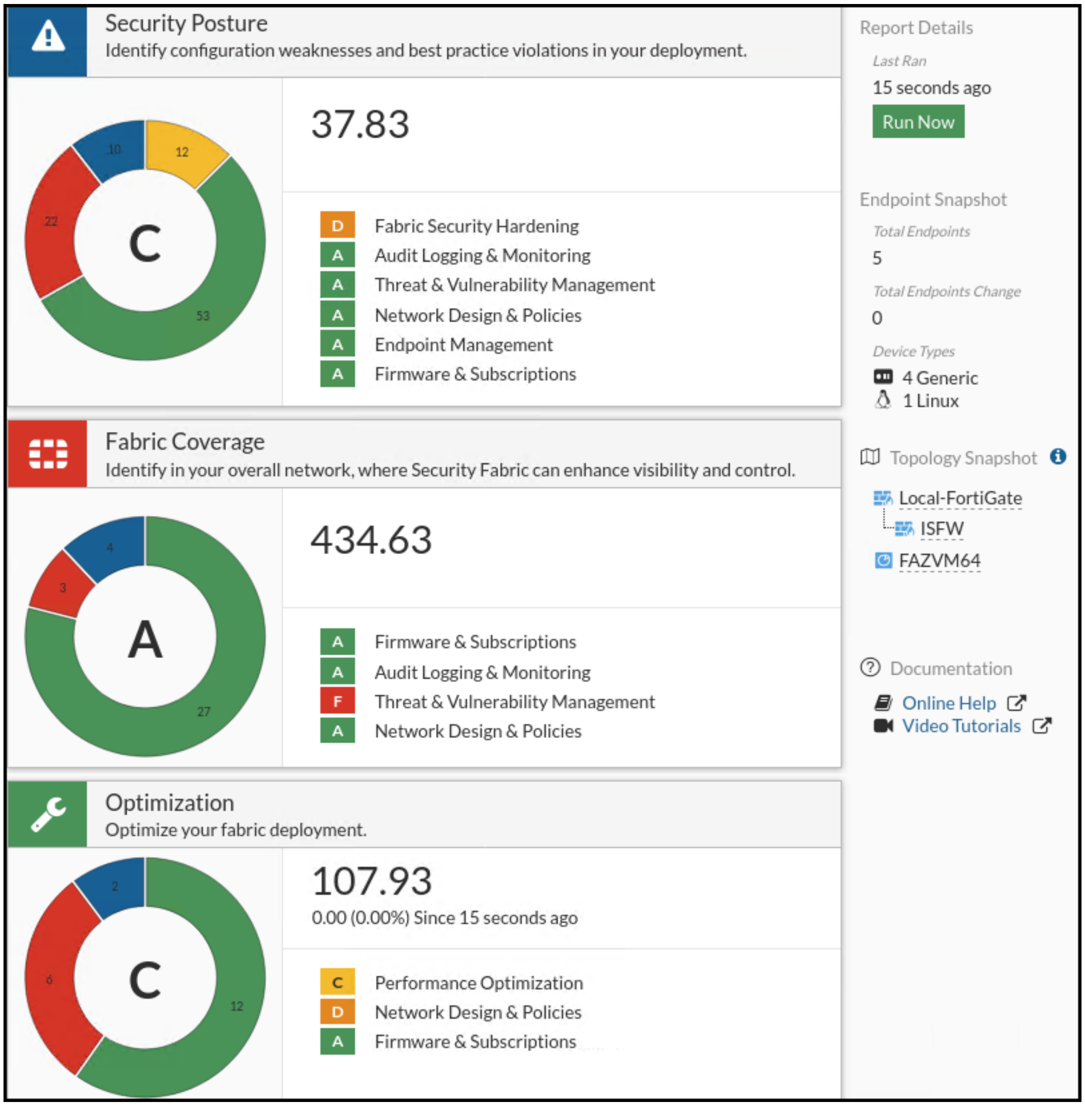
37.83

D	Fabric Security Hardening
A	Audit Logging & Monitoring
A	Threat & Vulnerability Management
A	Network Design & Policies
A	Endpoint Management
A	Firmware & Subscriptions

Your **Security Posture** widget might not match what is shown in this example.

To generate new security rating scores on the root FortiGate

1. On the Local-FortiGate GUI, click **Security Fabric** > **Security Rating**.



Security Posture

Identify configuration weaknesses and best practice violations in your deployment.

37.83

D	Fabric Security Hardening
A	Audit Logging & Monitoring
A	Threat & Vulnerability Management
A	Network Design & Policies
A	Endpoint Management
A	Firmware & Subscriptions

Fabric Coverage

Identify in your overall network, where Security Fabric can enhance visibility and control.

