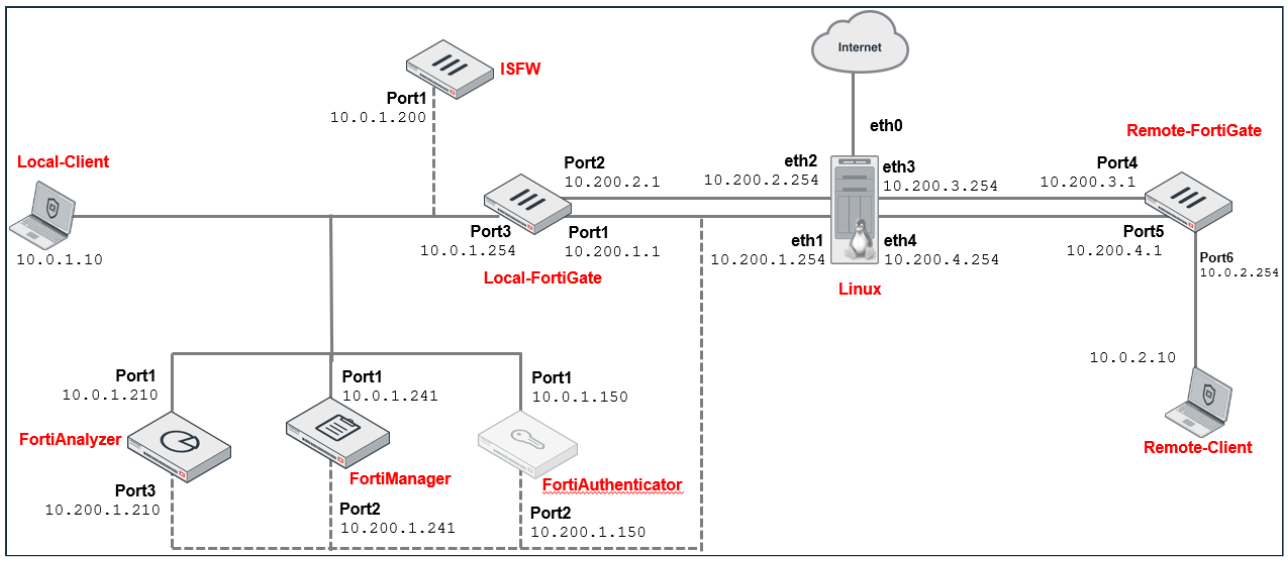
()Network Topology



Network Topology

Lab 1: System and Network Settings

In this lab, you will learn about FortiGate basic system and network factory default settings and apply changes and modify the default factory settings. You will also perform administrative tasks through the CLI and GUI and back up and restore a configuration file, as well as create a new administrator account and modify administrator access permissions.

Objectives

- Review and change network settings
- 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: 30 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: Configuring FortiGate System Settings

In this exercise, you will review the Local-FortiGate system settings and make changes to complete setting up FortiGate on your network. You will enable the internal network DHCP server to allow hosts to receive the IP address when connecting to Local-FortiGate.

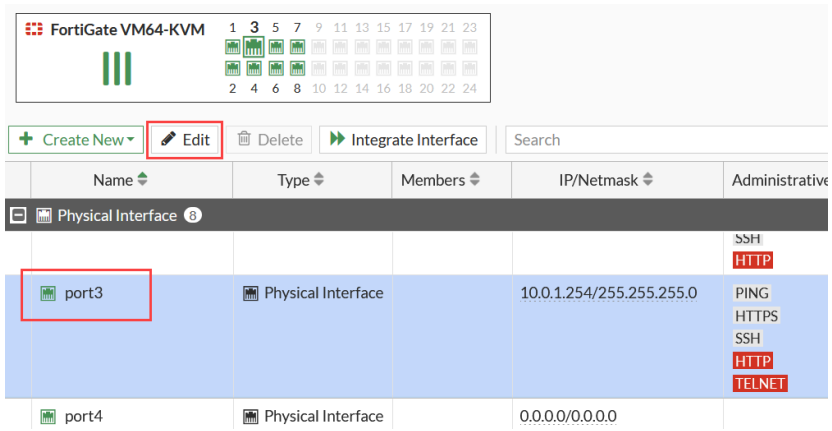
Some of the settings in this lab have been preconfigured and are not the factory default settings of FortiGate.

Review Local-FortiGate Network Settings

You will review the port3 network interface on Local-FortiGate and you will also review the static routes.

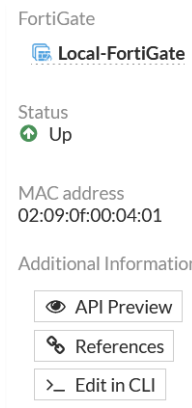
To review the port3 network interface

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Network** > **Interfaces**.
3. Click **port3**, and then click **Edit**.



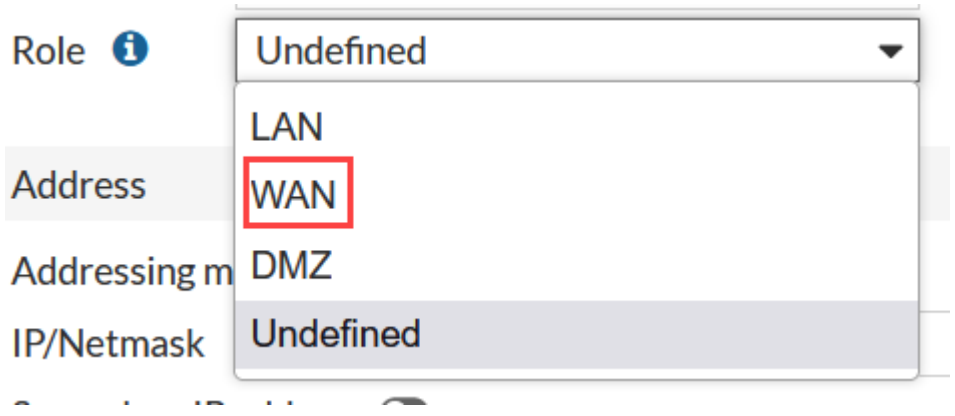
You can double-click an object on the FortiGate GUI to view or edit the content of the object.

4. In the **Edit Interface** window, review the information available on the right.



FortiGate displays its host name and status without the need to navigate away from your current work.

5. In the **Role** field, select **WAN**.



Stop and think!

Why do some of the settings appear or disappear when the role of an interface changes?

Each role reflects the appropriate settings required to configure the interface.The **Undefined** role displays all of the settings you can configure on an interface.

The purpose of choosing **WAN** as the role of the interface is to see that when this interface is connected to an external connection, you may need to disable some settings to configure the DHCP server setting.

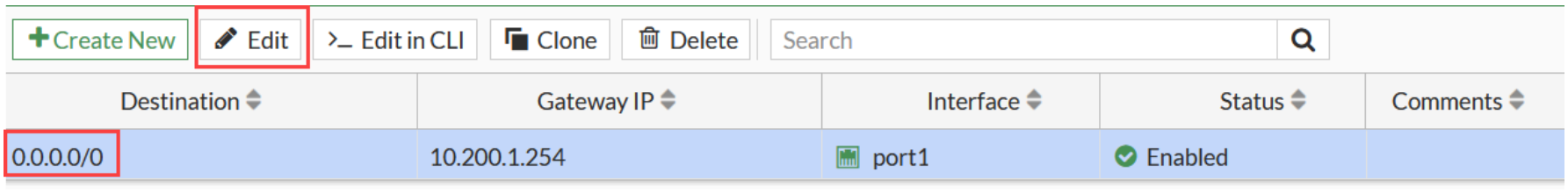
6. In the **Estimated bandwidth** fields, review the WAN utilization values.

When the role of the interface is set to **WAN**, you can set the downstream and upstream maximum bandwidth.

7. Click **Cancel** to clear any changes made.

To review the static default gateway on Local-FortiGate

1. Continuing on the Local-FortiGate GUI, click **Network** > **Static Routes**.
2. Click the static route entry, and then click **Edit**.



3. Expand the **Advanced Options** section.

You can set the priority value of the static route. When two routes have an equal distance, the route with a lower priority number takes precedence

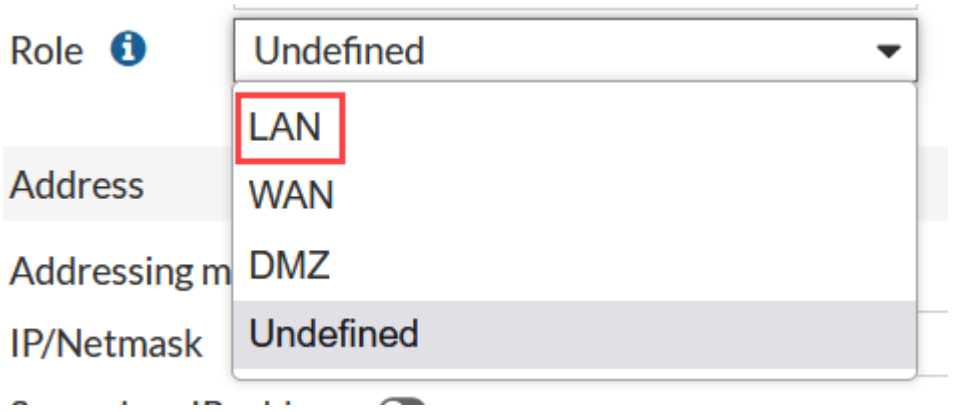
4. Click **Cancel** to clear any changes made.

Enable the DHCP Server on Local-FortiGate

You will enable the DHCP server on port3.

To enable the DHCP server on port3

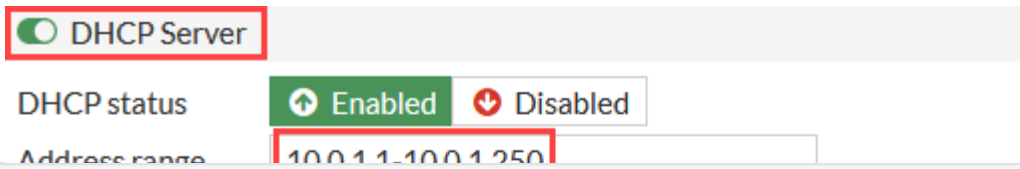
1. Continuing on the Local-FortiGate GUI, click **Network** > **Interfaces**.
2. Click **port3**, and then click **Edit**.
3. In the **Role** field, select **LAN**.



4. Enable **DHCP Server**.

Notice in the **LAN** role, the DHCP server appears on the GUI, unlike when the role is set to **WAN**.

5. In the **Address range** field, type `10.0.1.1-10.0.1.250`.


DHCP Server
DHCP status
Enabled
Disabled
Address range
10.0.1.1-10.0.1.250

Exercise 2: 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 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`

Action	Command
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 3: 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.

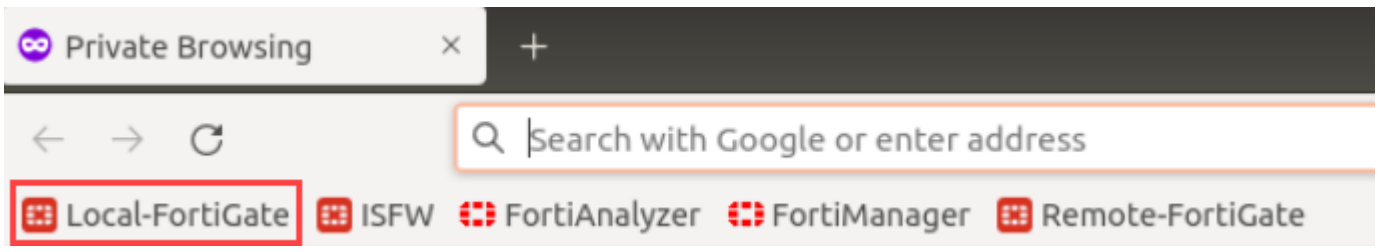
To restore a configuration from a backup

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.

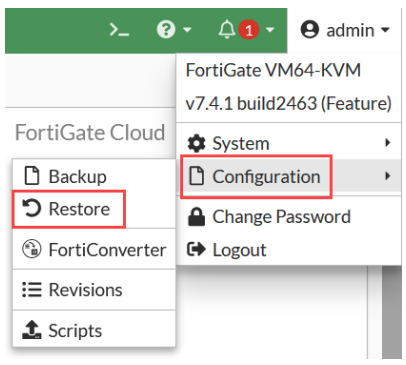
2. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.

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

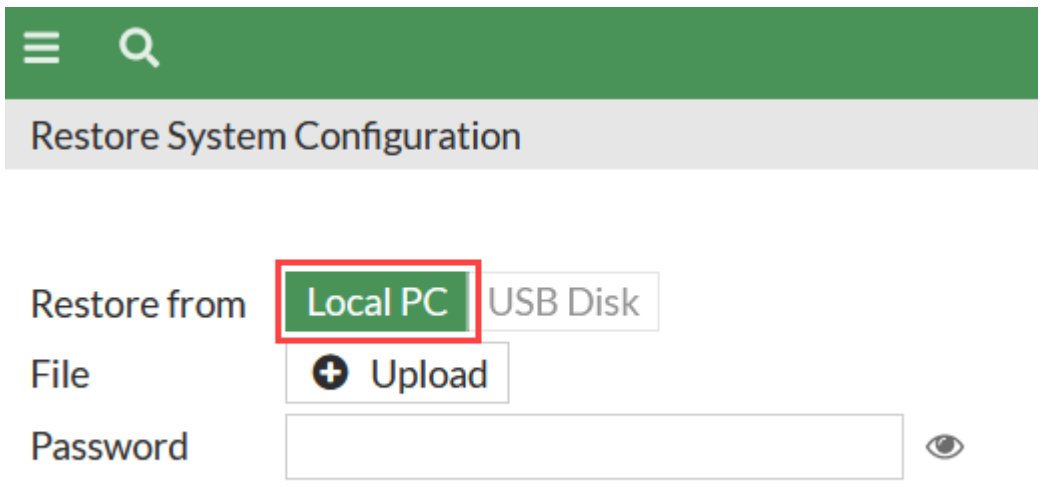


All lab exercises were tested running Firefox on the Local-Client and Remote-Client VMs. To get consistent results, you should use Firefox to access both the internet and the FortiGate GUIs in this virtual environment.

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



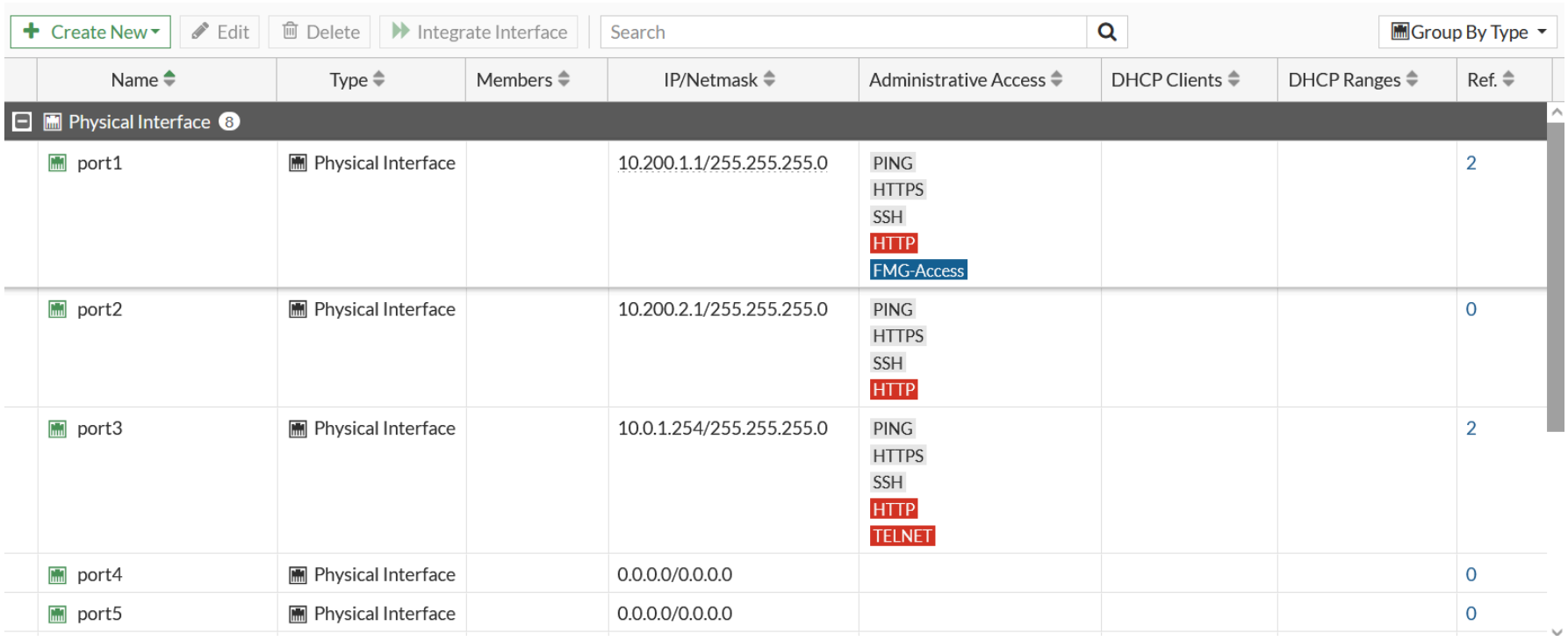
4. Click **Upload** to select the backup configuration file from your local PC.



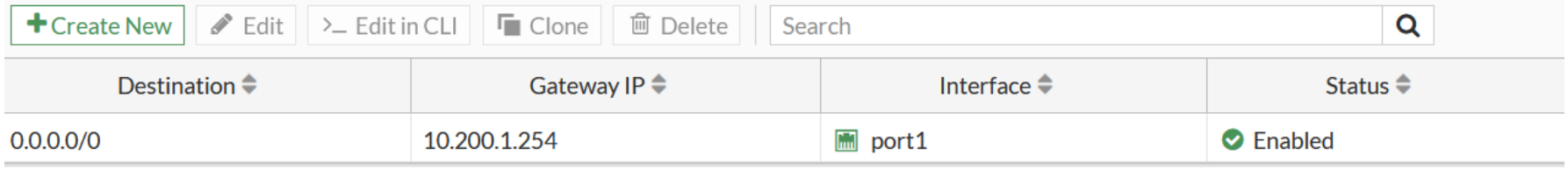
5. Click **Desktop** > **Resources** > **FortiGate-Administrator** > **Introduction** > `local-initial.conf`, and then click **Select**.
6. Click **OK**.
7. Click **OK** to reboot.

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.



10. Click **Network** > **Static Routes**, and then verify that the default route was restored.



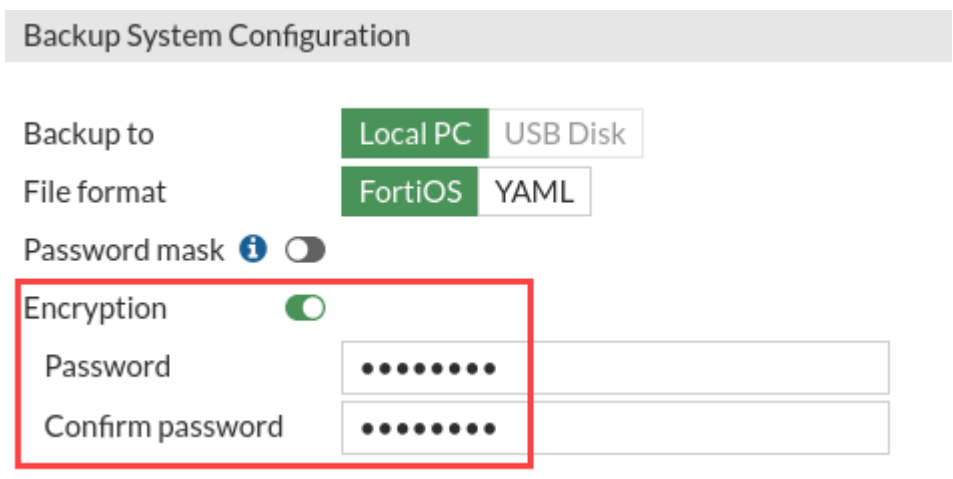
Back Up and Encrypt a Configuration File

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`.



5. Click **OK**.

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 download arrow button 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 1 (#Compare).

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

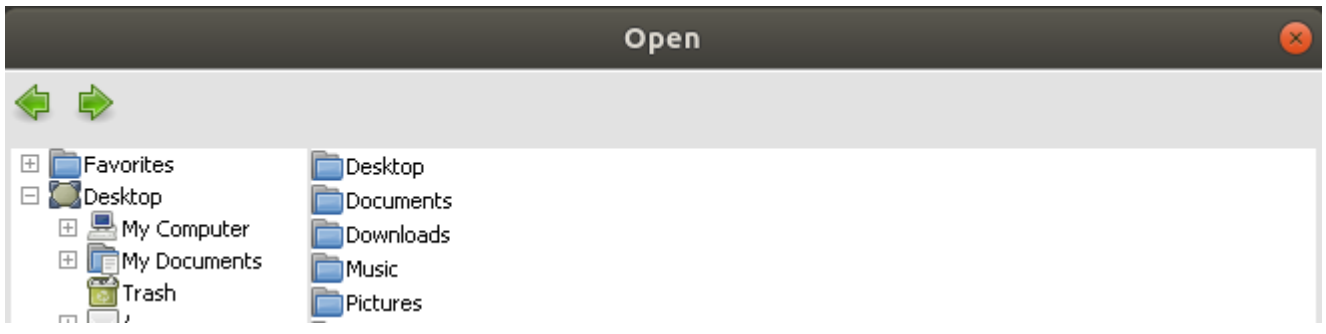
When you troubleshoot issues, or when you restore FortiGate to an earlier OS version or build, it is useful to know where to find the version and build number in a configuration file. This task shows you where to find this information.

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.



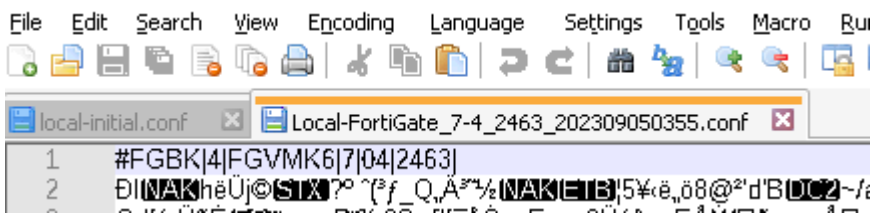
3. Click **File** > **Open**, and then browse to the initial configuration file:

Desktop\Resources\FortiGate-Security\Introduction\local-initial.conf

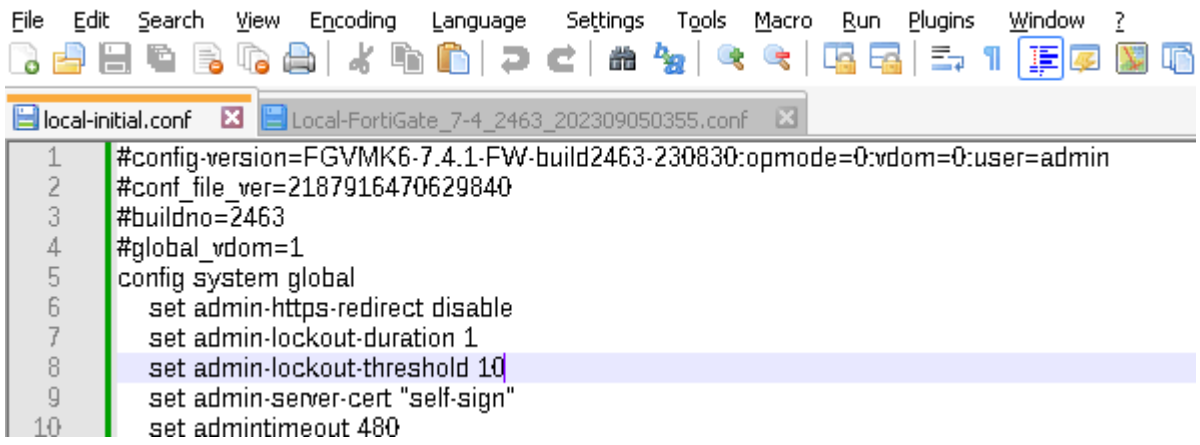
The configuration file opens in a second tab in Notepad++.

4. Compare the headers in the two files.

The following example is an encrypted file:



The following example is a cleartext file:



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.

Exercise 4: 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.

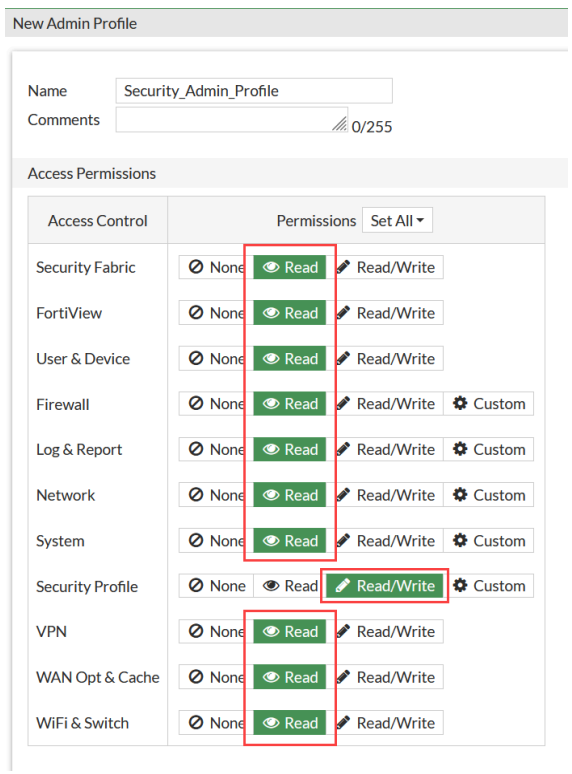
In this exercise, you will work with administrator profiles and administrator user accounts. An administrator profile is a role that is assigned to an administrator user that defines what the user is permitted to do on the FortiGate GUI and CLI.

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**.



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.

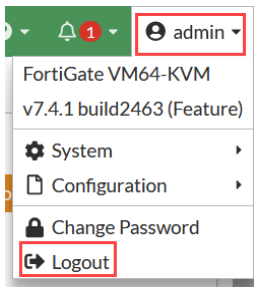
4. Click **OK** to save the changes.

Test the New Administrator Account

You will confirm that the new administrator account has read-write access to only the security profile 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 settings that are available on 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-1 > Configuring Administrator Accounts

Lab 2: Firewall Policies and NAT

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.

You will also examine how to configure and test a firewall policy for destination network address translation (DNAT) using a virtual IP (VIP) address, and source network address translation (SNAT) using an IP pool. You will configure and test SNAT using the central SNAT policy, and DNAT using the DNAT policy and VIPs. You can use network address translation (NAT) to perform SNAT and DNAT for the traffic passing through FortiGate.

Objectives

- Configure firewall objects and firewall policies
- Configure source and destination matching in firewall policies
- Apply service objects to a firewall policy
- Configure firewall policy logging options
- Reorder firewall policies
- Read and understand logs
- Configure DNAT settings using a VIP
- Configure SNAT settings using overload IP pools

Time to Complete

Estimated: 60 minutes
LAB-2 > Firewall Policies and NAT

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
Interface	any
Type	Subnet
IP/Netmask	10.0.1.0/24

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**.

The FortiGate GUI may ask to use the new policy list layout. Click **Cancel** to continue using the classic layout. The new policy list layout is ideal to improve performance when viewing large list of firewall policies.

2. Expand the **port3** → **port1** firewall policy section.
3. 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

Field	Value
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.
Log Allowed Traffic	Select **All Sessions**.
Generate Logs when Session Starts	<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

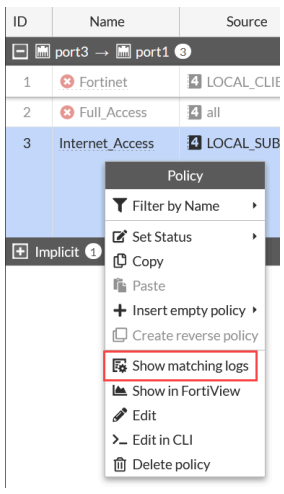
Now that you have configured the firewall policy, you will test it by passing traffic through it and viewing the generated logs.

To test and view logs for a firewall policy

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

- www.google.com (http://www.google.com/)
- www.cnn.com (http://docs.fortinet.com/)
- www.bbc.com (http://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.

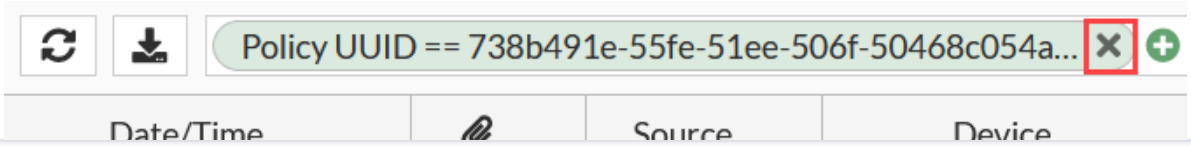
With the current settings, you should have a few log messages that have **Accept (Start)** in the **Result** column. These are the session start logs.

When sessions close, a separate log entry lists 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 == 738b491e-55fe-51ee-506f-50468c054a...
Date/Time
Source
Device

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 1 (#Add).

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
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>

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**.

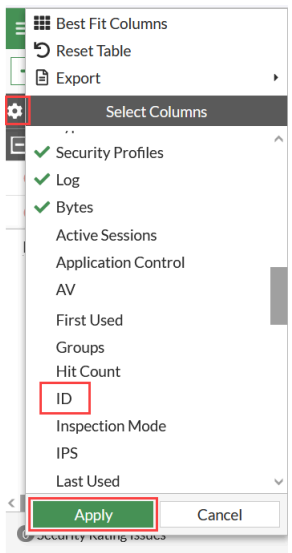
On the **Firewall Policy** page, if the **ID** column is visible, skip to step 8.

---

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	IP Pool	NAT	Type	Security Profiles	Log	Bytes
port3 → port1 4												
1	Fortinet	LOCAL_CLIENT	FORTINET	always	Web Access	ACCEPT		NAT	Standard	SSL no-inspection	UTM	0 B
2	Full_Access	all	all	always	ALL	ACCEPT		NAT	Standard	SSL no-inspection	All	0 B
3	Internet_Access	LOCAL_SUBNET	all	always	ALL_ICMP DNS HTTP HTTPS SSH	ACCEPT		NAT	Standard	SSL no-inspection	All	10.49 MB
4	Block_Ping	LOCAL_SUBNET	LINUX_ETH1	always	PING	DENY			Standard	SSL no-inspection	All	0 B
Implicit 1												

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	IP Pool	NAT	Type	Security Profiles	Log	Bytes
port3 → port1 4												
1	Fortinet	LOCAL_CLIENT	FORTINET	always	Web Access	ACCEPT		NAT	Standard	SSL no-inspection	UTM	0 B
2	Full_Access	all	all	always	ALL	ACCEPT		NAT	Standard	SSL no-inspection	All	0 B
4	Block_Ping	LOCAL_SUBNET	LINUX_ETH1	always	PING	DENY			Standard	SSL no-inspection	All	0 B
3	Internet_Access	LOCAL_SUBNET	all	always	ALL_ICMP DNS HTTP HTTPS SSH	ACCEPT		NAT	Standard	SSL no-inspection	All	10.49 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**.

Search | Disk | 5 minutes | Details

Date/Time		Source	Device	Destination	Application Name	Result	Policy ID
2023/09/18 02:11:18		10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:17		10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:16		10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:15		10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:14		10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:13		10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:13		10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:11		10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)
2023/09/18 02:11:10		10.0.1.10	02:09:0f:00:01:01	10.200.1.254	PING	Deny	4 (Block_Ping)

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

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

Exercise 3: 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

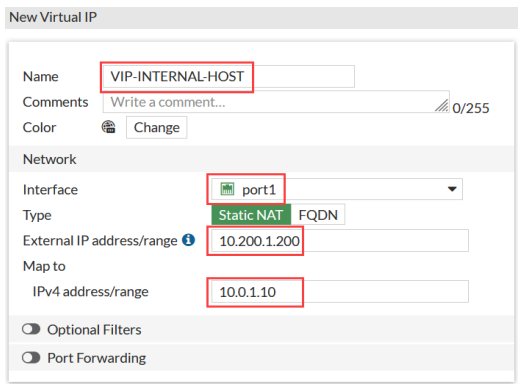
For DNAT on FortiGate, you use a VIP as the destination address field of a firewall policy.

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 1 (../Network_Topology.htm#top).

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**, and then click **Create New**.
3. 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.
Map to IPv4 address/range	10.0.1.10



4. Click **OK**.

()Create a Firewall Policy

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

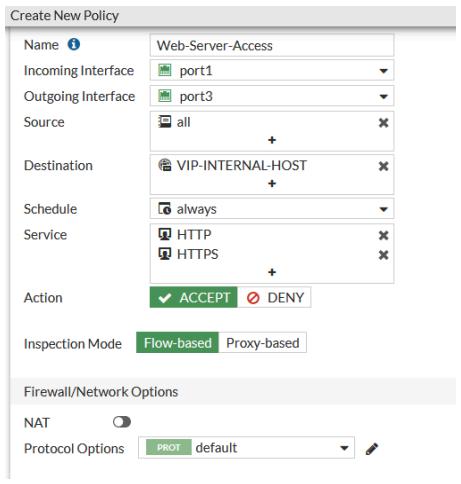
To create a firewall policy

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

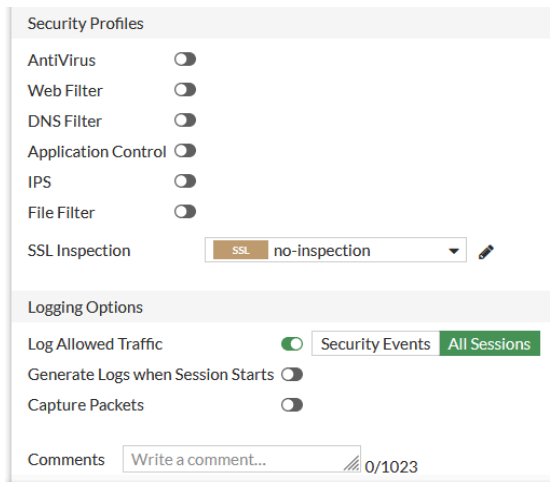
Field	Value
Name	Web-Server-Access
Incoming Interface	port1
Outgoing Interface	port3

Field	Value
Source	all
Destination	VIP-INTERNAL-HOST **Tip**: This is listed under the **VIRTUAL IP/SERVER** section.
Service	HTTP, HTTPS **Tip**: In the section on the right, in the search box, type the service name, and then click the services to add.

4. In the **Firewall/Network Options** section, disable **NAT**.



5. In the **Logging Options** section, select **All Sessions**.



6. Click **OK**.

()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 1 (../Network_Topology.htm#top).

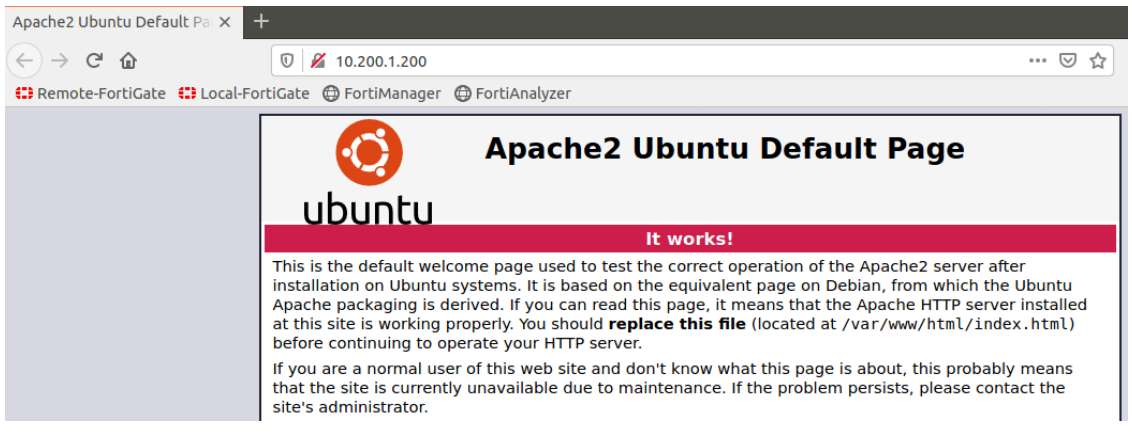
You will also test how the source address is translated by the VIP when traffic leaves the Local-Client VM.

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 (http://10.200.1.200)

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 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 internal-to-external 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 then connect to a few websites, such as:

- www.fortinet.com (http://www.fortinet.com)
- www.yahoo.com (http://www.yahoo.com)
- www.bbc.com (http://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 in 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.

Exercise 4: 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.

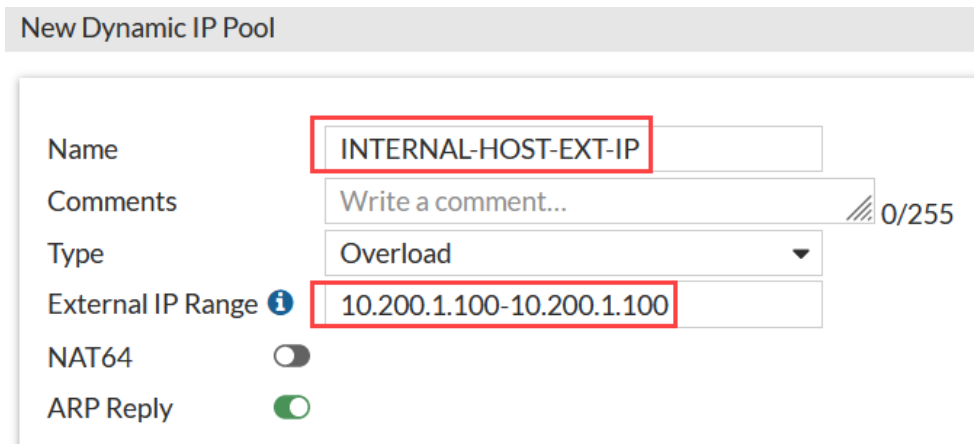
()Create an IP Pool

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
External IP Range	10.200.1.100-10.200.1.100



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.

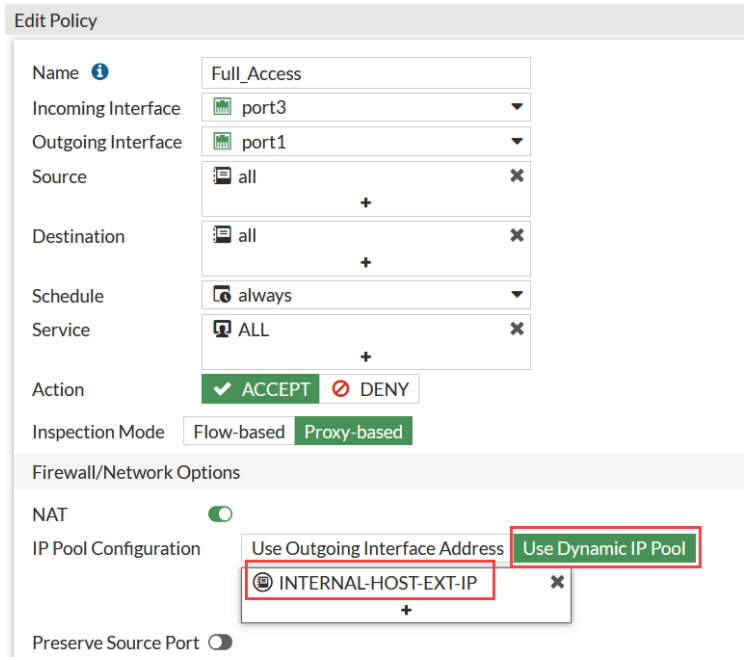
To edit the firewall policy

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

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

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

Your configuration will look similar to the following example:



7. 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 then connect to a few websites, such as:

- www.fortinet.com (http://www.fortinet.com)
- www.yahoo.com (http://www.yahoo.com)
- www.bbc.com (http://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 1: Configuring Route Failover

In the lab network, Local-FortiGate has two interfaces connected to the internet: port1 and port2. In this exercise, you will configure the port1 connection as the primary internet link and the port2 connection as the backup internet link. Local-FortiGate should use the port2 connection only if the port1 connection is down. To achieve this objective, you will configure two default routes with different administrative distances, and then you will disable the primary default route interface to activate the standby route.

Verify the Routing Configuration

You will verify the existing routing configuration on Local-FortiGate.

Take the Expert Challenge!

On the Local-FortiGate GUI (`admin/password`), complete the following:

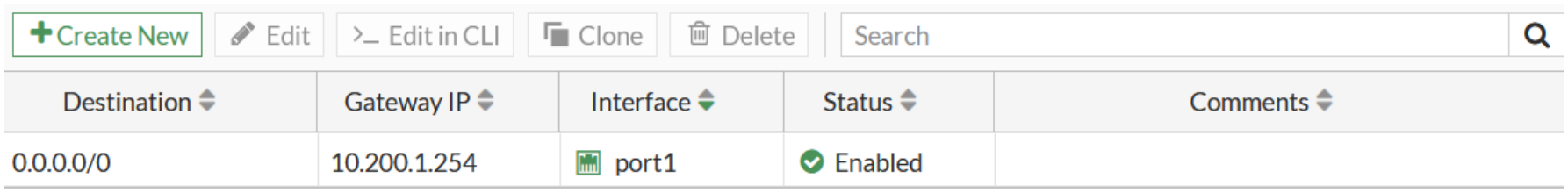
- View the existing static route configuration on Local-FortiGate.
- Enable the **Distance** and **Priority** columns on the static route configuration page.
- Make a note of the **Distance** and **Priority** values of the existing default route.

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

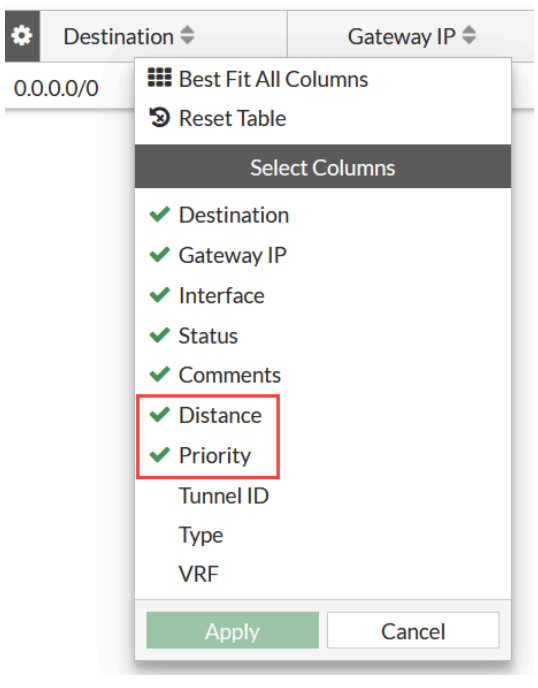
After you complete the challenge, see Configure a Second Default Route on page 1 (#To_configure_second_route).

()To verify the routing configuration

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Network** > **Static Routes**.
3. Verify the existing default route for **port1**.



4. Right-click any of the column headers to open the context-sensitive menu.
5. In the **Select Columns** section, select **Distance** and **Priority**, and then click **Apply**.



The **Distance** and **Priority** columns appear on the GUI.

Note that, by default, static routes have a **Distance** value of 10 and a **Priority** value of 1.

()Configure a Second Default Route

You will create a second default route using the port2 interface. To make sure this second default route remains the standby route, you will assign it a higher administrative distance than the first default route.

Take the Expert Challenge!

- On the Local-FortiGate GUI, configure a second default route using **port2**.
- Assign it a **Distance** of `20` and a **Priority** of `5`.

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

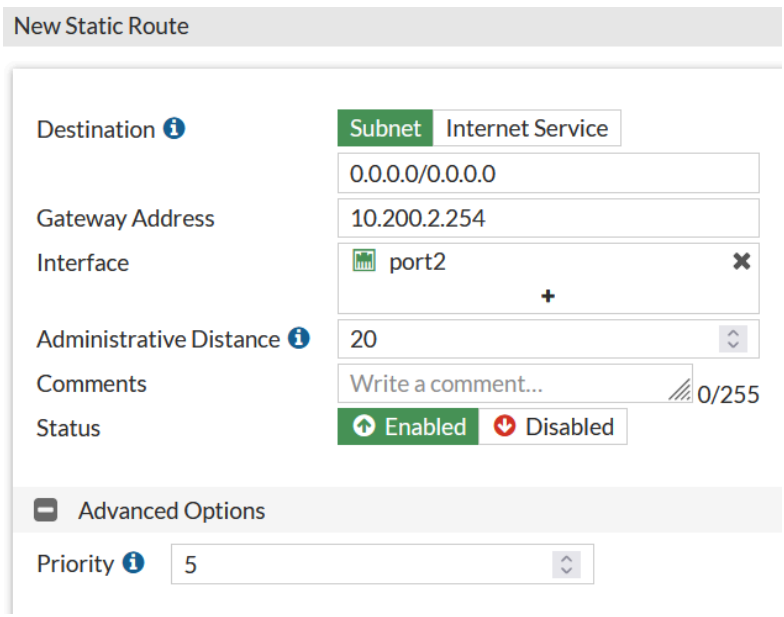
After you complete the challenge, see Configure the Firewall Policies on page 1 (#To_configure_policy).

To configure a second default route

1. Continuing on the Local-FortiGate GUI, click **Network** > **Static Routes**.
2. Click **Create New**.
3. Configure the following settings:

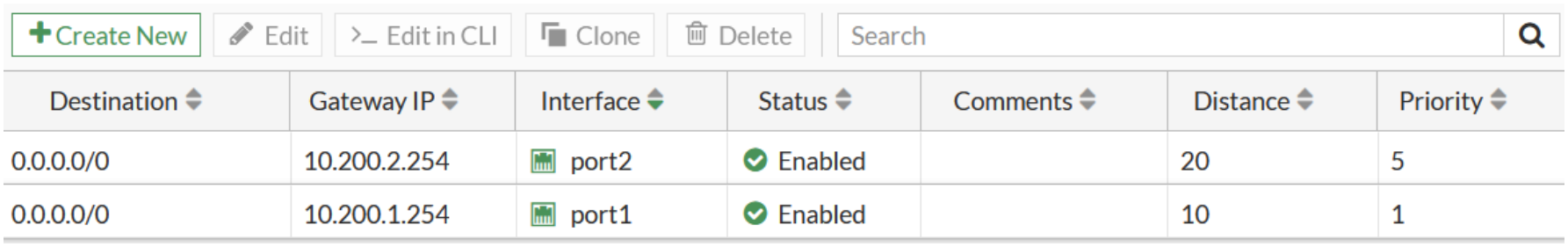
Field	Value
Gateway Address	10.200.2.254
Interface	port2
Administrative Distance	20

4. Click **+** to expand the **Advanced Options** section.
5. In the **Priority** field, type `5`.



6. Click **OK**.

FortiGate adds a second default route.



Destination	Gateway IP	Interface	Status	Comments	Distance	Priority
0.0.0.0/0	10.200.2.254	port2	Enabled		20	5
0.0.0.0/0	10.200.1.254	port1	Enabled		10	1

()Configure the Firewall Policies

You will modify the existing **Full_Access** firewall policy to log all sessions. You will also create a second firewall policy to allow traffic through the secondary interface.

Take the Expert Challenge!

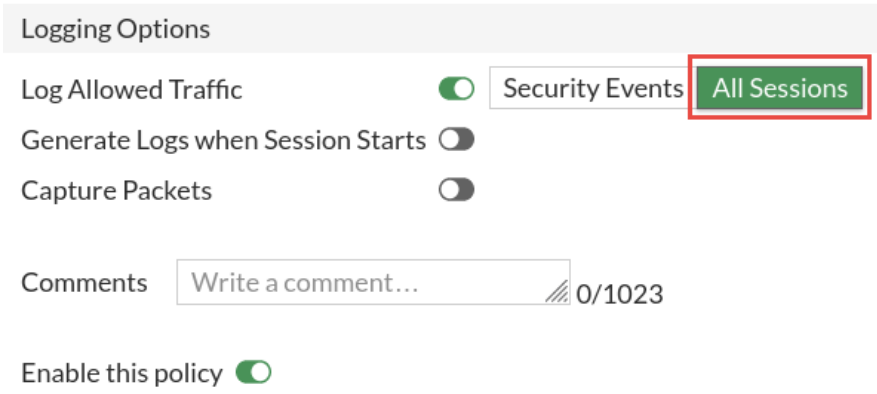
- Continuing on the Local-FortiGate GUI, enable logging for all sessions in the existing **Full_Access** firewall policy.
- Create a second firewall policy named `Backup_Access`.
- Configure the **Backup_Access** policy to allow traffic from **port3** to **port2** with NAT enabled.
- Enable logging on the **Backup_Access** policy for all sessions.

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

After you complete the challenge, see View the Routing Table on page 1 (#To_view_routing_table)

To configure the firewall policies

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Double-click the existing **Full_Access** policy to edit it.
3. Enable **Log Allowed Traffic**, and then select **All Sessions**.



All Sessions logging ensures that FortiGate logs all traffic, not only sessions that security profiles inspected. This will assist you in verifying traffic routing using the **Forward Traffic** logs.

4. Click **OK**.
5. Click **Create New**.
6. Configure a second firewall policy with the following settings:

Field	Value
Name	Backup_Access
Incoming Interface	port3
Outgoing Interface	port2
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Log Allowed Traffic	All Sessions

7. Click **OK**.

()View the Routing Table

The Local-FortiGate configuration now has two default routes with different distances. You will view the routing table to see which route was installed in the routing table and which route was installed in the routing table database.

To view the routing table

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

```
get router info routing-table all
```

Note that the second default route is not listed.

3. Enter the following command to list the routing table database entries:

```
get router info routing-table database
```

4. Confirm that the second default route is listed as inactive.

```
Local-FortiGate # get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S       0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S    *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
C    *> 10.0.1.0/24 is directly connected, port3
C    *> 10.200.1.0/24 is directly connected, port1
C    *> 10.200.2.0/24 is directly connected, port2
C    *> 172.16.100.0/24 is directly connected, port8
```

Only active routes show the > symbol, which means they are the selected and active routes. The routing table database contains all active, standby, and inactive routes on FortiGate.

Stop and think!

Why is the port2 default route the standby route?

The port2 default route has a higher administrative distance than the port1 default route. When two or more routes to the same destination have different distances, the higher distance route is not installed in the routing table, but you can still see it in the routing table database. Routes marked as inactive are marked inactive when the corresponding interface is down.

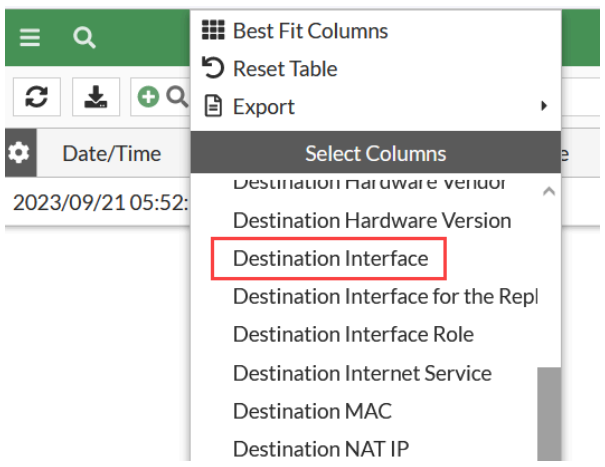
5. Close the Local-FortiGate CLI session.

Test the Route Failover

First, you will access various websites and use the **Forward Traffic** logs to verify that the port1 route is being used. Next, you will force a failover by reconfiguring the port1 interface setting and bringing the interface down. You will then generate some more traffic, and use the **Forward Traffic** logs to verify that the port2 route is being used.

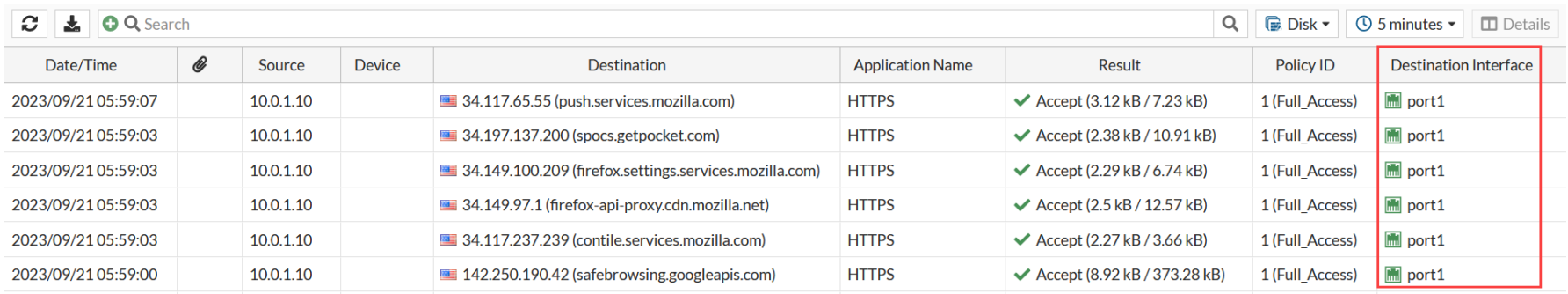
To confirm the port1 route is the primary route

1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.
2. Right-click any of the column headers to open the context-sensitive menu.
3. In the **Select Columns** section, select **Destination Interface**.



4. Scroll down in the context-sensitive menu, and then click **Apply**.

The **Destination Interface** column is displayed.



Date/Time	Source	Device	Destination	Application Name	Result	Policy ID	Destination Interface
2023/09/21 05:59:07	10.0.1.10		34.117.65.55 (push.services.mozilla.com)	HTTPS	Accept (3.12 kB / 7.23 kB)	1 (Full_Access)	port1
2023/09/21 05:59:03	10.0.1.10		34.197.137.200 (spocs.getpocket.com)	HTTPS	Accept (2.38 kB / 10.91 kB)	1 (Full_Access)	port1
2023/09/21 05:59:03	10.0.1.10		34.149.100.209 (firefox.settings.services.mozilla.com)	HTTPS	Accept (2.29 kB / 6.74 kB)	1 (Full_Access)	port1
2023/09/21 05:59:03	10.0.1.10		34.149.97.1 (firefox-api-proxy.cdn.mozilla.net)	HTTPS	Accept (2.5 kB / 12.57 kB)	1 (Full_Access)	port1
2023/09/21 05:59:03	10.0.1.10		34.117.237.239 (contile.services.mozilla.com)	HTTPS	Accept (2.27 kB / 3.66 kB)	1 (Full_Access)	port1
2023/09/21 05:59:00	10.0.1.10		142.250.190.42 (safebrowsing.googleapis.com)	HTTPS	Accept (8.92 kB / 373.28 kB)	1 (Full_Access)	port1

5. On the Local-Client VM, in the browser, open a few new tabs, and then visit a few websites, such as:

- http://neverssl.com (http://www.pearsonvue.com/fortinet)
- http://eu.httpbin.org (http://www.eicar.org/)

6. On the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.
7. Click the refresh icon.
8. Locate the relevant log entries for the websites you accessed, and then verify that the **Destination Interface** indicates **port1**.