434.63

A	Firmware & Subscriptions
A	Audit Logging & Monitoring
F	Threat & Vulnerability Management
A	Network Design & Policies

Optimization

Optimize your fabric deployment.

107.93

0.00 (0.00%) Since 15 seconds ago

C	Performance Optimization
D	Network Design & Policies
A	Firmware & Subscriptions

Report Details

Last Ran

15 seconds ago

Run Now

Endpoint Snapshot

Total Endpoints

5

Total Endpoints Change

0

Device Types

4 Generic

1 Linux

Topology Snapshot

Local-FortiGate

ISFW

FAZVM64

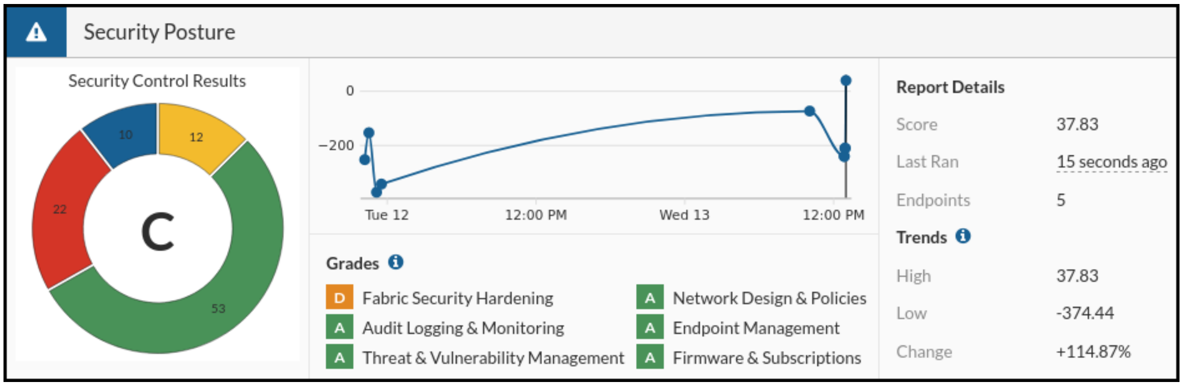
Documentation

Online Help

Video Tutorials

You can expand each scorecard section to view recommendations for each section.

2. Click **Security Posture** to show the scorecard details.



Security Posture

Security Control Results

Grades

D	Fabric Security Hardening	A	Network Design & Policies
A	Audit Logging & Monitoring	A	Endpoint Management
A	Threat & Vulnerability Management	A	Firmware & Subscriptions

Report Details

Score	37.83
Last Ran	15 seconds ago
Endpoints	5

Trends

High	37.83
Low	-374.44
Change	+114.87%

You may need to zoom out this page to see all details.

The **Security Posture** scorecard shows the following information:

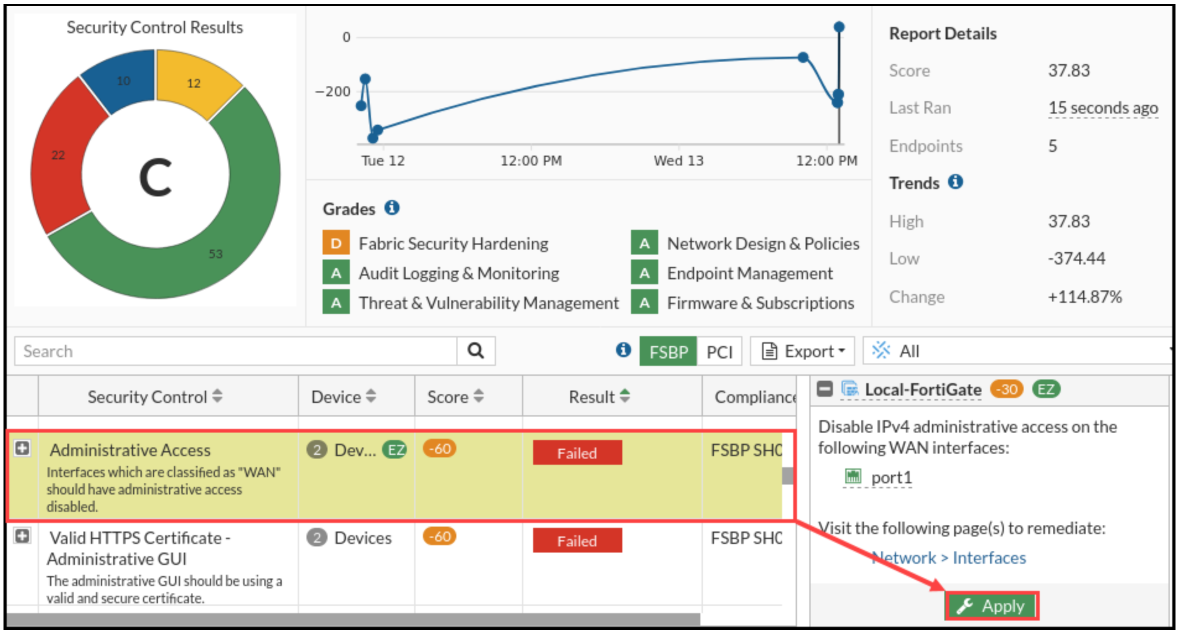
- A **Score** field that shows the score for your Security Fabric
- An overall count of how many checks passed and failed, with the failed checks divided by severity
- Information about each failed check, including which FortiGate device failed the check, the effect of the check failure on the security score, and recommendations to fix the issue