Date/Time		Source	Device	Destination	Application Name	Result	Policy ID	Destination Interface
2023/09/21 06:02:52		10.0.1.10		3.208.239.255 (eu.httpbin.org)	HTTP	Accept (3.85 kB / 481.05 kB)	1 (Full_Access)	port1
2023/09/21 06:02:51		10.0.1.10		3.208.239.255 (eu.httpbin.org)	HTTP	Accept (12.51 kB / 1.49 MB)	1 (Full_Access)	port1
2023/09/21 06:02:51		10.0.1.10		3.208.239.255 (eu.httpbin.org)	HTTP	Accept (1.04 kB / 89.65 kB)	1 (Full_Access)	port1
2023/09/21 06:02:44		10.0.1.200		96.45.45.45	tcp/853	Accept (8.92 kB / 11.66 kB)	1 (Full_Access)	port1
2023/09/21 06:02:04		10.0.1.10		8.8.8.8 (dns.google)	DNS	Accept (84 B / 168 B)	1 (Full_Access)	port1
2023/09/21 06:02:04		10.0.1.10		8.8.8.8 (dns.google)	DNS	Accept (84 B / 202 B)	1 (Full_Access)	port1
2023/09/21 06:01:52		10.0.1.10		172.217.13.195 (fonts.gstatic.com)	HTTPS	Accept (1.48 kB / 5.44 kB)	1 (Full_Access)	port1
2023/09/21 06:01:51		10.0.1.10		172.217.13.195 (fonts.gstatic.com)	HTTPS	Accept (1.42 kB / 5.44 kB)	1 (Full_Access)	port1
2023/09/21 06:01:36		10.0.1.10		34.223.124.45 (brightgrandinnerspell.neverssl.com)	HTTP	Accept (1.63 kB / 2.9 kB)	1 (Full_Access)	port1
2023/09/21 06:01:35		10.0.1.10		34.223.124.45 (brightgrandinnerspell.neverssl.com)	HTTP	Accept (612 B / 2.59 kB)	1 (Full_Access)	port1

This verifies that the port1 route is currently the route in use.

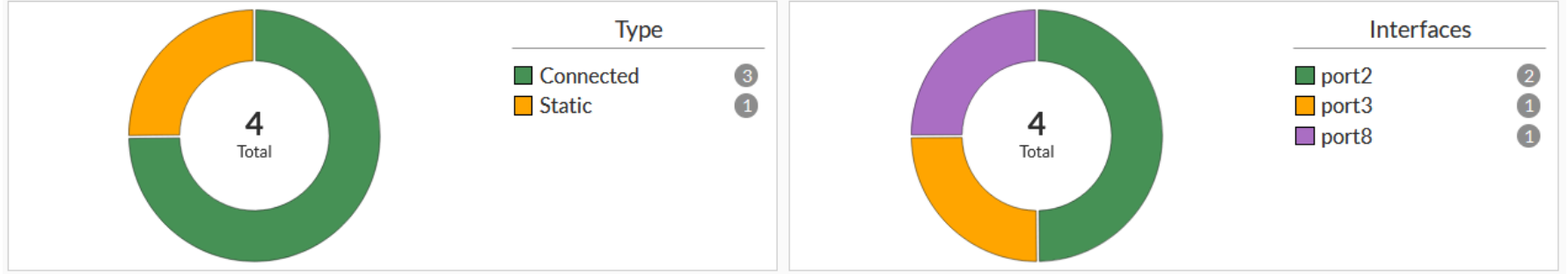
To force the failover

1. Continuing on the Local-FortiGate GUI, click **Network** > **Interfaces**.
2. Double-click the **port1** interface to edit it.
3. In the **Miscellaneous** section, click **Disabled** as the status.
4. Click **OK**.

The port1 internet connection is now down, and FortiGate removes the corresponding route from the routing table.

To verify the route change

1. Continuing on the Local-FortiGate GUI, click **Dashboard** > **Network**, and then click **Static & Dynamic Routing** to expand it to full screen.
2. In the routing table, verify that the **port2** route replaced the **port1** route.



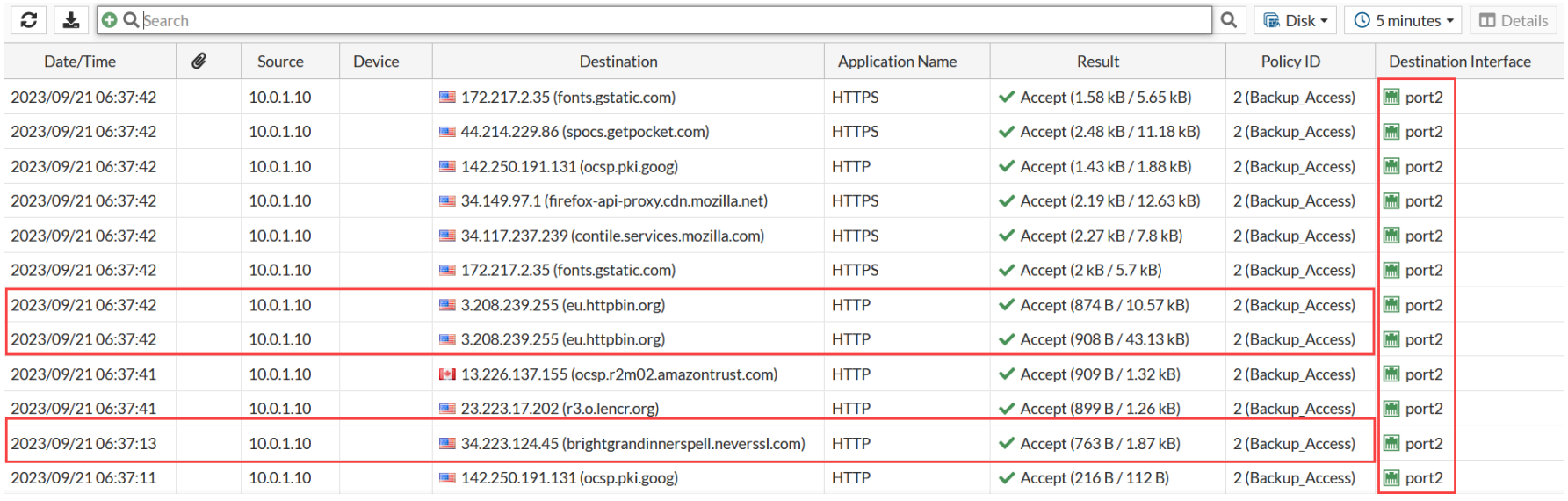
Network	Gateway IP	Interfaces	Distance	Type	Metric
0.0.0.0/0	10.200.2.254	port2	20	Static	0
10.0.1.0/24	0.0.0.0	port3	0	Connected	0
10.200.2.0/24	0.0.0.0	port2	0	Connected	0
172.16.100.0/24	0.0.0.0	port8	0	Connected	0

To verify traffic logs

1. On the Local-Client VM, in the browser, open a few new tabs, and then visit a few websites, such as:

- http://neverssl.com (http://www.pearsonvue.com/fortinet)
- http://eu.httpbin.org (http://www.eicar.org/)

2. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and then click **Log & Report** > **Forward Traffic**.
3. Locate the relevant log entries for the websites you accessed, and then verify that the **Destination Interface** indicates **port2**.



Date/Time		Source	Device	Destination	Application Name	Result	Policy ID	Destination Interface
2023/09/21 06:37:42		10.0.1.10		172.217.2.35 (fonts.gstatic.com)	HTTPS	Accept (1.58 kB / 5.65 kB)	2 (Backup_Access)	port2
2023/09/21 06:37:42		10.0.1.10		44.214.229.86 (spocs.getpocket.com)	HTTPS	Accept (2.48 kB / 11.18 kB)	2 (Backup_Access)	port2
2023/09/21 06:37:42		10.0.1.10		142.250.191.131 (ocsp.pki.goog)	HTTP	Accept (1.43 kB / 1.88 kB)	2 (Backup_Access)	port2
2023/09/21 06:37:42		10.0.1.10		34.149.97.1 (firefox-api-proxy.cdn.mozilla.net)	HTTPS	Accept (2.19 kB / 12.63 kB)	2 (Backup_Access)	port2
2023/09/21 06:37:42		10.0.1.10		34.117.237.239 (contile.services.mozilla.com)	HTTPS	Accept (2.27 kB / 7.8 kB)	2 (Backup_Access)	port2
2023/09/21 06:37:42		10.0.1.10		172.217.2.35 (fonts.gstatic.com)	HTTPS	Accept (2 kB / 5.7 kB)	2 (Backup_Access)	port2
2023/09/21 06:37:42		10.0.1.10		3.208.239.255 (eu.httpbin.org)	HTTP	Accept (874 B / 10.57 kB)	2 (Backup_Access)	port2
2023/09/21 06:37:42		10.0.1.10		3.208.239.255 (eu.httpbin.org)	HTTP	Accept (908 B / 43.13 kB)	2 (Backup_Access)	port2
2023/09/21 06:37:41		10.0.1.10		13.226.137.155 (ocsp.r2m02.amazontrust.com)	HTTP	Accept (909 B / 1.32 kB)	2 (Backup_Access)	port2
2023/09/21 06:37:41		10.0.1.10		23.223.17.202 (r3.o.lencr.org)	HTTP	Accept (899 B / 1.26 kB)	2 (Backup_Access)	port2
2023/09/21 06:37:13		10.0.1.10		34.223.124.45 (brightgrandinnerspell.neverssl.com)	HTTP	Accept (763 B / 1.87 kB)	2 (Backup_Access)	port2
2023/09/21 06:37:11		10.0.1.10		142.250.191.131 (ocsp.pki.goog)	HTTP	Accept (216 B / 112 B)	2 (Backup_Access)	port2

This verifies that the Local-FortiGate is using the port2 default route.

Restore the Routing Table

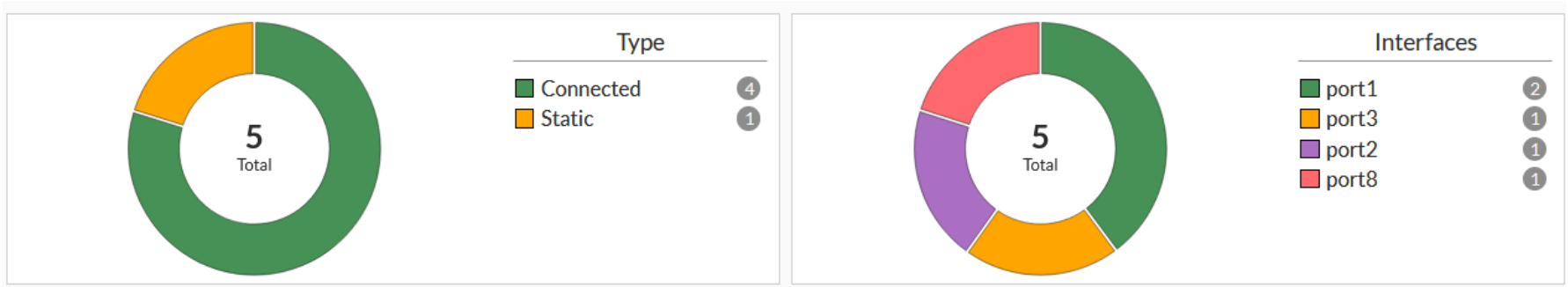
Before you begin the next exercise, you will restore the port1 interface settings and bring it up, which will restore the port1 default route as the best route in the routing table.

To restore the port1 health monitor configuration

1. Continuing on the Local-FortiGate GUI, click **Network** > **Interfaces**.
2. Double-click the **port1** interface to edit it.
3. In the **Miscellaneous** section, click **Enabled** as the status.
4. Click **OK**.

To verify the routing table

1. Continuing on the Local-FortiGate GUI, click **Dashboard** > **Network**, and then click **Static & Dynamic Routing** to expand it to full screen.
2. In the routing table, verify that the **port1** route replaced the **port2** route.



Route Lookup | Create Address | Edit | Search

Network	Gateway IP	Interfaces	Distance	Type	Metric
0.0.0.0/0	10.200.1.254	port1	10	Static	0
10.0.1.0/24	0.0.0.0	port3	0	Connected	0
10.200.1.0/24	0.0.0.0	port1	0	Connected	0

Exercise 2: Configuring Equal-Cost Multi-Path Routing

In this exercise, you will configure equal-cost multi-path (ECMP) routing on Local-FortiGate to load balance the internet traffic between port1 and port2.

Configure Administrative Distance

To establish ECMP, first, you will configure multiple static routes with the same administrative distance.

Take the Expert Challenge!

On the Local-FortiGate GUI (`admin/password`), complete the following:

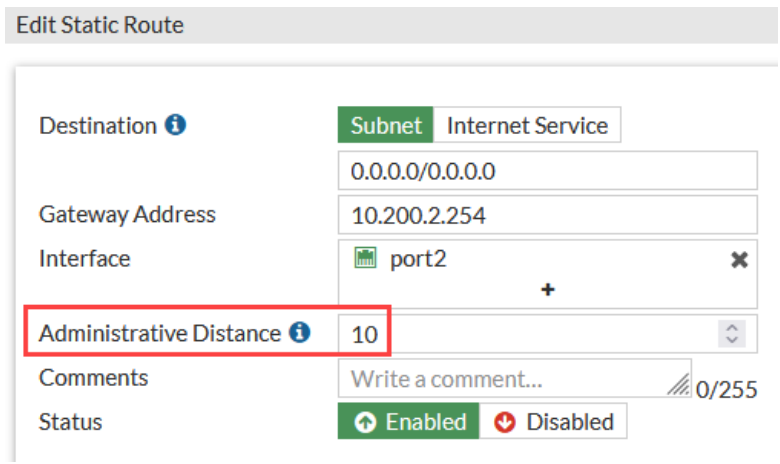
- Change the **port2** static route **Administrative Distance** to `10` .
- Verify that both **port1** and **port2** default routes are present in the routing table.

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

After you complete the challenge, see Change the ECMP Load Balancing Algorithm on page 1 (#To_modify_ECMP_method).

()To configure administrative distance

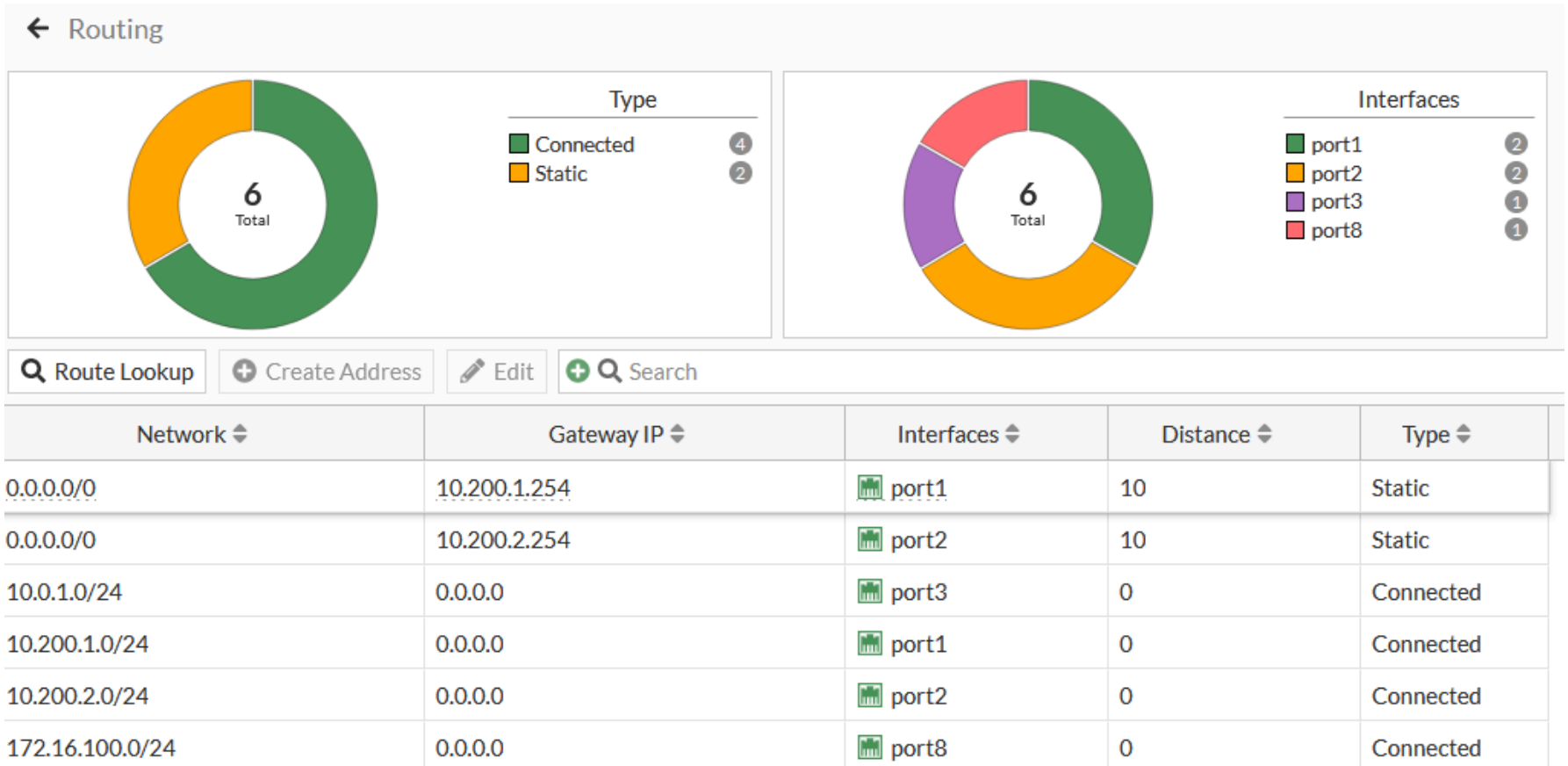
1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password` .
2. Click **Network** > **Static Routes**.
3. Double-click the **port2** static route to edit it.
4. In the **Administrative Distance** field, change the value to `10` .



5. Click **OK**.

()To verify the routing table

1. Continuing on the Local-FortiGate GUI, click **Dashboard** > **Network**, and then click **Static & Dynamic Routing** to expand it to full screen.
2. Verify that both default routes are installed in the routing table.



()Change the ECMP Load Balancing Algorithm

By default, the ECMP load balancing algorithm is based on the source IP address. This works well when there are multiple clients generating traffic. In the lab network, because you have only one client (the Local-Client VM), the source IP address method does not balance any traffic to the second route. FortiGate always uses only one route. For this reason, you will change the load balancing method to use both source and destination IP addresses. Using this method, as long as the traffic goes to multiple destination IP addresses, FortiGate load balances the traffic across both routes.

To modify the ECMP load balancing method

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following commands to change the ECMP load balancing method:

config system settings

set v4-ecmp-mode source-dest-ip-based

end

3. Leave the Local-FortiGate CLI session open.

Verify Traffic Routing

You will generate some HTTP traffic and verify traffic routing using the **Forward Traffic** logs.

Take the Expert Challenge!

- On the Local-Client VM, open a few new browser tabs, and then generate some HTTP traffic.
- Verify the traffic routing on Local-FortiGate, using the **Forward Traffic** logs.
- Identify why all the outgoing packets are still being routed through **port1**.

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

After you complete the challenge, see Configure Priority on page 1 (#To_configure_priority).

()To verify traffic routing

1. On the Local-Client VM, in the browser, open a few new tabs, and then visit a few websites, such as:

- http://neverssl.com (http://www.pearsonvue.com/fortinet)
- http://example.com (http://cve.mitre.org/)
- http://eu.httpbin.org (http://www.eicar.org/)

2. On the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.
3. In the relevant log entries for the websites you accessed, identify the **Destination Interface**.

Search

Date/Time		Source	Device	Destination	Application Name	Result	Policy ID	Destination Interface
2023/09/26 04:36:04		10.0.1.10		54.85.134.100 (eu.httpbin.org)	HTTP	Accept (1.12 kB / 43.29 kB)	1 (Full_Access)	port1
2023/09/26 04:36:03		10.0.1.200		173.243.143.6	HTTPS	Accept (5.49 kB / 8.56 kB)	1 (Full_Access)	port1
2023/09/26 04:36:03		10.0.1.10		54.85.134.100 (eu.httpbin.org)	HTTP	Accept (1.45 kB / 1.24 kB)	1 (Full_Access)	port1
2023/09/26 04:36:03		10.0.1.10		54.85.134.100 (eu.httpbin.org)	HTTP	Accept (1.81 kB / 170.8 kB)	1 (Full_Access)	port1
2023/09/26 04:35:58		10.0.1.200		96.45.46.46	tcp/853	Accept (10.56 kB / 18.24 kB)	1 (Full_Access)	port1
2023/09/26 04:35:36		10.0.1.10		34.117.65.55 (push.services.mozilla.com)	HTTPS	Accept (2.26 kB / 6.37 kB)	1 (Full_Access)	port1
2023/09/26 04:35:27		10.0.1.10		192.229.211.108 (ocsp.digicert.com)	HTTP	Accept (1.37 kB / 1.58 kB)	1 (Full_Access)	port1
2023/09/26 04:35:07		10.0.1.10		172.217.2.35 (fonts.gstatic.com)	HTTPS	Accept (100 B / 60 B)	1 (Full_Access)	port1
2023/09/26 04:35:07		10.0.1.10		172.217.2.35 (fonts.gstatic.com)	HTTPS	Accept (100 B / 60 B)	1 (Full_Access)	port1
2023/09/26 04:35:03		10.0.1.10		54.85.134.100 (eu.httpbin.org)	HTTP	Accept (1.08 kB / 541 B)	1 (Full_Access)	port1

Why are all the outgoing packets still being routed through port1?

Stop and think!

The **port2** route is not being used to route internet traffic. Why?

At the beginning of this exercise, you set a distance of 10 on the port2 route but you didn't change its priority. The port2 route priority is still 5, as you configured it in the previous exercise (see Configure a Second Default Route on page 1 (1_Route_Failover.htm#To_configure_second_route)). In addition, the port1 route has distance and priority values of 10 and 1, respectively.

When two routes to the same destination have the same distance, both remain in the routing table. However, if the priorities are different, FortiGate uses the route with the lowest priority value—port1 in this case. To achieve ECMP with static routes, the distance and priority values must be the same for all routes.

()Configure Priority

You will change the priority value for the **port2** route to match the **port1** route.

Take the Expert Challenge!

On the Local-FortiGate GUI, modify the static routing configuration so both default routes are eligible for ECMP.

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

After you complete the challenge, see Verify ECMP on page 1 (#To_verify_cli_routing_table)

To configure priority

1. Continuing on the Local-FortiGate GUI, click **Network** > **Static Routes**.
2. Double-click the **port2** default route to edit it.
3. Click **+** to expand the **Advanced Options** section.
4. Change the **Priority** value to `1`.
5. Click **OK**.

()Verify ECMP

Now that both port1 and port2 routes share the same distance and priority values, they are eligible for ECMP. First, you will verify the routing table, and then you will verify traffic routing using the **Forward Traffic** logs.

To verify the routing table

1. Return to the Local-FortiGate CLI session, and then enter the following command on Local-FortiGate:

get router info routing-table all

2. Verify that both default routes are currently active.

```
Local-FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
                  [10/0] via 10.200.2.254, port2, [1/0]
C       10.0.1.0/24 is directly connected, port3
C       10.200.1.0/24 is directly connected, port1
C       10.200.2.0/24 is directly connected, port2
C       172.16.100.0/24 is directly connected, port8
```

()To configure the CLI sniffer

1. Continuing on the Local-FortiGate CLI session, enter the following command:

diagnose sniffer packet any 'not host 172.16.100.1 and not host 172.16.100.3 and tcp[13]&2==2 and port 80' 4

The filter `'tcp[13]&2==2'` matches packets with the SYN flag on, so the output will show all SYN packets for port 80 (HTTP).

2. Leave the Local-FortiGate CLI window open in the background.

()To verify ECMP routing

1. On the Local-Client VM, in the browser, open a few new tabs, and then visit a few websites, such as:

- http://neverssl.com (http://www.pearsonvue.com/fortinet)
- http://example.com (http://cve.mitre.org/)
- http://eu.httpbin.org (http://www.eicar.org/)

2. Return to the Local-FortiGate CLI session, and then press `Ctrl` + `C` to stop the sniffer.
3. Analyze the sniffer output.

```
interfaces=[any]
filters=[ not host 172.16.100.1 and not host 172.16.100.3 and tcp [13]&2==2 and port 80]
```

Lab 3: Routing

In this lab, you will configure the router settings and test scenarios to learn how FortiGate makes routing decisions.

Objectives

- Route traffic based on the destination IP address, as well as other criteria
- Balance traffic among multiple paths
- Implement route failover
- Diagnose a routing problem

Time to Complete

Estimated: 50 minutes
LAB-3 > Routing

Exercise 1: Configuring an LDAP Server

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

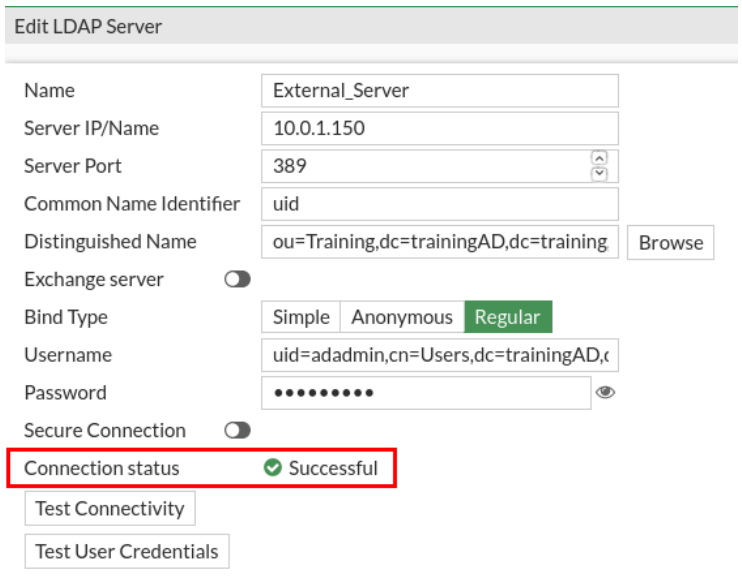
You will configure FortiGate to point to a preconfigured FortiAuthenticator acting as an LDAP server for server-based password authentication.

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 1 (../Network_Topology.htm).
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.
Password	Training! This is the password preconfigured for the adadmin user. You must use it to be able to bind.

4. Click **Test Connectivity**.



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.

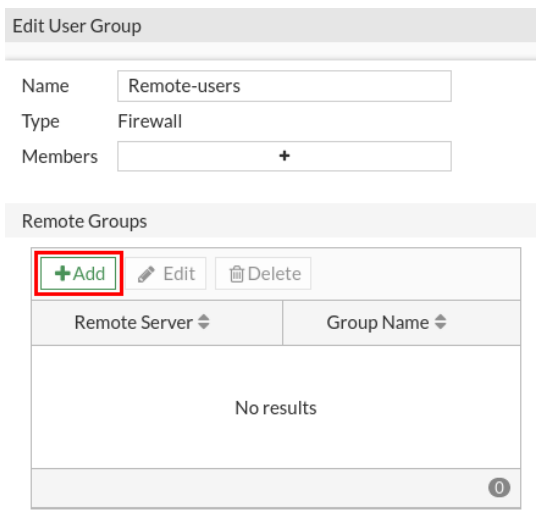
After you have completed this exercise, see Configuring an LDAP Server on page 1 (#Adding).

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.

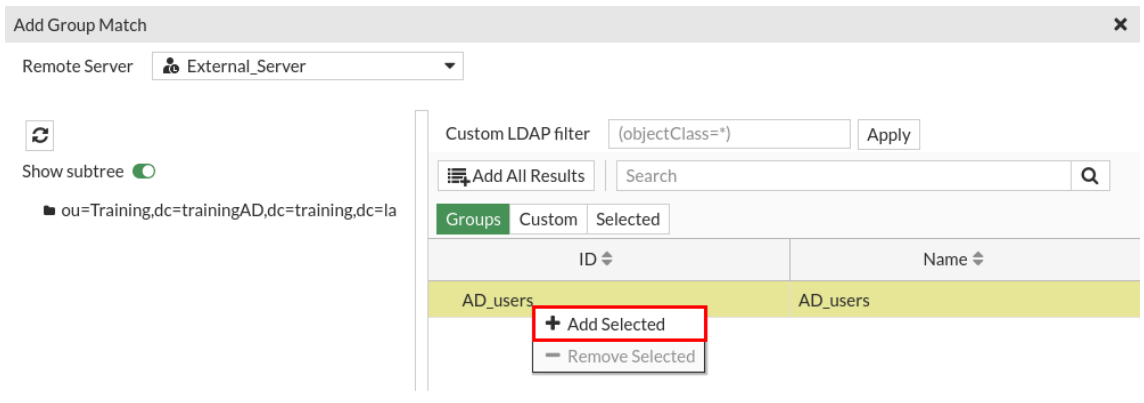
Notice that it's currently configured as a firewall group.

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

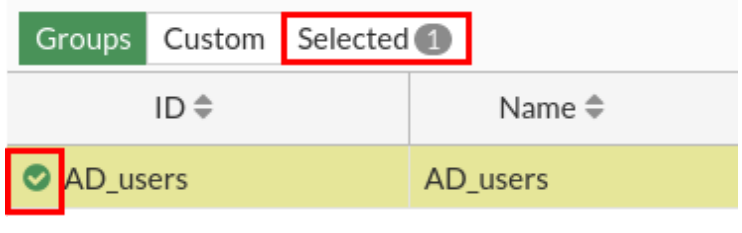


The **Add Group Match** window opens.

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

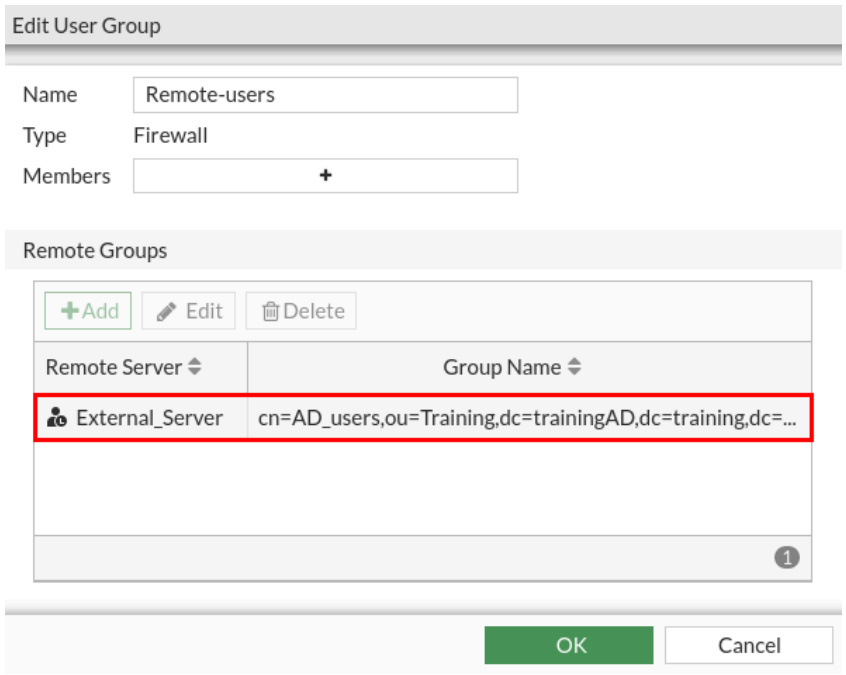


AD_users has a green check mark beside it, which indicates that it was added.



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.



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.

ID	Name	From	To	Source	Destination	Schedule	Service	Action
1	Full_Access	port3	port1	LOCAL_SUBNET	all	always	ALL	ACCEPT

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**.

From	To	Source	Destination	Schedule	Service	Action	I...	NAT	Type	Security Profiles
port3	port1	Remote-users LOCAL_SUBNET	all	always	ALL	ACCEPT		NAT	Standard	WEB Category_Monitor SSL certificate-inspection
any	any	all	all	always	ALL	DENY				

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.

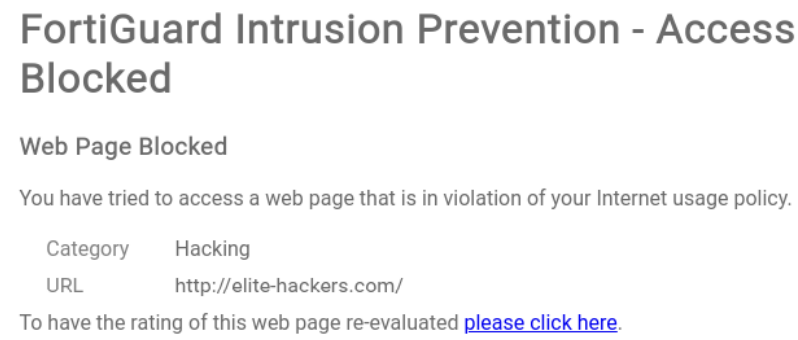
To authenticate as a remote user

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!`.

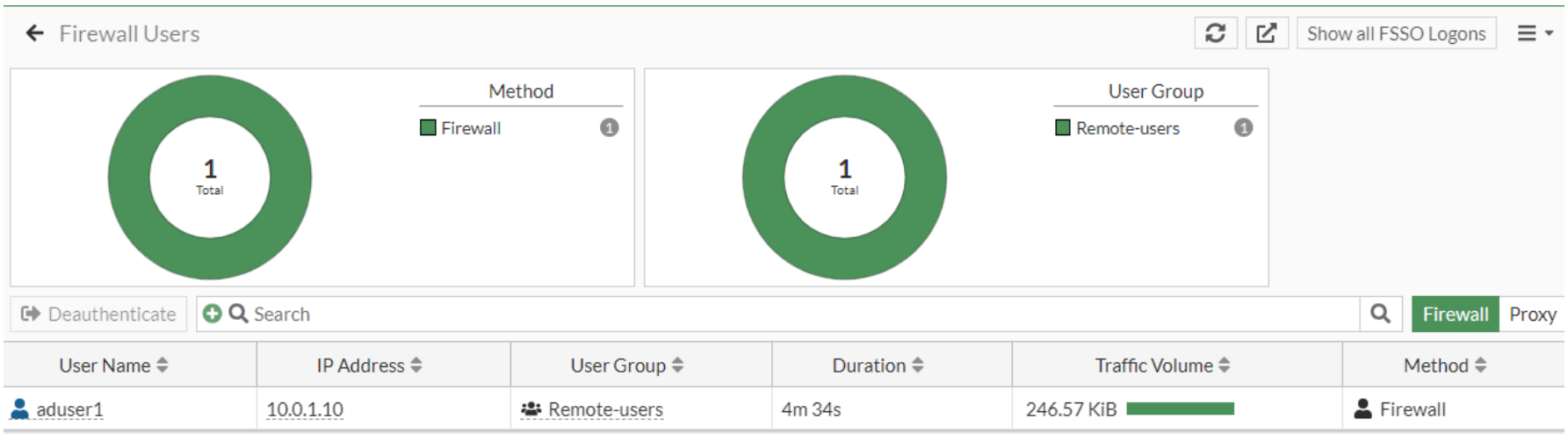
This URL is set to be blocked by the web filter security profile you enabled in the firewall policy.



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

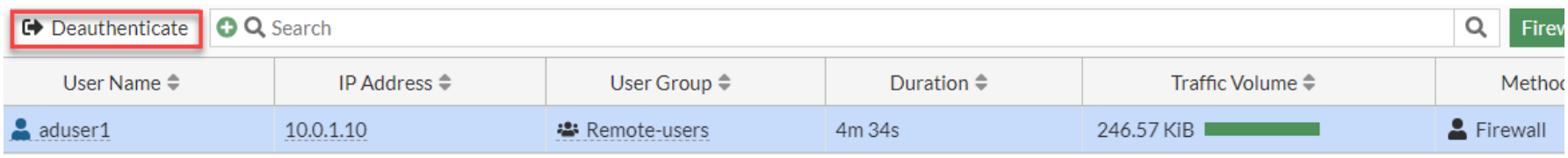
To monitor active authenticated users

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



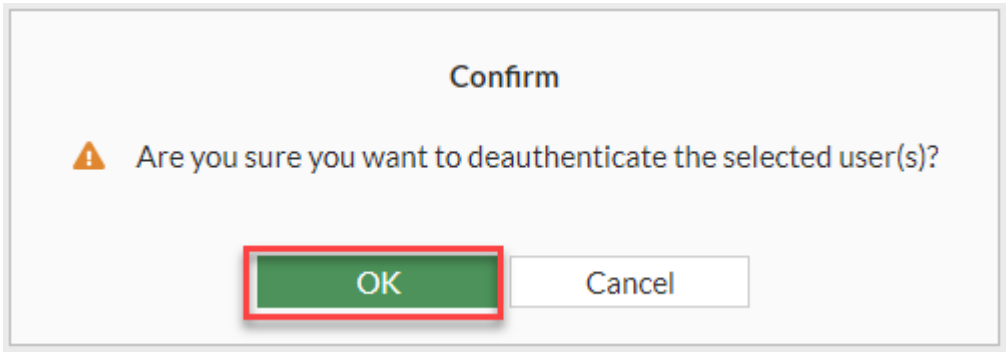
You will see **aduser1** listed along with other information, such as **User Group** and **IP Address**.

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



The `config user setting` CLI command determines how long a user can remain authenticated. However, you can choose to manually revoke a 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**.



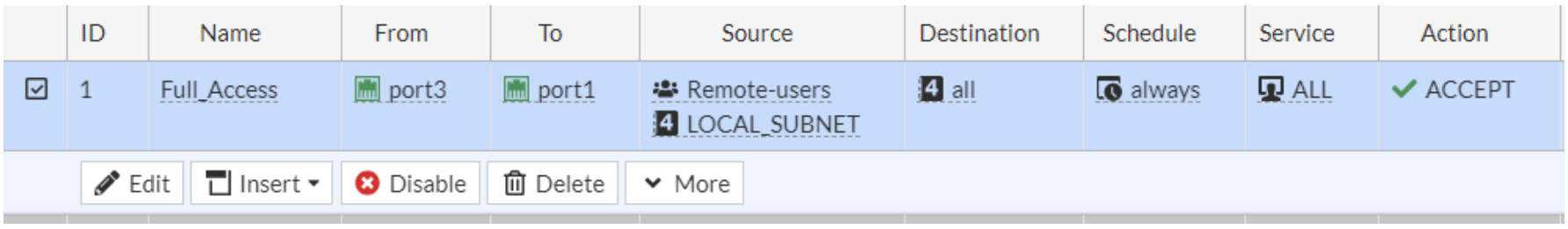
This deauthenticates the user. The user must log in again to access the resources that the firewall policy protects.

Remove the User Group From the Firewall Policy

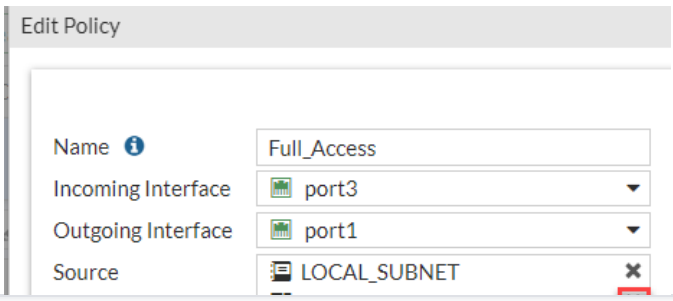
You will remove the user group assigned to the firewall policy for authentication.

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.



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



Exercise 2: Configuring a RADIUS Server on FortiGate

In this exercise, you will examine how to configure a RADIUS 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 a RADIUS Server on FortiGate

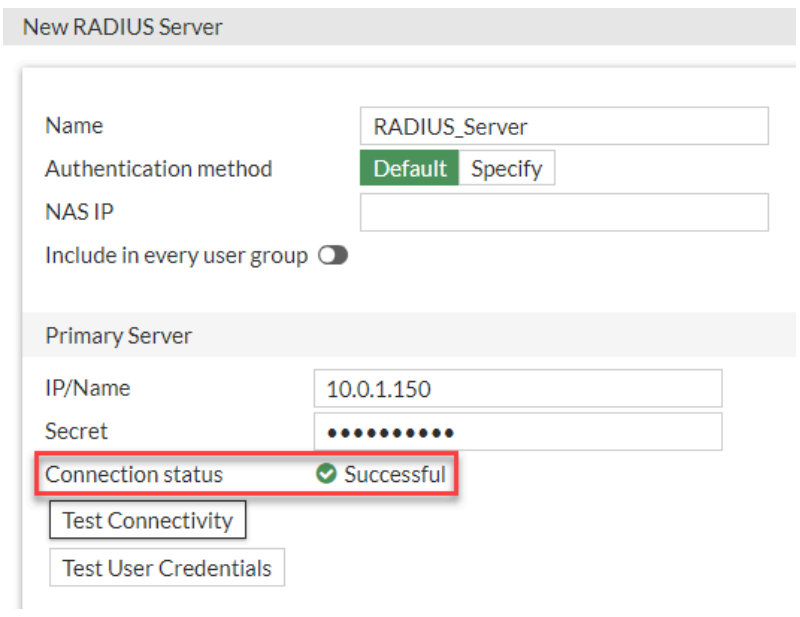
You can configure FortiGate to point to a preconfigured FortiAuthenticator acting as a RADIUS server for server-based password authentication.

To configure a RADIUS 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** > **RADIUS Servers**, and then click **Create New**.
3. Configure a server using the following settings:

Field	Value
Name	RADIUS_Server
Authentication method	Default
Primary Server IP/Name	10.0.1.150 This is the IP address of the FortiAuthenticator acting as the RADIUS server. For more information, see Network Topology on page 1 (../Network_Topology.htm).
Secret	Training1!

4. Click **Test Connectivity**.



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

5. Click **OK**.

Assign a RADIUS User Group to a Firewall Group

You will assign a RADIUS user group (**Training**) that includes a user (**radius1**) to a firewall user group, called **Training**, 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 **Training** firewall group is preconfigured for you. However, you must modify it to add the users from the remote RADIUS server you configured in the previous procedure.

Take the Expert Challenge!

On Local-FortiGate (`10.0.1.254`), assign the RADIUS user group called **Training** to the FortiGate firewall user group called **Training**.

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

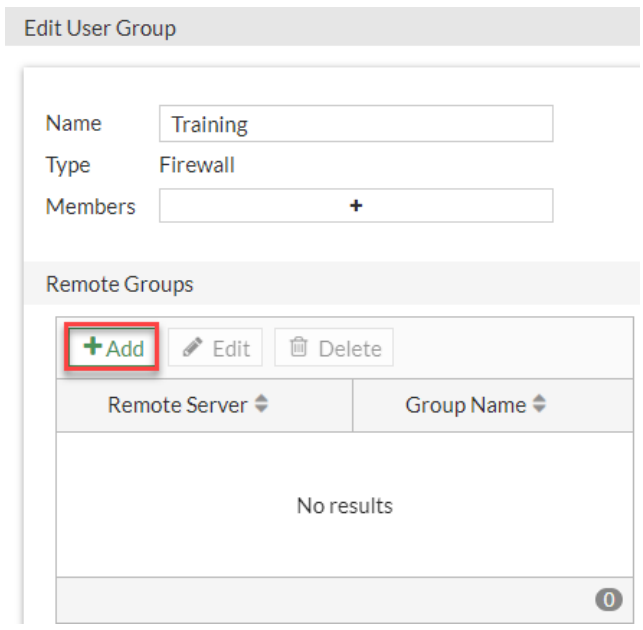
After you have completed this exercise, see Configuring a RADIUS Server on FortiGate on page 1 (#Adding).

To assign a user to a user group

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

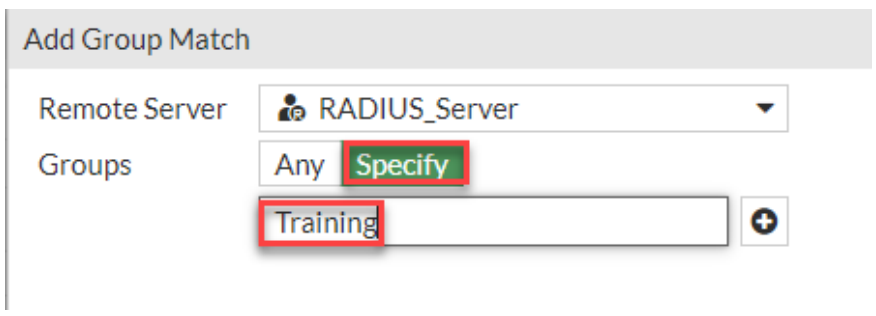
Notice that it's currently configured as a firewall group.

2. In the **Training** table, click **Add** to add users from the remote RADIUS server.



The **Add Group Match** window opens.

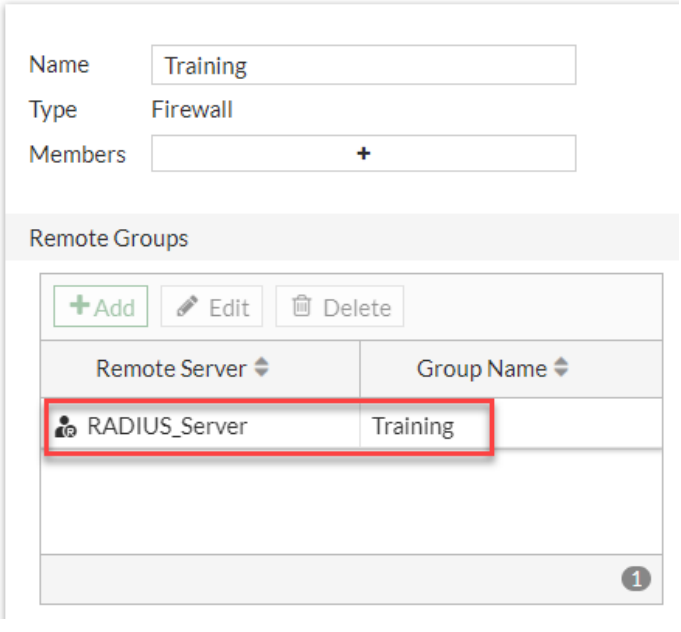
3. In the **Remote Server** field, select **RADIUS_Server**.
4. In the **Groups** field, select **Specify**, and then type the group name `Training`.



5. Click **OK**.

The user in this RADIUS server group is now included in the FortiGate **Training** firewall user group. Only users from the remote RADIUS server that match this user group entry can authenticate.

The remote RADIUS server is configured with using the RADIUS attribute value pair (AVP) 26, known as a vendor-specific attribute (VSA). This attribute allows the Fortinet-Group-Name VSA to be included in the RADIUS response. In FortiOS, the user group must be configured to specifically match this group.



6. Click **OK**.

Add the Training User Group to the Firewall Policy

Now that you have added the RADIUS server to the **Training** 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 Training 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.

ID	Name	From	To	Source	Destination	Schedule	Service	Action
1	Full_Access	port3	port1	LOCAL_SUBNET	all	always	ALL	ACCEPT

2. Configure the following setting:

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

3. Click **OK**.

	ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
	1	Full_Access	port3	port1	Training LOCAL_SUBNET	all	always	ALL	ACCEPT	NAT	Standard	WEB Category_Monitor SSL certificate-inspection
	0	Implicit Deny	any	any	all	all	always	ALL	DENY			

To test whether the radius1 user 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 radius <RADIUS server name> mschap2 <RADIUS user name> <password>

Where:

- `<RADIUS server name>` is `RADIUS_Server` (case sensitive)
- `<RADIUS user name>` is `radius1`
- `<password>` is `Training!`

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

```
Local-FortiGate # diagnose test authserver radius RADIUS_Server mschap2 radius1 Training!
authenticate 'radius1' against 'mschap2' succeeded, server=primary assigned_rad_session_id=1644739491
session_timeout=0 secs idle_timeout=0 secs!
Group membership(s) - Training
```

3. Close the Local-FortiGate CLI window.

Authenticate and Monitor the Authentication

You will authenticate through the firewall policy as `radius1`. This user is a member of the **Training** group on FortiGate. Then, you will monitor the authentication.

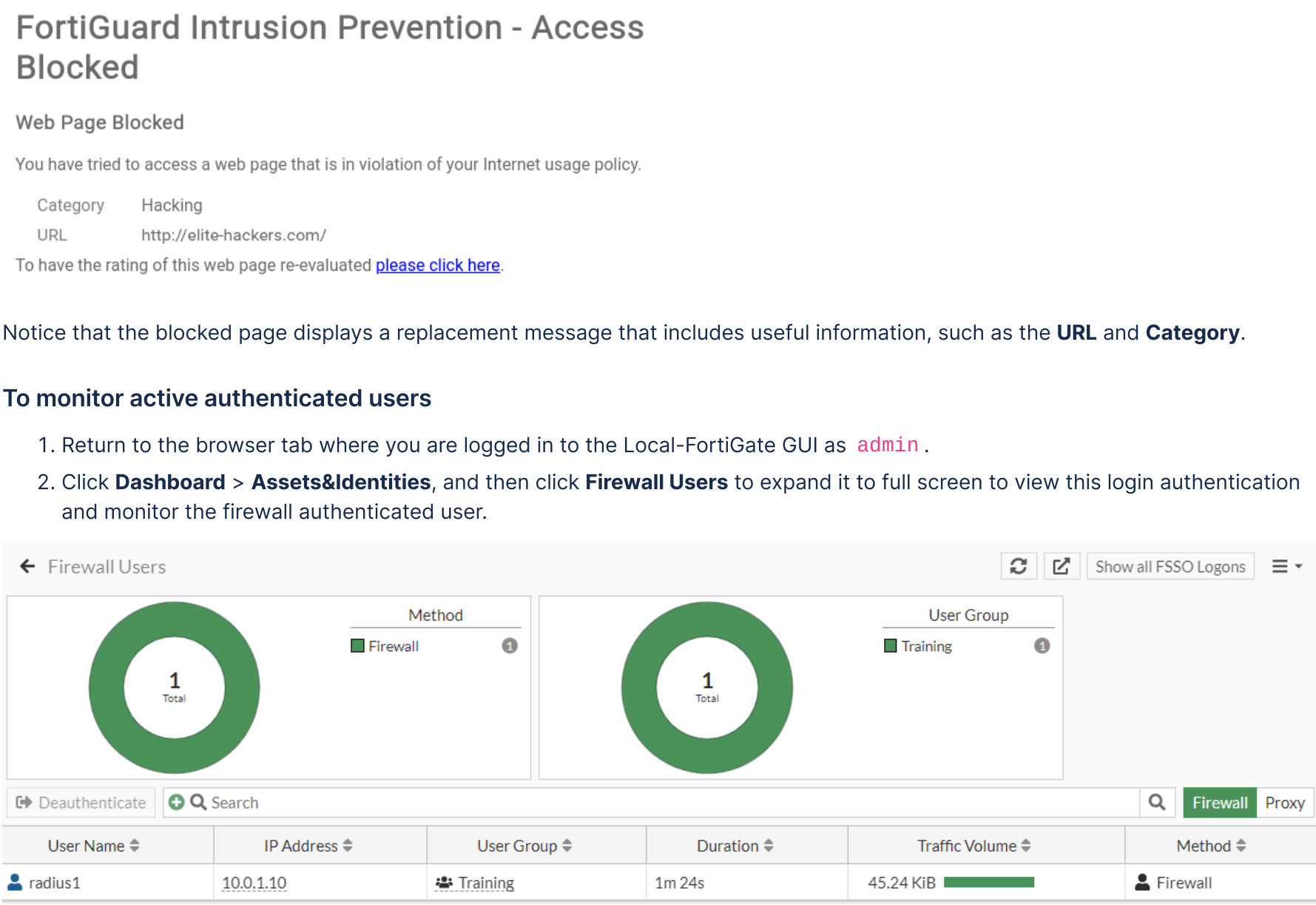
To authenticate as a remote RADIUS user

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 `radius1` with the password `Training!`.

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



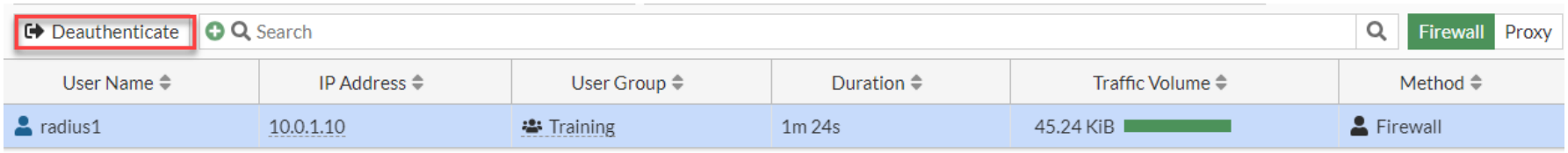
Notice that the blocked page displays a replacement message that includes useful information, such as the **URL** and **Category**.

To monitor active authenticated users

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

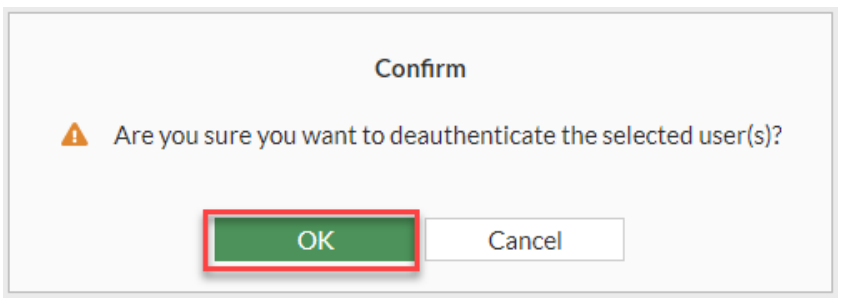
You will see the user **radius1** listed along with other information, such as **User Group** and **IP Address**.

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



The `config user setting` CLI command determines how long a user can remain authenticated. However, you can choose to manually revoke a 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**.



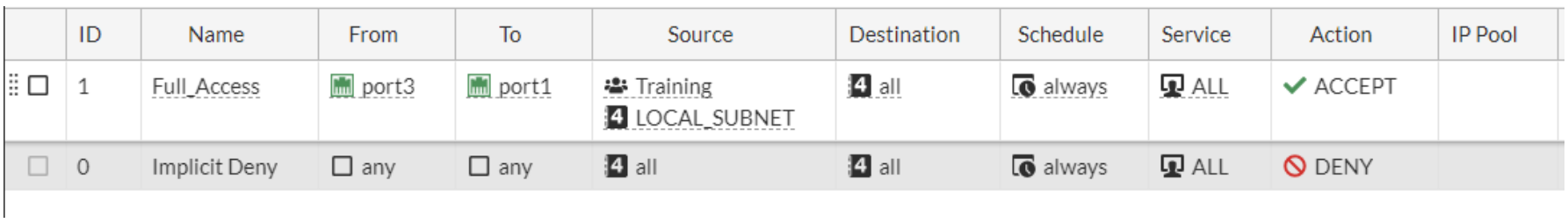
This deauthenticates the user. The user must log in again to access the resources that the firewall policy protects.

Remove the User Group From the Firewall Policy

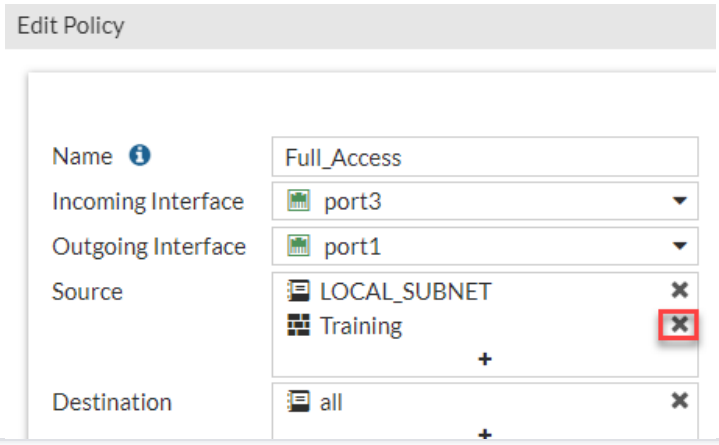
You will remove the user group assigned to the firewall policy for authentication.

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.



2. In the **Source** field, remove the **Training** user group.



Lab 4: Firewall Authentication

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

Objectives

- Configure server-based password authentication with an LDAP server
- Configure server-based password authentication with a RADIUS server

Time to Complete

Estimated: 35 minutes
LAB-4 > Firewall Authentication

Exercise 1: Configuring FortiGate for FSSO Authentication

In this exercise, you will configure FortiGate for FSSO and test user authentication. The lab uses a demo environment to emulate the behavior of an active FSSO DC agent from the Local-Client VM using a Python script. Therefore, you will not configure a DC agent to send logon events from the Local-Client VM.

In a real-world environment, you must configure FortiGate to identify users by polling their logon events using an FSSO agent, and you must install and configure a collector agent. FSSO agents are available on the Fortinet Support website (http://support.fortinet.com (http://support.fortinet.com)).

For FortiGate to communicate and poll information from the FSSO collector agent, you must assign the polled user to a firewall user group, and then add the user group as a source on a firewall policy.

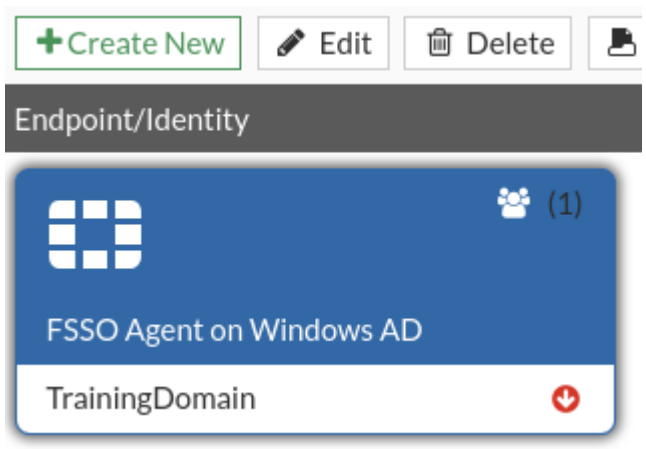
Finally, you can verify the user logon event that FortiGate collects. This event is generated after a user logs in to the Windows Active Directory domain. Therefore, no firewall authentication is required.

Review the FSSO Configuration on FortiGate

You will review the FSSO configuration and FSSO user groups on FortiGate. FSSO allows FortiGate to automatically identify the users who connect using SSO. Then, you will add FSSO user groups to the firewall policies.

To review the FSSO server and FSSO user group configuration on FortiGate

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Security Fabric** > **External Connectors**.
3. Select **TrainingDomain**, and then click **Edit**.



4. In the upper-right corner, review the **Endpoint/Identity** status, and see that the status is **Disconnected**.
5. Leave the browser window open.

To run a script to simulate a user logon event

1. On the Local-Client VM, open a terminal window, and then enter the following commands to simulate a user logon event:

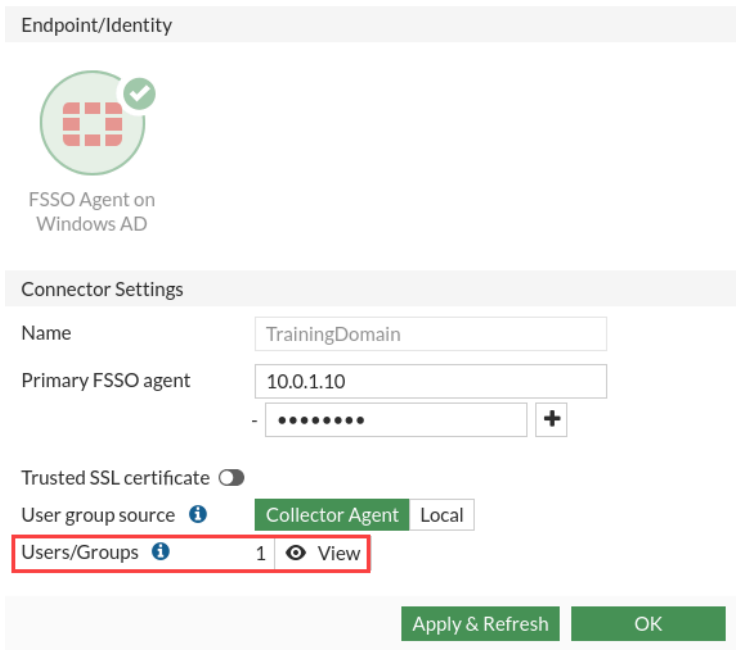
```
cd Desktop/FSSO/
python2 fssoreplay.py -l 8000 -f sample.log
```

2. Keep the terminal window open.

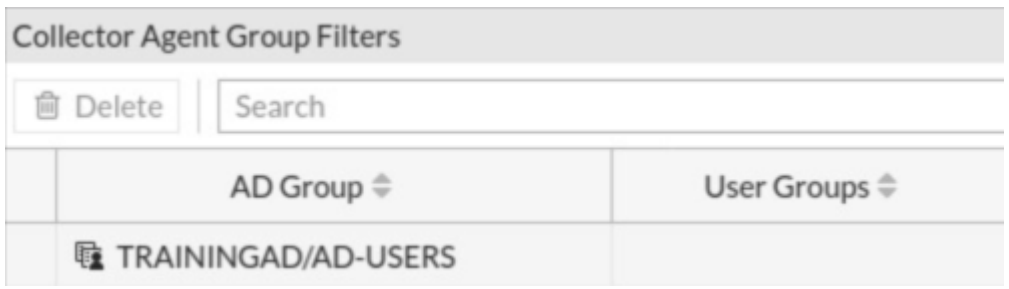
The script continues to run in the background.

To review the FSSO connection and FSSO user groups

1. Continuing in the **TrainingDomain** window, click **Apply & Refresh**.
2. Select **TrainingDomain**, and then click **Edit**.
3. In the **Users/Groups** field, click **View**.

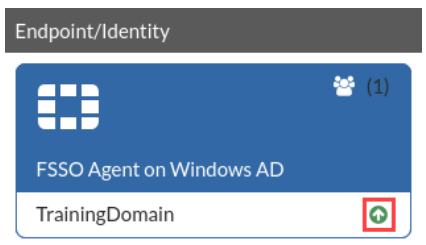


The **TRAININGAD/AD-USERS** monitored group is displayed.



4. Click **X** to close the **Collector Agent Group Filters** window.
5. Click **OK**.

A green up arrow confirms that the communication with the FSSO collector agent is up.



To assign the FSSO user to an FSSO user group

1. Continuing on the Local-FortiGate GUI, click **User & Authentication** > **User Groups**.
2. Click **Create New**, and then configure the following settings:

Field	Value
Name	Training
Type	Fortinet Single Sign-On (FSSO)
Members	TRAININGAD/AD-USERS

The FSSO user is automatically listed because of the selected group type—FSSO.

3. Click **OK**.

Assign FSSO Users to a Firewall Policy

You will assign your FSSO user group as a source in a firewall policy. This allows you to control access to network resources based on user identity.

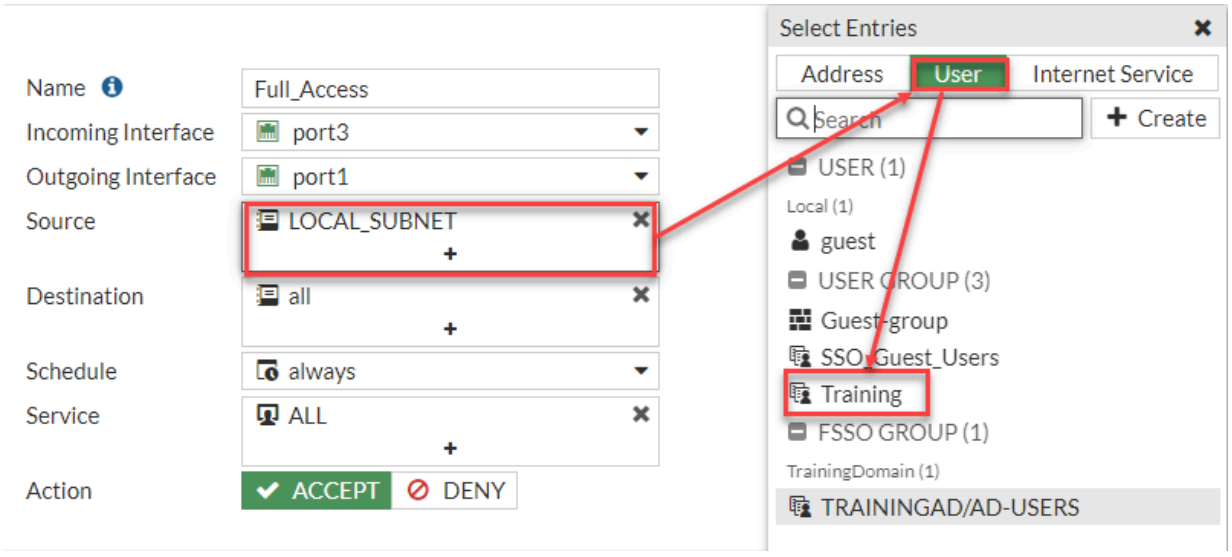
To test the connection without assigning the FSSO user group to a firewall policy

1. On the Local-Client VM, open a new browser, and then go to https://www.fortinet.com (https://www.fortinet.com/).

You can see that all users can access the Fortinet website.

To add the FSSO user group to your firewall policy

1. Return to the browser where you are logged in to the Local-FortiGate GUI, and then click **Policy & Objects** > **Firewall Policy**.
2. Edit the **Full_Access** firewall policy.
3. In the **Source** field, click **LOCAL_SUBNET**.
4. In the **Select Entries** section, select **User**, and then add the **Training** group.



5. Click **Close**, and then click **OK**.

Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles	Log
Full_Access	port3	port1	Training LOCAL_SUBNET	all	always	ALL	ACCEPT	NAT	Standard	SSL no-inspection	UTM

Test FSSO

After a user logs in, they are automatically identified based on their IP address. As a result, FortiGate allows the user to access network resources as policy decisions are made. You will test FSSO.

To test the connection after assigning the FSSO user to the firewall policy

1. On the Local-Client VM, open a new browser tab, and then go to http://support.fortinet.com (http://support.fortinet.com/).

The Python script that is running on the Local-Client VM is already sending user logon events with the following information:

- **user**: aduser1
- **IP**: 10.0.1.10

In this case, the website loads successfully because aduser1 belongs to the configured user group on a firewall policy.

To review the connection status between the FSSO collector agent and FortiGate

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following commands to show the connection status between FortiGate and each collector agent:

diagnose debug enable

diagnose debug authd fsso server-status

3. Observe the CLI output.

Your FortiGate is connected to the FSSO collector agent.

Server Name Connection Status Version Address

---------- ---------- ------- -------

TrainingDomain connected FSAE server 1.1 10.0.1.10

To monitor communication between the FSSO collector agent and FortiGate

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

diagnose debug enable

diagnose debug application authd 8256

3. On the Local-Client VM, on a terminal window, press `Ctrl` + `C` to stop the script, and then enter the following command again to simulate a user logon event:

python2 fssoreplay.py -l 8000 -f sample.log

4. View the output of the `diagnose` command.

[_process_logon: 1079]: ADUSER1(10.0.1.10, 0) logged on from TrainingDomain.

[_process_logon:1122di]: ADUSER1 (10.0.1.10, 0) from TrainingDomain exists

fsae_io_ctx_process_msg[TrainingDomain]: received heartbeat 100004

fsae_io_ctx_process_msg[TrainingDomain]: received heartbeat 100005

You generated a logon event on the Local-Client VM using the script, and it was forwarded to FortiGate.

5. Enter the following command to stop the debug process:

diagnose debug reset

To display the FSSO logon events

1. Continuing on the Local-FortiGate VM, enter the following command:

diagnose debug authd fsso list

2. Review the output, which shows the FSSO logon events.

----FSSO logons----

IP:10.0.1.10 User: ADUSER1 Groups: TRAINING/AD-USERS Workstation

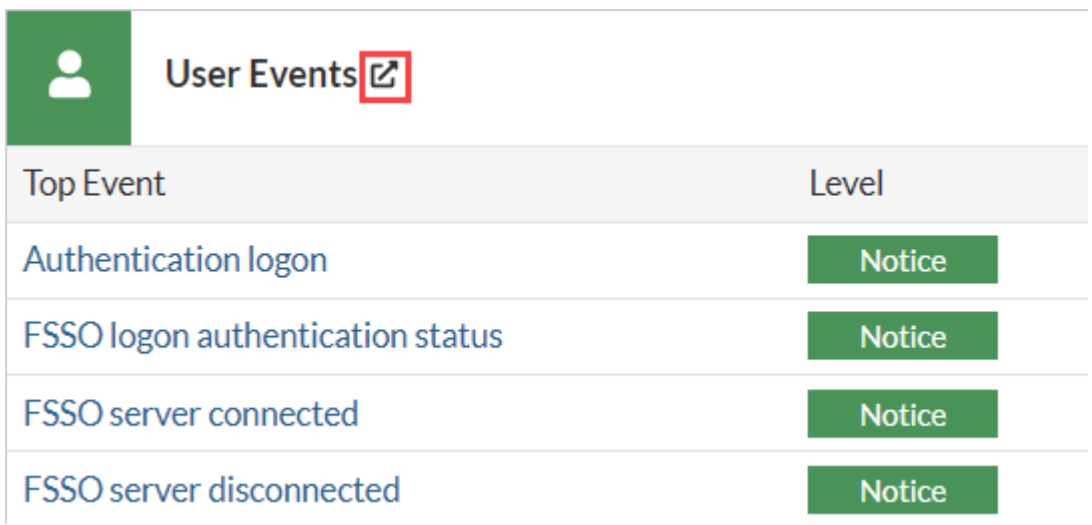
C7280677811.TRAININGAD.TRAINING.LAB MemberOf: Training TRAININGAD/AD-USERS

Total number of logons listed: 1, filtered: 0

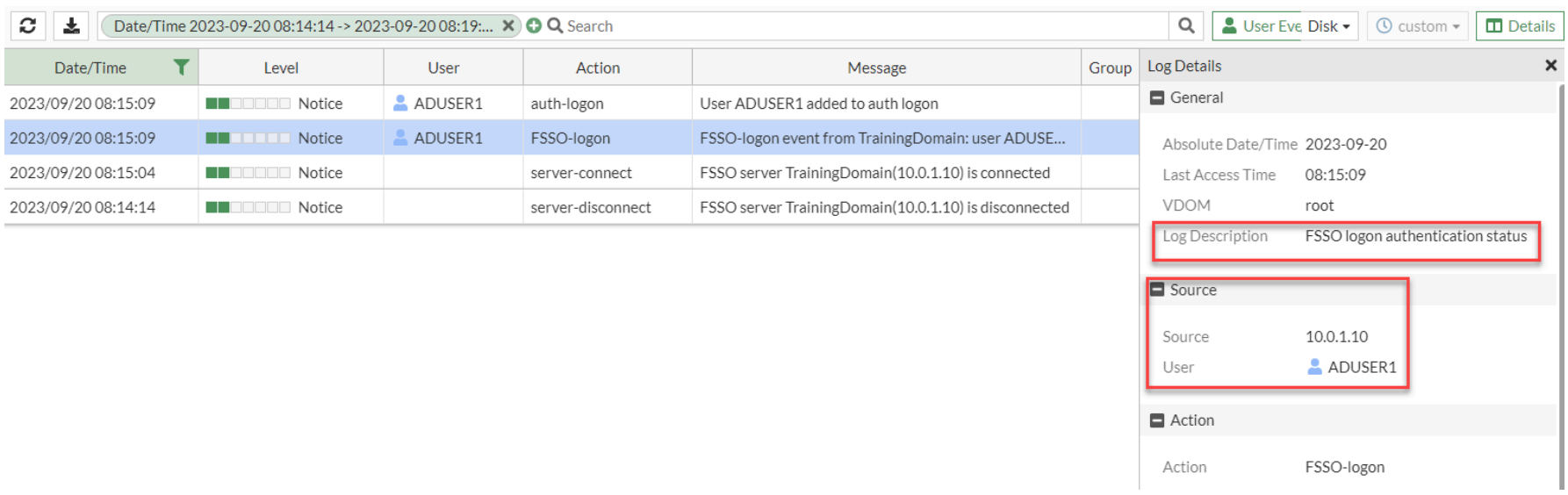
----end of FSSO logons----

To review the user event logs

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Log & Report** > **System Events**, and then in the **User Events** widget, click the **View Logs** arrow.

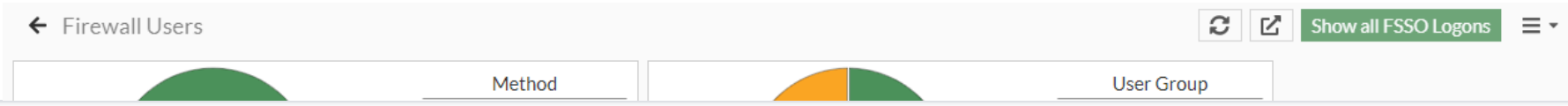


3. Select a log, and then click **Details** to view more information about it.



To monitor FSSO logon events

1. Continuing on the Local-FortiGate GUI, click **Dashboard** > **Assets & Identities**, and then double-click **Firewall Users** to expand it to full screen.
2. Click **Show all FSSO Logons**, and then click **Refresh** if the user's details don't appear.


Firewall Users
Show all FSSO Logons
Method
User Group

Lab 5: Fortinet Single Sign-On Configuration

In this lab, you will test user authentication using Fortinet Single Sign-On (FSSO). The lab uses a demo environment to emulate the behavior of an active FSSO DC agent from the Local-Client VM using a Python script. Therefore, you will not configure a DC agent to send logon events from the Local-Client VM.

Objectives

- Review the FSSO configuration on FortiGate
- Test the transparent or automatic user identification by generating user logon events
- Monitor the FSSO status and operation

Time to Complete

Estimated: 35 minutes
LAB-5 > Fortinet Single Sign-On Configuration

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. Next, you will review some situations that prevent full SSL inspection, and implement workarounds. Finally, you will learn how to deal with some certificate anomalies.

Objectives

- Configure and enable full SSL inspection on outbound traffic
- Deal with certificate anomalies

Time to Complete

Estimated: 40 minutes
LAB-6 > Certificate Operations

Dealing With Anomalies

When you work with certificates, you might face some issues due to invalid or revoked certificates. You might also have to deal with restrictions that prevent the use of full SSL inspection.

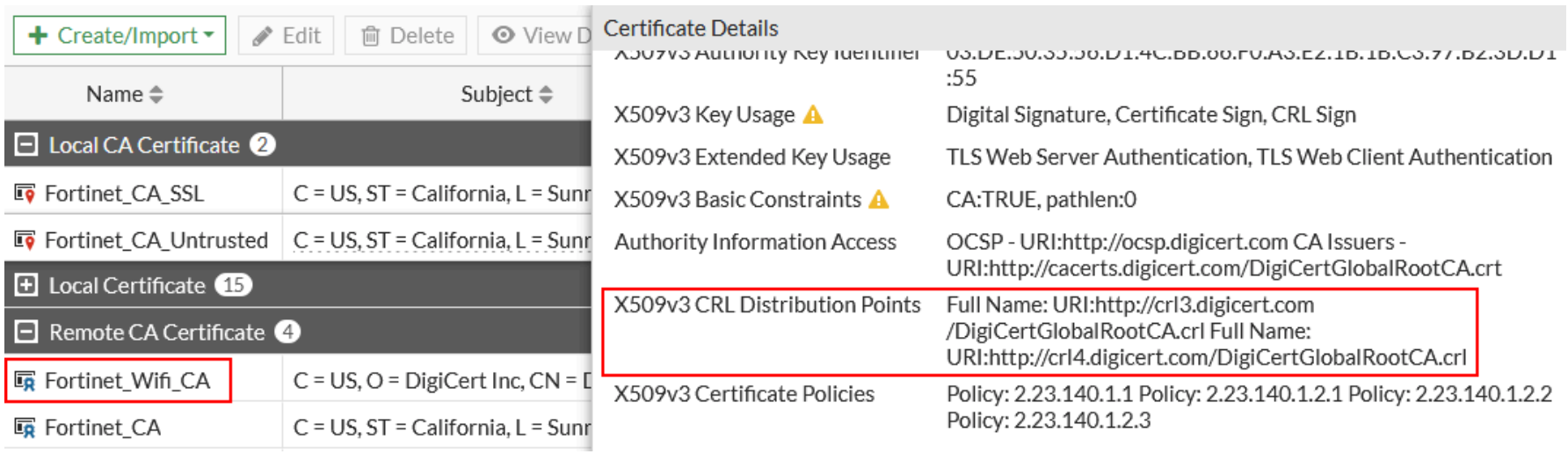
In this exercise, you will learn how to import a certificate revocation list (CRL) on the FortiGate GUI. Next, you will explore how FortiGate responds when it receives invalid certificates for traffic that match a deep inspection SSL profile. Finally, you will configure an exception to exclude a website from SSL full inspection.

Manage Invalid Certificates

A certificate can be invalid because it expired or because the CA that issued it revoked it. A company might want to revoke a certificate because it was compromised, the key was lost, or, for example, because it was assigned to a user who left the company. To inform others of revoked certificates, CA administrators periodically publish CRLs. You will import a CRL.

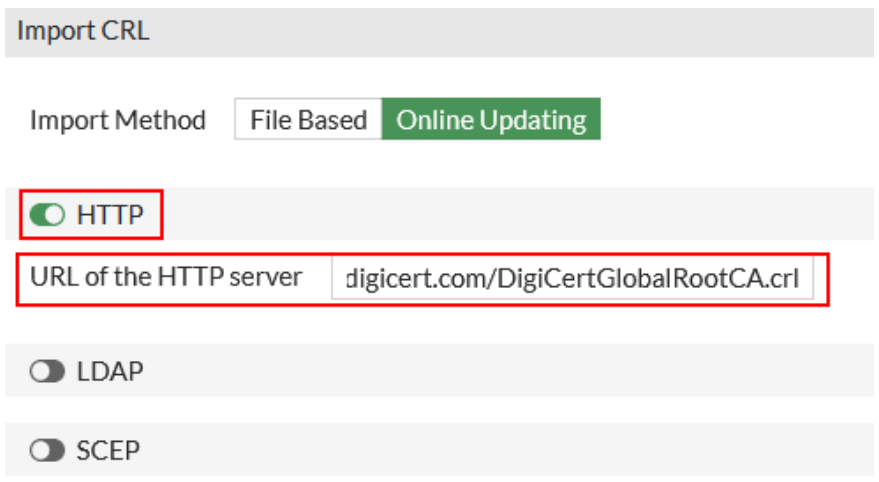
To import a CRL

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **System** > **Certificates**.
3. In the **Remote CA Certificate** section, right-click the **Fortinet_Wifi_CA** certificate, and then select **View Details**.
4. Scroll down to the **Extensions** section, and look for **X509v3 CRL Distribution Points**.
5. Highlight one of the URIs, and then press `Ctrl` + `C` to copy it for the distribution point.



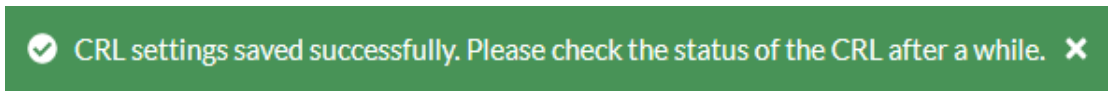
1. Click **Close** to exit the **Certificate Details** window.
2. Click **Create/Import** > **CRL**.

1. Enable **HTTP**, and then paste the URI of the CRL HTTP server that you just copied.



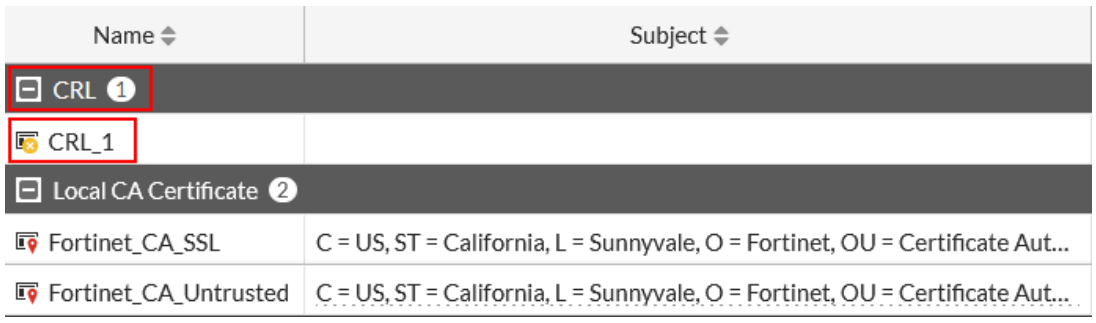
1. Click **OK**.

The FortiGate GUI briefly displays an acknowledgment message similar to the following example:



1. Wait a few seconds, and then click **System** > **Certificates** again to refresh the page.

The CRL section now includes the CRL you just added.



Note that you can load CRLs on the FortiGate only for a CA that FortiGate trusts. If you want to load the CRL that corresponds to your company CA, you must first load your company CA certificate on FortiGate.

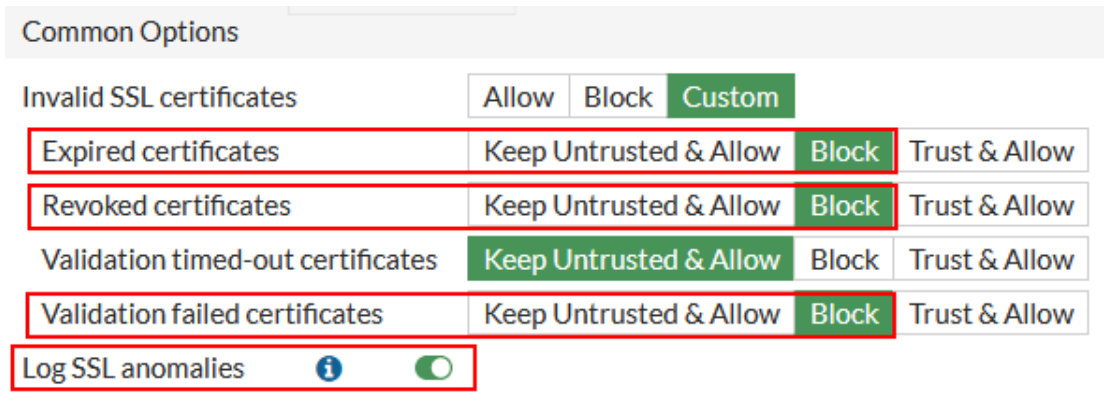
The Online Certificate Status Protocol (OCSP) is used for obtaining the revocation status of an X.509 digital certificate. It can be used as an alternative to CRLs. OCSP is disabled by default on FortiGate.

In this lab, we activated OCSP using the CLI commands shown below to receive certificate validation from well-known CAs that support OCSP.

```
config vpn certificate setting
set ocsp-option certificate
set ocsp-status enable
set strict-ocsp-check enable
end
```

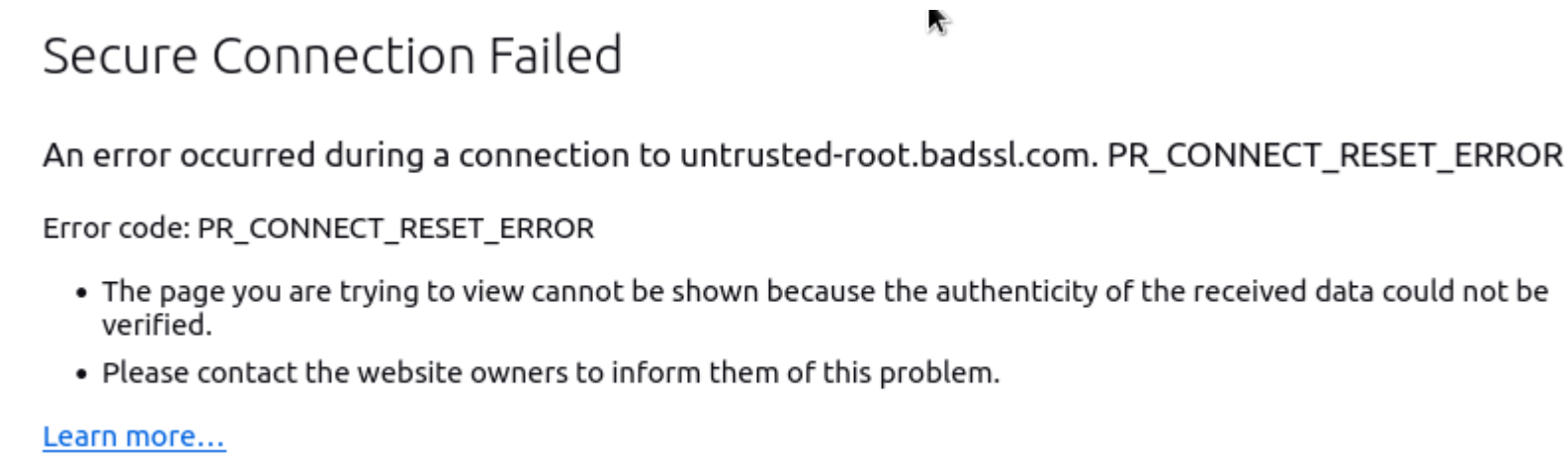
To block an invalid certificate with SSL full inspection

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Select the **Full_Access** policy, and then click **Edit**.
3. Scroll down to the **Security Profiles** section, and then click the pen icon to edit the **SSL Inspection** profile **Custom_Full_Inspection**.
4. Confirm that the settings are the same as what is shown in the following image:



1. Do not make any changes, and then click **Cancel** to exit the SSL inspection profile menu.
2. Click **Cancel** to exit the policy configuration menu.
3. Connect to the Local-Client VM, and then log in with the username `Administrator` and password `password`.
4. Open a browser, and then visit `https://revoked.badssl.com/`.
5. In another browser tab, visit `https://expired.badssl.com/`.

FortiGate blocks access to the website and the browser displays a warning message similar to the following image:



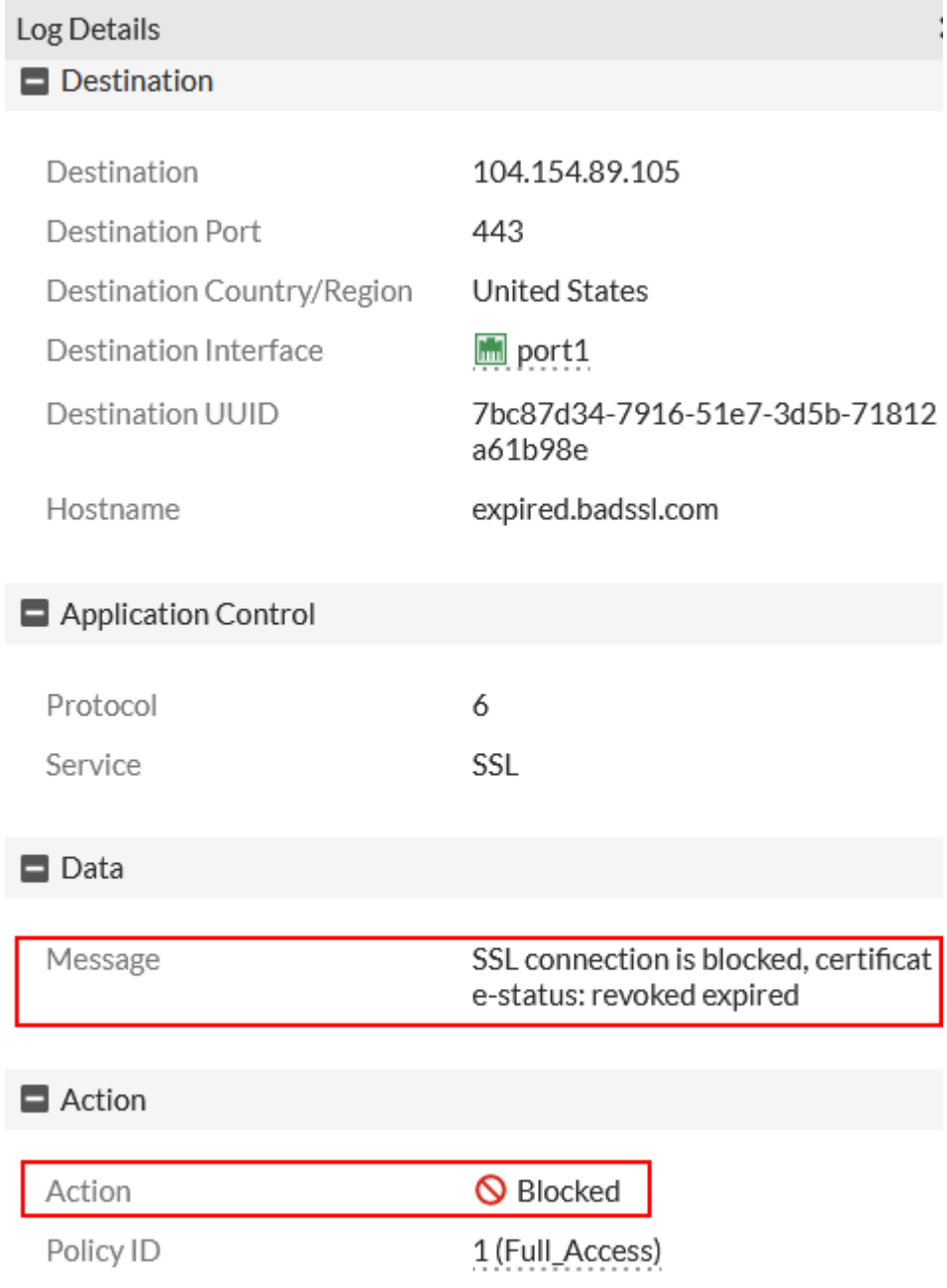
To review SSL log messages

1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Security Events**.
2. Expand the **SSL** widget to display the log list.

You can see that FortiGate blocked access to the website.

Relative Date/Time	Action	Source	Source Int...	Destination	Destination Interface
3 minutes ago	Blocked	10.0.1.10	port3	104.154.89.105 (untrusted-root.badssl.com)	port1
3 minutes ago	Blocked	10.0.1.10	port3	104.154.89.105 (untrusted-root.badssl.com)	port1
3 minutes ago	Blocked	10.0.1.10	port3	104.154.89.105 (untrusted-root.badssl.com)	port1

1. Double-click a log message to review the details.



You can see that the log message is similar for expired and revoked certificates.

Allow Exceptions to SSL Full Inspection

When replacing a certificate prevents users from accessing some websites, you can define exceptions and exclude some websites from full SSL inspection. You can also exclude some websites or website categories from full SSL inspection for legal reasons. For example, in some countries, it is forbidden to perform deep inspection on traffic between users and financial institution servers.

You will add an exception to the SSL/SSH deep inspection profile that you have already configured.

To configure a site exception to SSL full 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. Edit the **Custom_Full_Inspection** profile.
4. In the **Exempt from SSL Inspection** section, click **+** to create new **Addresses**.
5. Create a new address object with the following parameters:

New Address	Value
Name	badssl
Type	Subnet
IP/Netmask	104.154.89.105/32

1. Click **OK**.

2. In the SSL/SSH inspection profile, select the newly created address object **badssl**.
3. Click **OK** to save the configuration change of the SSL/SSH inspection profile.
4. Click **Policy & Objects** > **Firewall Policy**.
5. Edit the **Full_Access** policy and set **Custom_Full_Inspection** as the SSL inspection profile.
6. Click **OK**.

To check the SSL full inspection exception

1. On the Local-Client VM, navigate to one of the websites you tested previously:

- `https://revoked.badssl.com/`.
- `https://expired.badssl.com/`.

1. Click **Advanced**, and then click **Accept the Risk and Continue** to accept the browser warning.

Now, you can visit the website.

Usually, you will configure SSL full inspection exceptions only for websites that do not support MITM and that your company trusts. Those websites should have a valid certificate and therefore do not trigger a browser warning.

Exercise 1: Configuring Full SSL Inspection on Outbound Traffic

Full SSL inspection on outbound traffic allows FortiGate to inspect encrypted internet traffic and apply security profiles to that traffic. It protects your network and end users from potential malware that could come from secure websites, like HTTPS websites, that internal users visit. FortiGate employs a man-in-the-middle (MITM) technique to inspect the traffic and apply security profiles, such as antivirus, web filter, and application control.

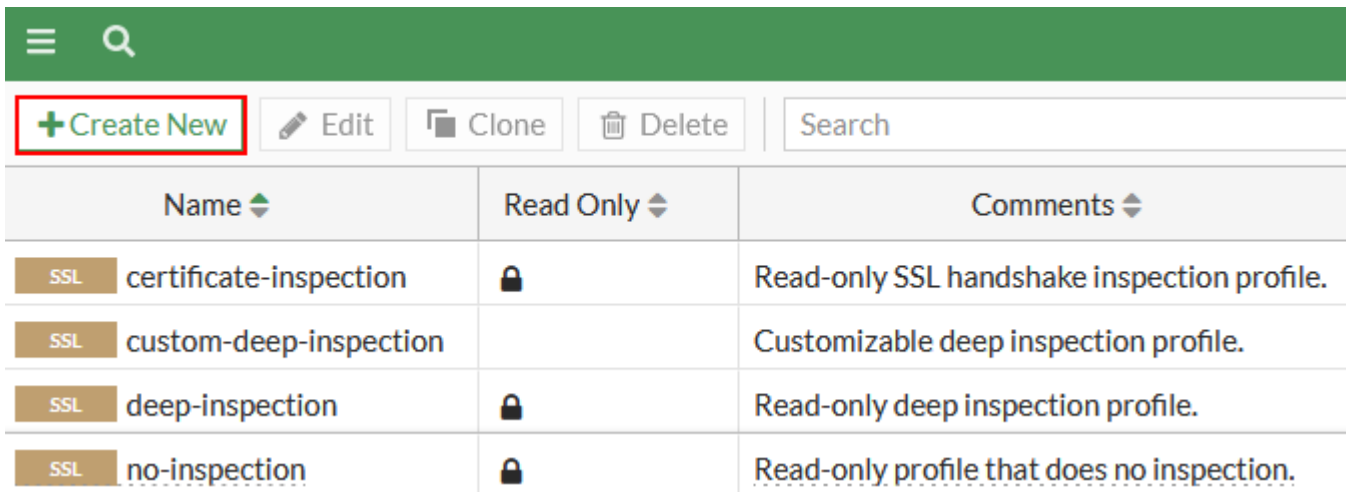
In this exercise, you will configure and enable full SSL inspection on all outbound traffic.

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 or create a personalized profile. 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.

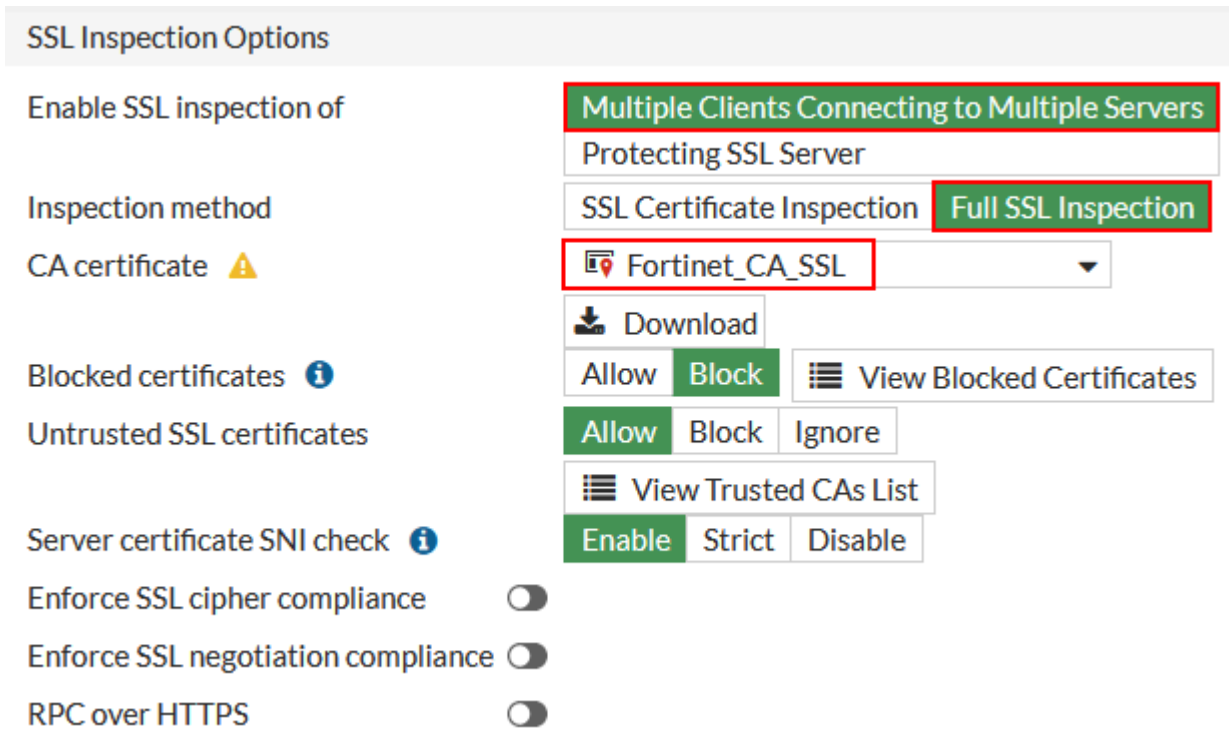
To configure SSL inspection

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. Click **Create New** to create a new profile.



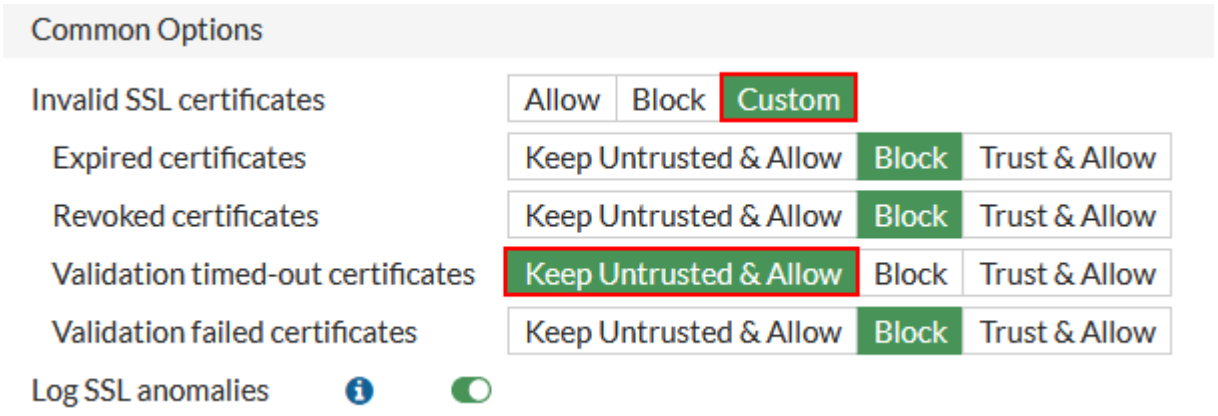
4. In the **Name** field, type `Custom_Full_Inspection`.
5. In the **SSL Inspection Options** section, verify that the following settings are configured (default values):

Field	Value
Enable SSL inspection of	Multiple Clients Connecting to Multiple Servers
Inspection method	Full SSL Inspection
CA certificate	Fortinet_CA_SSL



6. Scroll down to the bottom of the page, and then in the **Common Options** section, do the following:

- In the **Invalid SSL certificates** field, select **Custom**.
- Confirm that the other settings are configured as shown in the following image (default values):



7. Click **OK**.

Enable SSL Inspection in a Firewall Policy

You must enable SSL inspection in a firewall policy to start inspecting SSL traffic. In this policy, you will use SSL inspection associated with web filtering. For the purposes of this lab, you will enable the default web filter security profile.

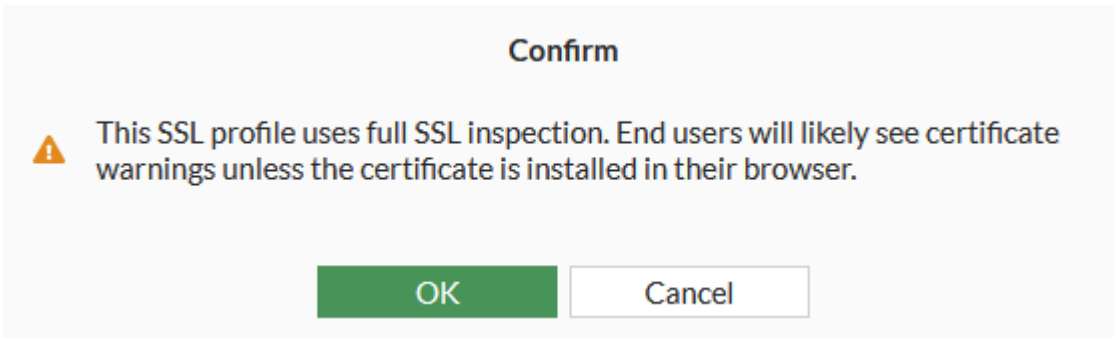
To enable SSL inspection in a firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Edit the **Full_Access** firewall policy.
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**.

FortiGate displays a warning message to highlight that full SSL inspection is activated and might trigger warnings in users' browsers.



6. Read the warning message, and then 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. The SSL inspection profile you created in the previous step uses it. This certificate 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 a secure website, the browser displays a certificate warning. This is because the browser receives traffic encrypted by certificates signed by FortiGate, using 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.

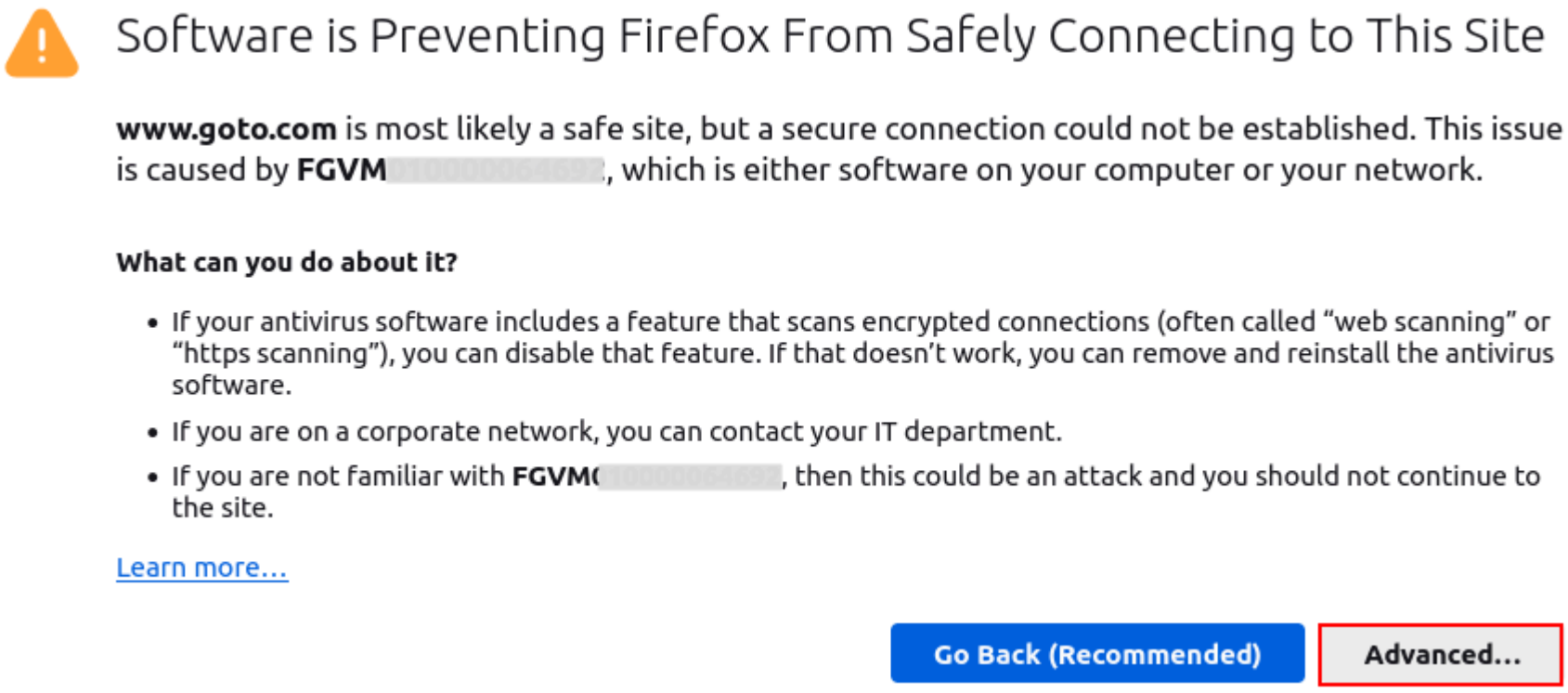
You will first test access to a secure website *without* the Fortinet_CA_SSL certificate installed in the browser. Then, you will install the Fortinet_CA_SSL certificate in the browser and test access to the secure website again.

To test full SSL inspection without a trusted CA

1. Connect to the Local-Client VM, and then log in with the username `Administrator` and password `password`.
2. Open a browser, and then go to an HTTPS site, such as:

https://www.goto.com

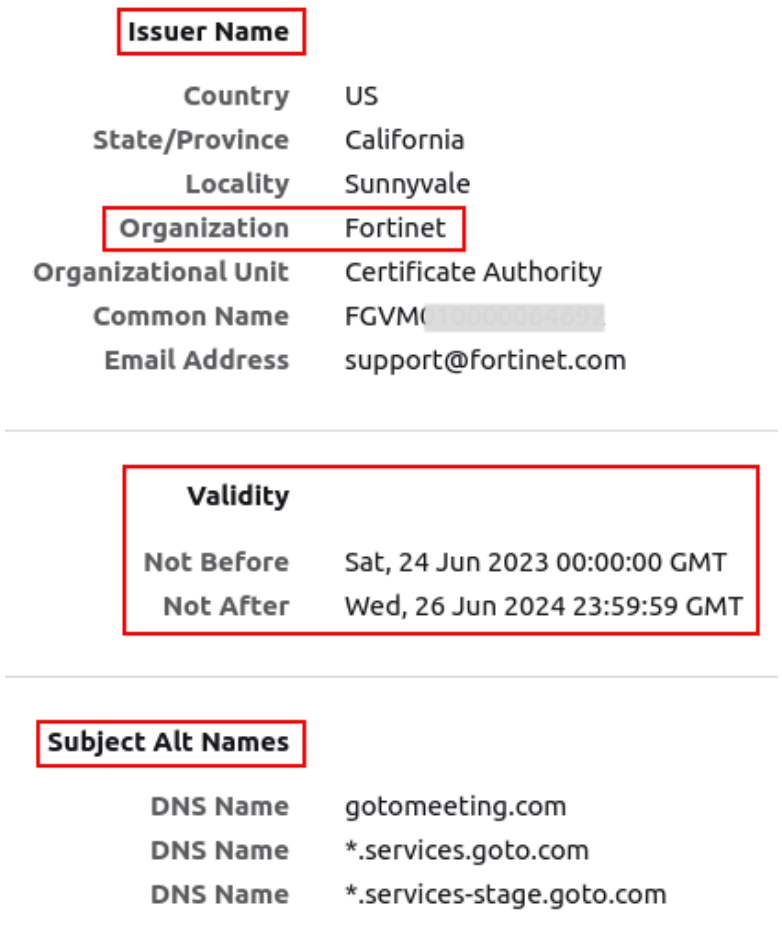
3. Notice the certificate warning.



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

4. Click **Advanced**, and then click **View Certificate**.

You can see that the certificate is issued by Fortinet (Issuer Name), and that it is valid. The subject alternative names list includes a reference to the website you visited (`goto.com` , in our example).

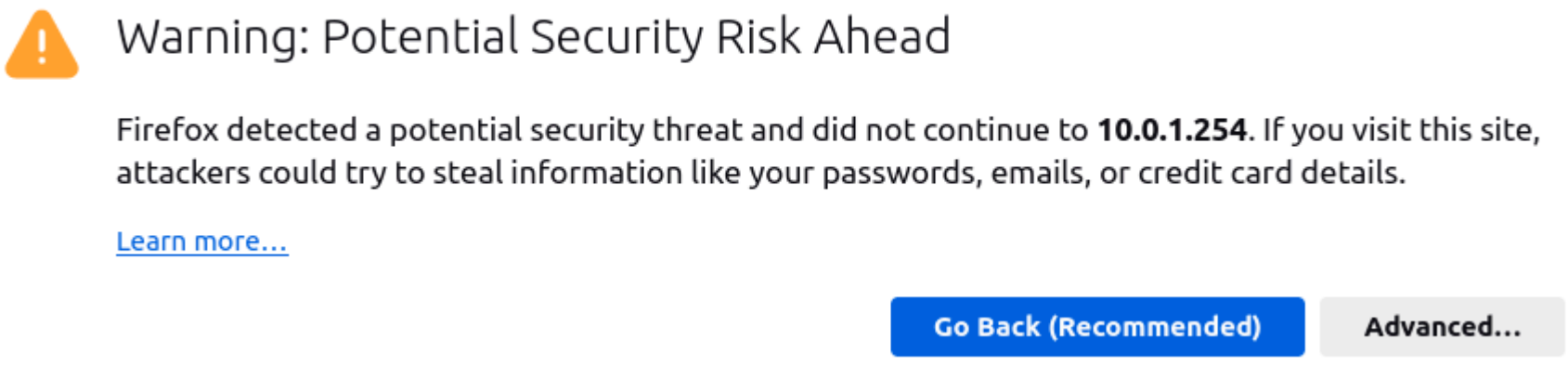


5. Do *not* click **Accept the Risk and Continue**.
6. Leave the browser tab open, and then continue to the next procedure.