Your **Security Posture** score might not match what is shown in this example.

3. In the **Security Control** column, expand **Failed**, and then select **Administrative Access**.

   The **Apply** option appears with recommendations that the wizard can apply.

4. In the right pane, under **Local-FortiGate**, click **Apply**.



Security Control Results

Grades

D	Fabric Security Hardening	A	Network Design & Policies
A	Audit Logging & Monitoring	A	Endpoint Management
A	Threat & Vulnerability Management	A	Firmware & Subscriptions

Report Details

Score	37.83
Last Ran	15 seconds ago
Endpoints	5

Trends

High	37.83
Low	-374.44
Change	+114.87%

Security Control	Device	Score	Result	Complianc
Administrative Access Interfaces which are classified as "WAN" should have administrative access disabled.	2 Dev... EZ	-60	Failed	FSBP SHC
Valid HTTPS Certificate - Administrative GUI The administrative GUI should be using a valid and secure certificate.	2 Devices	-60	Failed	FSBP SHC

Local-FortiGate -30 EZ

Disable IPv4 administrative access on the following WAN interfaces:

port1

Visit the following page(s) to remediate:

Network > Interfaces

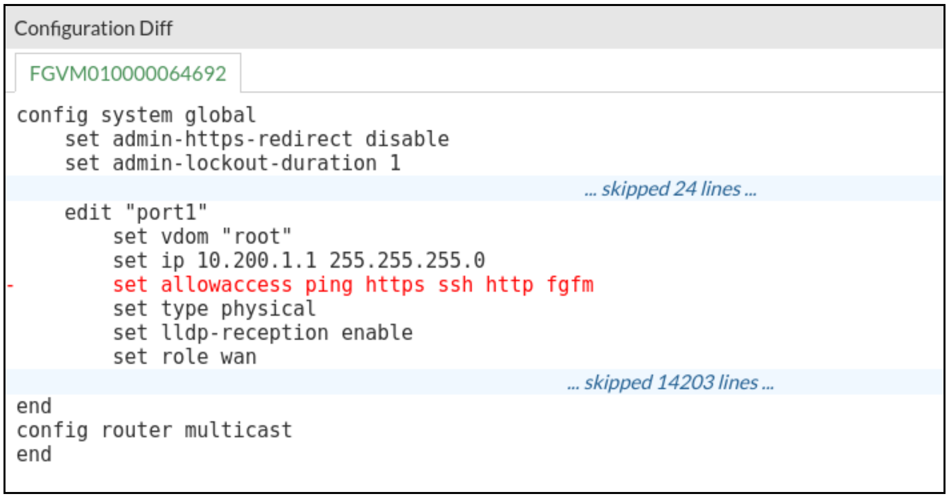
Apply

If you can't see the **Apply** button, zoom out on the web page to view the full page.

5. Click **OK** to save the configuration file.

   The **View Diff** button appears beside **Apply** after audit log settings are applied successfully.