To install the Fortinet_CA_SSL certificate in the browser

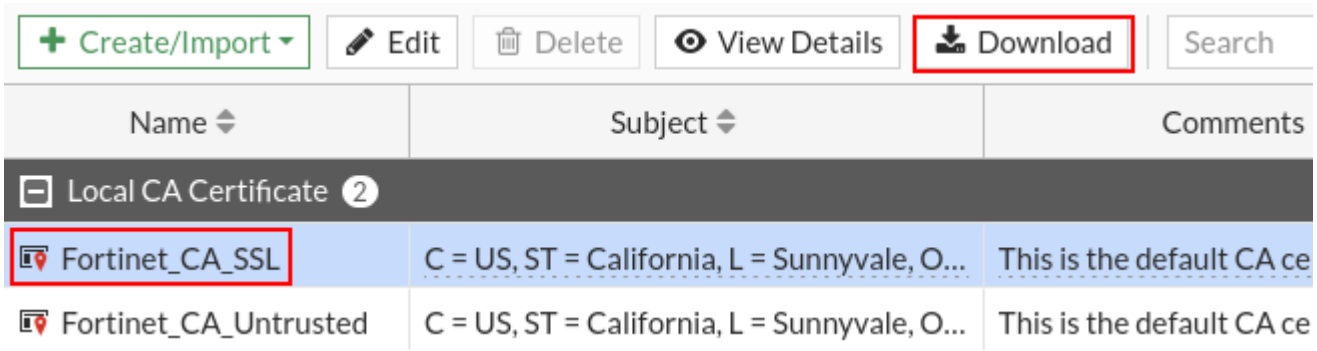
1. On the Local-Client, open a new browser tab, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password` .

This time, you might see a warning because the FortiGate GUI presented a certificate signed by a CA that your browser doesn't trust.



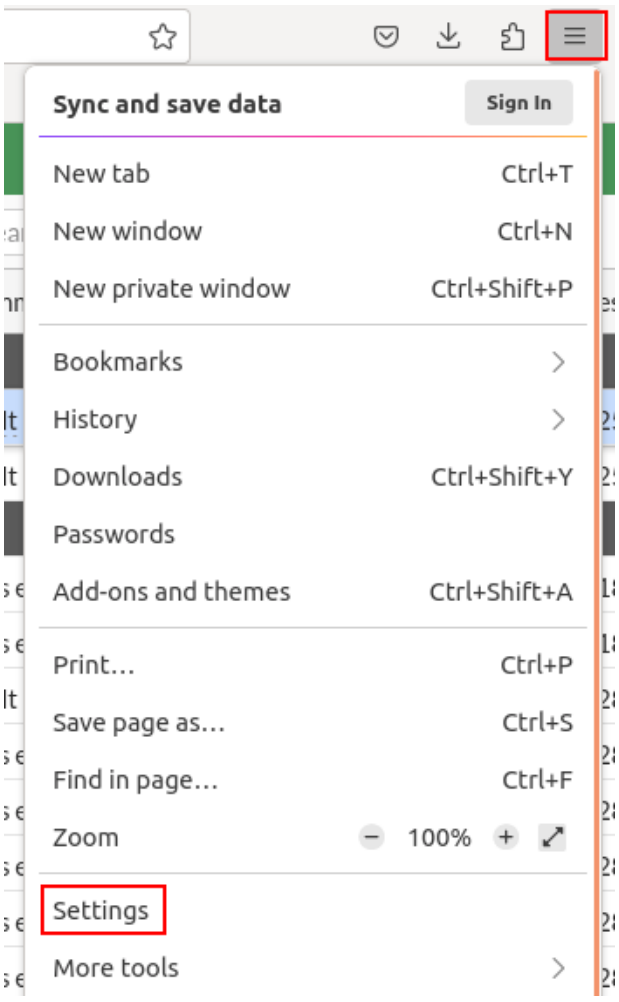
2. If you get the warning message, click **Advanced**, and then click **Accept the Risk and Continue**.

3. Click **System** > **Certificates**.
4. In the **Local CA Certificate** section, click **Fortinet_CA_SSL**, and then click **Download**.

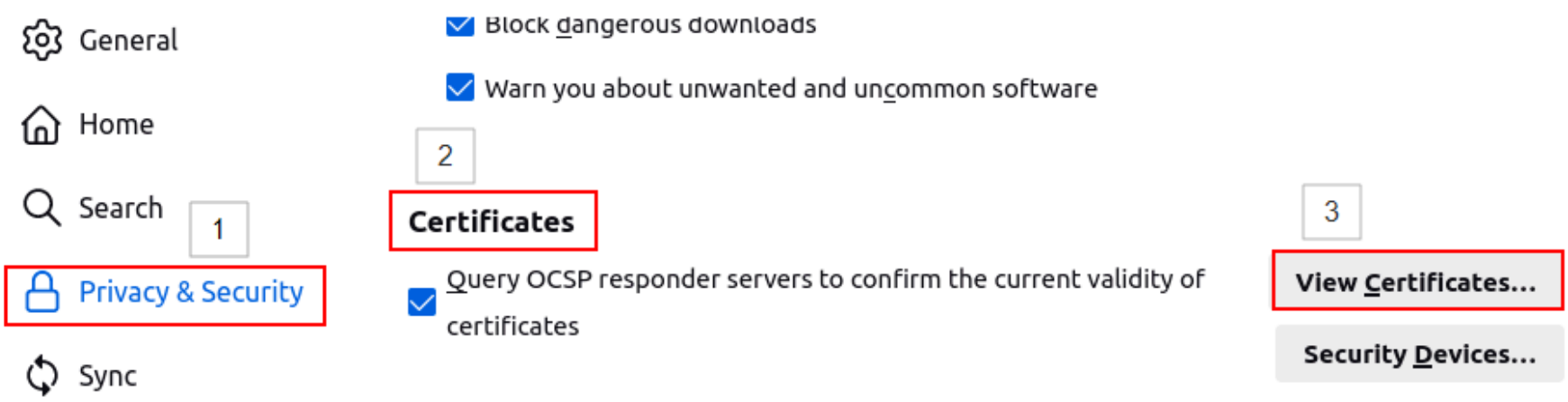


The browser downloads the certificate to the **Downloads** folder of your Local-Client VM.

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

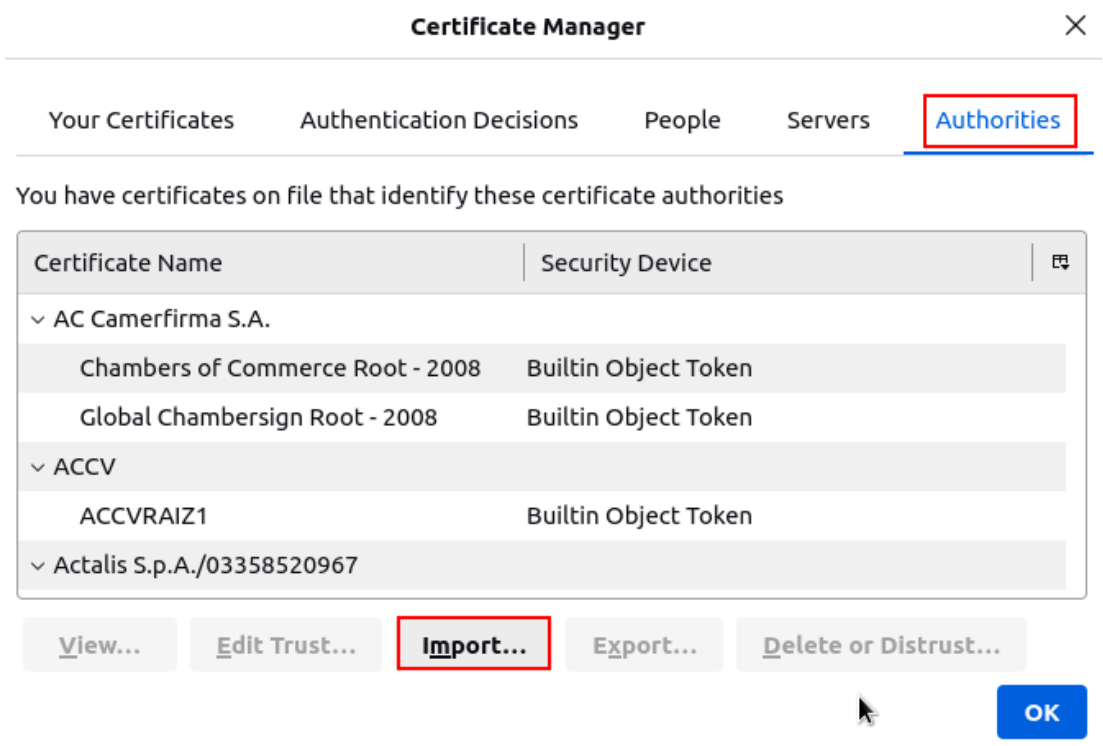


6. Click **Privacy & Security**.
7. In the **Certificates** section, click **View Certificates**.



8. In the **Certificate Manager** window, click the **Authorities** tab.

You can see a list of certificates from the public CA. They are loaded by default in your browser.



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

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

You can scroll down to see it in the list of authority certificates.

12. Click **OK** to exit the **Certificate Manager**.
13. Restart Firefox.

Test Full SSL Inspection

Now that you have imported the Fortinet_CA_SSL certificate into your browser, you will not receive certificate warnings when you access a secure website.

The CA that signed this certificate is not public, but your browser trusts it, because you added it as a trusted authority in the previous procedure.

Lab 7: 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

Time to Complete

Estimated: 30 minutes
LAB-7 > Antivirus

Exercise 1: Configuring Flow-Based Antivirus Scanning

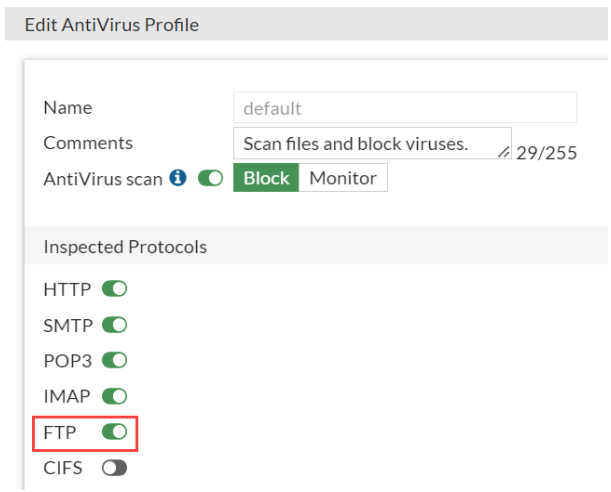
In this exercise, you will configure a firewall policy with an antivirus profile in flow-based inspection mode. Next, you will perform a test to download a file located on an FTP server. Finally, you will view the logs and summary information related to the antivirus scanning.

Configure the Antivirus Profile Inspection Mode

You will verify that the antivirus profile is configured with an inspected protocol of FTP and that flow-based is selected.

To verify the antivirus profile

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 **Inspected Protocols** section, verify that **FTP** is enabled.



Stop and think!

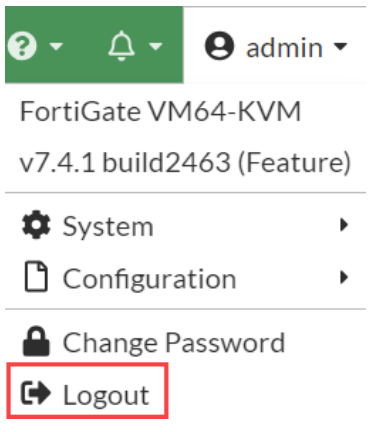
Why is the **Feature set** field not available?

For low-end platforms, the feature is available on the GUI only after you enable the `gui-proxy-inspection` CLI command.

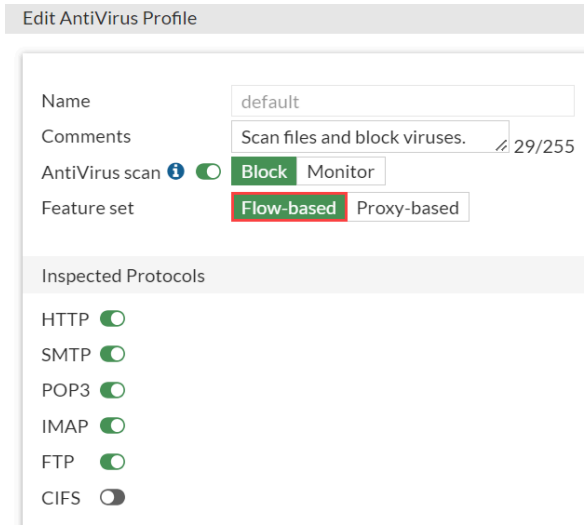
5. Connect to the Local-FortiGate CLI, and then log in with the username `admin` and password `password`.
6. Enter the following commands:

```
config system settings
set gui-proxy-inspection enable
end
```

7. Continuing on the Local-FortiGate GUI, in the upper-right corner, click **admin**, and then click **Logout**.



8. Log in with the username `admin` and password `password`.
9. Click **Security Profiles** > **AntiVirus**.
10. Right-click the **default** antivirus profile, and then click **Edit**.
11. In the **Feature set** field, verify that **Flow-based** is selected.



12. Click **OK**.

Enable the Antivirus Profile on a Firewall Policy

By default, flow-based inspection mode is enabled on the FortiGate firewall policy. You will configure the antivirus profile in the firewall policy.

To configure the firewall policy with the antivirus profile

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, verify that **Flow-based** is selected.

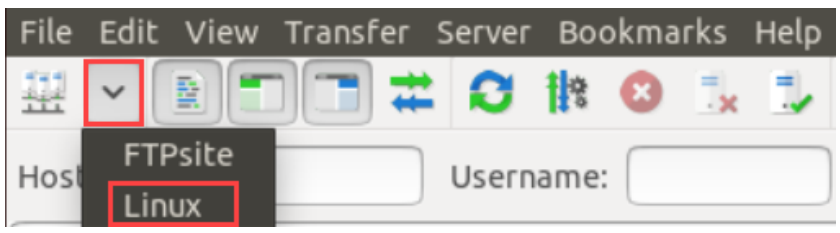
4. In the **Security Profiles** section, enable **AntiVirus**, and then select **default**.
5. Keep the default values for the remaining settings, and then click **OK** to save the changes.

Test the Flow-Based Antivirus Profile

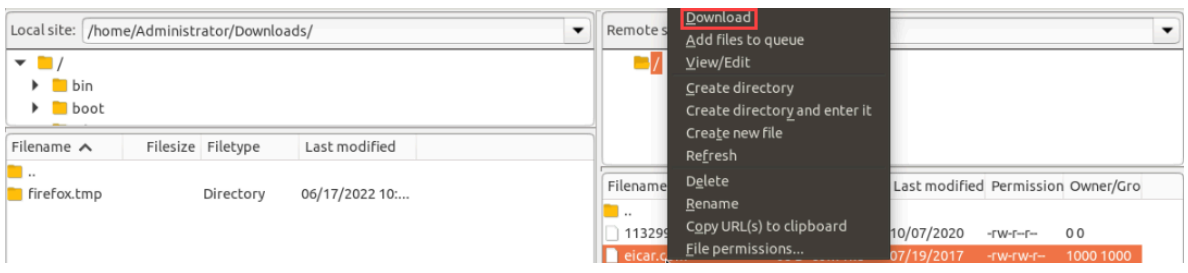
You will test the flow-based antivirus profile using FTP.

To test the antivirus configuration

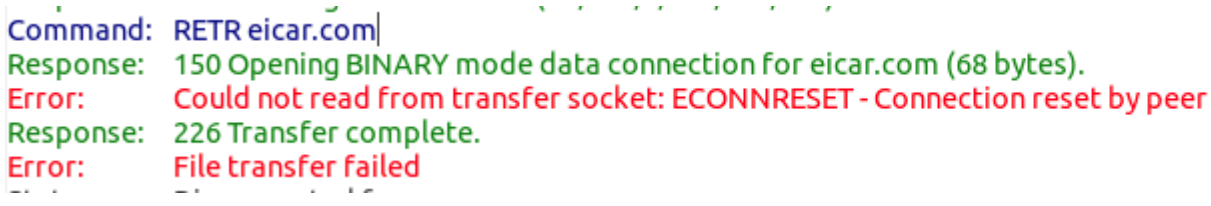
1. On the Local-Client VM, on the desktop, open the FileZilla FTP client software.
2. In the upper-left corner, click the **Site Manager** icon, and then select **Linux**.



3. In the **Remote site** section, 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.



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.

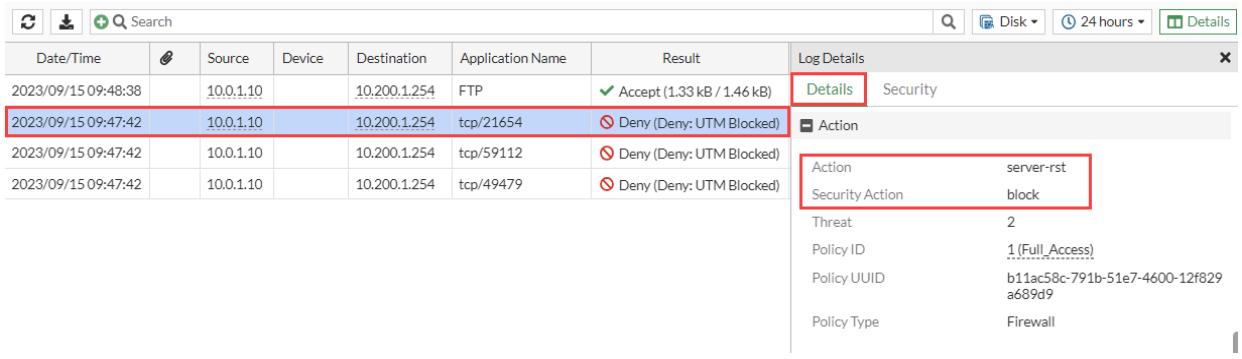
View the Antivirus Logs

The purpose of logs is to help you monitor your network traffic, locate problems, establish baselines, and make adjustments to network security, if necessary. You will view the antivirus logs.

To view the forward logs

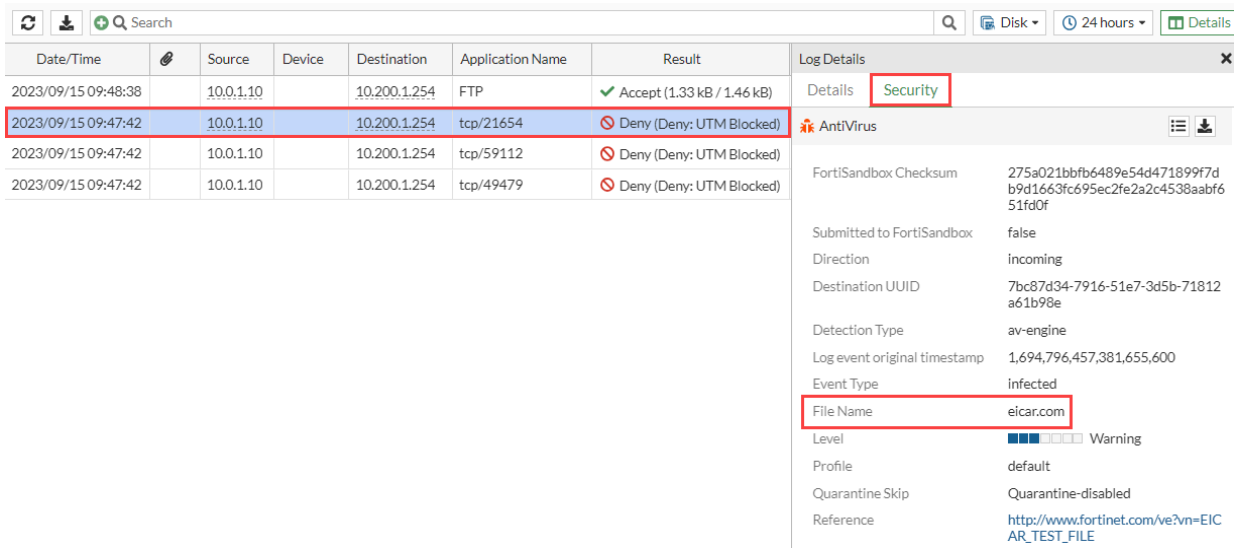
1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.
2. Locate the antivirus log message from when you tried to access the file using FTP, and then double-click the log entry to view the details.

The **Details** tab shows forward traffic log information, along with the action taken.



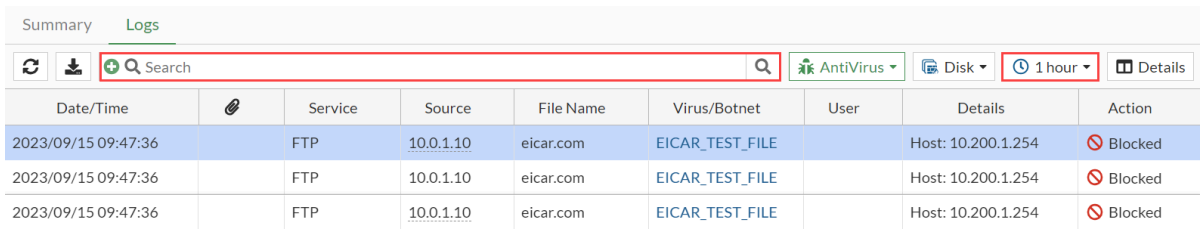
3. Click **Security**.

The **Security** tab shows virus information.



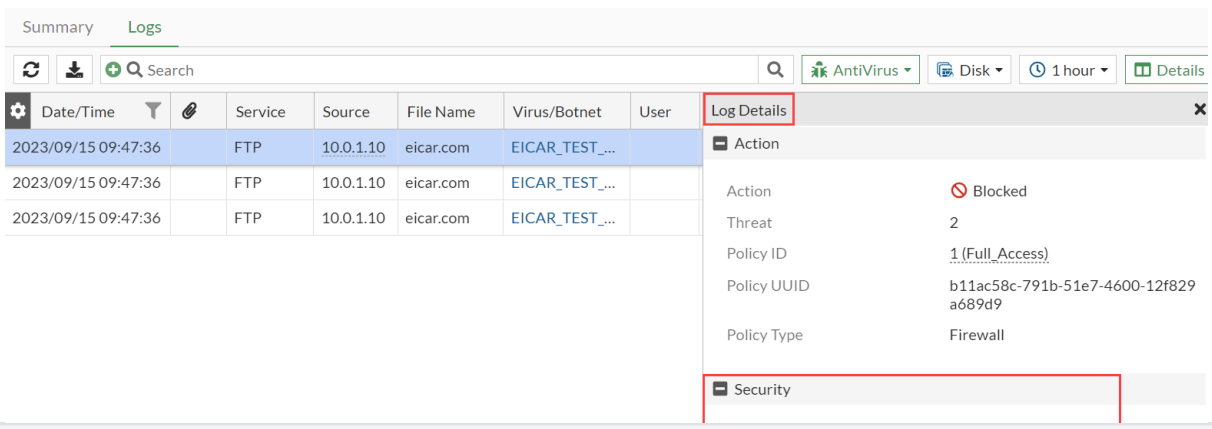
To view the security logs

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



To view the logs, you may need to clear the filters in the search bar and increase the time frame to 1 hour.

2. Locate the antivirus log message from when you tried to access the file using FTP, and then double-click the log entry to view the security details.



Exercise 2: Using Antivirus Scanning in Proxy-Based Inspection Mode

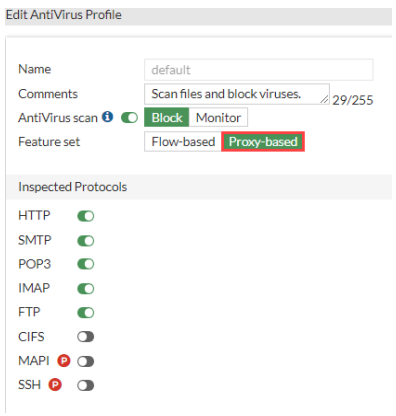
In this exercise, you will examine how to use antivirus in proxy-based inspection mode to understand how FortiGate performs antivirus scanning. You will observe the behavior of antivirus scanning, with and without deep inspection, to understand the importance of performing full-content inspection.

Change the Inspection Mode in an Antivirus Profile

You will change the inspection mode in the default antivirus profile, which is applied to the firewall policy, to inspect traffic.

To change the inspection mode in an antivirus profile

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. Click **OK**.

Change the Inspection Mode in a Firewall Policy

Inspection mode is configured on a per-policy basis on FortiGate. You will change the inspection mode from flow-based to proxy-based.

Take the Expert Challenge!

On the Local-FortiGate GUI, complete the following:

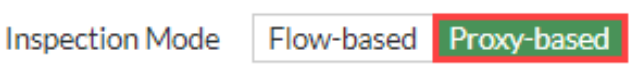
- Edit the **Full_Access** firewall policy, and change the **Inspection Mode** to **Proxy-based**.
- Enable the **default** antivirus profile.
- Use the **certificate-inspection** profile for SSL inspection.

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 1 (#Testing).

To change the inspection mode in 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 **Inspection Mode** field, select **Proxy-based**.



4. In the **Protocol Options** field, verify that the **default** profile is selected.
5. In the **Security Profiles** section, in the **AntiVirus** field, verify that the **default** profile is selected.
6. In the **SSL Inspection** field, 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 field.

7. Keep the default values for the remaining settings, and then 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:

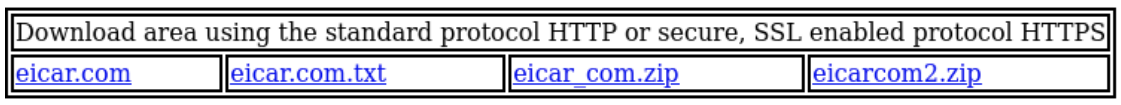
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

To test the antivirus configuration

1. On the Local-Client VM, open a browser, 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.



FortiGate should block the download attempt, and insert a replacement message similar to the following example:

Stop and think!

Why can FortiGate display a replacement message?

In proxy-based inspection mode, the file is buffered. If a virus is detected, FortiGate can then replace the file by a message, which provides security information.

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 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**.

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++**, click **Select** to open the file you downloaded, and then scroll to read the bottom of the text file.

Is the content of the file what it is 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, 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

You will check and confirm the logs for the tests you just performed.

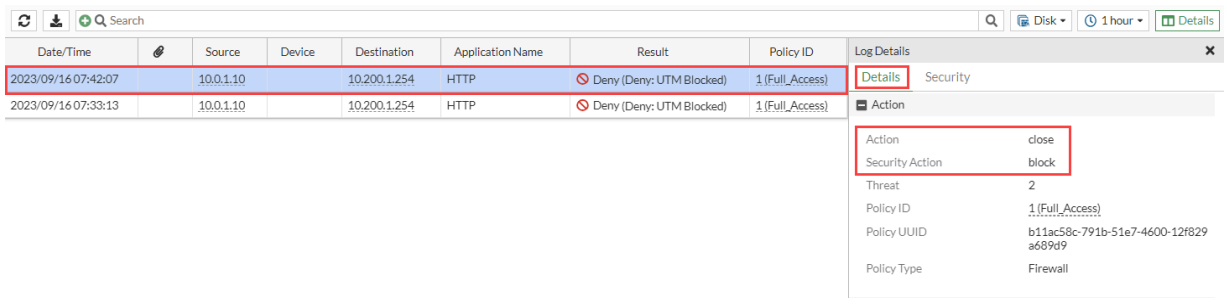
To view the antivirus logs

1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.

You may need to remove any log filter in the search bar and increase the time frame.

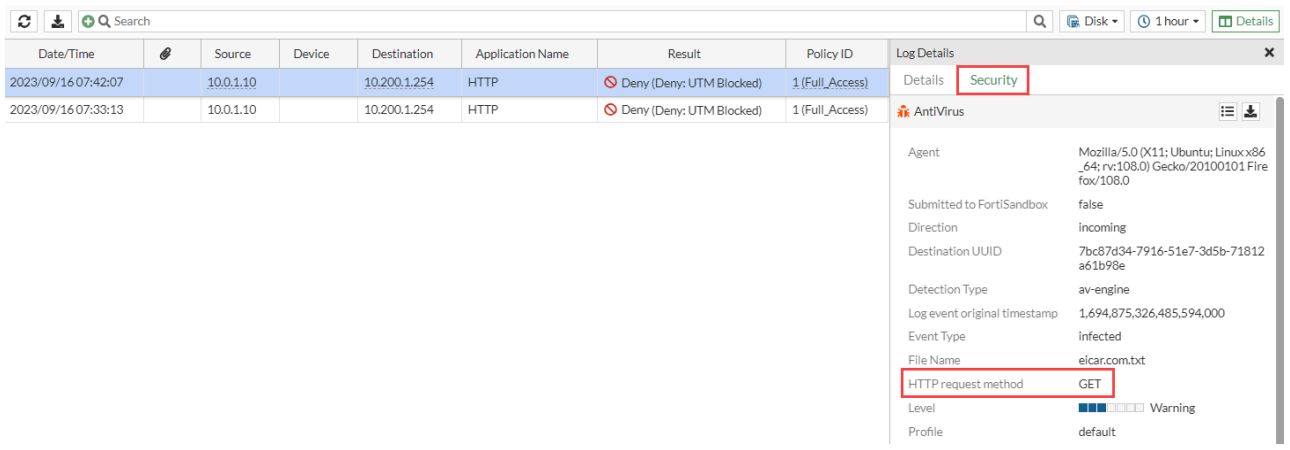
2. Locate the antivirus log message, and then double-click it.

The **Details** tab shows forward traffic log information, along with the action taken.



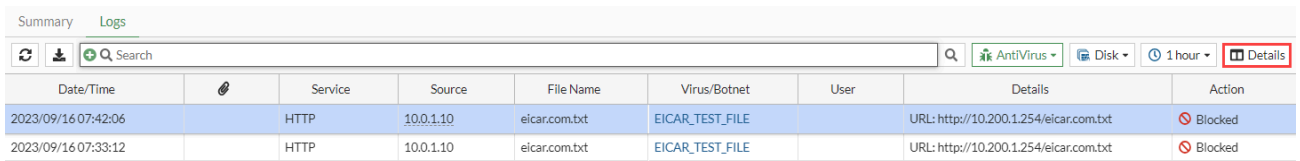
3. Select the **Security** tab to view security logs.

Security logs provide information that is more specific to security events, such as filename, virus or botnet, and reference.



4. Click **Log & Report** > **Security Events** > **AntiVirus** to view antivirus security logs.

The logs should be similar to the following example:



You can click **Details** to view more virus information related to an antivirus log entry.

Enable SSL Inspection in 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 in 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 in the **Full Access** firewall policy.

- Configure Local-FortiGate to scan secure protocols by enabling **SSL Inspection**, using the **deep-inspection** profile in 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.

After you complete the challenge, seeReview the Antivirus History on page 1 (#History).

To test antivirus scanning without SSL inspection enabled in the firewall policy

1. On the Local-Client VM, open a 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.

5. On the Local-Client VM, close the browser.

To enable and test the SSL inspection profile in a firewall policy

1. Return to the Local-FortiGate GUI, and then 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** field, select **deep-inspection**.
4. Keep the remaining default settings, and then click **OK** to save the changes.
5. Click **OK** to confirm.
6. On the Local-Client VM, open a browser, and then go to the same website:

https://10.200.1.254/test_av.html

7. 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 in the browser, end users will see a certificate warning message. In this environment, the FortiGate self-signed SSL inspection certificate is installed in the browser. If the block page does not appear after 2 minutes, close all browser tabs, and then restart the browser.

You may also need to clear your cache. In Firefox, click **Settings** > **Privacy & Security**. Scroll to **History**, click **Clear History**, and then ensure the time range to clear is set to **Everything**. Click **OK**.

FortiGate should block the download and replace it with a message.

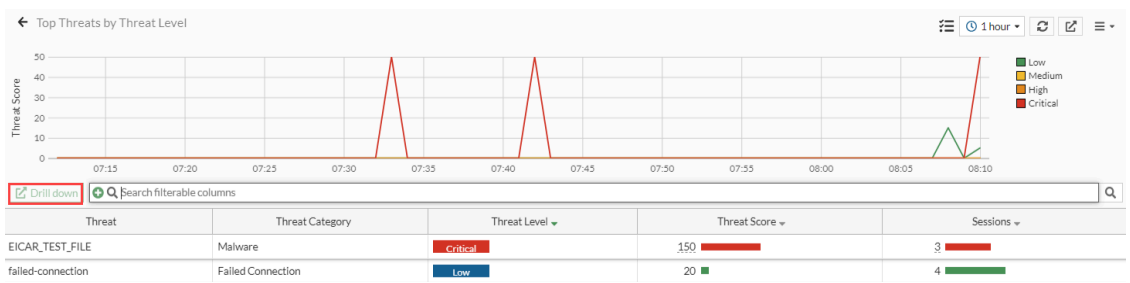
()Review the Antivirus History

You will check the security history and the virus definition status.

To view the security history

1. Continuing on the Local-FortiGate GUI, click **Dashboard** > **Security** > **Top Threats by Threat Level**.

The graph should be similar to the following example:



You can click **Drill down** to view more details about a specific threat.

To verify the antivirus definitions status

1. Connect over SSH to Local-FortiGate.

2. Log in with the username `admin` and password `password`.
3. Enter the following commands:

diagnose debug application update -1

diagnose debug enable

execute update-av

After a few seconds, the output should include information similar to the following example:

```
upd_on_status_change[1153]-VM license number old:0, new:0
upd_on_status_change[1166]-VM vdom number old:0, new:0
installUpdObjRest[1026]-Step 9:Delete backup /tmp/update.backup
installUpdObjRest[1065]-Step 10:Tell parent to respawn
upd_install_pkg[1435]-AVEN028 is up-to-date
upd_install_pkg[1435]-AVDB002 is up-to-date
upd_install_pkg[1435]-AVDB007 is up-to-date
upd_install_pkg[1435]-AVDB019 is up-to-date
upd_install_pkg[1435]-FCNI000 is up-to-date
upd_install_pkg[1435]-FDNI000 is up-to-date
upd_install_pkg[1461]-FSCI000(contract) installed successfully
upd_install_pkg[1435]-FLDB002 is up-to-date
upd_install_pkg[1435]-MMDB001 is up-to-date
upd_install_pkg[1435]-DBDB001 is up-to-date
upd_install_pkg[1435]-SFAS000 is up-to-date
upd_install_pkg[1435]-ALCI000 is up-to-date
upd_status_save_status[135]-try to save on status file
upd_status_save_status[201]-Wrote status file
__upd_act_update[319]-Package installed successfully
upd_comm_disconnect_fds[500]-Disconnecting FMG 10.0.1.241:8890
[206] __ssl_data_ctx_free: Done
[1094] ssl_free: Done
[198] __ssl_cert_ctx_free: Done
[1104] ssl_ctx_free: Done
[1085] ssl_disconnect: Shutdown
do_update[696]-UPDATE successful
```

The output confirms that the device has the latest antivirus packages for correct protection.

4. Enter the following commands:

diagnose debug disable

diagnose debug application update 0

5. Log out of the SSH session and Local-FortiGate GUI.

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 in a firewall policy to inspect the HTTP traffic.

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

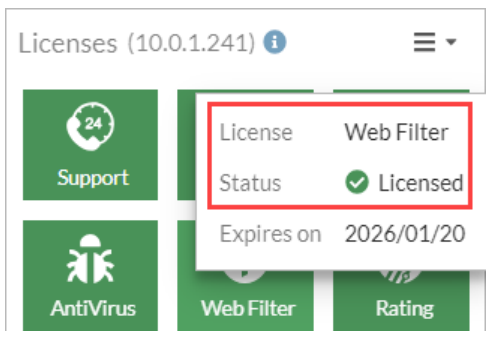
Review the FortiGate Settings

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

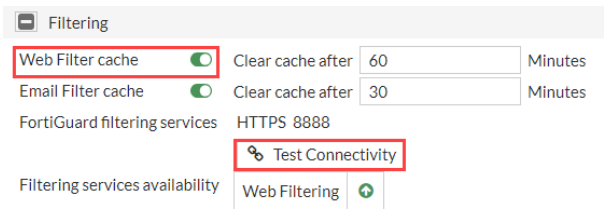
To review the restored settings on FortiGate

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 hover over **Web Filter** to confirm that the service is licensed and active.

You should see information similar to the following example:



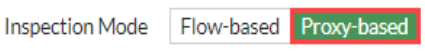
Because of the reboot following the restoration of the configuration file, the web filter license status may be **Unavailable**. In this case, navigate to **System** > **FortiGuard**. In the **Filtering** section, click **Test Connectivity** to force an update, and then click **OK** to confirm. You can confirm, at the same time, that **Web Filter cache** is enabled.



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. In the **Inspection Mode** field, select **Proxy-based**.



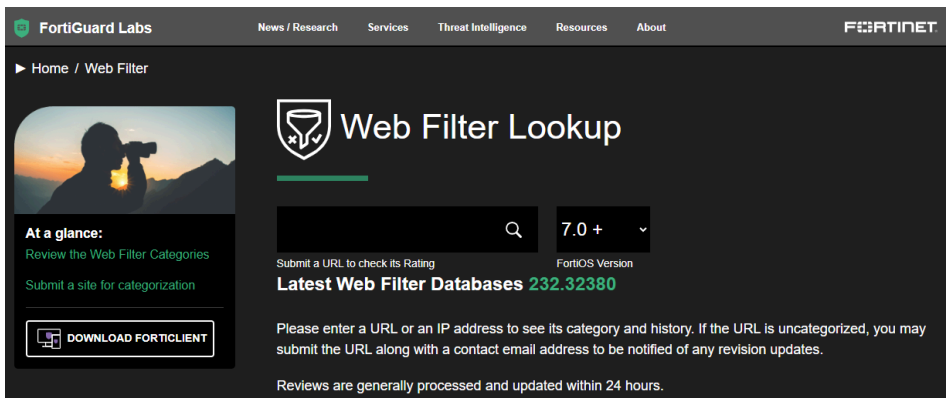
7. Click **OK**.

Determine Web Filter Categories

To configure web filter categories, you must first identify how FortiGuard Web Filtering categorizes specific websites.

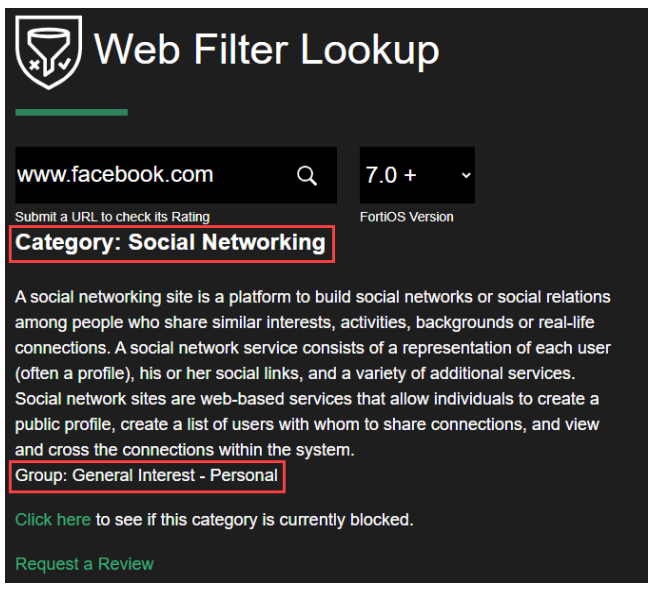
To determine web filter categories

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



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

www.facebook.com (http://www.youtube.com)



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

As you can see, Facebook 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 FortiGate to take based on your web filter security profile:

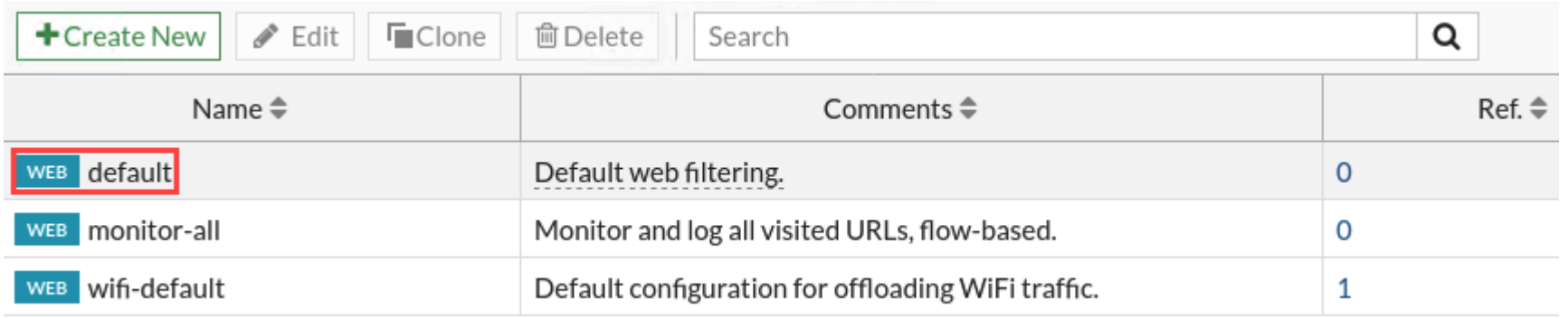
Website	Category	Action
www.facebook.com	Social Networking	Block
www.skype.com	Internet Telephony	Warning
www.bing.com	Search Engines and Portals	Allow
www.ask.com	Search Engines and Portals	Allow

Configure a FortiGuard Category-Based Web Filter

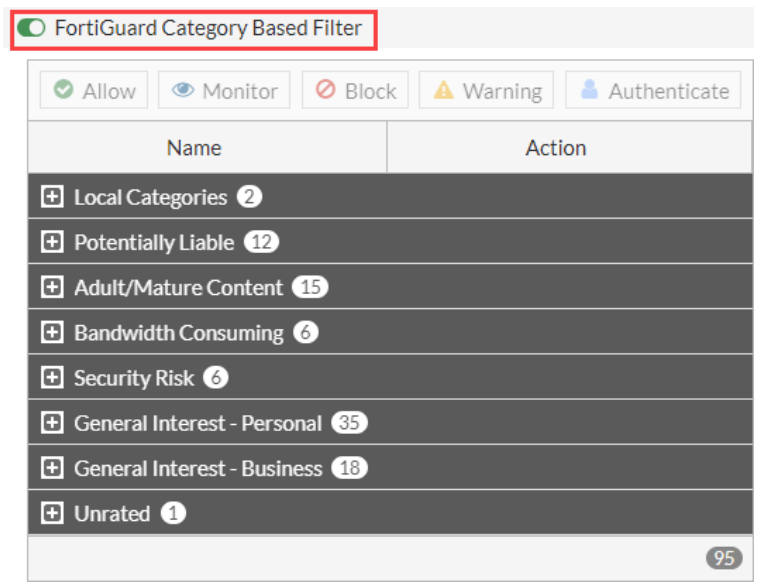
You will review the default web filtering profile, and then configure the FortiGuard category-based filter.

To configure the web filter security profile

1. Return to the Local-FortiGate GUI, and then click **Security Profiles** > **Web Filter**.
2. Double-click the **default** web filter profile to edit it.



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

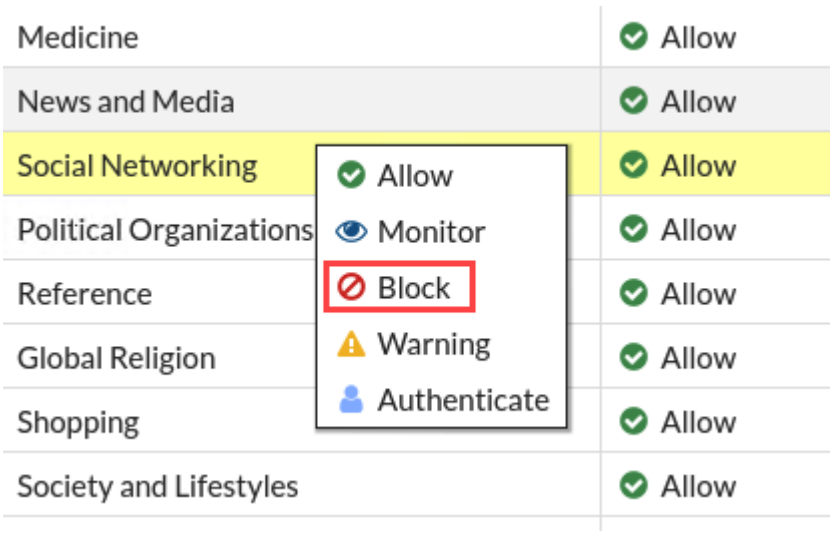


> You can click **+** to expand a category or **-** to collapse a category.

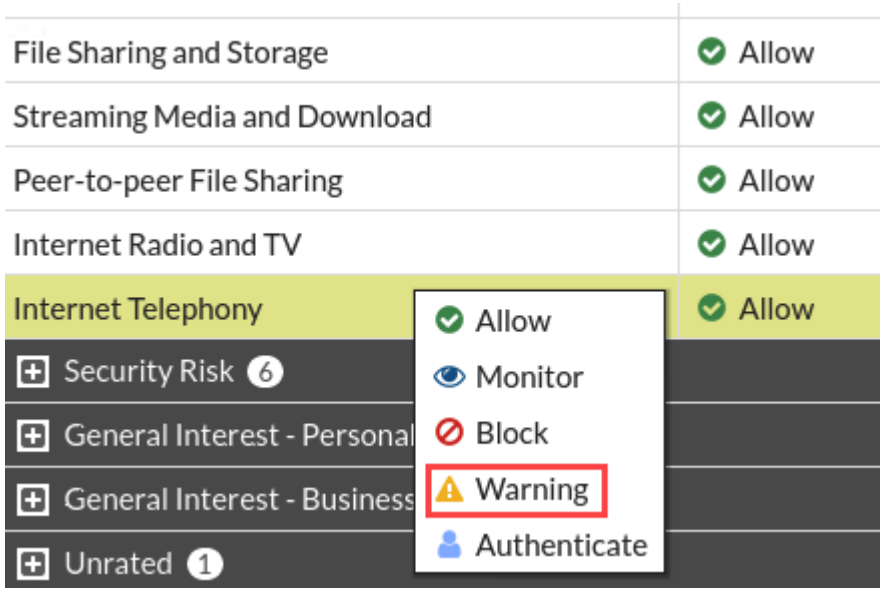
4. Review the default actions for each category.

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**.



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



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

9. Keep the default setting of 5 minutes, and then click **OK**.
10. Click **OK**.

Apply the Web Filter Profile to a Firewall Policy

Now that you have 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!

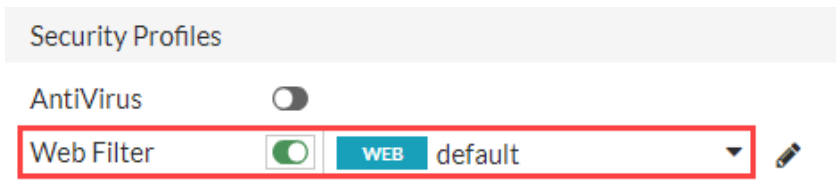
On the Local-FortiGate GUI, apply the web filter profile to the existing **Full_Access** firewall policy. Make sure that logging is also enabled and set to **Security Events**.

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 1 (#Test).

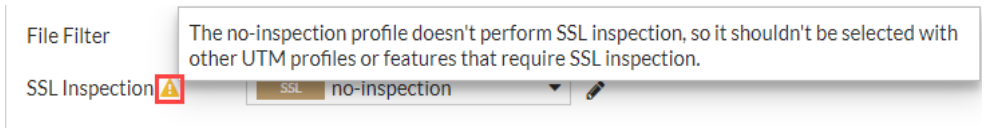
To apply a security profile in a firewall policy

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 select **default**.



4. Hover over the warning sign that appears beside the **SSL Inspection** field.

The message should be similar to the following example:



5. In the **SSL Inspection** field, select **certification-inspection**.

> Because web filtering requires URL information and does not inspect the full payload, you can select **certification-inspection** instead of **deep-inspection**.

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

()Test the Web Filter

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:

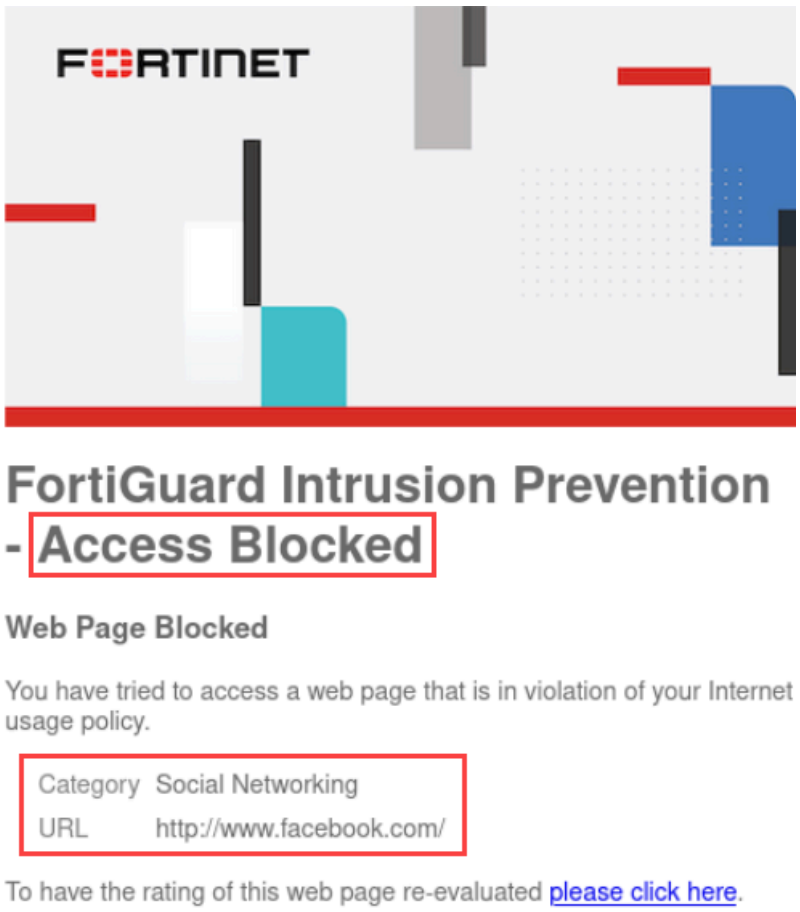
```
get webfilter status
```

The `get webfilter status` and `diagnose debug rating` commands show the list of FDS that 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 2 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 to the public FDS. For this reason, the output of the command lists the FortiManager IP address only.

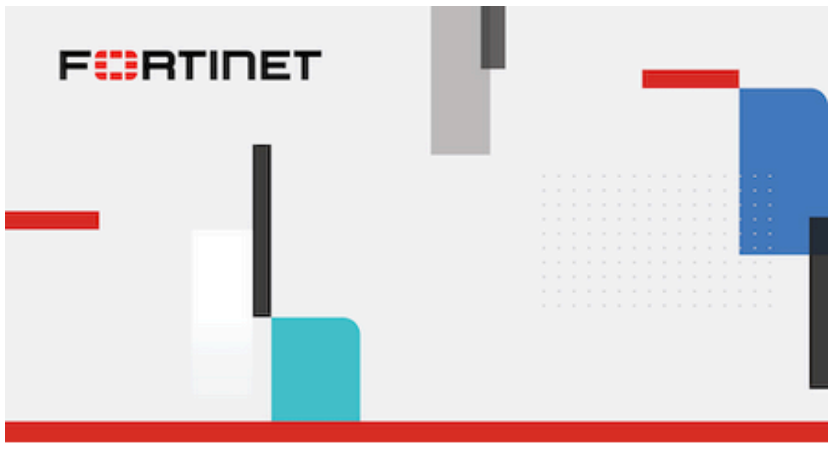
3. On the Local-Client VM, open a new browser tab, and then go to `www.facebook.com`.

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



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.



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**.

7. Close the Local-Client VM browser tabs.

Create a Web Rating Override

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

To create a web rating override

1. Return 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**.

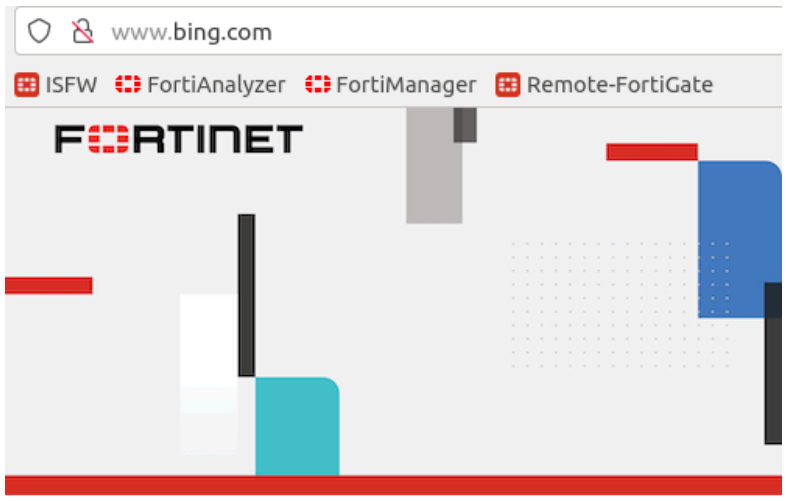
Test the Web Rating Override

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.



Stop and think!

Why is the website `www.bing.com` blocked?

The web rating override changes the category. In the default web profile applied in the firewall policy, the **Malicious Websites** category is set to **Block**. As a consequence, the website `www.bing.com` is now blocked.

Configure an Authenticate Action

You will set the action for the **Malicious Websites** FortiGuard category to **Authenticate**. You will then define a user in order to test the authenticate action.

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** window opens, which allows you to modify the warning interval and select the user groups.

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**.

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

Field	Value
Password	fortinet

5. Click **Next**.
6. Click **Next**.
7. Enable **User Group**, and then 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

To test the web rating override

Exercise 2: Configuring Static URL Filtering

In this exercise, you will configure a static URL filter and apply the security profile to a firewall policy in flow-based inspection mode. You will then review the web filter logs.

Set Up the Static URL Filter in Flow-Based Inspection Mode

You will create a static URL filter entry and change the inspection mode to flow-based.

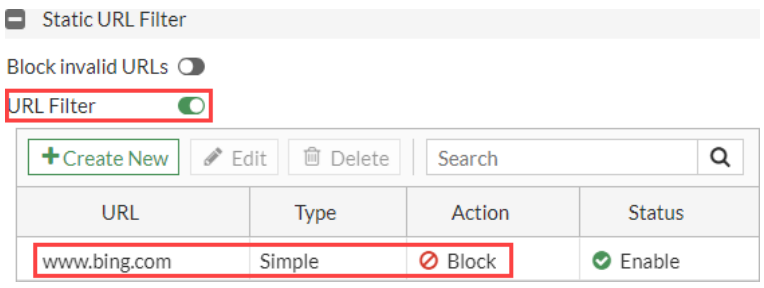
To create a static URL filter

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Security Profiles** > **Web Filter**.
3. Double-click the **default** web filter profile to edit it.
4. In the **Static URL Filter** section, enable **URL Filter**.
5. Click **Create New**, and then configure the following settings:

Field	Value
URL	www.bing.com
Type	Simple
Action	Block
Status	Enable

6. Click **OK**.

Your configuration should match the following example:



7. Click **OK**.

To change the inspection mode to flow-based

1. Continuing on the Local-FortiGate GUI, click **Security Profiles** > **Web Filter**.
2. Double-click the **default** web filter profile to edit it.
3. In the **Feature set** field, select **Flow-based**.