6. Click **View Diff** to view the configuration changes that the wizard applied to **Local-FortiGate**.

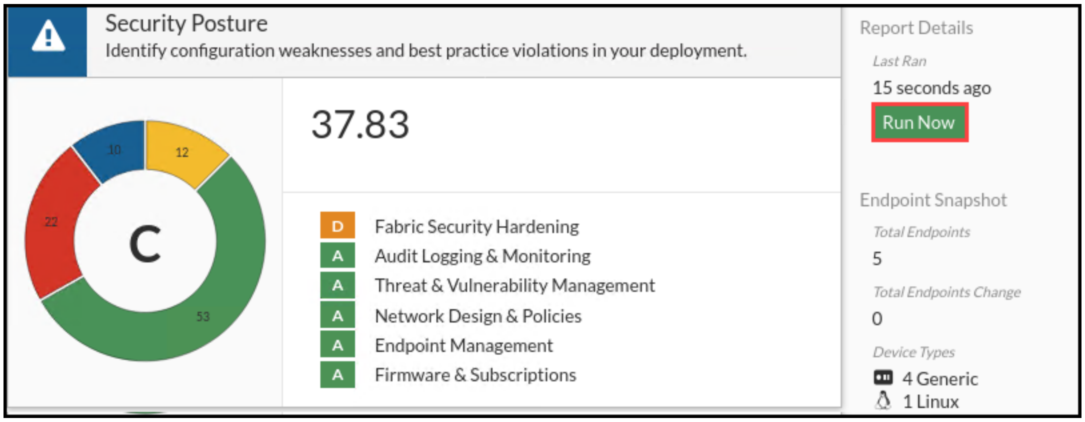


Configuration Diff

FGVM010000064692

```
config system global
    set admin-https-redirect disable
    set admin-lockout-duration 1
                                        ... skipped 24 lines ...
    edit "port1"
        set vdom "root"
        set ip 10.200.1.1 255.255.255.0
-       set allowaccess ping https ssh http fgfm
        set type physical
        set lldp-reception enable
        set role wan
                                        ... skipped 14203 lines ...
end
config router multicast
end
```

7. Click **Close**.
8. Click **Security Fabric** > **Security Rating**.
9. Click **Run Now** to get the new **Security Posture** score.



Security Posture

Identify configuration weaknesses and best practice violations in your deployment.

37.83

D Fabric Security Hardening
A Audit Logging & Monitoring
A Threat & Vulnerability Management
A Network Design & Policies
A Endpoint Management
A Firmware & Subscriptions

Report Details

Last Ran
15 seconds ago

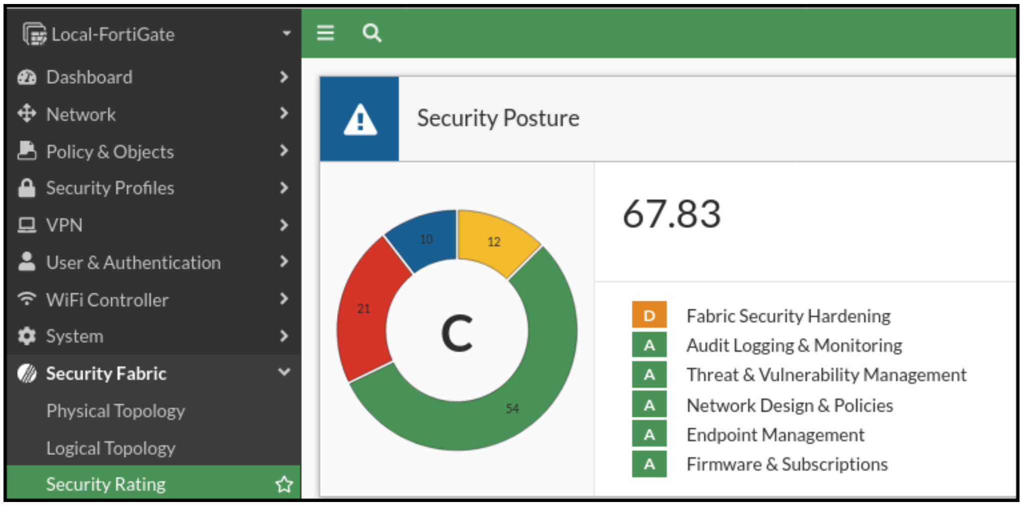
Endpoint Snapshot

Total Endpoints
5

Total Endpoints Change
0

Device Types
4 Generic
1 Linux

You will notice the **Security Posture** widget displays information from the most recent security rating check.



67.83

D	Fabric Security Hardening
A	Audit Logging & Monitoring
A	Threat & Vulnerability Management
A	Network Design & Policies
A	Endpoint Management
A	Firmware & Subscriptions

When you run a Security Fabric rating, your organization's Security Fabric receives a Security Fabric score. The score is positive or negative, and a higher score represents a more secure network. The score is based on how many checks your network passes and fails, as well as the severity level of these checks.

You can repeat steps 2–7 for all other sections and devices to apply recommendations, which will improve your Security Fabric score.

Your security rating scores might not match what is shown in this example.