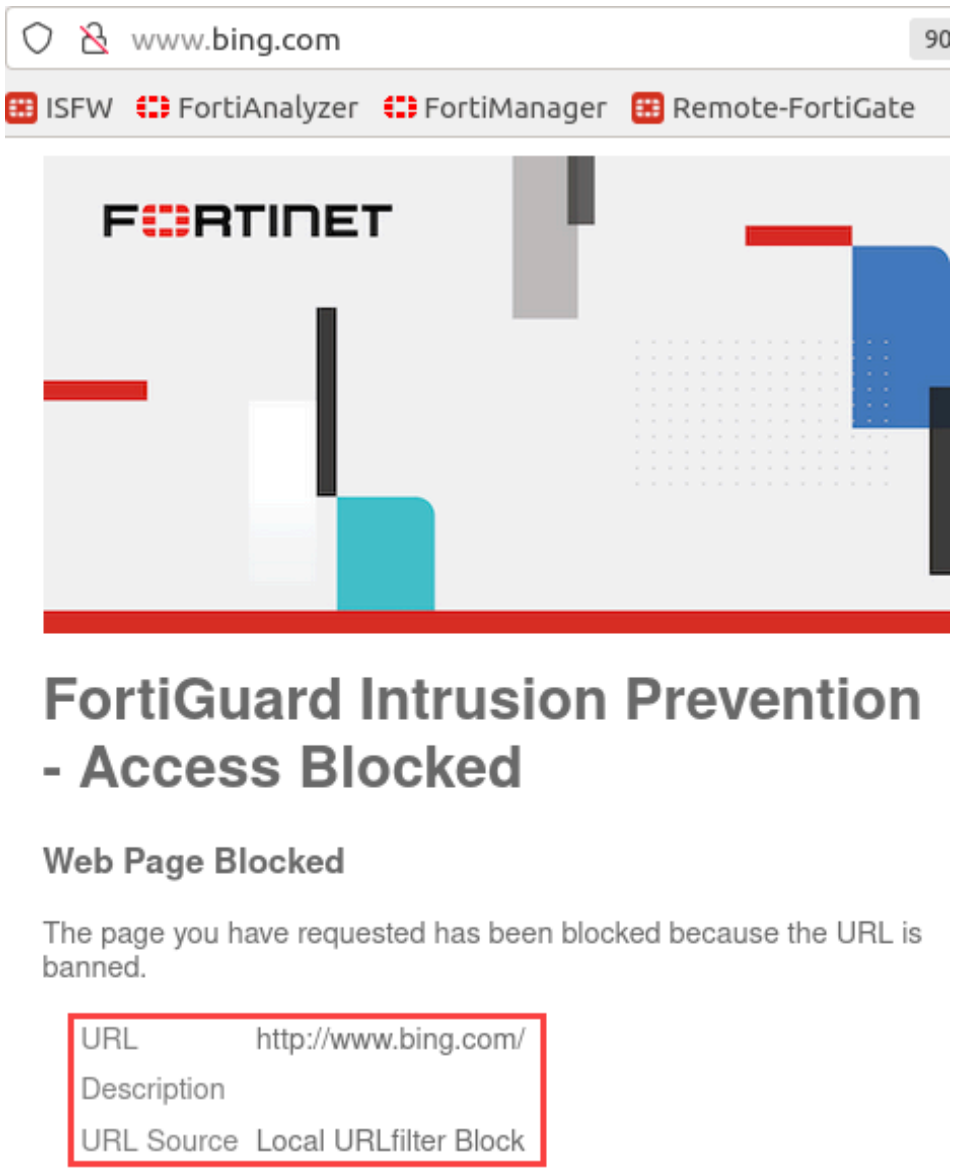
4. Click **OK**.
5. Click **Policy & Objects** > **Firewall Policy**.
6. Double-click the **Full_Access** policy to edit it.
7. In the **Inspection Mode** field, select **Flow-based**.

8. Click **OK**.

To test the static URL filter

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

A warning appears. Notice that it is a different message from the one that appeared before.



Stop and think!

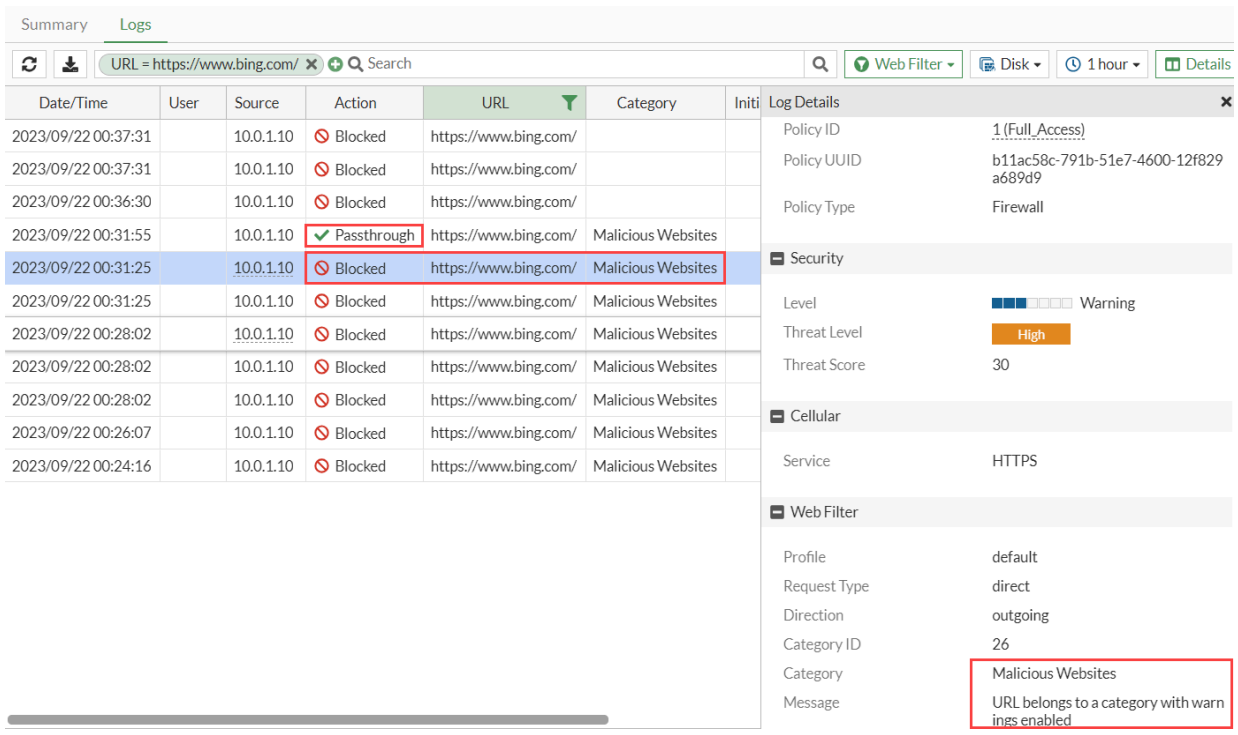
Why is the replacement message different?

FortiGate applies the static URL filter before the FortiGuard category filter. The `www.bing.com` URL matches the URL filter pattern and therefore is now blocked, and FortiGate displays the corresponding URL filter message.

To review the web filter logs

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**.

You should see information similar to the following example:



Stop and think!

Why is the first log entry for the `www.bing.com` website defined as blocked?

Initially, the `www.bing.com` website has the category **Search Engines and Portals**, which was set to **Allow** and does not generate a security log.

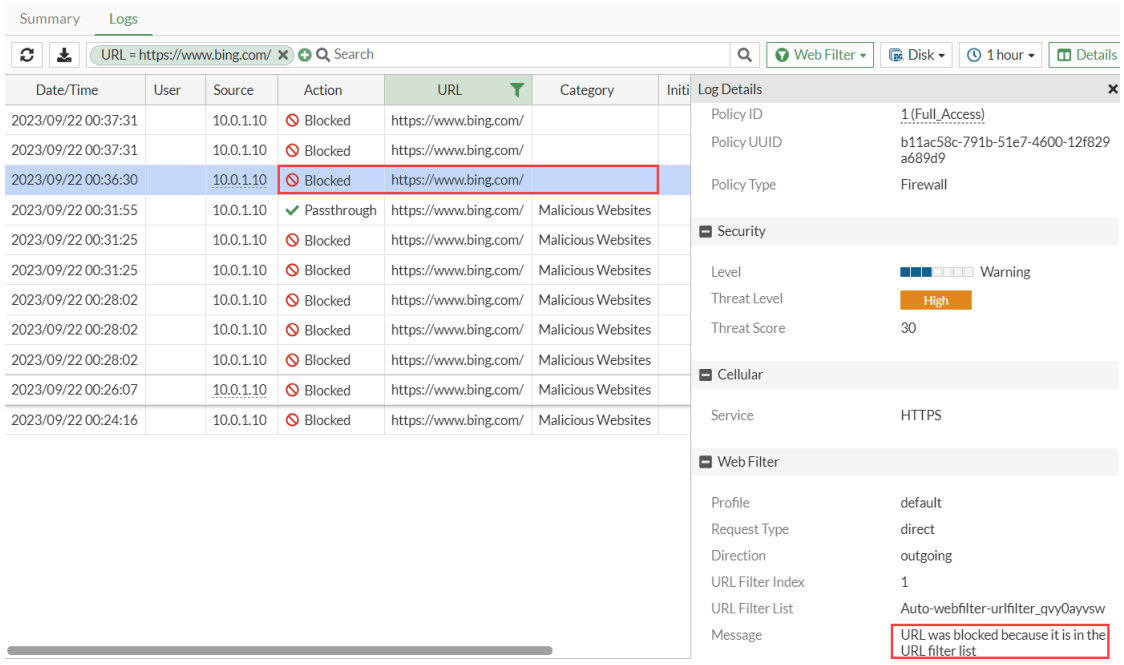
To allow a website and generate a security log at the same time, you must set the category to **Monitor**.

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

Remember that you overrode the **Search Engines and Portals** category to **Malicious Websites**, which was set to **Block**, and then to **Authenticate**.

3. Double-click a log entry with an empty category.

You should see information similar to the following example:



Stop and think!

Why is the category field empty?

Because the website is blocked by the static URL filter, FortiGuard does not apply the FortiGuard web rating, and does not provide the category.

Lab 8: Web Filtering

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

Objectives

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

Time to Complete

Estimated: 30 minutes

LAB-8 > Web Filtering

Exercise 1: Blocking Known Exploits

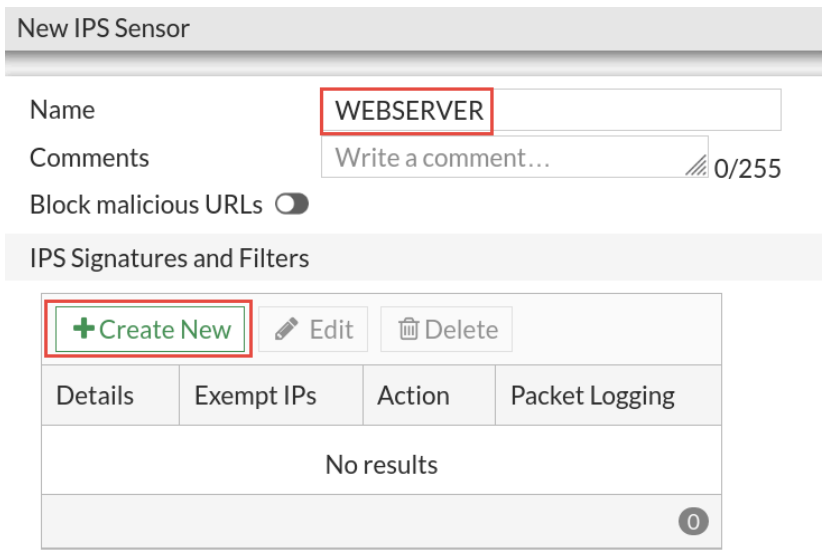
In this exercise, you will configure and monitor IPS inspection on Local-FortiGate.

Configure IPS Inspection

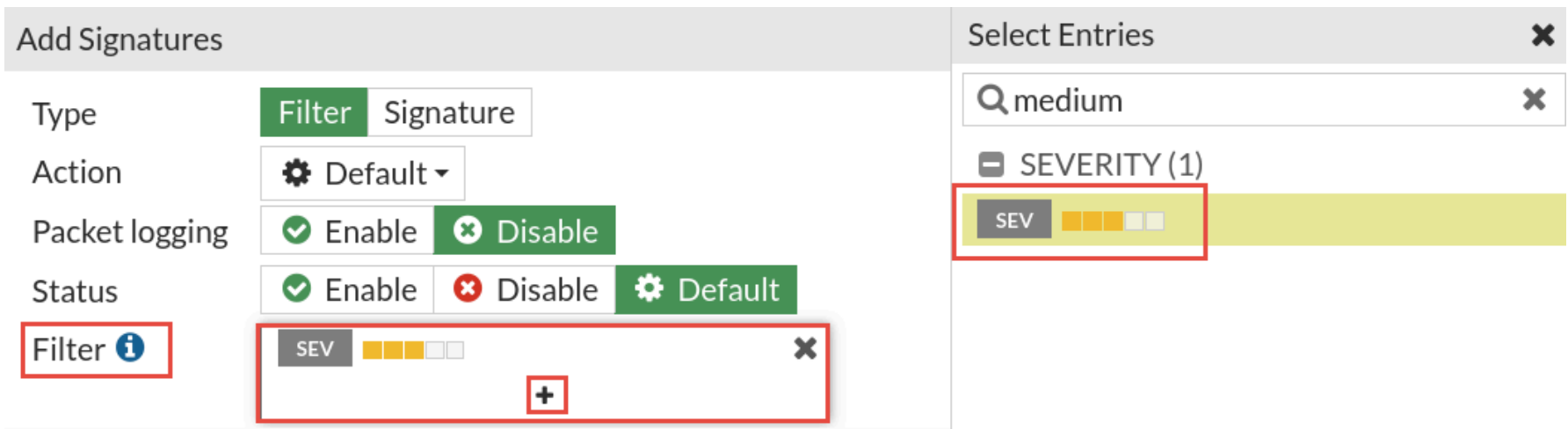
You will configure an IPS sensor that includes the signatures for known attacks based on different severity levels.

To configure IPS inspection

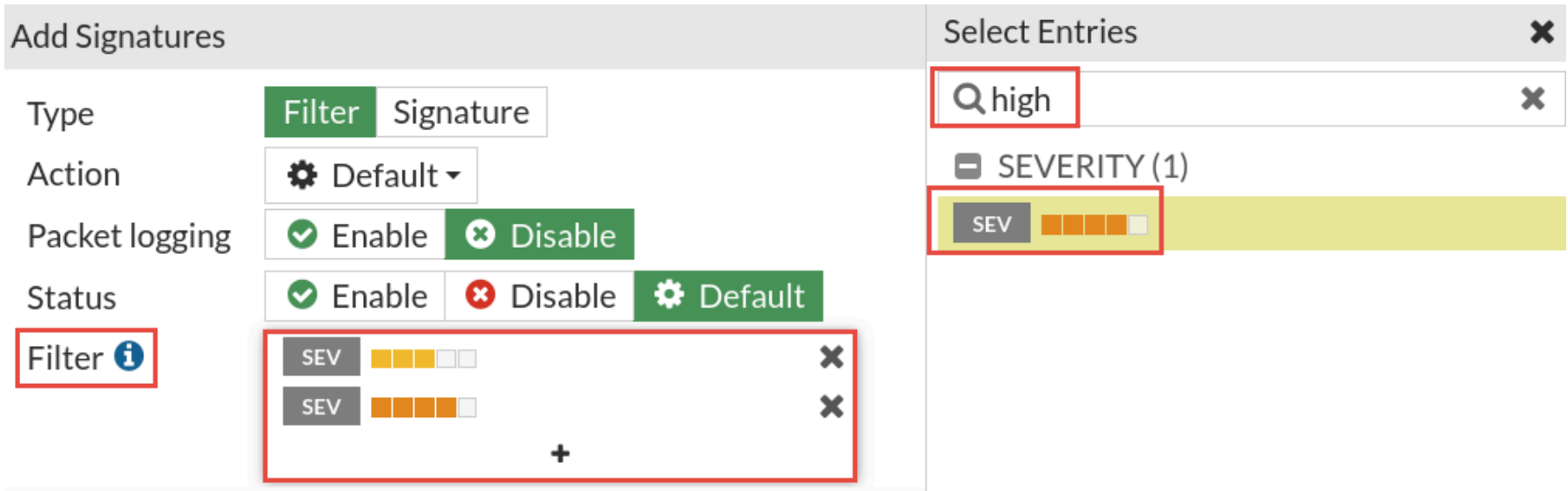
1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Security Profiles** > **Intrusion Prevention**.
3. Click **Create New**.
4. In the **Name** field, type `WEBSERVER`.
5. In the **IPS Signatures and Filters** section, click **Create New**.



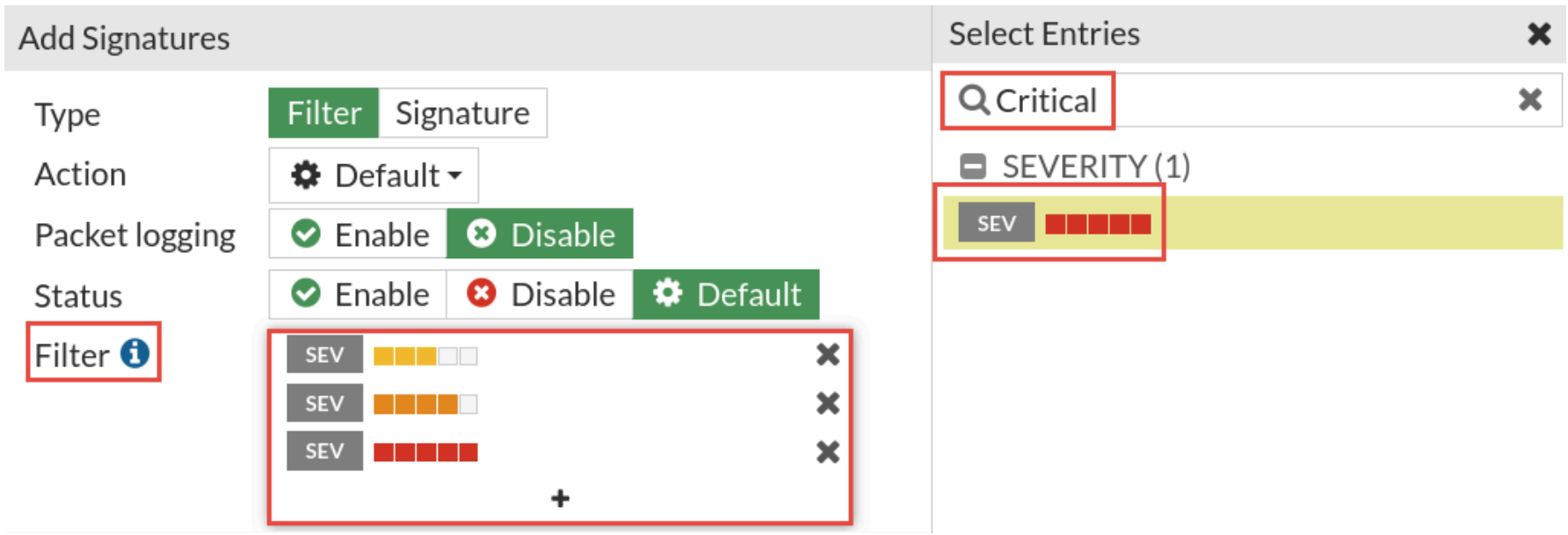
6. In the **Add Signatures** window, click **+** to add a **Filter**.
7. In the search bar, type `medium`, and then click **SEV** to select the medium-severity filter.



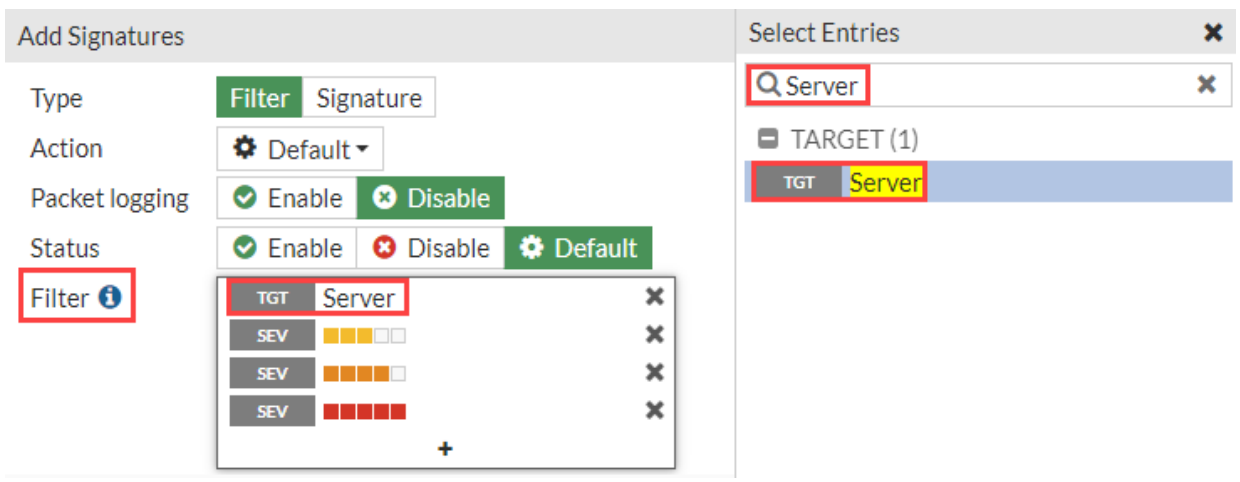
8. In the search bar, delete `medium`, and then type `high`.
9. Click **SEV** to select the high-severity filter.



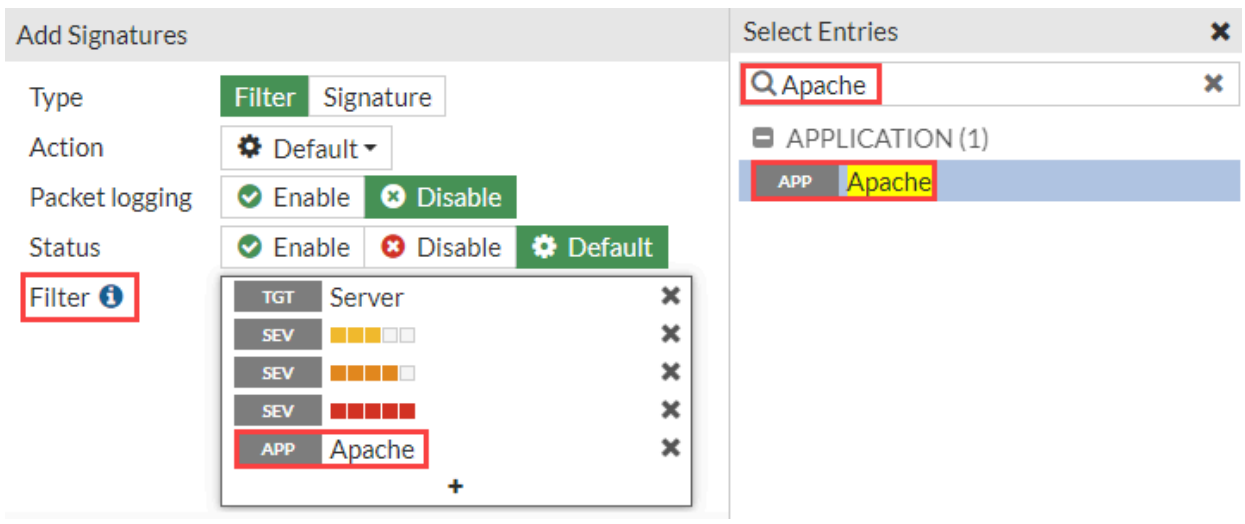
10. In the search bar, delete `high`, and then type `critical`.
11. Click **SEV** to select the critical-severity filter.



12. In the search bar, delete `critical`, and then type `Server`.
13. Click **TGT** to select the server-target filter.



14. Click **OK** to add the selected filters.
15. In the search bar, delete `Server`, and then type `Apache`.
16. Click **App** to select the Apache application filter.



17. Click **OK** to add the selected filters.

Because FortiGate adds all signatures that match the filters to the IPS sensor, you must configure the filters as specifically as possible.

In this exercise, FortiGate protects an Apache server, and takes the default action for the corresponding signatures.

18. 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 VM.

Take the Expert Challenge!

On the Local-FortiGate GUI, do the following:

- Configure a new virtual IP to map the external IP address `10.200.1.200` to the internal IP address `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 1 (#To_Generate_Attacks)

To create a virtual IP

1. Continuing on the Local-Fortigate GUI, click **Policy & Objects** > **Virtual IPs**.
2. Click **Create New**.
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**.

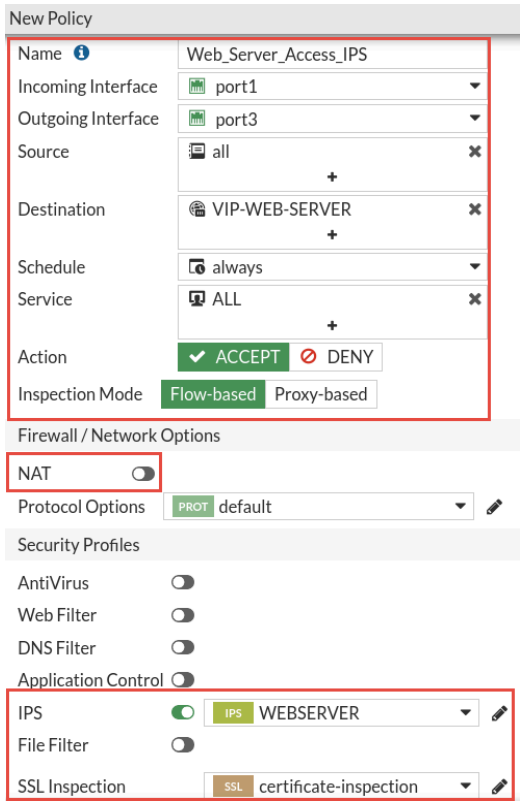
To configure a firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Create New**, and then 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
Schedule	always
Service	ALL
Action	ACCEPT
Inspection Mode	Flow-based
NAT	disabled

3. In the **Security Profiles** section, enable **IPS**, and then in the **IPS** field, select **WEBSERVER**.
4. In the **SSL Inspection** field, select **certificate-inspection**.

The policy should look like the following example:



Using 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.

5. 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 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. Enter the following command to start the attacks:

nikto.pl -host 10.200.1.200

4. Leave the PuTTY session open (you can minimize it) so that 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 that Local-FortiGate is detecting and dropping.

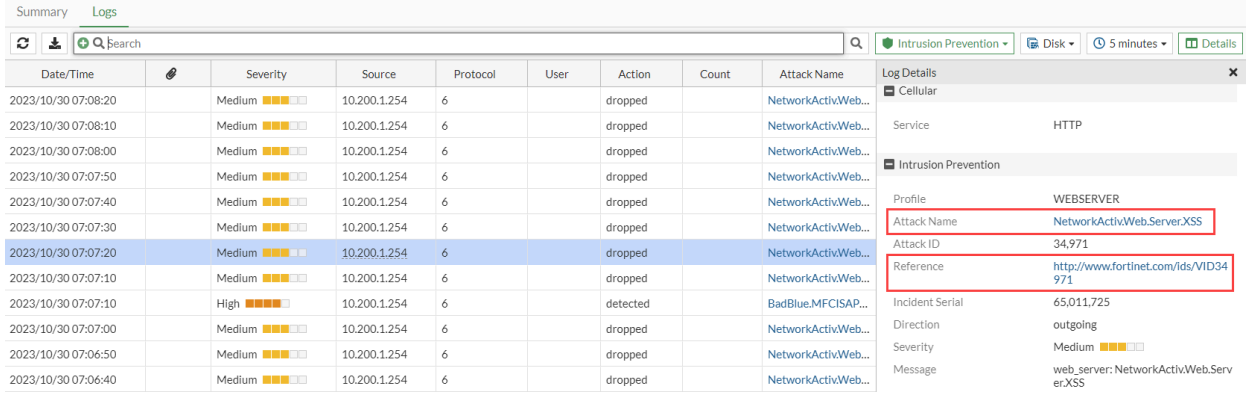
To monitor the IPS

1. Return to the Local-FortiGate GUI, and then 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:

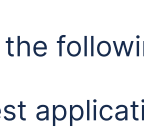
- Detected attack without blocking it
- Dropped attack with blocking it

3. Click a log entry, and then click **Details**.
4. Click the **Attack Name** link.



5. Review the FortiGuard Labs *Threat Encyclopedia* for the signatures.

The FortiGuard Labs *Threat Enclyclopedia* provides information about signatures, such as severity, coverage, affected products, impact, and recommended actions that you can take.



Are the signatures matching the product currently installed on the Local-Client VM? This information is important to make a note of before you tune the **WEBSERVER** IPS sensor. If the signatures do not apply to your product, is it really necessary to inspect those packets?

Troubleshoot IPS Activity

You will troubleshoot and monitor IPS activity.

To troubleshoot IPS activity

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

diagnose test application ipsmonitor 1

The output should be similar to the following example:

```
Local-FortiGate # diag test app ipsmonitor 1
pid = 1949, engine count = 1 (+1)
0 - pid:1990:1990 cfg:1 master:0 run:1
1 - pid:2171:2171 cfg:0 master:1 run:1

pid:          2171 index:1 master
version:      07004000FLEN07600-00007.00004.00509-2308102314
up time:      0 days 0 hours 30 minutes
init time:    0 seconds
socket size: 256(MB)
database:     ipsetdb isdb fmwpdb
bypass:       disable
```

3. Enter the following command to enable the IPS bypass mode:

diagnose test application ipsmonitor 5

If you then enter the `diagnose test application ipsmonitor 1` command, the last line shows the new bypass status of `enable`.

On the Local-FortiGate GUI, you can also verify in **Log & Report** > **Security Events** > **Intrusion Prevention** that no new log entry is generated.

4. Enter the following command to restart the IPS-related engines:

diagnose test application ipsmonitor 99

5. Enter the following command to verify the status:

diagnose test application ipsmonitor 1

Exercise 2: 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.

You will also view the application control logs to confirm that FortiGate identifies applications. Then, you will monitor the traffic that matches the application control profile.

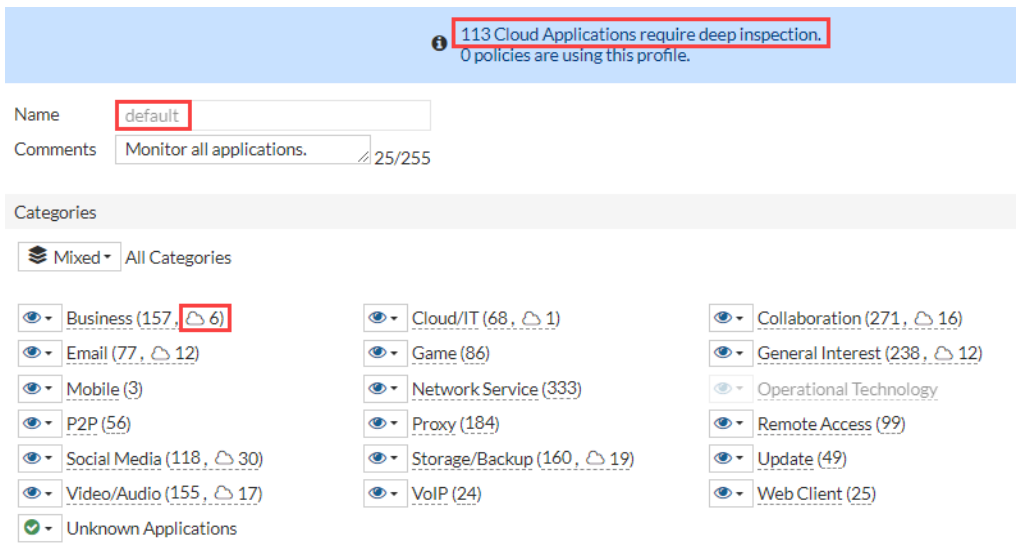
Configure Filter Overrides

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

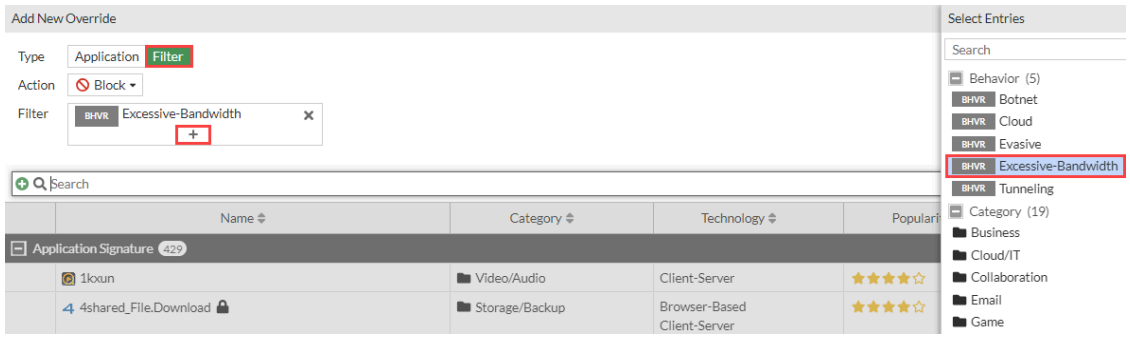
1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **Security Profiles** > **Application Control**.
3. Double-click the **default** application control profile to edit it.



There are 113 cloud-based application signatures available in the application control signatures database that require deep inspection. This number of cloud-based application signatures can vary.

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.

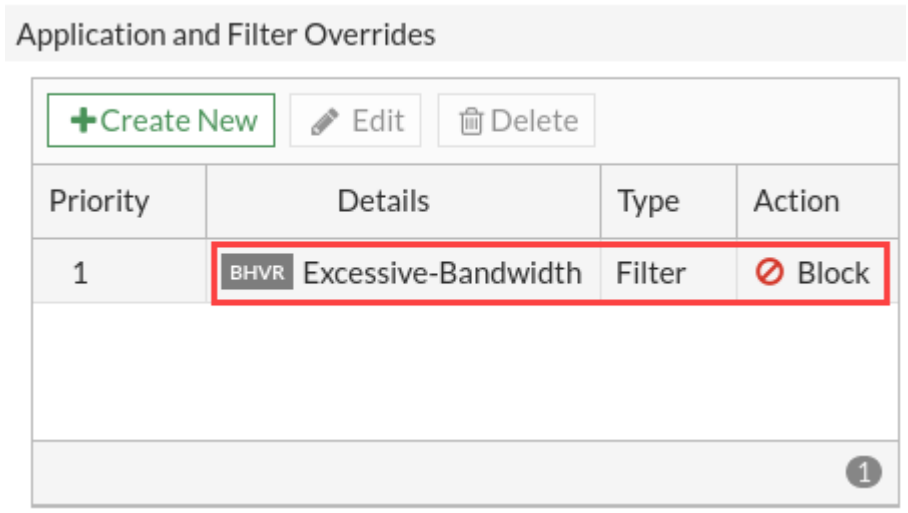
4. In the **Application and Filter Overrides** section, click **Create New** to add a filter override.
5. On the **Add New Override** page, in the **Type** field, select **Filter**.
6. Click **+** to add a filter.
7. Under **BEHAVIOR**, click **Excessive-Bandwidth**.



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**.

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



9. Click **OK**.

Apply the Application Control Profile to the Firewall Policy

Now that you have 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:

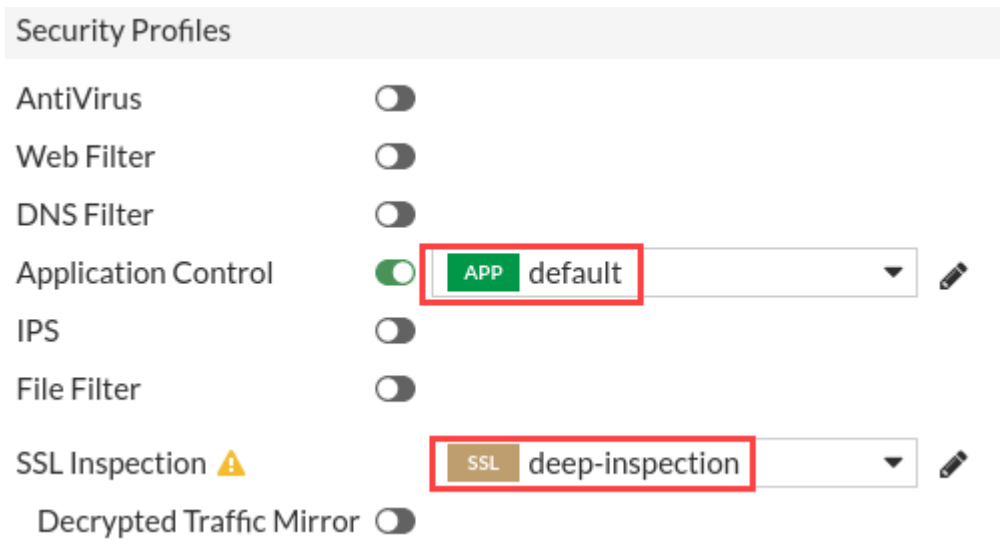
- Enable the **default** application control profile.
- Enable **deep-inspection** in the SSL/SSH inspection profile.

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 1 (#Testing).

To apply the application control profile to the firewall policy

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



If the FortiGate self-signed, full-inspection certificate has not been imported into the browser, end users see a certificate warning message. In this lab environment, the FortiGate self-signed SSL inspection certificate has been imported into the browser.

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

()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

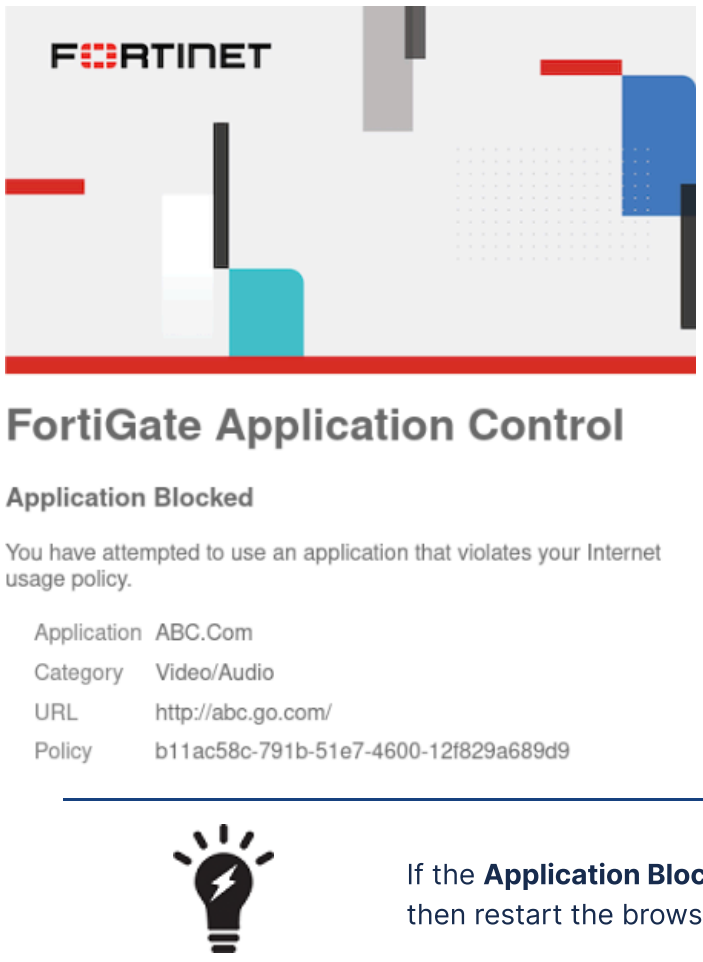
1. On the Local-Client VM, open a new browser tab, and then go to the following URL: `http://abc.go.com`.

You should see that you cannot connect to this site—it times out.

2. Return to the Local-FortiGate GUI, and then click **Security Profiles** > **Application Control**.
3. Double-click the **default** application sensor.
4. In the **Options** section at the bottom of the page, enable **Replacement Messages for HTTP-based Applications**.

5. Click **OK**.
6. On the Local-Client VM, 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 2 minutes for the **Application Blocked** page to appear because of the change in configuration.



If the **Application Blocked** page does not appear after 2 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**.

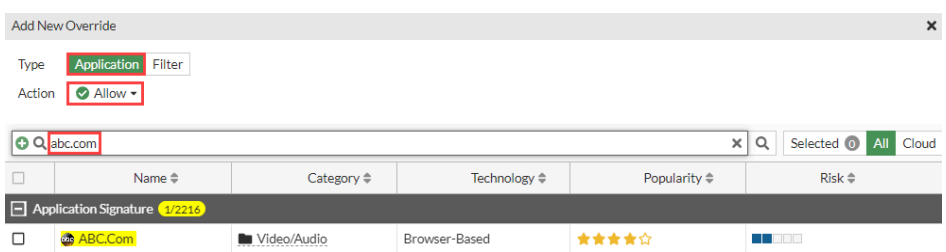
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Test Application Overrides on page 1 (#Testing2).

To configure application overrides

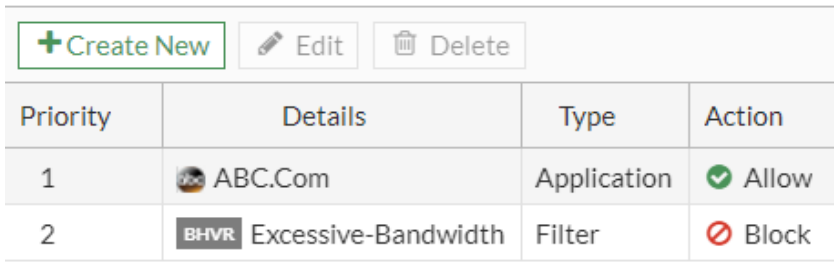
1. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and then click **Security Profiles** > **Application Control**.
2. Double-click the **default** application sensor.
3. In the **Application and Filter Overrides** section, click **Create New**.
4. On the **Add New Override** 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`.

FortiGate returns a signature.



7. Click **ABC.Com** to select it.
8. Click **OK**.
9. Drag the **ABC.Com** application filter and place it above the **Excessive-Bandwidth** filter.

The configuration should look like the following image:



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 and Traffic Matching With the Application Control Profile

You will view the logs and traffic that matched the test you just performed.

To view logs

1. Return 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 that FortiGate took.

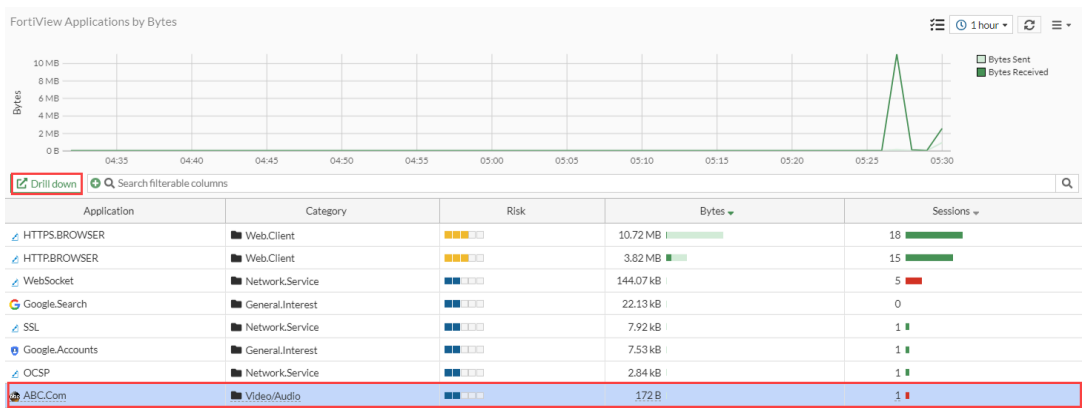
5. Click **Log & Report** > **Forward Traffic**, and then search and view the log information for **ABC.Com**.

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

To view the traffic that matched the application control profile

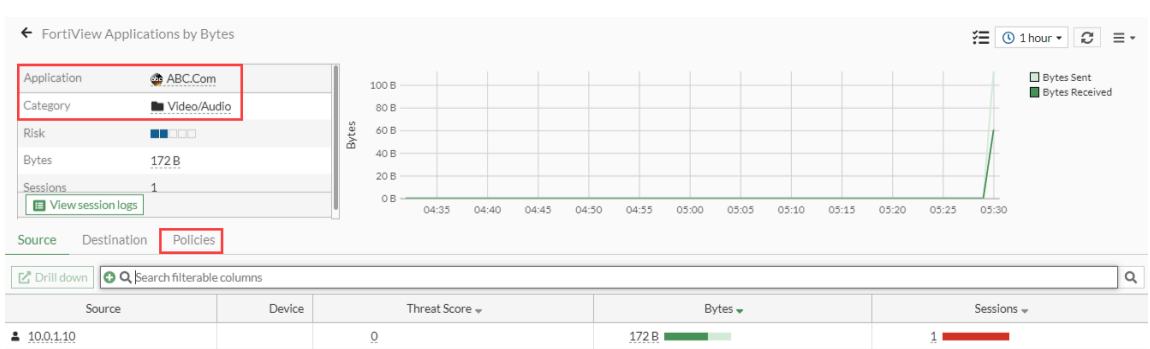
1. On the Local-FortiGate GUI, click **Dashboard** > **FortiView Applications**.

The display should be similar to the following example:



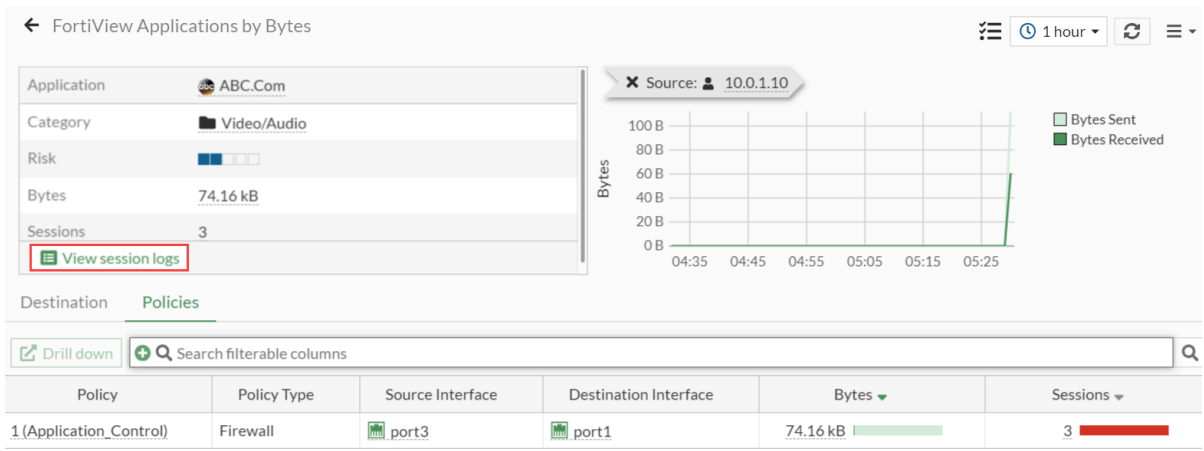
2. Click the line including **ABC.Com** to select it, and then click **Drill down**.

The display should be similar to the following example:



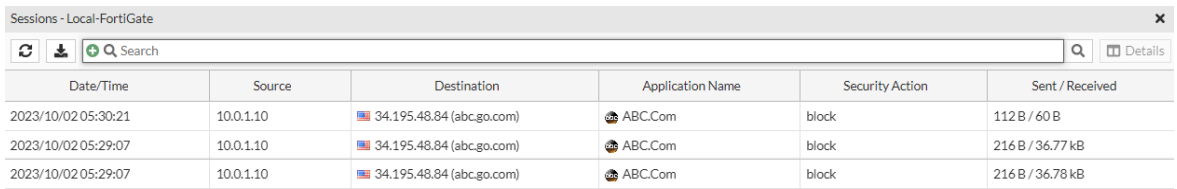
3. Click **Policies**.

The display should be similar to the following example:



4. Click **View session logs**.

The display should be similar to the following example:



You now have the information (bytes, sessions, and policy ID) regarding the traffic that

Lab 9: IPS and Application Control

In this lab, you will set up and monitor intrusion prevention system (IPS) profiles. Next, you will configure and use application control in profile-based mode to apply an appropriate action to specific application traffic. Finally, you will analyze the generated logs.

Objectives

- Protect your network against known attacks using IPS signatures
- Configure and test application control in NGFW profile mode
- Read and understand application control logs

Time to Complete

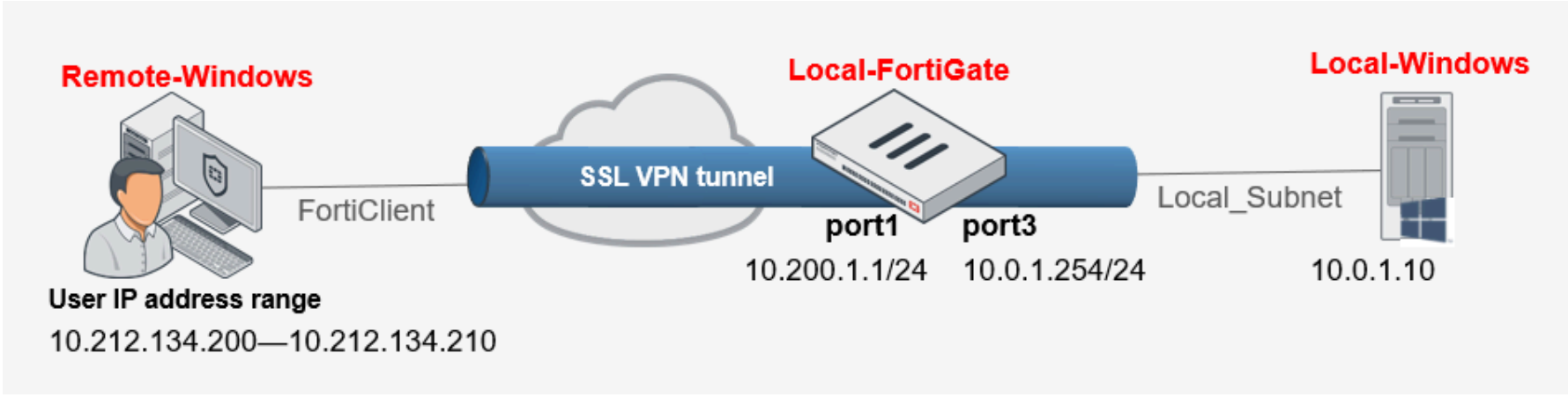
Estimated: 40 minutes
LAB-9 > IPS and Application Control

Exercise 1: Configuring SSL VPN Tunnel Mode

In this exercise, you will examine how to change the SSL VPN settings to allow remote access to the resources in the local subnet (`10.0.1.0/24`), but perform a connection in tunnel mode from the Remote-Client VM.

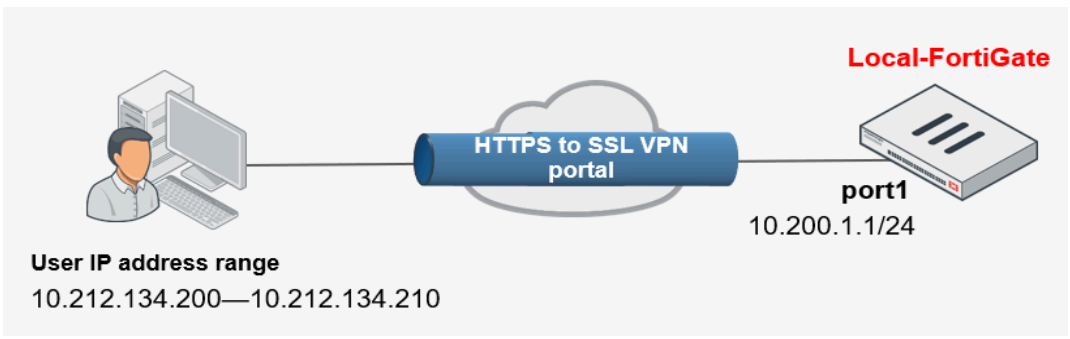
You will use the remote access module of FortiClient, which supports the Fortinet SSL VPN client.

FortiClient is already installed on the Remote-Client VM.



Configure the SSL VPN Settings

You will configure the SSL VPN settings to allow the remote connection shown in the following image:



By default, SSL VPN tunnel mode settings and the **VPN** > **SSL-VPN** menus are hidden on the GUI in FortiOS version 7.4. To enable the GUI menu, enter the following CLI commands:

config system settings

set gui-sslvpn enable

end

The configuration file is preconfigured for you to show the SSL VPN menus.

To create a user for SSL VPN connections

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **User & Authentication** > **User Definition**.
3. Click **Create New**.
4. Click **Local User**, and then click **Next**.
5. Type the following credentials for the remote user, and then click **Next**:

Username	student
Password	fortinet

6. Leave the contact information field empty, and then click **Next**.
7. In the **User Account Status** field, verify that **Enabled** is selected.
8. Enable **User Group**, click **+**, and then in the section on the right, select **SSL_VPN_USERS**.
9. Click **Submit**.

The **SSL_VPN_USERS** group was preconfigured for this lab.

To review the settings of this group, click **User & Authentication** > **User Groups**.

To configure the SSL VPN settings for access

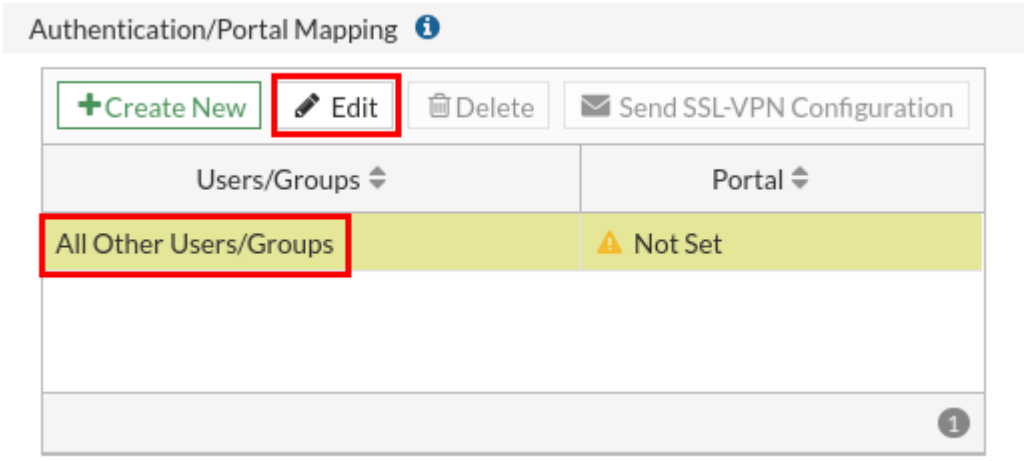
1. Continuing on the Local-FortiGate GUI, click **VPN** > **SSL-VPN Settings**.
2. In the **Connection Settings** section, configure the following settings:

Field	Value
Listen on Interface(s)	port1
Listen on Port	10443
Server Certificate	Fortinet_Factory
Restrict Access	Allow access from any host
Inactive For	3000 seconds

3. In the **Tunnel Mode Client Settings** section, verify the following setting:

Field	Value
Address Range	Automatically assign addresses

4. In the **Authentication/Portal Mapping** section, select **All Other Users/Groups**, and then click **Edit**.



5. In the **Portal** field, select **tunnel-access**, and then click **OK**.
6. Click **Apply** to save the changes.

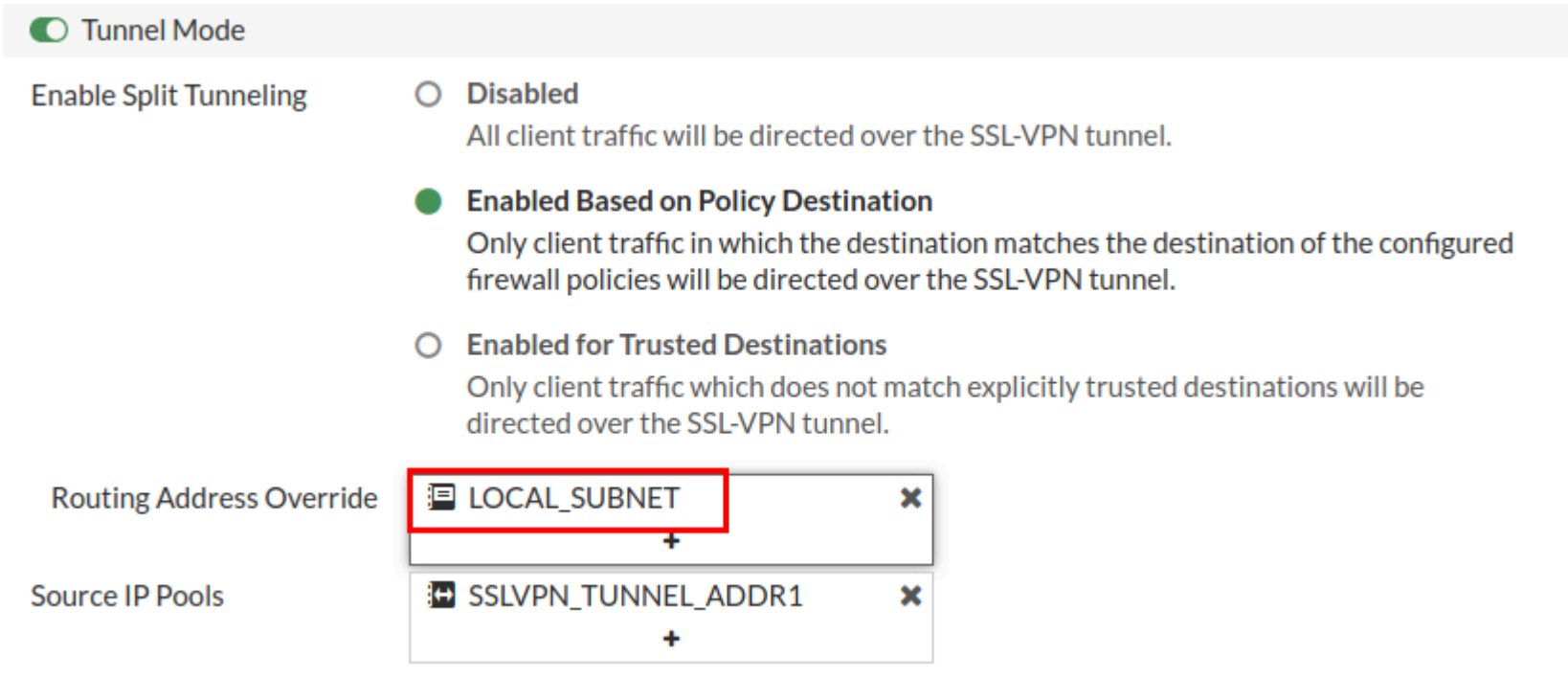
Configure the Routing for Tunnel Mode

You will establish the routing address to use in tunnel mode.

In tunnel mode, FortiClient establishes one or more routes in the SSL VPN user's host after the tunnel is connected. Traffic destined to the internal subnets is correctly routed through the tunnel.

To configure the routing for tunnel mode

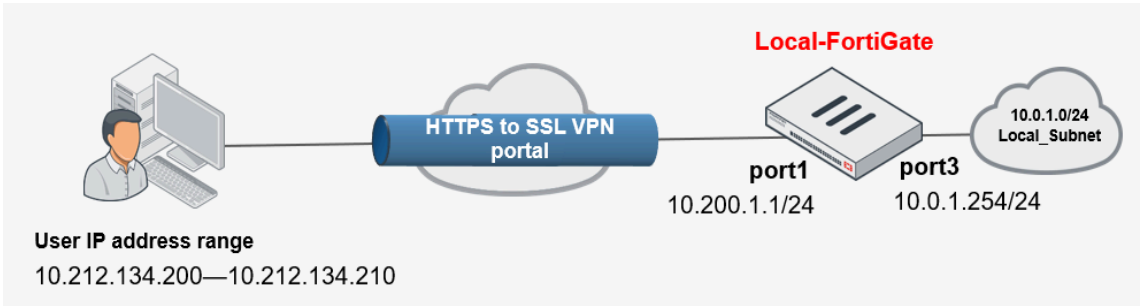
1. Continuing on the Local-FortiGate GUI, click **VPN** > **SSL-VPN Portals**.
2. Select the **tunnel-access** portal, and then click **Edit**.
3. In the **Tunnel Mode** section, in the **Routing Address Override** field, select **LOCAL_SUBNET**.



4. Click **OK**.

Create a Firewall Policy for SSL VPN

You will create a firewall policy that allows traffic to the local subnet (`10.0.1.0/24`) from remote users connected to the SSL VPN.



To create a firewall policy for SSL VPN

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Create New**, and then configure the following firewall policy settings:

Field	Value
Name	SSL-VPN-Access
Incoming Interface	SSL-VPN tunnel interface (ssl.root)
Outgoing Interface	port3
Source	Address > SSLVPN_TUNNEL_ADDR1 User > SSL_VPN_USERS
Destination	LOCAL_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT
Inspection mode	Flow-based
NAT	Disabled

3. Click **OK** to save the configuration.

Configure FortiClient for SSL VPN Connections

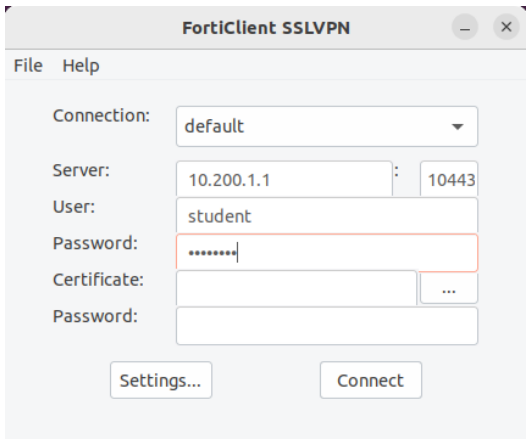
SSL VPN connections in tunnel mode require FortiClient. You will use FortiClient, which is installed on the Remote-Client VM, to test your configuration.

To configure FortiClient for SSL VPN in tunnel mode

1. Connect to the Remote-Client VM with the username `Administrator` and password `password` .
2. Click **Desktop** > **forticlientsslvpn** > **64bit**, and then double-click **forticlientsslvpn** to configure SSL VPN client settings.
3. Configure the following settings for the FortiClient SSL VPN application:

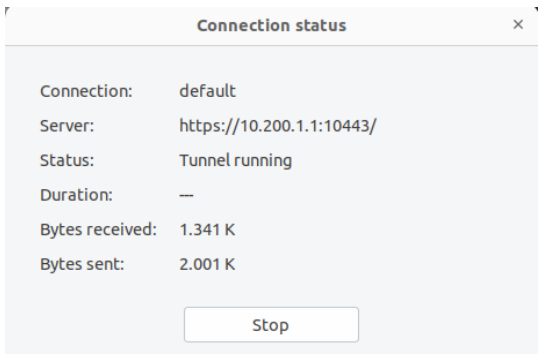
Field	Value
Server	10.200.1.1
Customize port	10443

4. Continuing on the FortiClient SSL VPN application, in the **User** field, type `student` , and then in the **Password** field, type `fortinet` .



5. Click **Connect**.
6. Click **Continue** to accept the certificate.

The tunnel is connected.



To test the tunnel

1. Continuing on the Remote-Client VM, open Firefox, and then access the following URL:

http://10.0.1.10 (http://10.0.1.10)

2. Look at the URL.

You are connected to the web server URL as if you were based in the local subnet (`10.0.1.0/24`).

Monitor an SSL VPN User

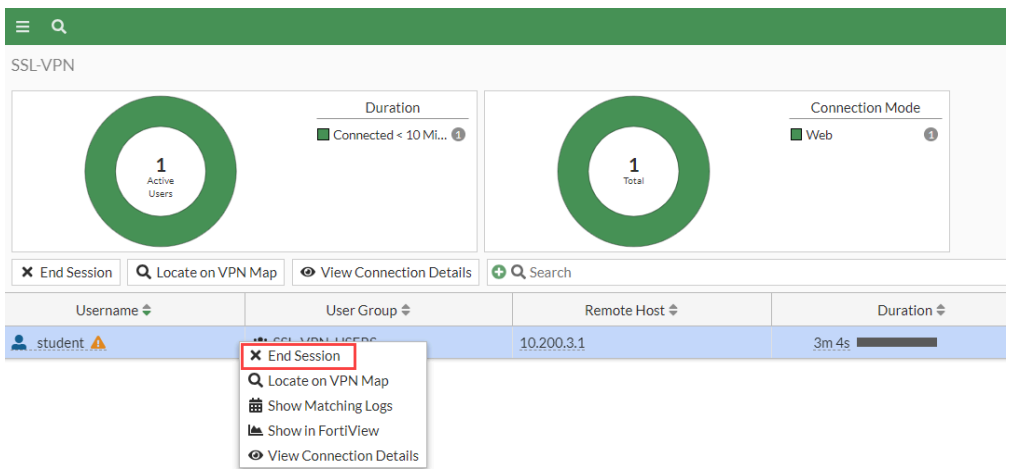
You will monitor and disconnect an SSL VPN user from the FortiGate GUI.

To monitor and disconnect an SSL VPN user

1. Return to the Local-FortiGate GUI.
2. Click **Dashboard** > **Network**, and then view the **SSL-VPN** widget.

You can see that the student user is connecting from the remote host `10.200.3.1` .

3. Right-click **student**, and then select **End Session**.
4. Click **OK**.



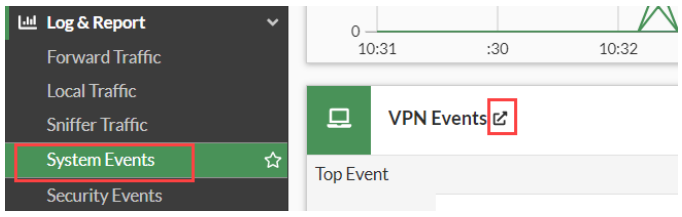
The student user no longer appears in the SSL VPN monitor.

Review VPN Events

You will review the VPN events for the SSL VPN connection you performed in this lab.

To review VPN events for the SSL VPN connection

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password` .
2. Click **Log & Report** > **System Events**, and then expand the **VPN Events** widget to view the logs.

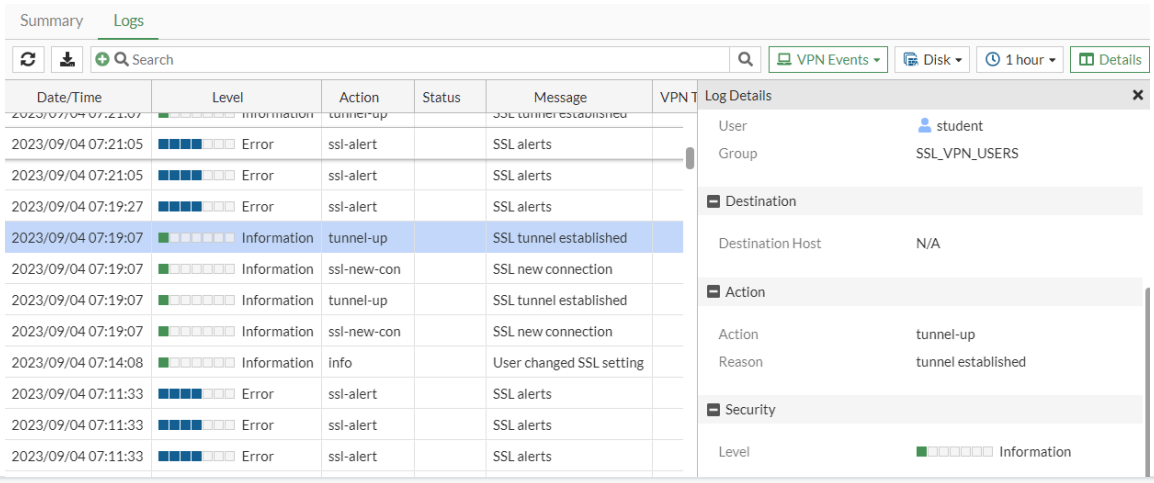


3. View the log details of the **tunnel-up** log you see.

Hint: Use your log filters to filter on **Action** = **tunnel-up**.

The **tunnel-up** log in the VPN event list shows the SSL VPN connection in tunnel mode through FortiClient. Notice this log displays two IP addresses:

- **Remote IP**: IP address of the remote user's gateway (egress interface)
- **Tunnel IP**: IP address FortiGate assigns to the virtual network adapter `fortissl`



Lab 10: SSL VPN

In this lab, you will examine how to configure an SSL VPN connection in tunnel mode. You will also manage user groups and portals for an SSL VPN.

Objectives

- Configure and connect to an SSL VPN
- Enable authentication security
- Configure a firewall policy for SSL VPN users to access private network resources
- Configure FortiClient for the SSL VPN connection in tunnel mode

Time to Complete

Estimated: 30 minutes
LAB-10 > SSL VPN

Exercise 1: Configuring a Dial-Up IPsec VPN Between Two FortiGate Devices

In this exercise, you will configure a dial-up VPN between Local-FortiGate and Remote-FortiGate. Local-FortiGate will act as the dial-up server and Remote-FortiGate will act as the dial-up client.

Create Phase 1 and Phase 2 Negotiations on Local-FortiGate (Dial-Up Server)

You will configure the IPsec VPN by creating phase 1 and phase 2 negotiations.

To create phase 1 and phase 2 negotiations

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **VPN** > **IPsec Tunnels**, and then click **Create New** > **IPsec Tunnel**.
3. Configure the following settings:

Field	Value
Name	ToRemote
Template type	Custom

4. Click **Next**.
5. In the **Network** section, configure the following settings:

Field	Value
Remote Gateway	Dialup User
Interface	port1
Dead Peer Detection	On Idle

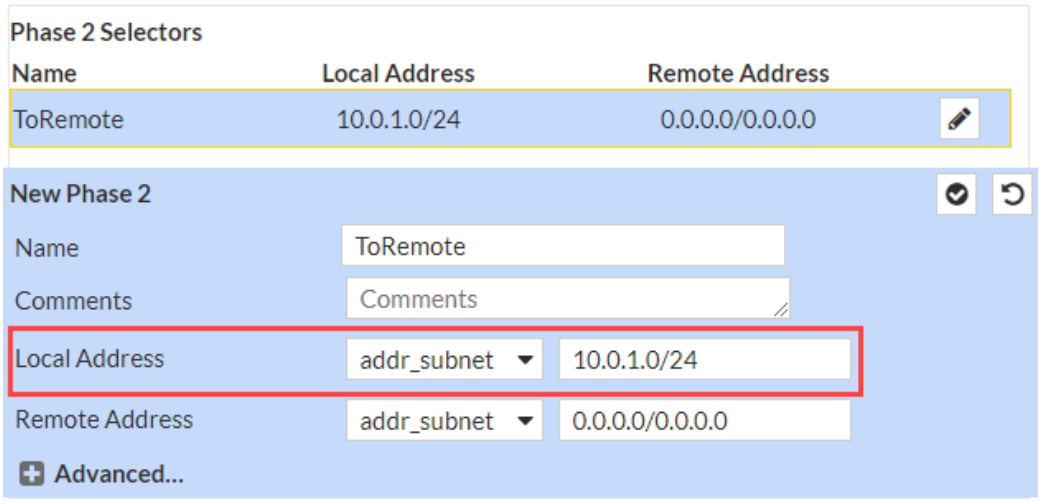
6. In the **Authentication** section, configure the following settings:

Field	Value
Method	Pre-shared Key
Pre-shared Key	fortinet
Version	1
Mode	Aggressive
Accept Types	Specific peer ID
Peer ID	Remote-FortiGate

Setting a peer ID is useful when the FortiGate acting as the dial-up server has multiple dial-up tunnels, and you want dial-up clients to connect to a specific tunnel.

7. In the **Phase 2 Selectors** section, configure the following setting:

Field	Value
Local Address	10.0.1.0/24



8. Keep the default values for the remaining settings.
9. Click **OK**.

- You do not need to add a static route because it is a dial-up VPN. FortiGate dynamically adds or removes appropriate routes to each dial-up peer, each time the peer VPN is trying to connect.
- Even though you could have configured `10.0.2.0/24` as the **Remote Address** instead of `0.0.0.0/0`, it is more convenient to use the latter for scalability purposes. That is, when you have multiple remote peers, each with different remote subnets, using `0.0.0.0/0` as the remote subnet results in the dial-up server accepting any subnet during the tunnel negotiation. This allows multiple remote peers to use the same phase 2 selector configuration.
- This exercise has only one remote peer (Remote-FortiGate). Local-FortiGate then learns about the remote subnet `10.0.2.0/24` when Remote-FortiGate connects to the tunnel. However, if there are more remote peers with different remote subnets, you do not need to change the existing dial-up server configuration for the additional remote peers to be able to connect.

Create Firewall Policies for VPN Traffic on Local-FortiGate (Dial-Up Server)

You will create two firewall policies between **port3** and **To Remote**—one for each traffic direction.

To create firewall policies for VPN traffic

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

Field	Value
Name	Remote_out
Incoming Interface	port3
Outgoing Interface	ToRemote
Source	HQ_SUBNET
Destination	BRANCH_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

4. In the **Firewall/Network Options** section, disable **NAT**.
5. Click **OK**.
6. Click **Create New** again.
7. Configure the following settings:

Field	Value
Name	Remote_in

Field	Value
Incoming Interface	ToRemote
Outgoing Interface	port3
Source	BRANCH_SUBNET
Destination	HQ_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

8. In the **Firewall/Network Options** section, disable **NAT**.
9. Click **OK**.

ID	Name	Source	Destination	Schedule	Service	Action	NAT
port3 → port1 1							
port3 → ToRemote 1							
2	Remote_out	HQ_SUBNET	BRANCH_SUBNET	always	ALL	ACCEPT	Disabled
ToRemote → port3 1							
3	Remote_in	BRANCH_SUBNET	HQ_SUBNET	always	ALL	ACCEPT	Disabled

Create Phase 1 and Phase 2 on Remote-FortiGate (Dial-Up Client)

You will create phase 1 and phase 2 on Remote-FortiGate.

To create phase 1 and phase 2

1. Connect to the Remote-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **VPN** > **IPsec Tunnels**, and then click **Create New** > **IPsec Tunnel**.
3. Configure the following settings:

Field	Value
Name	ToLocal
Template type	Custom

4. Click **Next**.
5. In the **Network** section, configure the following settings:

Field	Value
Remote Gateway	Static IP Address
IP Address	10.200.1.1
Interface	port4
Dead Peer Detection	On Idle

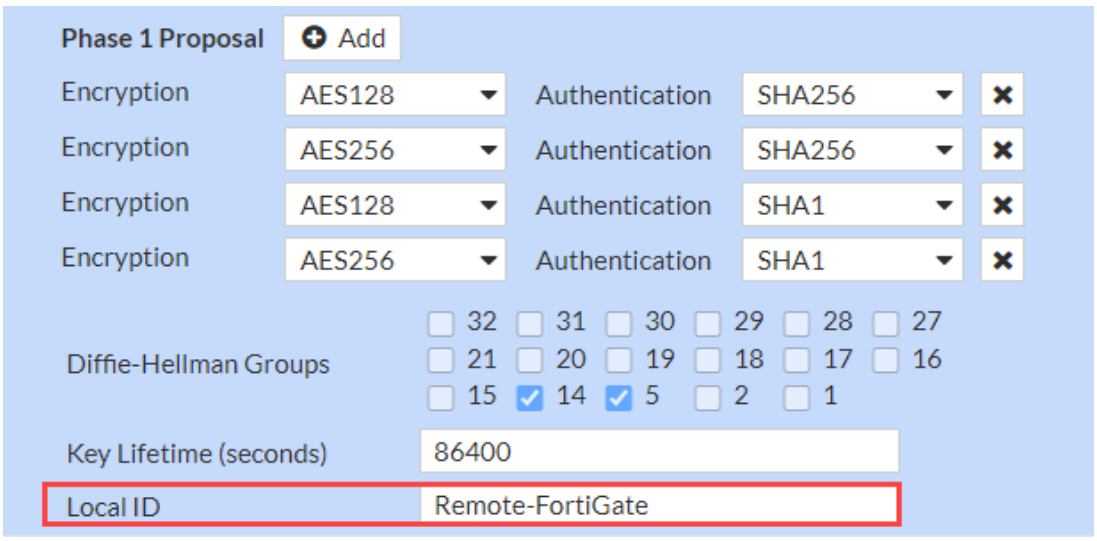
6. In the **Authentication** section, configure the following settings:

Field	Value
Method	Pre-shared Key
Pre-shared Key	fortinet
Version	1

Field	Value
Mode	Aggressive
Accept Types	Any peer ID

7. In the **Phase 1 Proposal** section, configure the following setting:

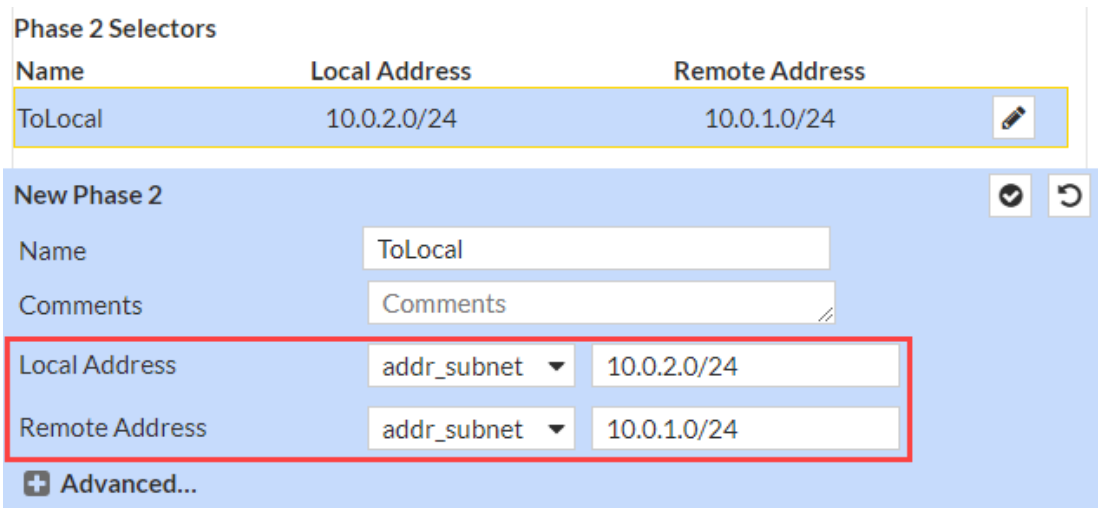
Field	Value
Local ID	Remote-FortiGate



> The local ID should be the same as the peer ID that you configured on Local-FortiGate, which is acting as the dial-up server.
>
> Note that the **Peer ID** and **Local ID** fields are case sensitive.

8. In the **Phase 2 Selectors** section, configure the following settings:

Field	Value
Local Address	10.0.2.0/24
Remote Address	10.0.1.0/24



9. Keep the default values for the remaining settings.
10. Click **OK**.

> Except for the **Local Address** and **Remote Address** settings, all phase 1 and phase 2 settings on both VPN peers mirror each other. For dial-up IPsec VPN, the local and remote addresses do not have to mirror each other for the tunnel to come up.

Create a Static Route for VPN Traffic on Remote-FortiGate (Dial-Up Client)

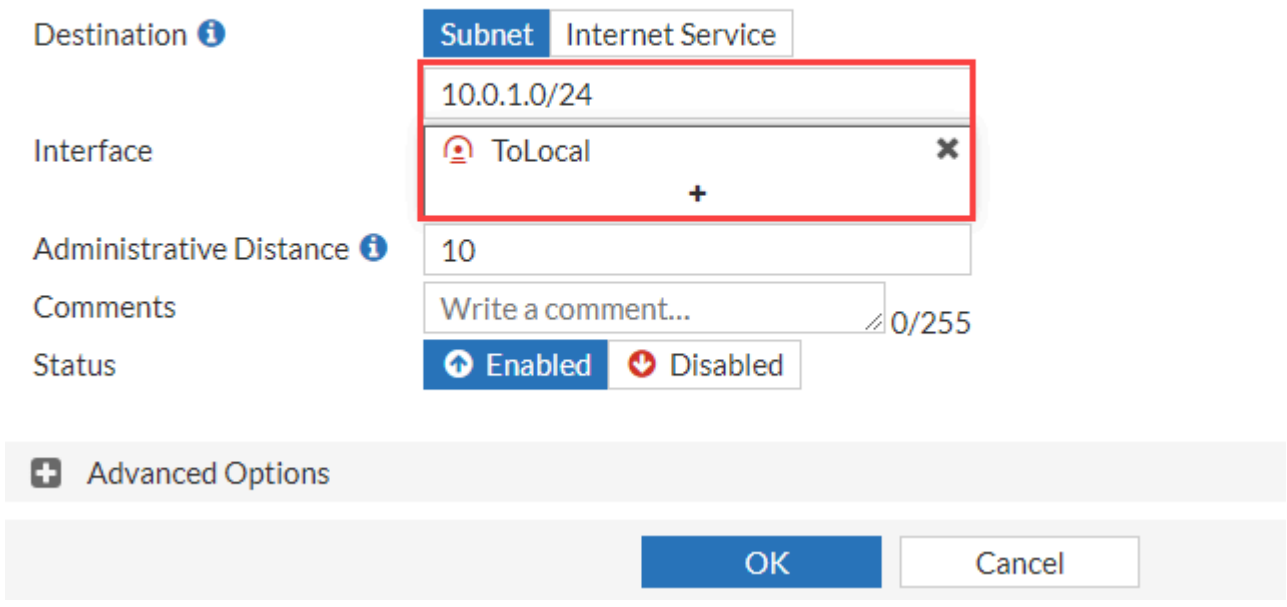
You will create one static route on Remote-FortiGate. This step was not necessary on Local-FortiGate because, as the dial-up server, it automatically adds the route for the remote network after the tunnel comes up.

To create a static route for VPN traffic on Remote-FortiGate

1. Continuing on the Remote-FortiGate GUI, click **Network** > **Static Routes**.
2. Click **Create New**.

3. Configure the following settings:

Field	Value
Destination	Subnet 10.0.1.0/24
Interface	ToLocal



4. Click **OK**.

Create the Firewall Policies for VPN Traffic on Remote-FortiGate (Dial-Up Client)

You will create two firewall policies between **port6** and **ToLocal**—one for each traffic direction.

To create firewall policies for VPN traffic

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

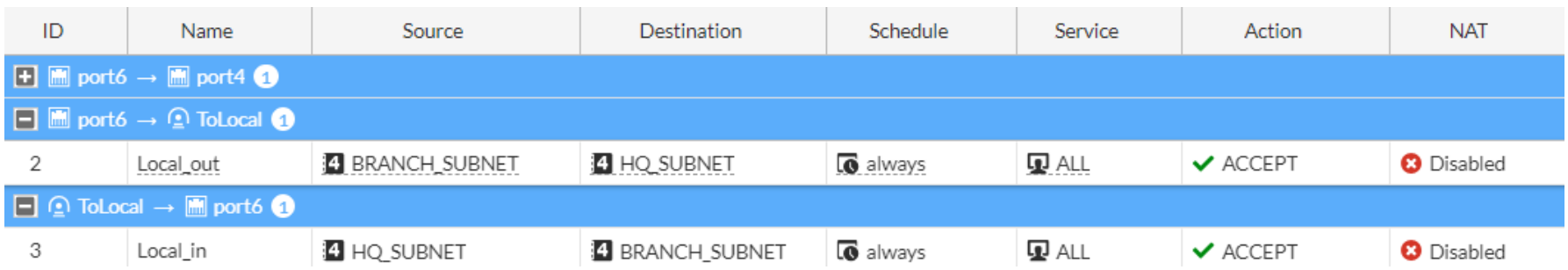
Field	Value
Name	Local_out
Incoming Interface	port6
Outgoing Interface	ToLocal
Source	BRANCH_SUBNET
Destination	HQ_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

4. In the **Firewall/Network Options** section, disable **NAT**.
5. Click **OK**.
6. Click **Create New** again.
7. Configure the following settings:

Field	Value
Name	Local_in

Field	Value
Incoming Interface	ToLocal
Outgoing Interface	port6
Source	HQ_SUBNET
Destination	BRANCH_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

8. In the **Firewall/Network Options** section, disable **NAT**.
9. Click **OK**.



Test and Monitor the VPN

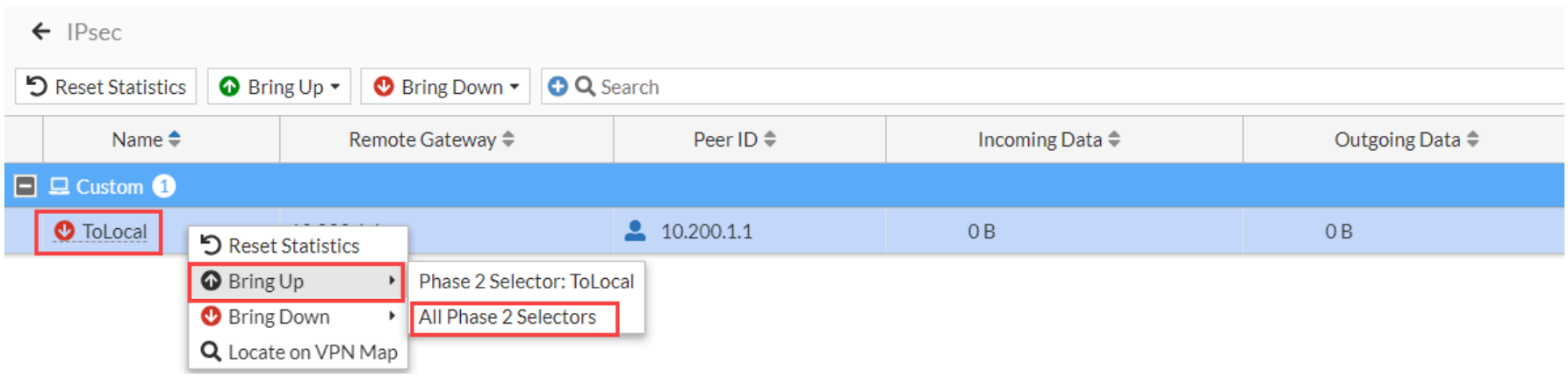
Now that you configured the VPN on both FortiGate devices, you will test the VPN.

To test the VPN

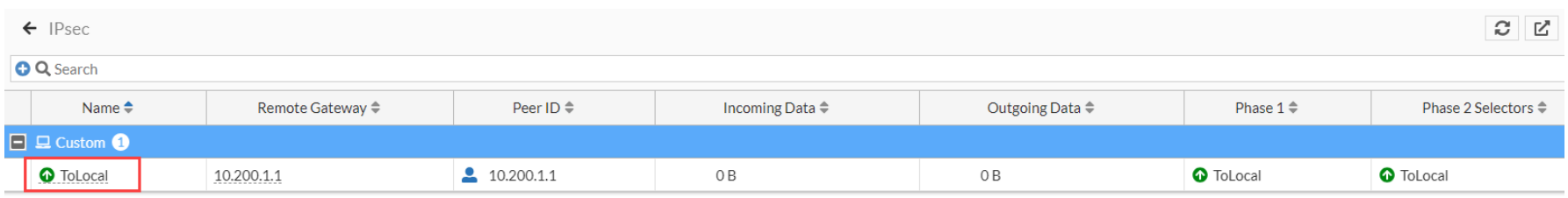
1. On the Remote-FortiGate GUI, click **Dashboard** > **Network** > **IPsec**.
2. Click **+** beside **Custom** to expand the custom VPN tunnel section.

Notice that the **ToLocal** VPN is currently down.

3. Right-click the VPN, and then click **Bring Up** > **All Phase 2 Selectors** to bring up the tunnel.



The **Name** column of the VPN now contains a green up arrow, which indicates that the tunnel is up. If required, click the refresh button in the upper-right corner to refresh the widget information.



Stop and think!

Do you always have to manually bring up the tunnel after you create it?

No. With the current configuration, the tunnel will stay down until you manually bring it up, or there is traffic that should be routed through the tunnel. Because you are not generating traffic between the `10.0.2.0/24` and `10.0.1.0/24` subnets yet, the tunnel is still down. If you had generated the required traffic while the tunnel was down, it would have come up automatically.

You can initiate a tunnel only from Remote-FortiGate because it is the dial-up client.

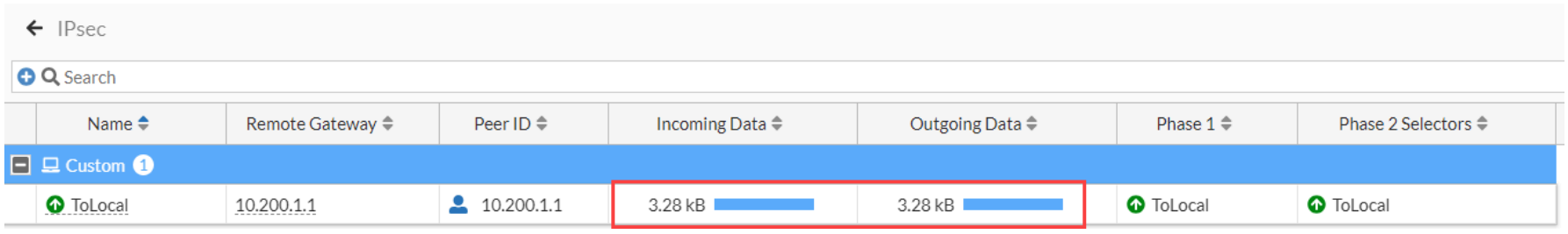
4. On the Remote-Client VM, open a terminal window, and then enter the following command to ping the Local-Client VM:

ping 10.0.1.10

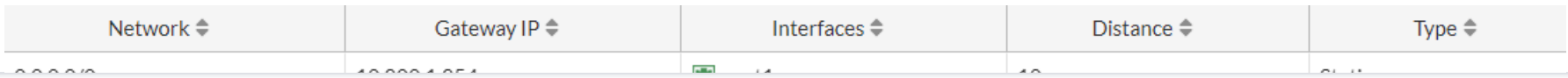
The ping should work.

5. On the Remote-FortiGate GUI, click **Dashboard** > **Network** > **IPsec**.
6. In the upper-right corner, click the refresh button multiple times to refresh the widget information.

You will notice that the counters in the **Incoming Data** and **Outgoing Data** columns increase over time. This indicates that the traffic between `10.0.1.10` and `10.0.2.10` is being encrypted successfully and routed through the tunnel.



7. On the Local-FortiGate GUI, click **Dashboard** > **Network** > **Static & Dynamic Routing**.
8. Find the static route that was dynamically added to the FortiGate.
9. View the route details.
10. Notice the address listed in the **Gateway IP** column for that route.



Exercise 2: Configuring a Static IPsec VPN Between Two FortiGate Devices

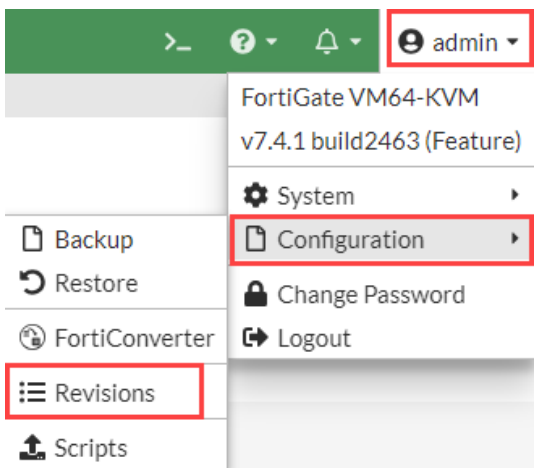
In this exercise, you will configure a static VPN between Local-FortiGate and Remote-FortiGate. You will also configure a static route on Local-FortiGate for VPN traffic.

Before you begin this lab, you must restore a configuration file on Local-FortiGate.

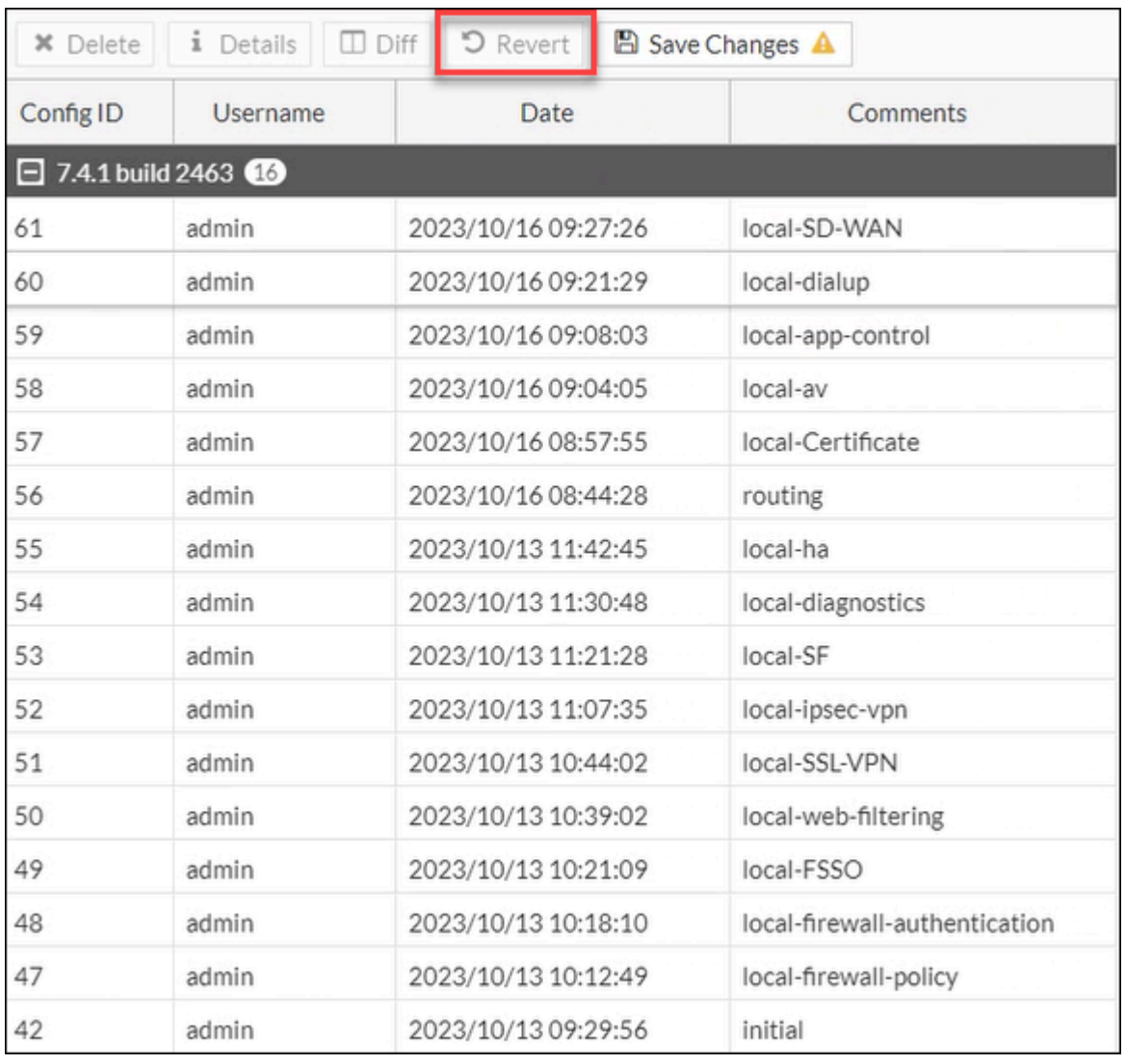
Make sure that you restore the correct configuration on Local-FortiGate, using the following steps. Failure to restore the correct configuration on Local-FortiGate will prevent you from doing the lab exercise.

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, click **admin**, and then click **Configuration** > **Revisions**.



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



Config ID	Username	Date	Comments
7.4.1 build 2463 16			
61	admin	2023/10/16 09:27:26	local-SD-WAN
60	admin	2023/10/16 09:21:29	local-dialup
59	admin	2023/10/16 09:08:03	local-app-control
58	admin	2023/10/16 09:04:05	local-av
57	admin	2023/10/16 08:57:55	local-Certificate
56	admin	2023/10/16 08:44:28	routing
55	admin	2023/10/13 11:42:45	local-ha
54	admin	2023/10/13 11:30:48	local-diagnostics
53	admin	2023/10/13 11:21:28	local-SF
52	admin	2023/10/13 11:07:35	local-ipsec-vpn
51	admin	2023/10/13 10:44:02	local-SSL-VPN
50	admin	2023/10/13 10:39:02	local-web-filtering
49	admin	2023/10/13 10:21:09	local-FSSO
48	admin	2023/10/13 10:18:10	local-firewall-authentication
47	admin	2023/10/13 10:12:49	local-firewall-policy
42	admin	2023/10/13 09:29:56	initial

5. Click **OK** to reboot.

Create Phase 1 and Phase 2 Negotiations on Local-FortiGate

You will configure the IPsec VPN by creating phase 1 and phase 2 negotiations.

To create phase 1 and phase 2 negotiations

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **VPN** > **IPsec Tunnels**, and then click **Create New** > **IPsec Tunnel**.
3. Configure the following settings:

Field	Value
Name	ToRemote
Template type	Custom

4. Click **Next**.
5. In the **Network** section, configure the following settings:

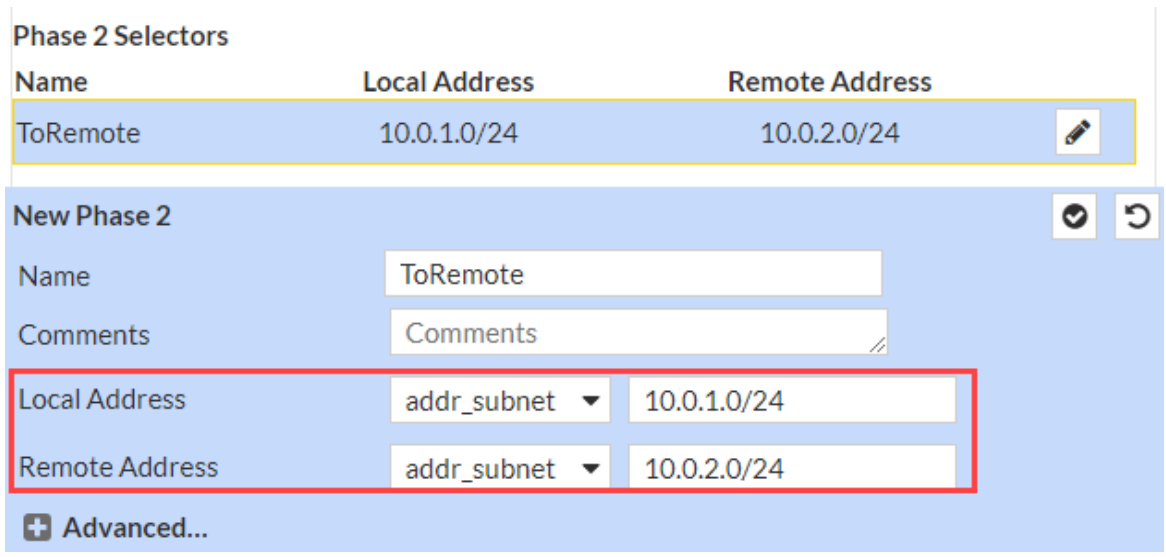
Field	Value
Remote Gateway	Static IP Address
IP Address	10.200.3.1
Interface	port1
Dead Peer Detection	On Idle

6. In the **Authentication** section, configure the following settings:

Field	Value
Method	Pre-shared Key
Pre-shared Key	fortinet
Version	1
Mode	Aggressive
Accept Types	Any peer ID

7. In the **Phase 2 Selectors** section, configure the following settings:

Field	Value
Local Address	10.0.1.0/24
Remote Address	10.0.2.0/24



8. Keep the default values for the remaining settings.
9. Click **OK**.

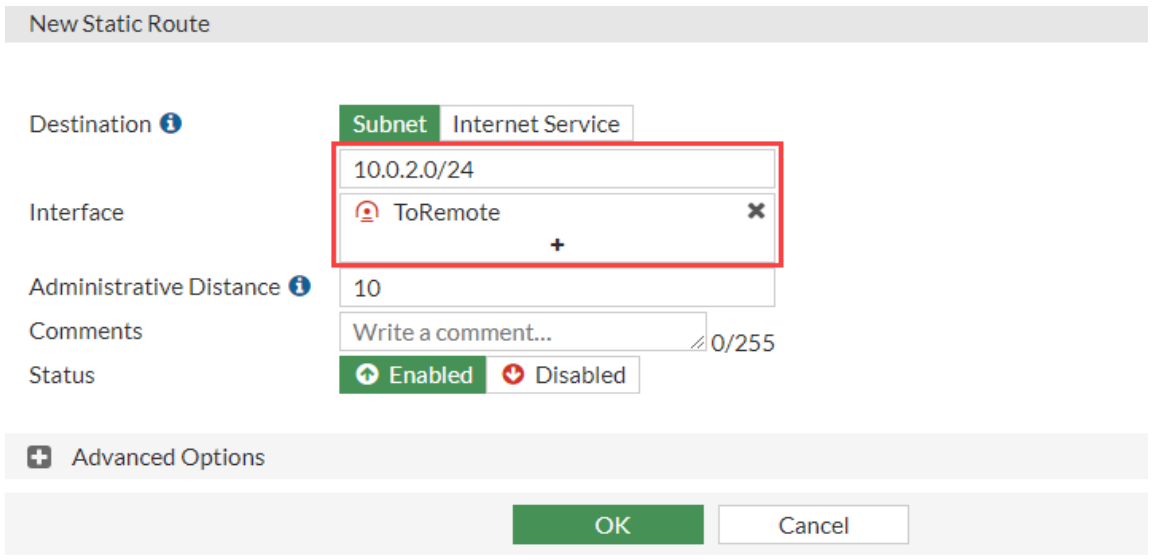
Create a Static Route for VPN Traffic on Local-FortiGate

You will create one static route on Local-FortiGate.

To create a static route for VPN traffic on Local-FortiGate

1. Continuing on the Local-FortiGate GUI, click **Network** > **Static Routes**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Destination	Subnet 10.0.2.0/24
Interface	ToRemote



4. Click **OK**.

Create Firewall Policies for VPN Traffic on Local-FortiGate

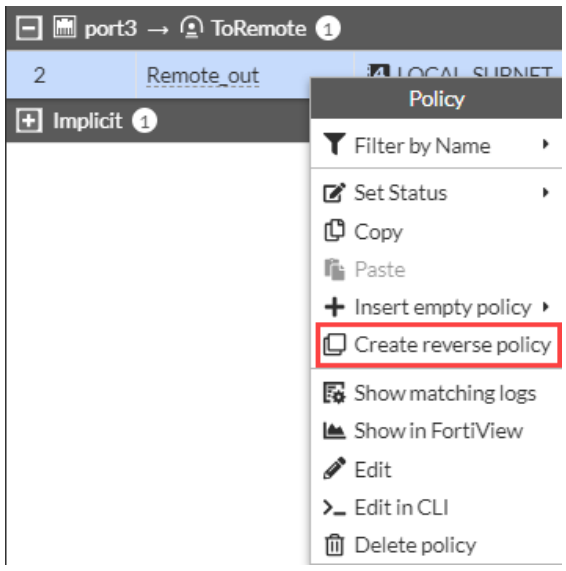
You will create two firewall policies between **port3** and **ToRemote**—one for each traffic direction.

To create firewall policies for VPN traffic

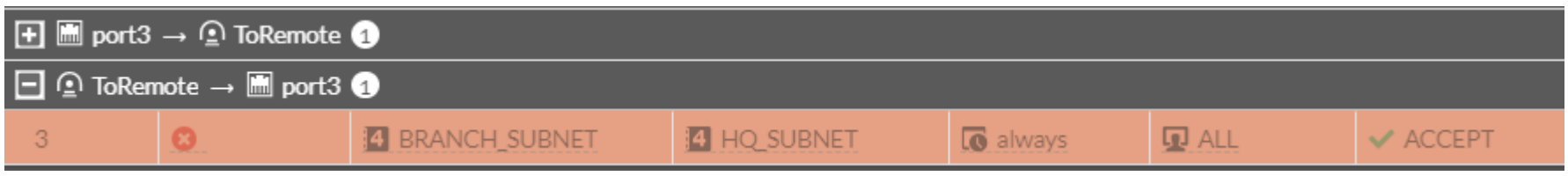
1. On the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	Remote_out
Incoming Interface	port3
Outgoing Interface	ToRemote
Source	HQ_SUBNET
Destination	BRANCH_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

4. In the **Firewall/Network Options** section, disable **NAT**.
5. Click **OK**.
6. Right-click the **Remote_out** policy, and then click **Create reverse policy**.



You will see the new reverse policy. By default, the policy is disabled.



7. Select the new policy, and then click **Edit**.
8. In the **Name** field, type `Remote_in`.
9. Verify the following settings:

Field	Value
Incoming Interface	ToRemote
Outgoing Interface	port3
Source	BRANCH_SUBNET
Destination	HQ_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

8. In the **Firewall/Network Options** section, disable **NAT**.
9. Click **Enable this policy** to enable the policy.
10. Click **OK**.

ID	Name	Source	Destination	Schedule	Service	Action	NAT
port3 → port1 1							
port3 → ToRemote 1							
2	Remote_out	HQ_SUBNET	BRANCH_SUBNET	always	ALL	ACCEPT	Disabled
ToRemote → port3 1							
3	Remote_in	BRANCH_SUBNET	HQ_SUBNET	always	ALL	ACCEPT	Disabled

Test and Monitor the VPN

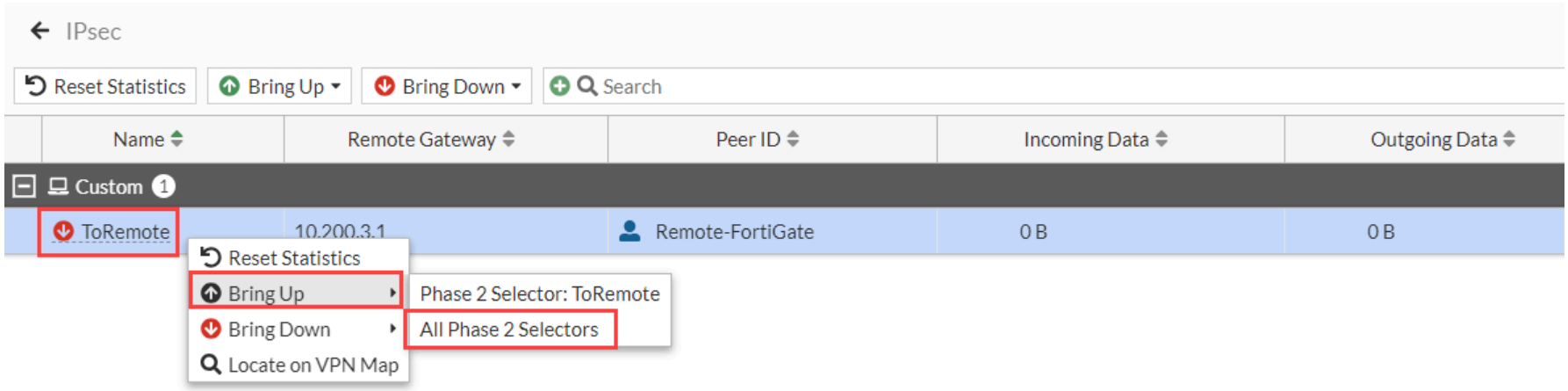
You will test the VPN and monitor its status.

To test the VPN

1. On the Local-FortiGate GUI, click **Dashboard** > **Network** > **IPsec**.
2. Click **+** beside **Custom** to expand the custom VPN tunnel section.

Notice that the **ToRemote** VPN is currently down.

3. Right-click the VPN, and then click **Bring Up** > **All Phase 2 Selectors**.



4. In the upper-right corner, click the refresh button to refresh the widget information.

The **Name** column of the VPN now contains a green up arrow, which indicates that the tunnel is up.

5. On the Remote-Client VM, open a terminal window, and then enter the following command to ping the Local-Client VM:

ping 10.0.1.10

The ping should work.

Lab 11: IPsec VPN Configuration

In this lab, you will configure site-to-site IPsec VPN tunnels between two FortiGate devices. First, you will configure a dial-up tunnel, and then a static tunnel.

Objectives

- Deploy a site-to-site VPN between two FortiGate devices
- Set up dial-up and static remote gateways

Time to Complete

Estimated: 40 minutes
LAB-11 > IPsec VPN Configuration

Configuring SD-WAN

In this exercise, you will configure a basic DIA setup using the FortiGate GUI. You will create a zone for port1 and port2 on Local-FortiGate, and then configure SD-WAN rules to steer traffic for critical and non-critical internet applications.

Remove Interface References

Before you can add port1 and port2 as SD-WAN member interfaces, you must remove all firewall policies that reference the two interfaces.

Take the Expert Challenge!

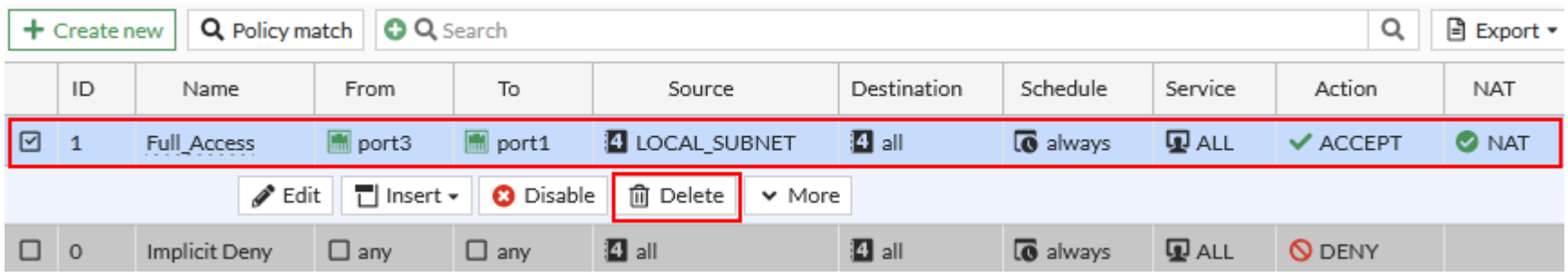
On the Local-FortiGate GUI (`admin/password`), remove all firewall policies that reference **port1** and **port2**.

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

After you complete the challenge, see Configure a Zone and Members for DIA on page 1.

To remove interface references

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. Select the **Full_Access** policy, and then click **Delete**.



1. Click **OK** to confirm the deletion.

()Configure a Zone and Members for DIA

You will configure the underlay zone, and then add port1 and port2 as members.

Take the Expert Challenge!

On the Local-FortiGate GUI (`admin/password`), complete the following:

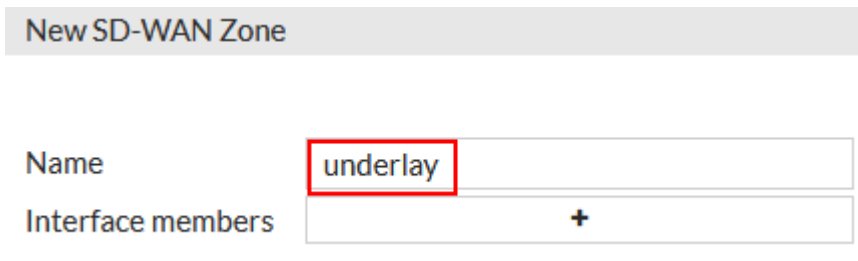
- Configure an **SD-WAN Zone** named `underlay`.
- Configure SD-WAN members with the following configuration, and add them to the **underlay** zone:
- **port1** with **Gateway** `10.200.1.254`
- **port2** with **Gateway** `10.200.2.254`

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

After you complete the challenge, see Configure a Performance SLA on page 1.

To create an SD-WAN zone

1. Continuing on the Local-FortiGate GUI, click **Network** > **SD-WAN** > **SD-WAN Zones**.
2. Click **Create New** > **SD-WAN Zone**.
3. In the **Name** field, type `underlay`.



1. Click **OK**.
2. Click **Create New** > **SD-WAN Member**.
3. Configure the following settings:

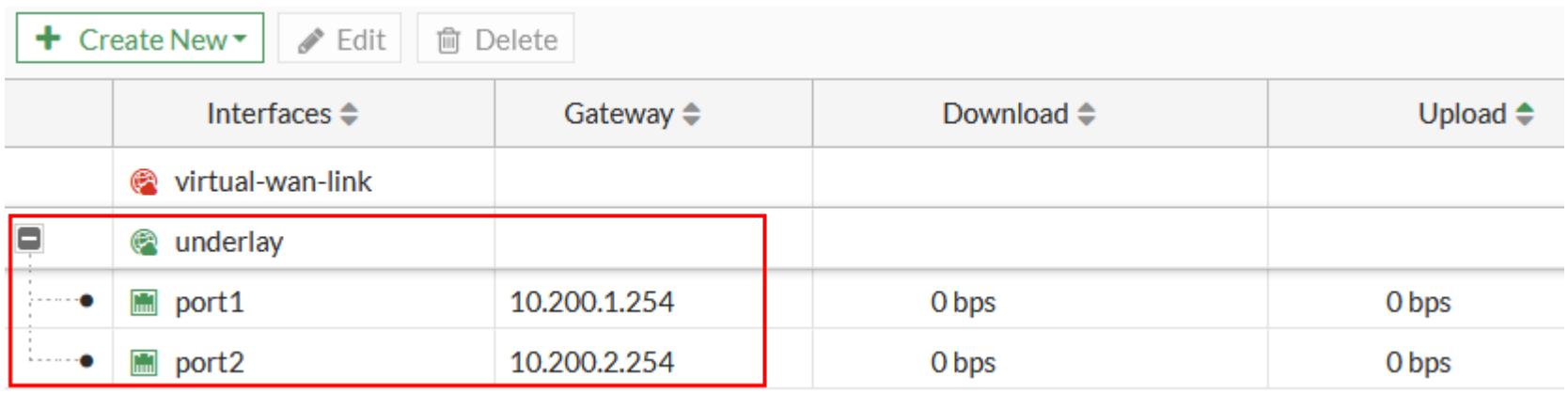
Field	Value
Interface	port1
SD-WAN Zone	underlay
Gateway	10.200.1.254
Status	Enabled

1. Click **OK**.
2. Click **Create New** > **SD-WAN Member**.
3. Configure the following settings:

Field	Value
Interface	port2
SD-WAN Zone	underlay
Gateway	10.200.2.254
Status	Enabled

1. Click **OK**.
2. On the **SD-WAN Zones** tab, expand the **underlay** zone.

Your page should look similar to the following example:



port1 and **port2** are members of the **underlay** zone.

The default SD-WAN zone **virtual-wan-link** has no members, and therefore is represented with a red icon.

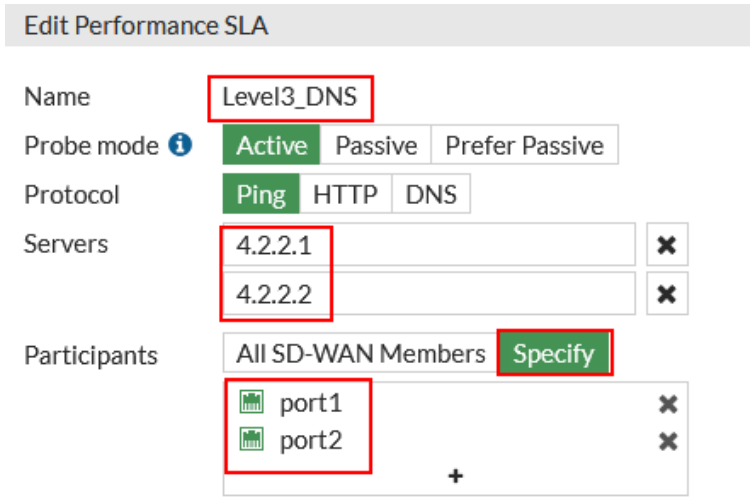
()Configure a Performance SLA

You will configure a performance SLA for monitoring the health of port1 and port2.

To configure a performance SLA

1. Continuing on the Local-FortiGate GUI, click **Network** > **SD-WAN**, and then click the **Performance SLAs** tab.
2. Click **Create New** to add a performance SLA.
3. Configure the following settings:

Field	Value
Name	Level3_DNS
Server	4.2.2.1 Click **+**, and then type `4.2.2.2`.
Participants	Click **Specify**, and then select **port1** and **port2**.



1. Click **OK** to save the settings.
2. Click **Network** > **SD-WAN**, and then click the **Performance SLAs** tab to refresh the page.

The page should show that port1 and port2 are up (green up arrow).

Name	Detect Server	Packet Loss	Latency	Jitter
Level3_DNS	4.2.2.1 4.2.2.2	port1: 0.00% port2: 0.00%	port1: 41.57ms port2: 26.00ms	port1: 0.24ms port2: 0.46ms

FortiGate can reach the detect server through port1 and port2, and displays a green arrow for **Packet Loss**, **Latency**, and **Jitter**.

1. To check the routing table, click **Dashboard** > **Network**, and then click the **Static & Dynamic Routing** widget.

Your page should look similar to the following example:

Network	Gateway IP	Interfaces	Distance	Type
10.0.1.0/24	0.0.0.0	port3	0	Connected
10.0.2.0/24	10.200.1.254	port1	10	Static
10.200.1.0/24	0.0.0.0	port1	0	Connected
10.200.2.0/24	0.0.0.0	port2	0	Connected
172.16.100.0/24	0.0.0.0	port8	0	Connected

Stop and think!

There are no routes to 4.2.2.1 and 4.2.2.2, yet the performance SLA shows that port1 and port2 are up. Why?

To route the health check probes, FortiOS installs special routes in the forwarding information base (FIB) using the gateway information of members. These routes are not displayed in the routing table, but you can enter the `get router info kernel` CLI command to see them.

Configure Rules

You will configure two SD-WAN rules. One rule will be used to steer the traffic of critical applications. The other rule will be used to steer the traffic of non-critical applications. Both rules will use manual mode.

By default, application detection for SD-WAN rules is not visible on the GUI. This feature has been enabled for you on the Local-FortiGate GUI.

The commands to enable the visibility of application detection for SD-WAN rules are:

config system global

set gui-app-detection-sdwan enable

end

To configure rules

1. Continuing on the Local-FortiGate GUI, click **Network** > **SD-WAN**, and then click the **SD-WAN Rules** tab.
2. Click **Create New** to add a rule.
3. Configure the following settings:

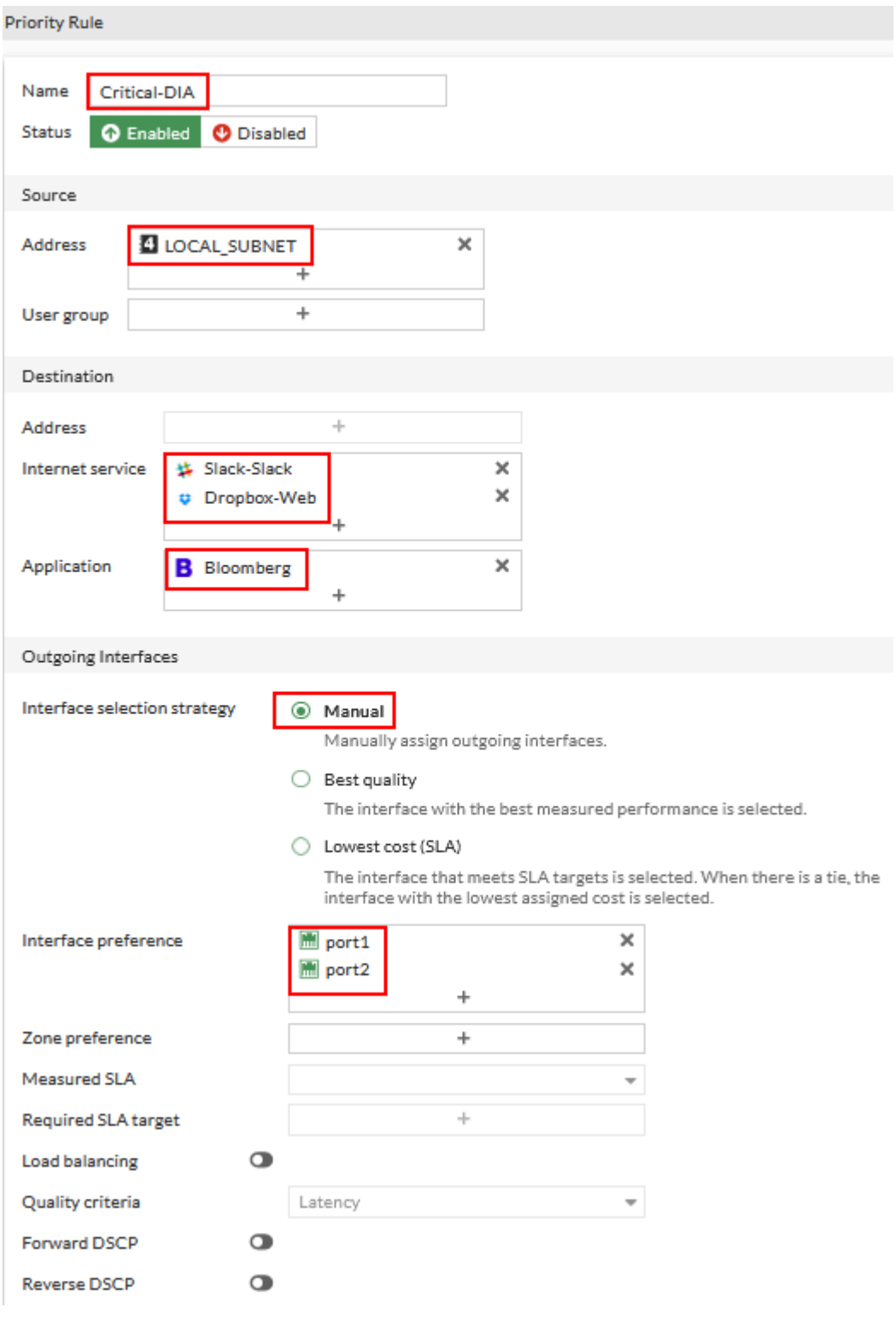
Field	Value
Name	Critical-DIA
Source address	LOCAL_SUBNET
Internet service	Select **Slack-Slack** and **Dropbox-Web**.
Application	Select **Bloomberg**.
Outgoing Interfaces	Select **Manual**.
Interface preference	Select **port1**, and then select **port2**.

You can combine the traffic detection for **Internet service** and **Application** in the same rule.

When you select **Internet service**, FortiGate uses the Internet Service Database (ISDB) list of IP addresses and protocols for each application. The FortiGuard server regularly updates and loads this list on FortiGate.

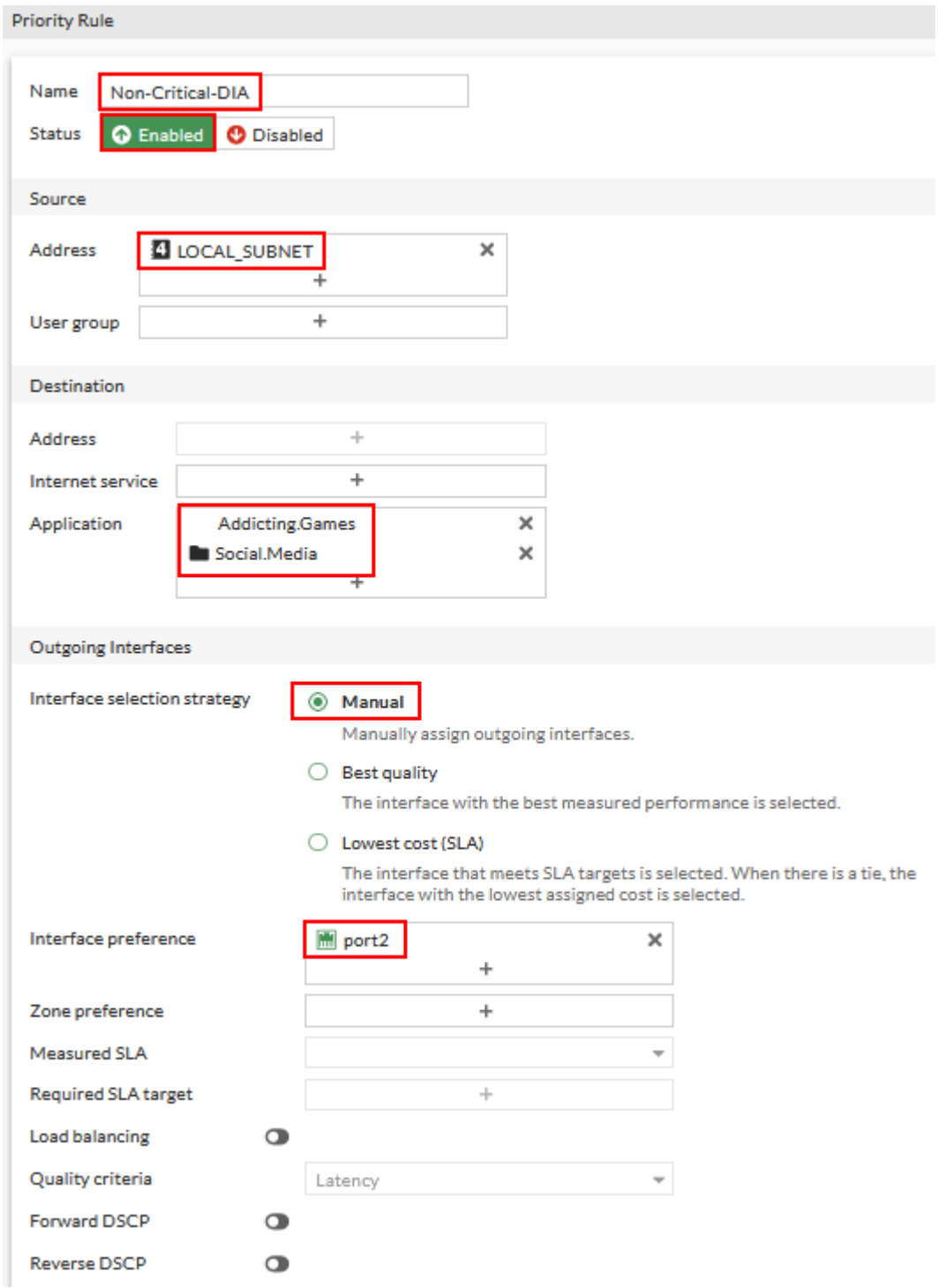
When you select **Application**, FortiGate detects the application according to the first packets exchanged with the initial session.

Your page should look similar to the following example. Note that you might not be able to view the application icons at this stage.



1. Click **OK** to save the settings.
2. Repeat the previous steps to configure a rule for non-critical traffic using the following settings:

Field	Value
Name	Non-Critical-DIA
Source address	LOCAL_SUBNET
Application	Select **Apps**, and then select **Addicting.Games**. Select **Category**, and then select **Social.Media**.
Outgoing Interfaces	Select **Manual**.
Interface preference	Select **port2**.



1. Click **OK** to save the settings.
2. Continuing on the **SD-WAN Rules** tab, double-click the implicit **sd-wan** rule.
3. Select the **Source-Destination IP** load balancing algorithm.
4. Click **OK** to save the settings.
5. Your page should look similar to the following example:

ID	Name	Source	Destination	Criteria	Members
IPv4 2					
1	Critical-DIA	LOCAL_SUBNET	Slack-Slack Dropbox-Web Bloomberg		port1 port2
2	Non-Critical-DIA	LOCAL_SUBNET	Addicting.Games Social.Media		port2
Implicit 1					
	sd-wan	all	all	Source-Destination IP	any

Stop and think!

port1 is the preferred member for rule 1, and **port2** is the preferred member for rule 2. Why?

port1 is the preferred member for rule 1 because it is configured first in the list and it is alive. **port2** is the preferred member for rule 2 because it is the only member for this rule and it is alive.

Configure a Static Route and Firewall Policy

You will configure a static route and firewall policy for routing and allowing SD-WAN traffic. Both objects will reference the underlay zone.

To create a static route for SD-WAN

1. Continuing on the Local-FortiGate GUI, click **Network** > **Static Routes**.
2. Click **Create New** to add a static route.
3. Configure the following settings:

Field	Value
Destination	Subnet 0.0.0.0/0.0.0.0
Interface	underlay

4. Click **OK**.

Your page should look similar to the following example:

Destination	Gateway IP	Interface	Status
10.0.2.0/24	10.200.1.254	port1	Enabled
0.0.0.0/0		underlay	Enabled

You don't need to configure a gateway when you use an SD-WAN zone as the outgoing interface for a static route. FortiGate automatically uses the gateway configured for each interface of the SD-WAN zone.

Stop and think!

The static route table shows two routes. The default route through the SD-WAN zone underlay that you have configured, and a static route through port1 that was already configured. Is this a valid configuration?

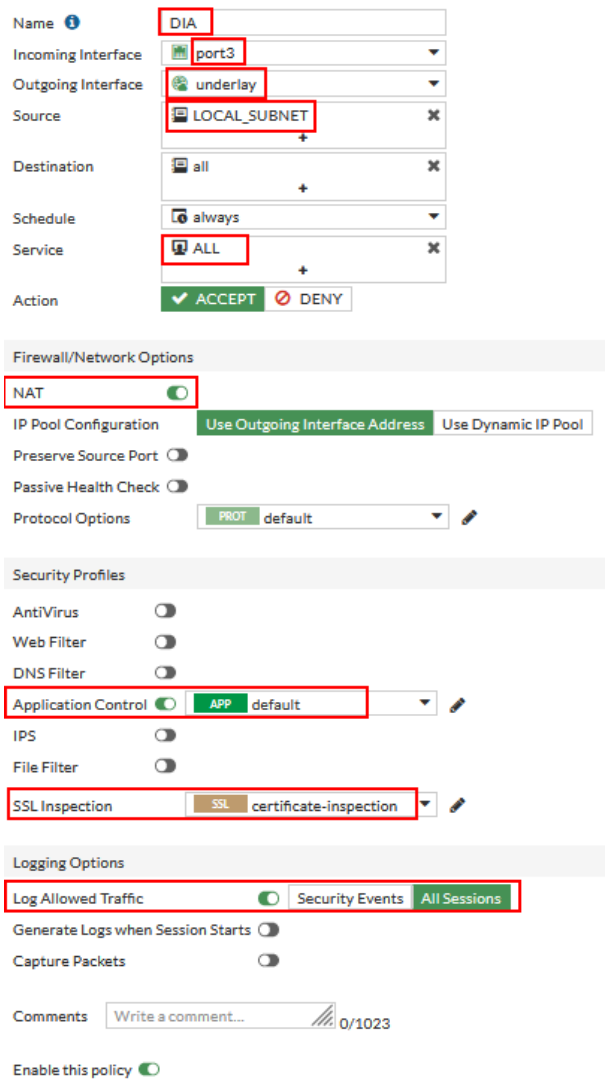
Yes, this configuration is valid. You can configure static routes for each SD-WAN zone and routes for each SD-WAN member for additional granularity.

To create a firewall policy to allow DIA traffic

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

Field	Value
Name	DIA
Incoming Interface	port3
Outgoing Interface	underlay
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL

Field	Value
Action	Accept
NAT	Enable
Security Profiles	Enable **Application Control**, and then select **default**. For **SSL Inspection**, select **certificate-inspection**.
Logging Options	Enable **Log Allowed Traffic**, and then select **All Sessions**.



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

To review the routing table

1. Open an SSH session to Local-FortiGate.
2. Log in with the username `admin` and password `password`.
3. Enter the following command to verify the list of active routes in the routing table:

get router info routing-table all

1. Verify that both default routes, through **port1** and **port2**, have the same distance value and are active in the routing table.

```
Local-FortiGate # Local-FortiGate # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [1/0] via 10.200.1.254, port1, [1/0]
                  [1/0] via 10.200.2.254, port2, [1/0]
C       10.0.1.0/24 is directly connected, port3
S       10.0.2.0/24 [10/0] via 10.200.1.254, port1, [1/0]
C       10.200.1.0/24 is directly connected, port1
C       10.200.2.0/24 is directly connected, port2
C       172.16.100.0/24 is directly connected, port8
```

After you create a static route for an SD-WAN zone, FortiGate automatically adds individual routes, with the same distance value, for all member interfaces. This ensures that all routes

Exercise 2: Monitoring the SD-WAN Setup

In this exercise, you will generate internet traffic from the Local-Client VM. Next, you will monitor DIA traffic distribution and logs using the SD-WAN tools available on the FortiGate GUI.

Generate Internet Traffic From the Local-Client VM

You will generate internet traffic from the Local-Client VM using a script.

To generate internet traffic from the Local-Client VM

1. On the Local-Client VM, log in with the username `Administrator` and password `password`.
2. Open a terminal window, and then enter the following commands:

cd Desktop

sh traffic-generation.sh

Your output should look similar to the following example:

```
Administrator@ubuntu-2204-desktop:~$ cd Desktop
Administrator@ubuntu-2204-desktop:~/Desktop$ sh traffic-generation.sh
[#############                              ] 33%
```

The Local-Client VM is generating various types of internet traffic.

The script takes about 2 minutes to complete, and then the terminal window displays `Script was successfully completed`. You can move to the next task while the script is running.

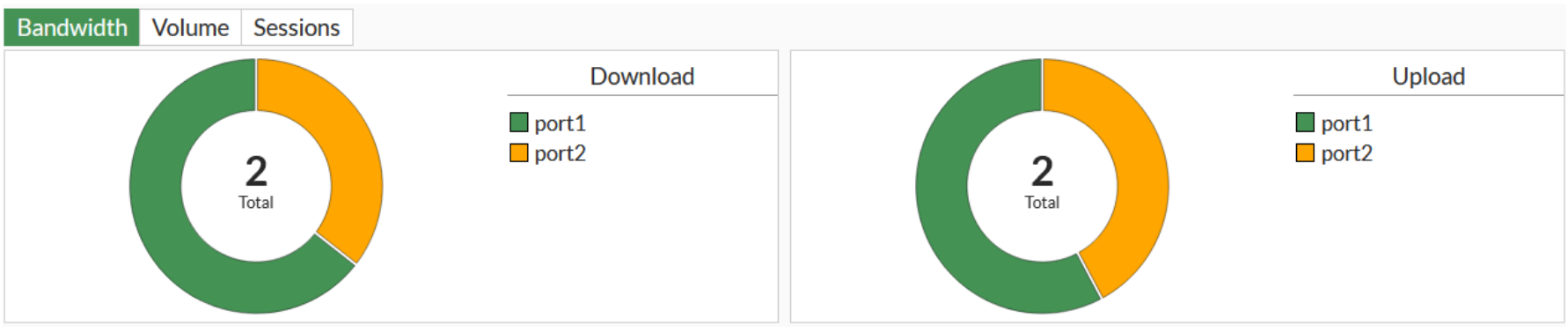
Monitor DIA Traffic Distribution

You will use the SD-WAN page on the FortiGate GUI to monitor the DIA traffic distribution. Next, you will view the traffic logs to obtain additional details.

To monitor DIA traffic distribution

1. On the Local-FortiGate GUI, log in with the username `admin` and password `password`.
2. Click **Network** > **SD-WAN**, and then click the **SD-WAN Zones** tab.
3. Click **Bandwidth** to display SD-WAN distribution graphs based on bandwidth.

Your page should look similar to the following example:



The traffic distribution in this example may be different from yours.

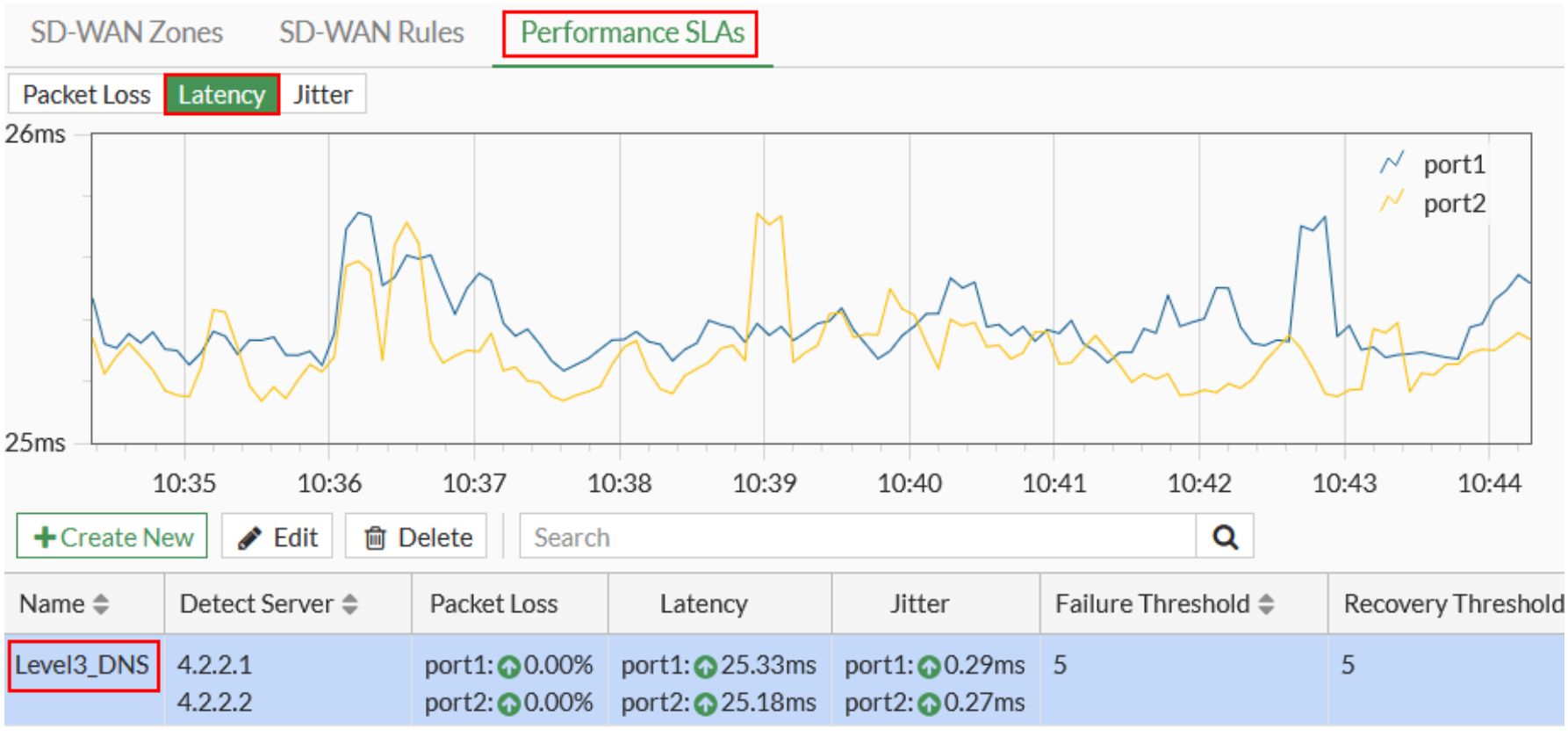
4. Hover over each graph to display the bandwidth that each member (port1 and port2) uses.
5. Click the **Volume** and **Sessions** graphs to explore them.

To monitor the performance SLAs

1. Click the **Performance SLAs** tab.

2. Click **Latency** to display a graph that shows the latency for the performance SLA **Level3_DNS** monitored over the past 10 minutes.

Your page should look similar to the following example:



3. Notice the green arrows beside port1 and port2 in the **Packet Loss**, **Latency**, and **Jitter** columns.

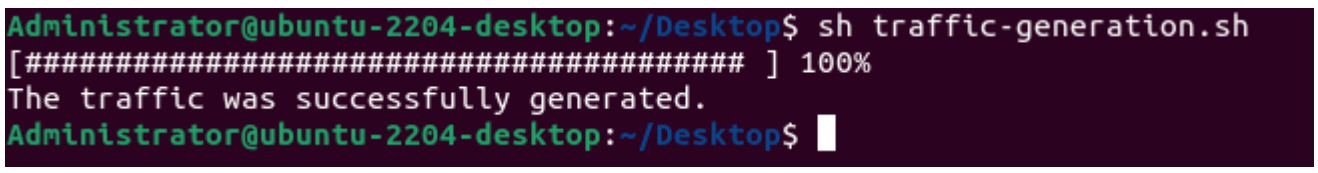
They indicate that the port is up and that the measured performances are within acceptable values.

4. Click **Packet Loss** and **Jitter** to explore them.

To view SD-WAN traffic logs

1. On the Local-Client VM, confirm that the script completed successfully.

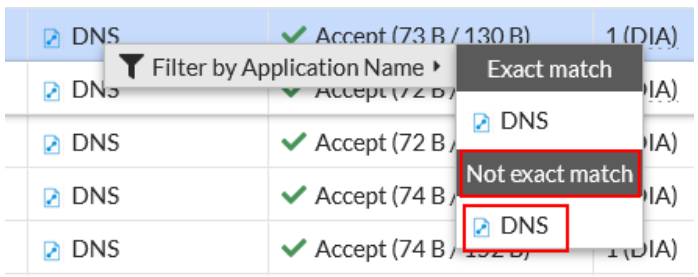
The terminal window should display `The traffic was successfully generated.`



2. On the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.
3. Hover over the upper-left corner of the log table to display the table column settings icon.

A gear icon is displayed.

4. Click the gear icon, select **Destination Interface**, select **SD-WAN Quality**, and then select **SD-WAN Rule Name**.
5. Click **Apply**.
6. For the display time period, select **1 hour**.
7. To simplify the view, beside a DNS log message, right-click **DNS**, and then select the **Not exact match** filter.



Your page should look similar to the following example:

Application Name	Result	Polic...	Destinatio...	SD-WAN Quality	SD-WAN Rule Name
SSL_TLSv1.3	✔ Accept (UTM ...	1 (DIA)	port1		
Bloomberg	✔ Accept (UTM ...	1 (DIA)	port1	Seq_num(1 port1 underlay), alive, selected	Critical-DIA
BBC	✔ Accept (UTM ...	1 (DIA)	port1		
Pinterest	✔ Accept (UTM ...	1 (DIA)	port2	Seq_num(2 port2 underlay), alive, selected	Non-Critical-DIA
Slack	✔ Accept (UTM ...	1 (DIA)	port1	Seq_num(1 port1 underlay), alive, selected	Critical-DIA
Duolingo	✔ Accept (UTM ...	1 (DIA)	port1		
Addicting.Games	✔ Accept (UTM ...	1 (DIA)	port2	Seq_num(2 port2 underlay), alive, selected	Non-Critical-DIA
Atlassian.JIRA	✔ Accept (UTM ...	1 (DIA)	port1		
Atlassian.JIRA	✔ Accept (1.65 k...	1 (DIA)	port1		
Dropbox	✔ Accept (UTM ...	1 (DIA)	port1	Seq_num(1 port1 underlay), alive, selected	Critical-DIA
Facebook	✔ Accept (UTM ...	1 (DIA)	port2	Seq_num(2 port2 underlay), alive, selected	Non-Critical-DIA
SSL_TLSv1.3	✔ Accept (UTM ...	1 (DIA)	port1		

8. Browse the log table, and then confirm the following:

- **Dropbox** traffic matches the **Critical-DIA** rule, and uses **port1**.
- **Social-Media**—Facebook and Pinterest— traffic matches the **Non-Critical-DIA** rule, and uses **port2**.

Stop and think!

Logs for all other traffic (**DNS**, **HTTP_BROWSER**, and so on) show no information in the **SD-WAN Quality** and **SD-WAN Rule Name** columns. Why?

The traffic doesn't match any of the configured SD-WAN rules. As a result, it matches the implicit SD-WAN rule. The SD-WAN implicit rule load balances sessions based on the source and destination IP addresses and the FIB contents.

Check SD-WAN System Events

You will use the **System Events** log page on the FortiGate GUI to review some messages related to SD-WAN activity.

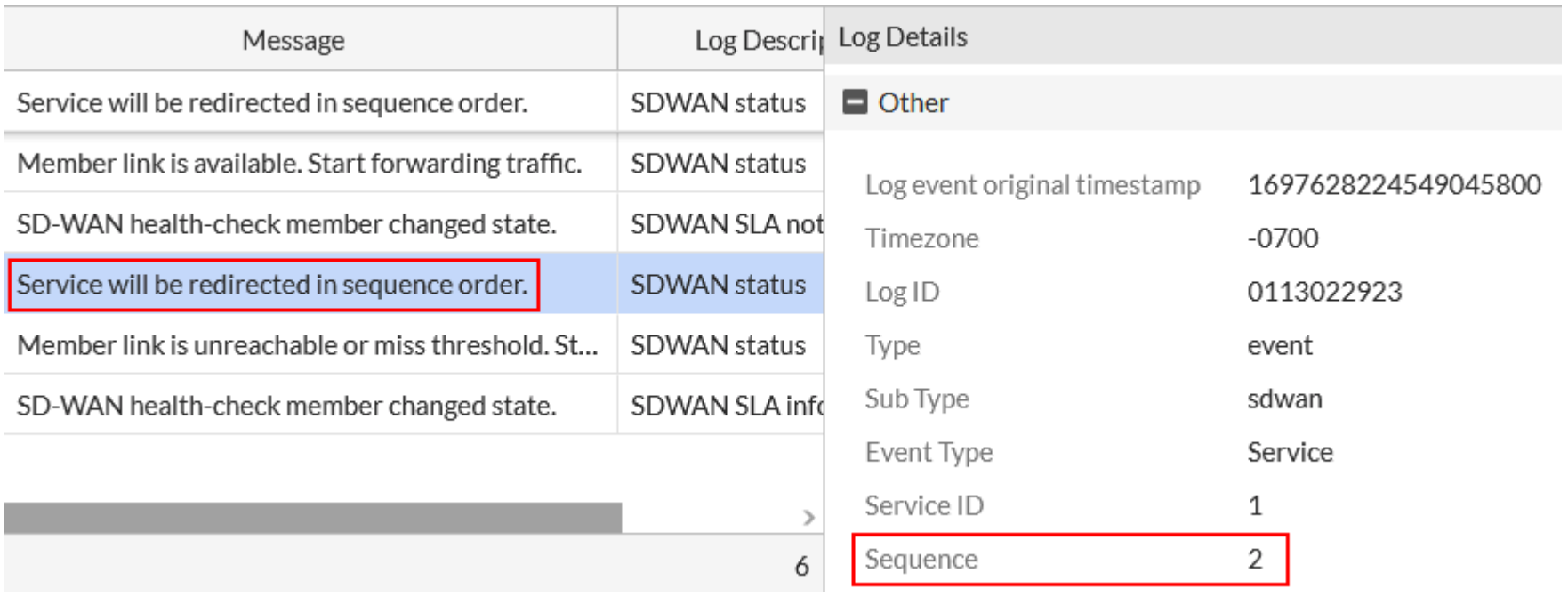
To monitor SD-WAN system events

1. Continuing on the Local-FortiGate GUI, click **Network** > **Interfaces**.
2. Right click **port1**, and then select **Set Status** > **Disable**.
3. Wait about 20 seconds, and then enable **port1**.
4. Click **Log & Reports** > **System Events**.
5. In the upper-right corner, click the time selection list, and then select **1 hour** to display a summary of events in the past hour.

6. On the **Summary** page, scroll down, and then click the **SD-WAN Events** summary widget to expand it.

Relative Date/Time	Level	Message	Log Description
7 minutes ago	Notice	Service will be redirected in sequence order.	SDWAN status
7 minutes ago	Notice	Member link is available. Start forwarding traffic.	SDWAN status
7 minutes ago	Notice	SD-WAN health-check member changed state.	SDWAN SLA notification
7 minutes ago	Notice	Service will be redirected in sequence order.	SDWAN status
7 minutes ago	Notice	Member link is unreachable or miss threshold. S...	SDWAN status
7 minutes ago	Warning	SD-WAN health-check member changed state.	SDWAN SLA information warning
Hour ago	Notice	SD-WAN health-check member initial state.	SDWAN SLA notification

7. Double-click a few messages to view the details.
8. Double-click the first **Service will be redirected in sequence order** message received, and then review the details.



You can see that FortiGate directs the traffic only to member 2 after you switched off port1.

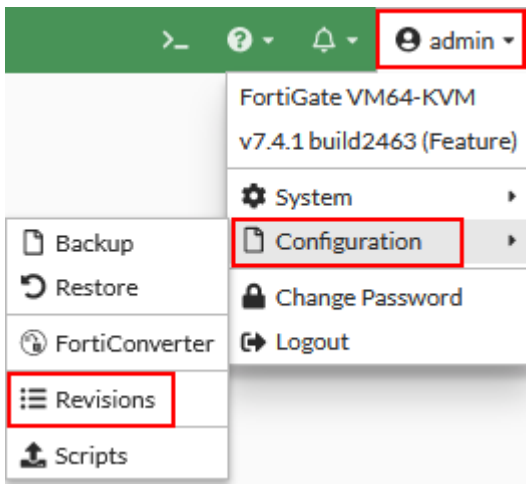
9. Double-click the second **Service will be redirected in sequence order** message received, and then review the details.

Prerequisites

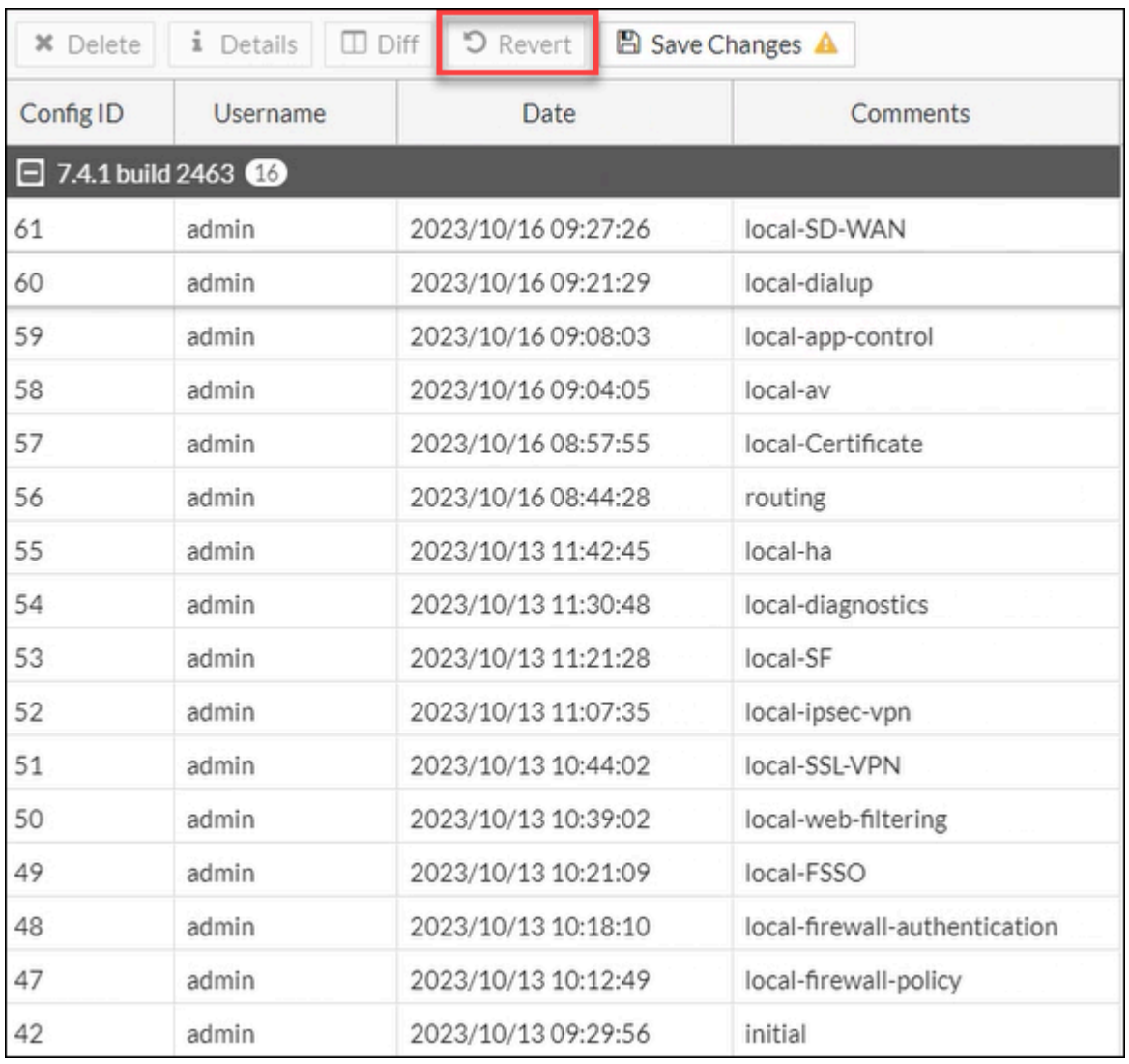
Before you begin this lab, you must restore a configuration file on Local-FortiGate.

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, click **admin**, and then click **Configuration** > **Revisions**.



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

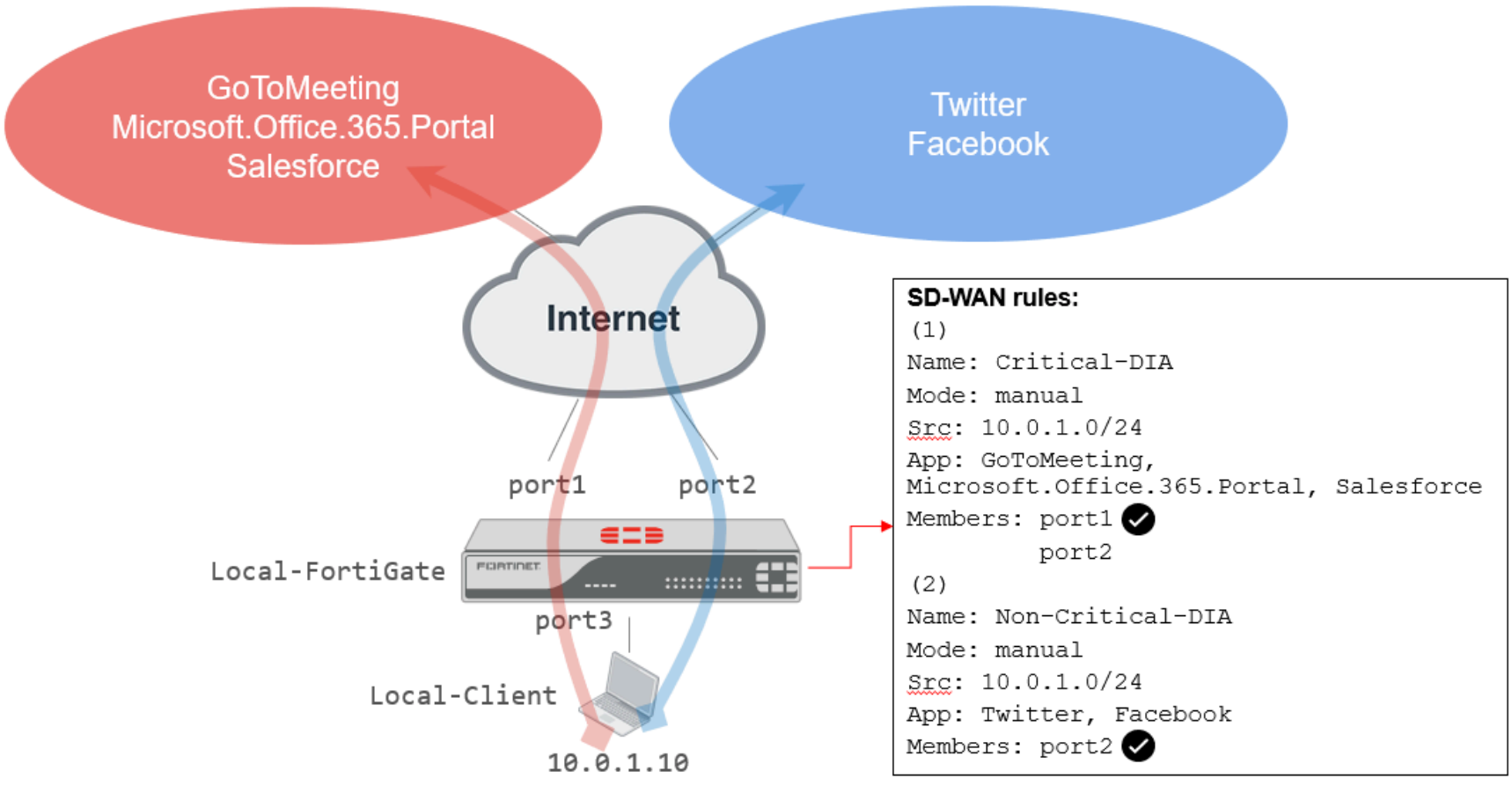


Config ID	Username	Date	Comments
7.4.1 build 2463 16			
61	admin	2023/10/16 09:27:26	local-SD-WAN
60	admin	2023/10/16 09:21:29	local-dialup
59	admin	2023/10/16 09:08:03	local-app-control
58	admin	2023/10/16 09:04:05	local-av
57	admin	2023/10/16 08:57:55	local-Certificate
56	admin	2023/10/16 08:44:28	routing
55	admin	2023/10/13 11:42:45	local-ha
54	admin	2023/10/13 11:30:48	local-diagnostics
53	admin	2023/10/13 11:21:28	local-SF
52	admin	2023/10/13 11:07:35	local-ipsec-vpn
51	admin	2023/10/13 10:44:02	local-SSL-VPN
50	admin	2023/10/13 10:39:02	local-web-filtering
49	admin	2023/10/13 10:21:09	local-FSSO
48	admin	2023/10/13 10:18:10	local-firewall-authentication
47	admin	2023/10/13 10:12:49	local-firewall-policy
42	admin	2023/10/13 09:29:56	initial

5. Click **OK** to reboot.

Lab 12: SD-WAN Configuration

In this lab, you will configure the following basic SD-WAN direct internet access (DIA) setup on Local-FortiGate.



Then, you will generate internet traffic on Local-Client and monitor the traffic distribution and events on the FortiGate GUI.

Objectives

- Configure SD-WAN members and an SD-WAN zone
- Configure routes
- Configure SD-WAN rules for an internet service
- Configure firewall policies
- Verify SD-WAN traffic distribution and events

Time to Complete

Estimated: 30 minutes
LAB-12 > SD-WAN Configuration

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).

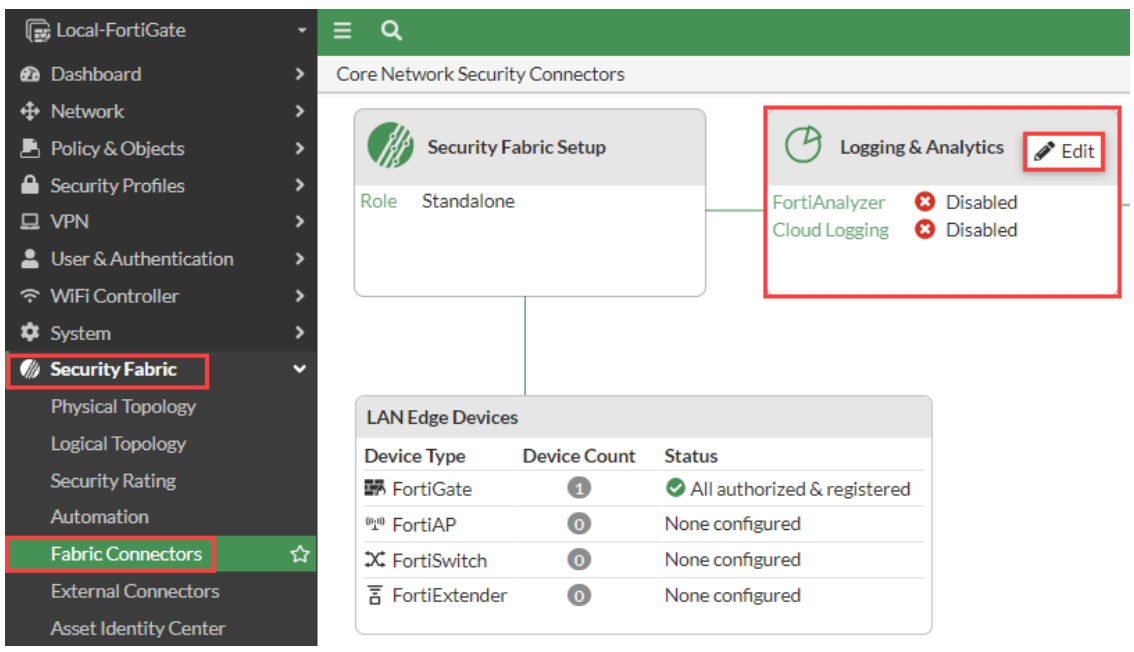
Configure FortiAnalyzer Logging on Local-FortiGate (Root)

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.

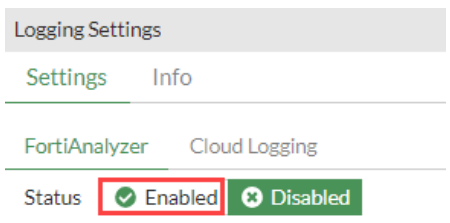
For this lab, FortiAnalyzer is already preconfigured to accept the registration requests that originate from all FortiGate devices in the topology.

To configure Local-FortiGate to send logs to FortiAnalyzer

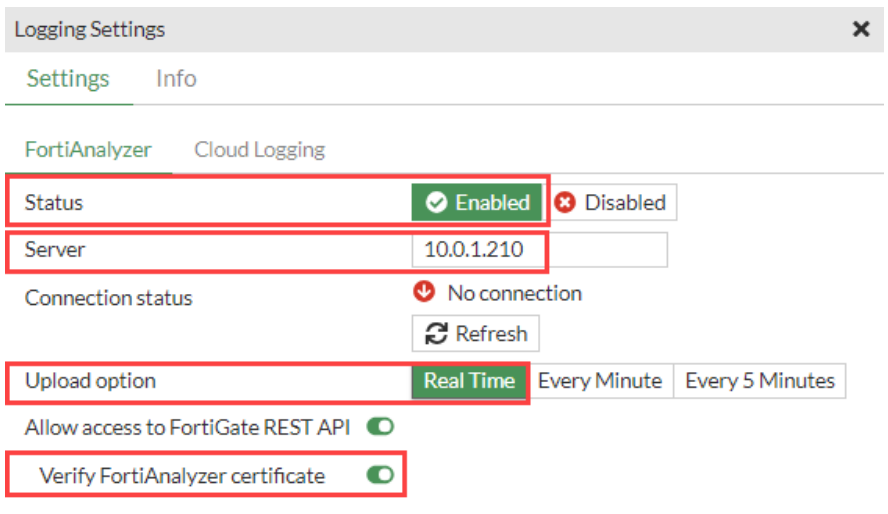
1. Log in to the Local-FortiGate GUI with the username `admin` and password `password`.
2. Click **Security Fabric** > **Fabric Connectors**.
3. Select **Logging & Analytics**, and then click **Edit**.



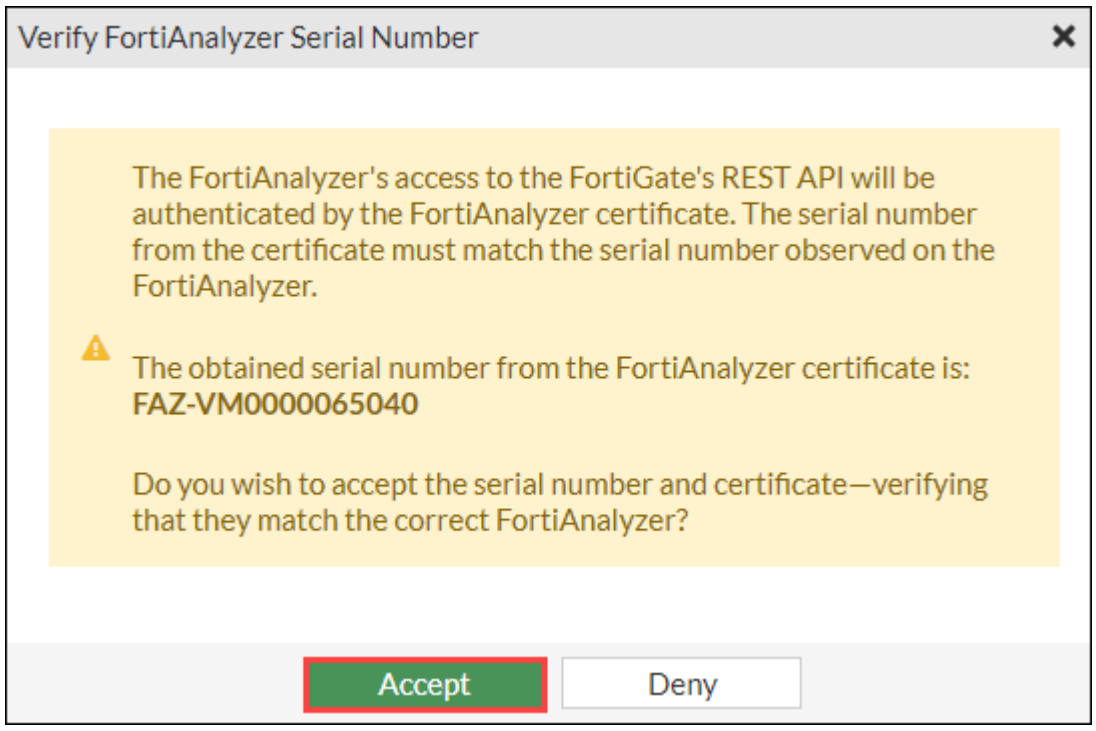
4. Enable **FortiAnalyzer Logging**.



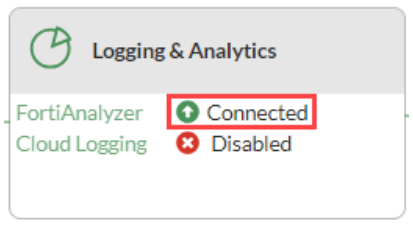
5. Edit the settings so they match the following image:



6. Click **OK**.
7. In the verification window that appears, click **Accept**.



8. Verify that the status of **Security Fabric** > **Fabric Connectors** > **Logging & Analytics** is **Connected**.



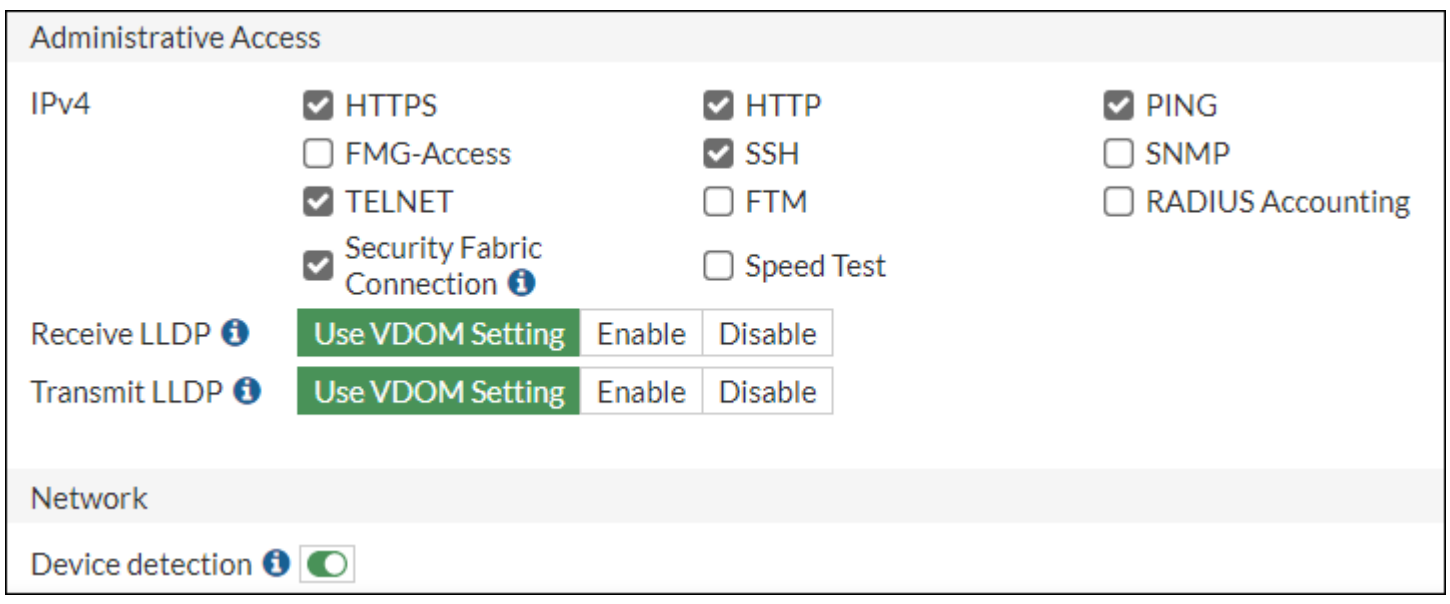
Configure the Security Fabric on Local-FortiGate (Root)

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:



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**.

Stop and think!

Why do you need to enable the **Security Fabric Connection** checkbox on the **port3** and **To-Remote-HQ2** interfaces on Local-FortiGate?

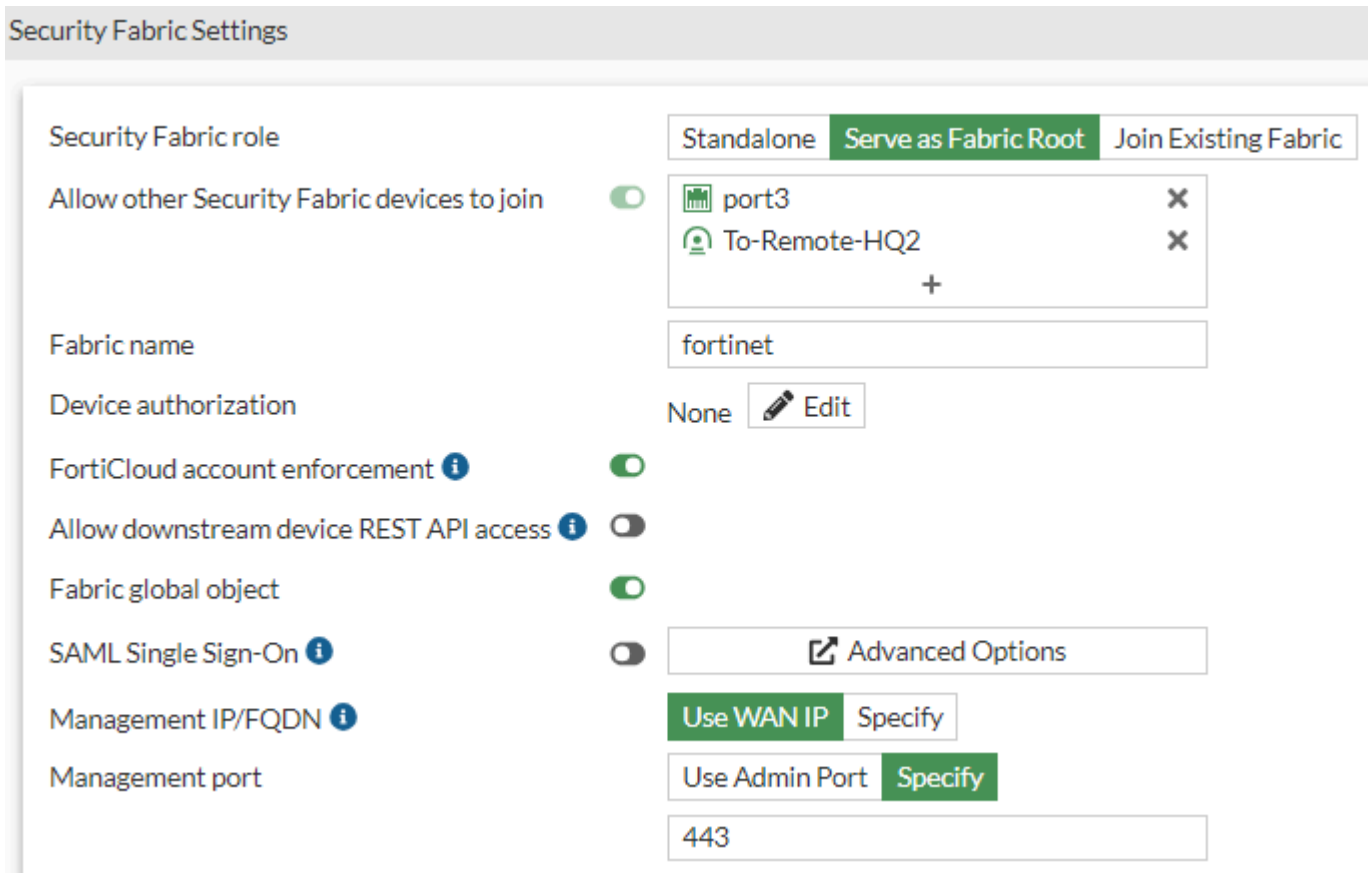
This is because both downstream FortiGate devices are connected to the root FortiGate (Local-FortiGate) through these ports, respectively. To join the Security Fabric, the root FortiGate must allow the Security Fabric connection on these ports.

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, in the **Security Fabric role** field, select **Serve as Fabric Root**.
4. Configure the following settings:

Field	Value
Allow other Security Fabric devices to join (ensure both interfaces are selected)	enable port3, To-Remote-HQ2
Fabric name	fortinet

Your configuration should look like the following example:



5. 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!

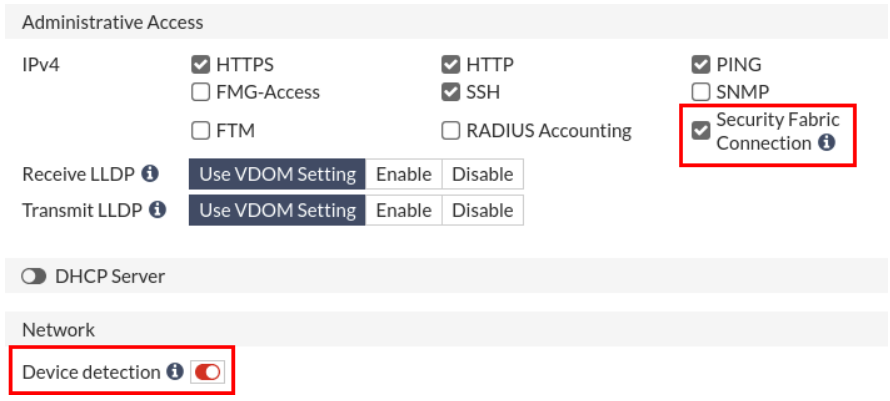
On the ISFW GUI, enable **Security Fabric Connection** on port1. Enable network device detection on the port. After you enable **Security Fabric Connection**, connect ISFW to the Security Fabric that has Local-FortiGate as its root device.

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 1 (#Test).

()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**.



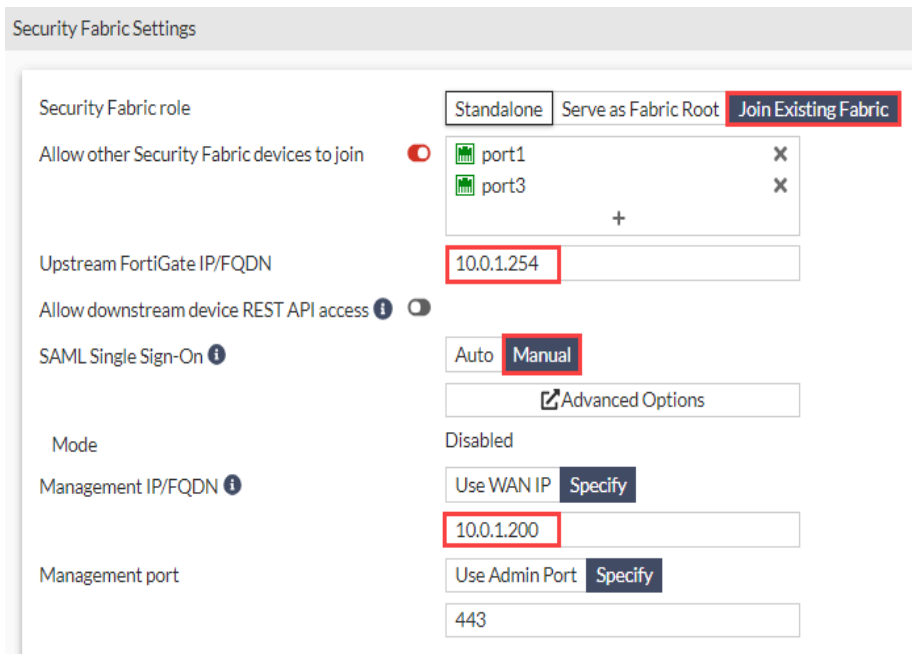
6. Click **OK**.

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, in the **Security Fabric role** field, select **Join Existing Fabric**.

4. In the **Upstream FortiGate IP**, type the IP address `10.0.1.254`.
5. In the **SAML Single Sign-On** field, select **Manual**.
6. In the **Management IP/FQDN** field, select **Specify**, and then type `10.0.1.200`.
7. In the **Management port** field, select **Specify**, and then type `443`.

Your configuration should look like the following example:



8. Click **OK**.
9. Click **OK** to confirm the settings.

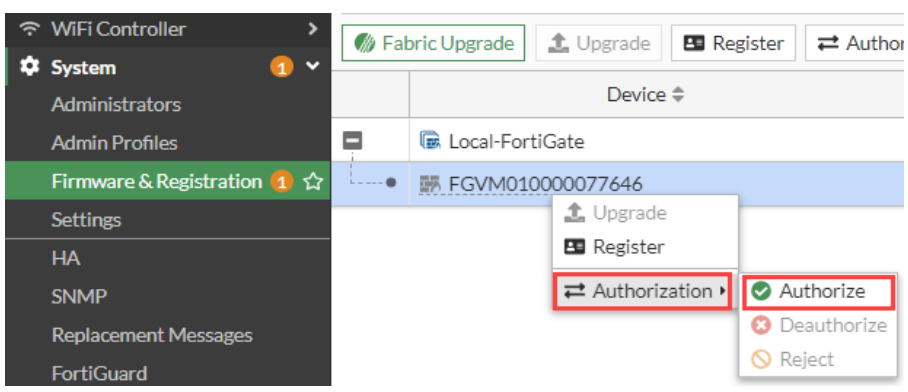
FortiAnalyzer logging is enabled on ISFW after the Security Fabric is enabled. Downstream FortiGate devices retrieve FortiAnalyzer settings from the root FortiGate when they join the Security Fabric.

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

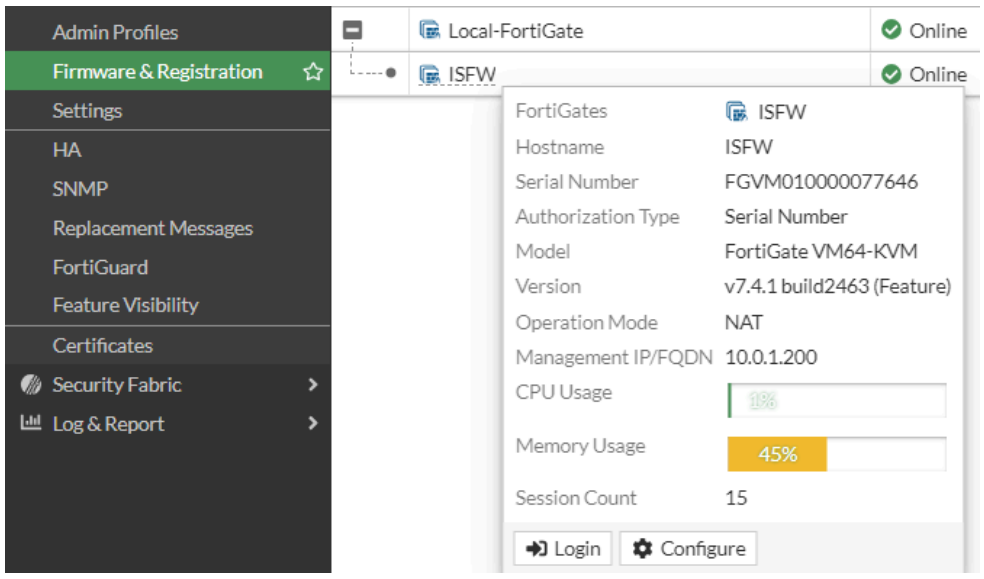
1. On the Local-FortiGate GUI, click **System** > **Firmware & Registration**.
2. Right-click the ISFW FortiGate serial number, select **Authorization**, and then click **Authorize**.



It may take a few minutes to authorize. You may need to refresh the page, or log out of the Local-FortiGate GUI and log in again.

After authorization, ISFW appears in the Security Fabric topology section, which means ISFW joined the Security Fabric successfully.

3. 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.



Check the Security Fabric Deployment Result

You will check the Security Fabric deployment result on Local-FortiGate (root).

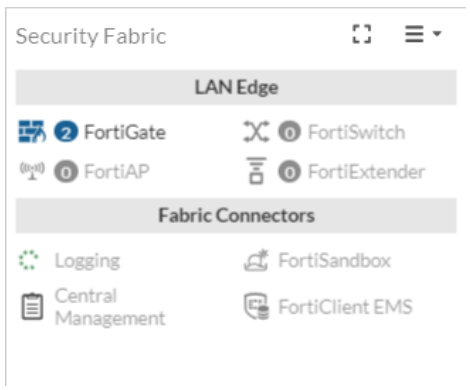
()To check the Security Fabric on Local-FortiGate

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

This is to generate some traffic from the Local-Client VM so it is included in the topology views.

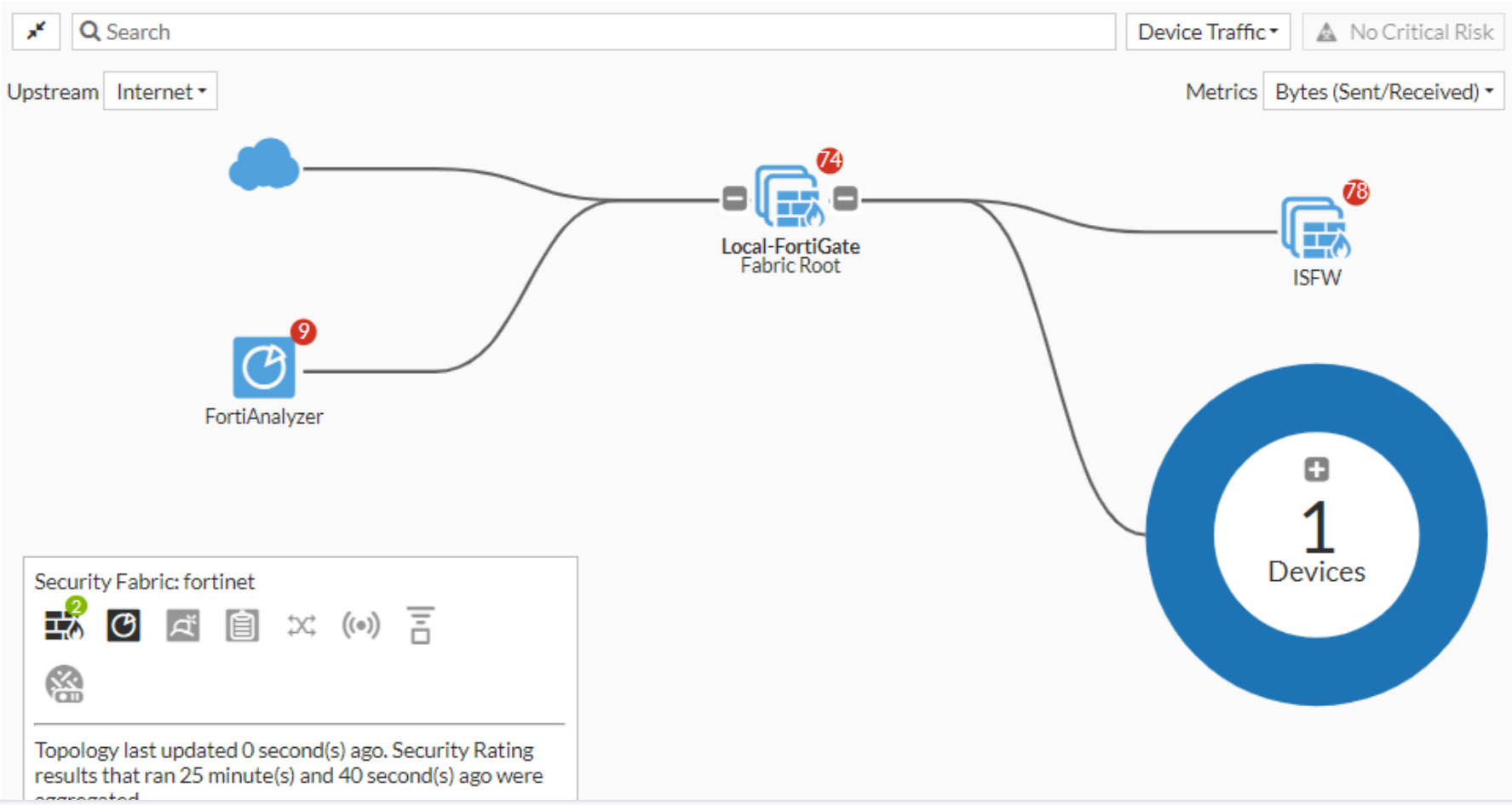
2. On the Local-FortiGate GUI, click **Dashboard** > **Status**.

The Security Fabric widget displays the FortiGate devices in the Security Fabric.



3. On the Local-FortiGate GUI, click **Security Fabric** > **Physical Topology**.
4. Click **Update Now** to update the topology view.

This page shows a visualization of access layer devices in the Security Fabric.


Search
Device Traffic
No Critical Risk
Upstream
Internet
Metrics
Bytes (Sent/Received)
74
Local-FortiGate
Fabric Root
78
ISFW
9
FortiAnalyzer
1
Devices
Security Fabric: fortinet
2
Topology last updated 0 second(s) ago. Security Rating results that ran 25 minute(s) and 40 second(s) ago were

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 1 (#Authoriz).

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.

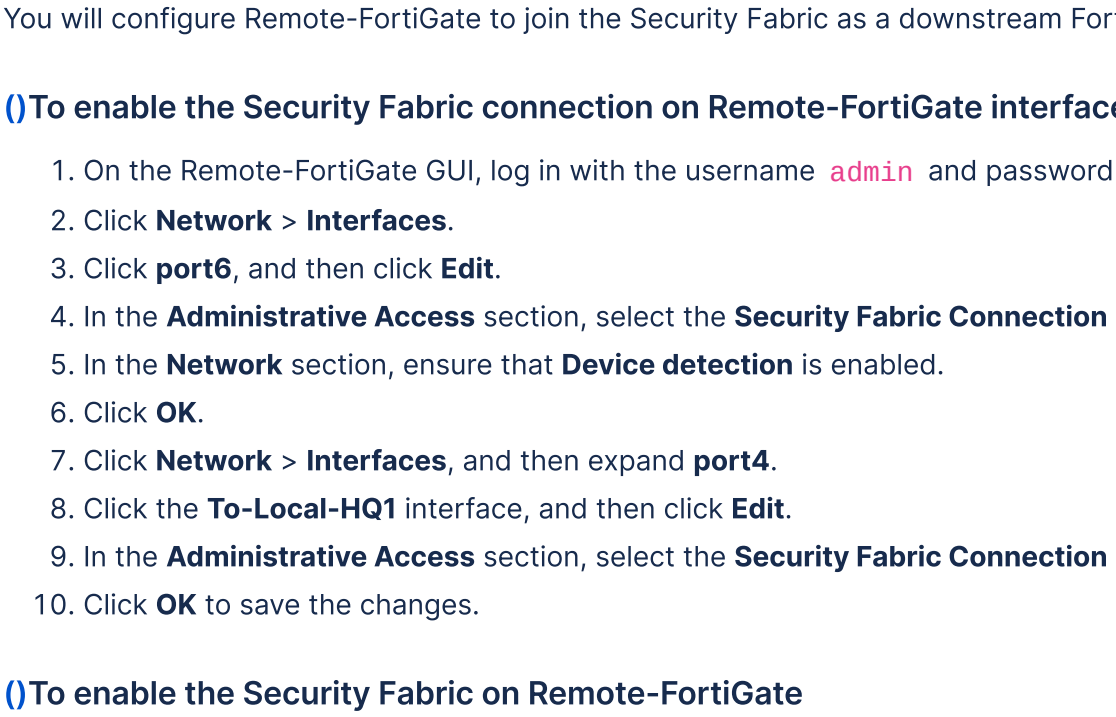
To enable the Security Fabric connection on Remote-FortiGate interfaces

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 role** field, ensure that **Join Existing Fabric** is selected.
4. In the **Upstream FortiGate IP** field, type `10.10.10.1`.
5. In the **SAML Single Sign-On** field, select **Manual**.
6. In the **Management IP/FQDN** field, click **Specify**, and then type `10.10.10.3`.

Your configuration should look like the following example:



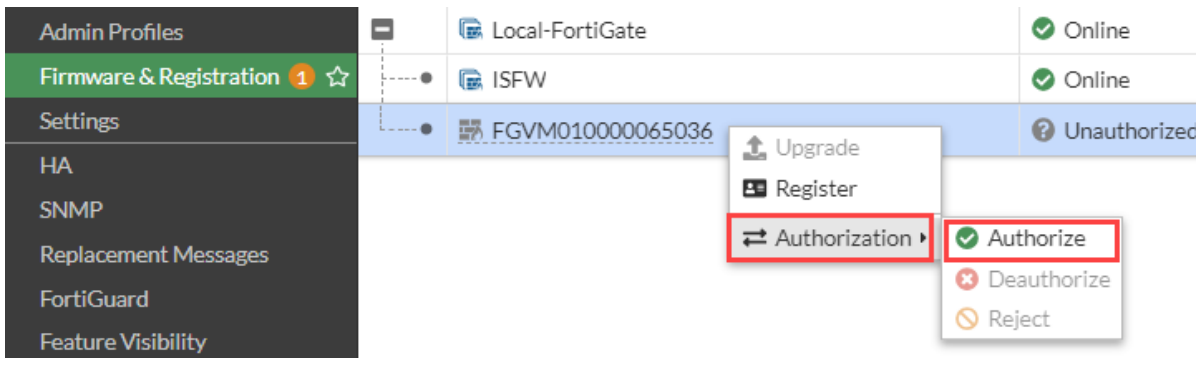
7. Click **OK**.
8. Click **OK** to confirm.

()Authorize Remote-FortiGate (Downstream) on Local-FortiGate (Root)

You will authorize Remote-FortiGate on Local-FortiGate to join the Security Fabric.

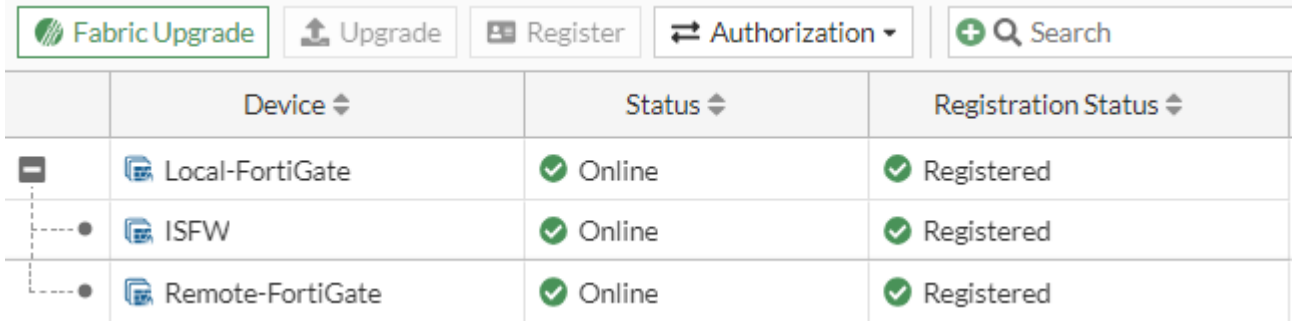
()To authorize Remote-FortiGate on Local-FortiGate

1. On the Local-FortiGate GUI, log in with the username `admin` and password `password`.
2. Click **System** > **Firmware & Registration**.
3. Right-click the Remote FortiGate serial number, select **Authorization**, and then click **Authorize**.



It may take a few minutes to authorize. You may need to refresh the page, or log out of the Local-FortiGate GUI and log in again.

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.

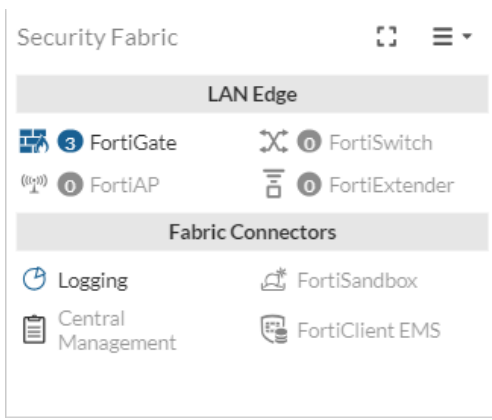
Check the Security Fabric Deployment Result

You will check the Security Fabric deployment result on the root, Local-FortiGate.

To check the Security Fabric on Local-FortiGate

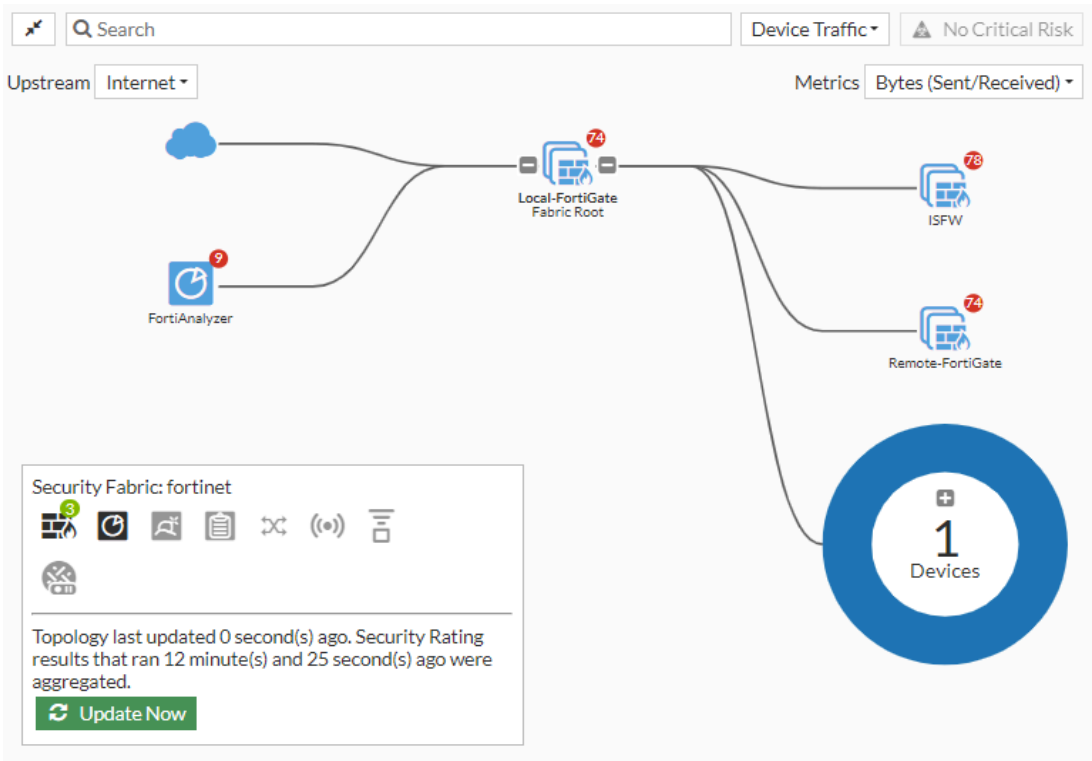
1. On the Local-FortiGate GUI, click **Dashboard** > **Status**.

The **Security Fabric** widget displays all FortiGate devices in the Security Fabric.



2. Click **Security Fabric** > **Physical Topology**.

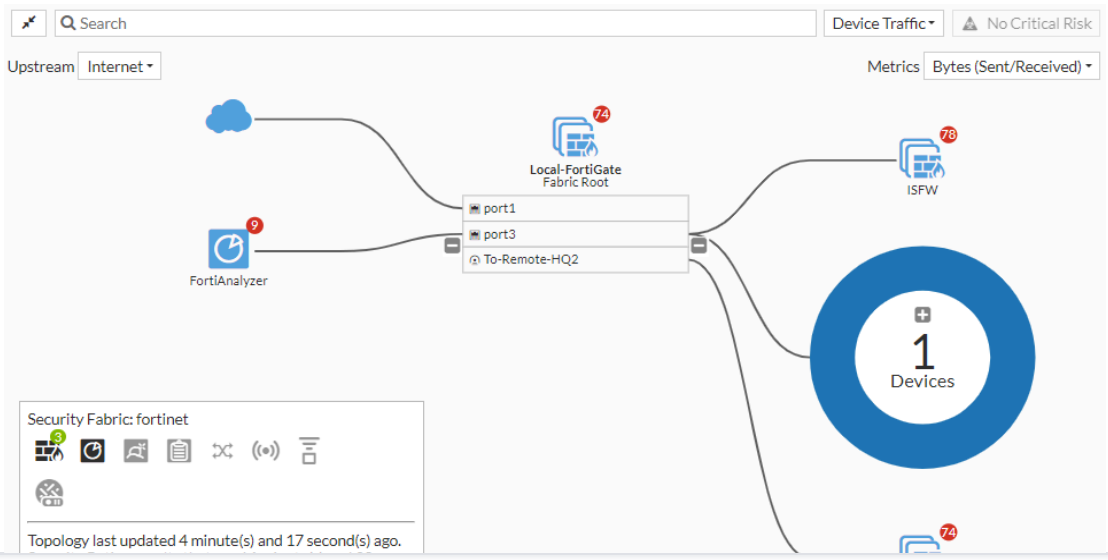
This page shows a visualization of access layer devices in the Security Fabric.



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.



Lab 13: Security Fabric

In this lab, you will learn how to configure the Fortinet Security Fabric. After you configure the Security Fabric, you will access the physical and logical topology views.

Objectives

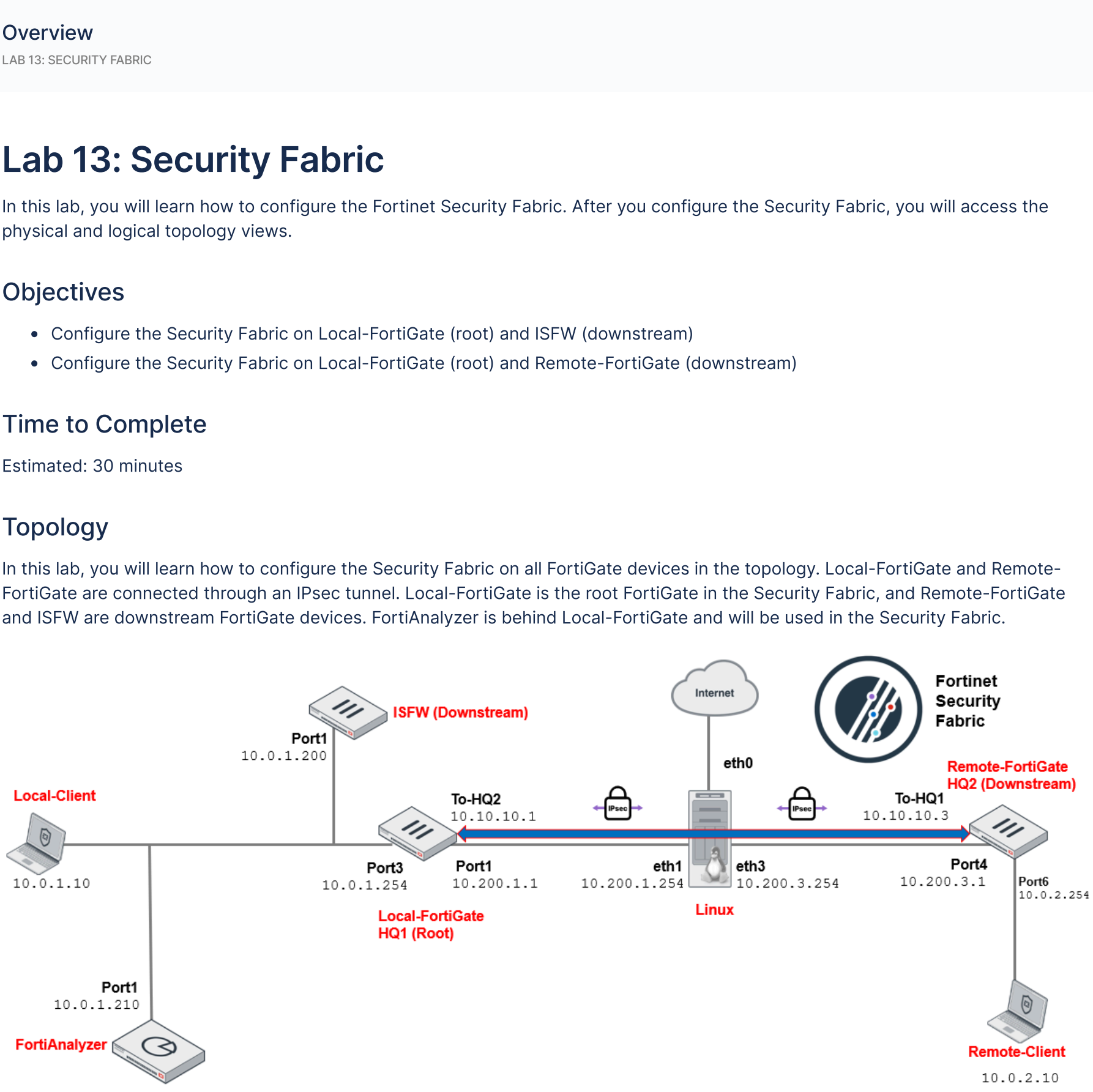
- Configure the Security Fabric on Local-FortiGate (root) and ISFW (downstream)
- Configure the Security Fabric on Local-FortiGate (root) and Remote-FortiGate (downstream)

Time to Complete

Estimated: 30 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.



LAB-13 > Security Fabric

Exercise 1: Configuring HA

FortiGate HA uses FGCP, which uses a heartbeat link for HA-related communications to discover other FortiGate devices in the same HA group, elect a primary device, synchronize configuration, and detect failed devices in an HA cluster.

In this exercise, you will examine how to configure HA settings on both FortiGate devices. You will observe the HA synchronization status, and use `diagnose` commands to verify that the configuration is in sync on both FortiGate devices.

Unless instructed otherwise, always use the console connection of Local-FortiGate and Remote-FortiGate to access the CLI. This ensures that you can access the CLI of the device regardless of the HA role.

Configure HA Settings on Local-FortiGate

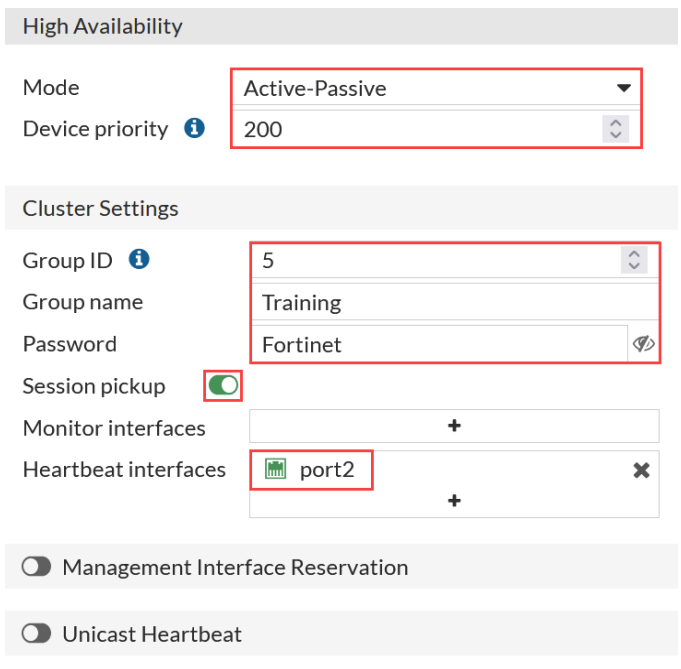
You will configure HA-related settings using the Local-FortiGate GUI.

To configure HA settings on Local-FortiGate

1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.
2. Click **System** > **HA**, and then configure the following HA settings:

Field	Value
Mode	Active-Passive
Device priority	200
Group ID	5
Group name	Training
Password	Fortinet **Tip**: Click **Change**, and then type the password.
Session pickup	<enable>
Monitor interfaces	Click **X** to remove any ports that are selected.
Heartbeat interfaces	Click **X** to remove port4, and then select port2.

The configuration should look like the following example:



3. Click **OK**.

Configure HA Settings on Remote-FortiGate

You will configure HA-related settings on Remote-FortiGate, using the console.

To configure HA settings on Remote-FortiGate

1. Connect to the Remote-FortiGate CLI, and then log in with the username `admin` and password `password`.
2. Enter the following commands:

config system ha

set mode a-p

set group-name Training

set group-id 5

set password Fortinet

set hbdev port2 0

set session-pickup enable

set override disable

set priority 100

end

Observe and Verify the HA Synchronization Status

Now that you have configured HA on both FortiGate devices, you will verify that HA is established and that the configurations are fully synchronized.

The checksums for all cluster members must match for the FortiGate devices to be synchronized.

To observe and verify the HA synchronization status

1. On the Remote-FortiGate CLI, notice the debug messages about the HA synchronization process.

These messages sometimes display useful status change information.

2. Wait 4–5 minutes for the FortiGate devices to synchronize.

After the FortiGate devices are synchronized, the Remote-FortiGate device logs out all admin users.

secondary succeeded to sync external files with primary

secondary starts to sync with primary

logout all admin users

3. When prompted, log back in to the Remote-FortiGate CLI with the username `admin` and password `password`.
4. Enter the following command to check the HA synchronization status:

diagnose sys ha checksum show

5. On the Local-FortiGate CLI, enter the following command to check the HA synchronization status:

diagnose sys ha checksum show

6. Compare the output from both FortiGate devices.

If both FortiGate devices are synchronized, the checksums match.

7. Alternatively, you can run the following CLI command on any member to view the checksums of all members:

diagnose sys ha checksum cluster

Verify FortiGate Roles in an HA Cluster

After the checksums of both FortiGate devices match, you will verify the cluster member roles to confirm the primary and secondary devices.

To verify FortiGate roles in an HA cluster

1. On both the Local-FortiGate CLI and Remote-FortiGate CLI, enter the following command to verify that the HA cluster is established:

get system status

2. On both FortiGate devices, view the `Current HA mode` line, and then write down the device serial number (`Serial-Number`).

Notice that Local-FortiGate is `a-p primary` and Remote-FortiGate is `a-p secondary` .

Stop and think!

Why was Local-FortiGate elected as the primary?

In the primary election process, FGCP first checks the number of connected monitored ports. Because you didn't configure monitored ports, FGCP then checks the next criterion.

As the override setting is disabled, FGCP checks the HA uptime next. Because you enabled HA on both devices about the same time, the HA uptime difference is less than 5 minutes.

Therefore, FGCP checks the next criterion, which is priority.

Local-FortiGate has a priority of 200, which is greater than Remote-FortiGate, which has a priority of 100. The result is that FGCP elects Local-FortiGate as the primary.

3. On the Local-FortiGate CLI , enter the following command to confirm the reason for the primary election:

get system ha status

4. In the output, look for the `Primary selected using` section to identify the reason for the latest primary election event.

Your output should look similar to the following example:

```
Primary selected using:
    <2023/09/21 10:52:56> vcluster-1: FGVM010000064692 is selected as the primary
 because its override priority is larger than peer member FGVM010000065036.
```

The output confirms that FGCP elected Local-FortiGate as the primary because of its higher priority.

If you see that the election reason is a higher uptime, then that is probably because you rebooted one of the members, and as a result, the HA uptime of that device was reset. The reboot then caused the HA uptime difference to be more than 5 minutes.

Exercise 2: Triggering an HA Failover

You set up an HA cluster. In this exercise, you will examine how to trigger an HA failover, and observe the renegotiation among devices to elect a new primary device.

Unless instructed otherwise, always use the console connection of Local-FortiGate and Remote-FortiGate to access the CLI. This ensures that you can access the device CLI regardless of the HA role.

Trigger a Failover by Rebooting the Primary FortiGate

You will reboot the primary FortiGate in the cluster to trigger a failover.

Take the Expert Challenge!

1. On the Local-Client VM, complete the following:
   - Play a long video (more than 5 minutes long) on https://www.youtube.com (https://www.youtube.com/).
   - Run a continuous ping to IP address `4.2.2.2`.
2. On the Local-FortiGate CLI, reboot Local-FortiGate.

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

After you have performed these steps, see Verify the HA Failover and FortiGate Roles on page 1 (#Verify_the_HA_Failover_and_FortiGate_Roles).

To trigger a failover by rebooting the primary FortiGate

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

https://www.youtube.com (https://www.youtube.com/)

2. Play a long video (more than 5 minutes long).
3. While the video is playing, open a terminal, and then enter the following command to run a continuous ping to a public IP address:

ping 4.2.2.2

4. On the Local-FortiGate CLI, enter the following command to reboot Local-FortiGate and trigger a failover:

execute reboot

5. Press `Y` to confirm that you want to reboot Local-FortiGate.

()Verify the HA Failover and FortiGate Roles

You will verify the HA failover, and check the roles of FortiGate in an HA cluster.

To verify the HA failover and FortiGate roles

1. On the Local-Client VM, check the video and terminal that you started earlier.

Because of the failover, Remote-FortiGate is now the primary processor of traffic. Your ping and video should still be running.

2. Close the browser tab with the video.
3. Return to the terminal, and then press `Ctrl` + `C` to stop the ping.
4. On the Remote-FortiGate CLI, enter the following command to verify that Remote-FortiGate is acting as the primary device in the HA cluster :

get system status

Stop and think!

When Local-FortiGate finishes rebooting and rejoins the cluster, does it rejoin as the *secondary* device, or resume its initial role of the *primary* device?

5. On any FortiGate in the cluster, enter the following command to see the status of all cluster members:

```
get system ha status
```

You should see that Local-FortiGate rejoins the cluster as a secondary device. It lost its role as the primary device.

```
Primary     : Remote-FortiGate, FGVM010000065036, HA cluster index = 0
Secondary   : Local-FortiGate , FGVM010000064692, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Primary: FGVM010000065036, HA operating index = 0
Secondary: FGVM010000064692, HA operating index = 1
```

Local-FortiGate becomes the secondary device in the cluster because it has a lower HA uptime than Remote-FortiGate. In addition, the HA uptime difference between the members is more than 5 minutes.

Also, the override setting is disabled, so priority does not take precedence over uptime.

Trigger an HA Failover by Resetting the HA Uptime

You will trigger a failover by resetting the HA uptime on the current primary FortiGate—which should be Remote-FortiGate—and then you will verify the role of Remote-FortiGate in the HA cluster.

To trigger an HA failover by resetting the HA uptime on FortiGate

1. On the Remote-FortiGate CLI console, enter the following command:

```
diagnose sys ha reset-uptime
```

After you reset the HA uptime on Remote-FortiGate, Local-FortiGate becomes the member with the highest HA uptime. Because the HA uptime difference between the members is more than 5 minutes, Local-FortiGate is elected as the new primary.

Remote-FortiGate now has the *secondary* role in the cluster.

2. On the Remote-FortiGate CLI, enter the following command to verify this:

```
get system status
```

Observe HA Leave and Join Messages Using Diagnostic Commands

The HA synchronization process is responsible for FGCP packets that communicate cluster status and build the cluster. You will use real-time diagnostic commands to observe this process.

To observe HA failover using diagnostic commands

1. On the Local-FortiGate CLI, enter the following commands:

```
diagnose debug enable
diagnose debug application hatalk 0
diagnose debug application hatalk 255
```

The `diagnose debug application hatalk 0` command stops the debug. You will use this command later.

2. On the Remote-FortiGate CLI, enter the following command to reboot Remote-FortiGate:

```
execute reboot
```

3. Press `Y` to confirm that you want to reboot Remote-FortiGate.
4. On the Local-FortiGate CLI, view the output while the secondary device reboots and starts communicating with the cluster.

```
Local-FortiGate # <hatalk> vcluster_1: ha_prio=0(primary), state/chg_time/now=2(work)/16
95334783/1695335504
<hatalk> member 'FGVM010000065036' lost heartbeat on hbdev 'port2': now=311076, last_hb_
jiffies+timeout=310674+400=311074
<hatalk> lost member 'FGVM010000065036' heartbeat, delete it
<hatalk> deleting gmember 'FGVM010000065036'
<hatalk> vcluster_1: deleting vmember 'FGVM010000065036'
<hatalk> vcluster_1: reelect=1, delete-vmember
<hatalk> cfg_changed is set to 1: hatalk_del_member
<hatalk> vcluster_1: reelect=0, hatalk_vcluster_timer_func
<hatalk> vcluster_1: 'FGVM010000064692' is elected as the cluster primary of 1 members

<hatalk> parse options for 'FGVM010000065036', packet_version=1
<hatalk> new member 'FGVM010000065036' is added into group
<hatalk> [hatalk_gmember_update_last_hb_jiffies:200] recv hb packet from 'FGVM0100000650
36' on hbdev='port2' since last_lost_jiffies=0/318220
<hatalk> vcluster_1: vmember 'FGVM010000065036' updated, override=0, usr_priority=100, m
ondev/pingsvr=0/0, uptime/reset_count=0/0, flag=0x00000000
<hatalk> cfg_changed is set to 1: hatalk_vcluster_add_vmember
<hatalk> cfg_changed is set to 0: hatalk_packet_setup_heartbeat
<hatalk> setup new heartbeat packet: hbdev='port2', packet_version=23
<hatalk> options buf is small: opt_type=41(DEVINFO), opt_sz=13806, buf_sz=1178
<hatalk> pack compressed dev info: dev_nr=8, orig_sz=13800, z_len=95
<hatalk> heartbeat packet is set on hbdev 'port2'
<hatalk> vcluster_1: reelect=1, vmember updated
<hatalk> vcluster_1: 'FGVM010000064692' is elected as the cluster primary of 2 members
<hatalk> vcluster_1: state changed, 2(work)->2(work)
<hatalk> vcluster_1: work_as_primary immediately
<hatalk> 'port2' is selected as 'port_ha'
<hatalk> vcluster_1: start sending garps
<hatalk> hatalk clear mgmt session total 2
```

The sanitized output shows that the current primary FortiGate is sending heartbeat packets and trying to synchronize its configuration with the configuration of the secondary FortiGate.

5. Press the up arrow key twice, select the second-last command (in this case, `diagnose debug application hatalk 0`), and

Exercise 3: Configuring the HA Management Interface

In this exercise, you will examine how to configure a spare interface in the cluster as a reserved HA management interface. This allows both FortiGate devices to be reachable for management purposes regardless of the member role.

If you don't configure a reserved HA management interface, the primary FortiGate handles your cluster management connections. However, you can access the CLI of the secondary FortiGate from the primary FortiGate CLI, or by using the console connection of the secondary FortiGate.

You can also configure an in-band HA management interface, which is an alternative to the reserved HA management interface, and does *not* require reserving an interface that is only for management access.

Unless instructed otherwise, always use the console connection of Local-FortiGate and Remote-FortiGate to access the CLI. This ensures that you can access the device CLI regardless of the HA role.

Access the Secondary FortiGate CLI Through the Primary FortiGate CLI

You will connect to the secondary FortiGate CLI through the primary FortiGate CLI.

To access the secondary FortiGate CLI through the primary FortiGate CLI

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following command to access the secondary FortiGate CLI through the primary FortiGate heartbeat interface:

execute ha manage <id> admin

Use `?` to list the values for `<id>`.

```
Local-FortiGate #
Local-FortiGate # execute ha manage
<id>    please input peer box index.
<0>     Subsidiary unit FGVM0100000

Local-FortiGate # execute ha manage 0 admin
```

3. When prompted, enter the password `password` to log in to Remote-FortiGate.

```
Local-FortiGate # execute ha manage 0 admin
Warning: Permanently added '169.254.0.1' (ED
admin@169.254.0.1's password:
Remote-FortiGate #
```

4. Enter the following command to get the status of the secondary FortiGate:

get system status

5. View the `Current HA mode` line.

You will notice that Remote-FortiGate is `a-p secondary`.

6. Enter the following command to return to the Local-FortiGate CLI:

exit

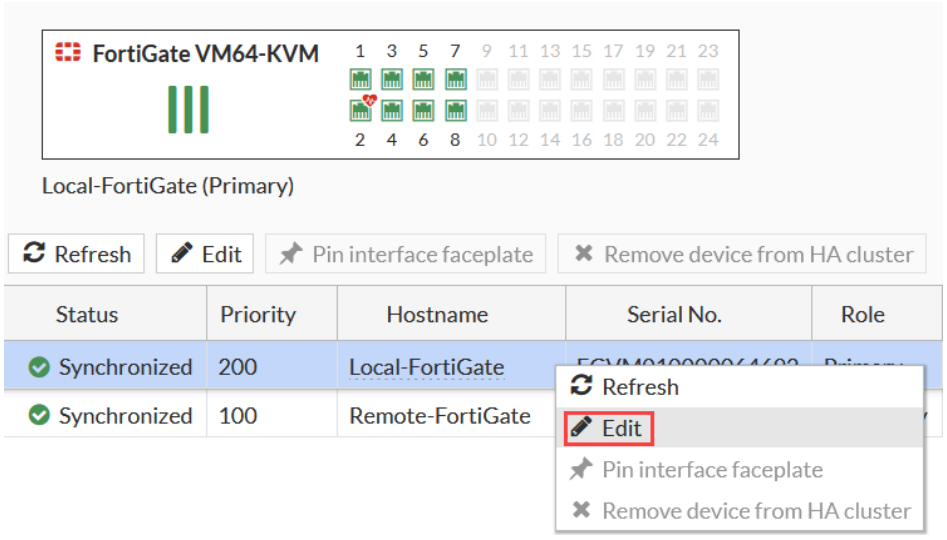
Set Up a Reserved HA Management Interface

You will use an unused interface on the FortiGate devices in an HA cluster to configure a reserved HA management interface and a unique IP address for each member. This way, you can access each member directly, regardless of its role.

To set up a reserved HA management interface

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. Click **System** > **HA**.
3. Right-click **Local-FortiGate**, and then click **Edit**.



4. Enable **Management Interface Reservation**, and then in the **Interface** field, select **port7**.
5. Click **OK**.

port7 connects to the same LAN segment as port3.

Configure and Access the Primary FortiGate Using the Reserved HA Management Interface

You will configure and verify access to the primary FortiGate using the reserved HA management interface.

To configure and verify access to the primary FortiGate using the reserved HA management interface

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following commands to configure port7:

```
config system interface
edit port7
set ip 10.0.1.253/24
set allowaccess ping ssh snmp http https
end
```

Even though this address overlaps with port3, which is not allowed by default (FortiGate does not allow overlapped subnets by default), it is allowed here because the routing entries for the reserved HA management interface are excluded from the routing table.

3. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.0.1.253` (note the IP address) with the username `admin` and password `password`.

This verifies connectivity to port7.

Configure and Access the Secondary FortiGate Using the Reserved HA Management Interface

You will configure and verify access to the secondary FortiGate using the reserved HA management interface.

Take the Expert Challenge!

1. On the Remote-FortiGate CLI, complete the following:

- Verify that the reserved HA management interface is synchronized with the secondary device.

`show system ha`

- Verify that **port7** has no configuration, and then configure **port7 IP/Netmask** as `10.0.1.252/24` with the same `allowaccess` configured for Local-FortiGate **port7**.

2. On the Local-Client VM, log in to the Remote-FortiGate GUI (`admin` / `password`) using the port7 IP address to verify connectivity.

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

After the configuration is ready, see Disconnect Remote-FortiGate From the Cluster on page 1 (#Disconnect_Remote-FortiGate_From_the_Cluster).

To configure and verify access to the secondary FortiGate using the management interface

1. On the Remote-FortiGate CLI, enter the following command to verify that the reserved HA management interface is synchronized with the secondary device:

```
show system ha
```

Look for `ha-mgmt-status` and `config ha-mgmt-interfaces`. These should already be set.

2. Enter the following command to verify that port7 has no configuration:

```
show system interface port7
```

3. Configure port7, using the following commands:

```
config system interface
edit port7
set ip 10.0.1.252/24
set allowaccess ping ssh snmp http https
next
end
```

4. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI at `10.0.1.252` (note the IP address) with the username `admin` and password `password`.

This will verify connectivity to port7.

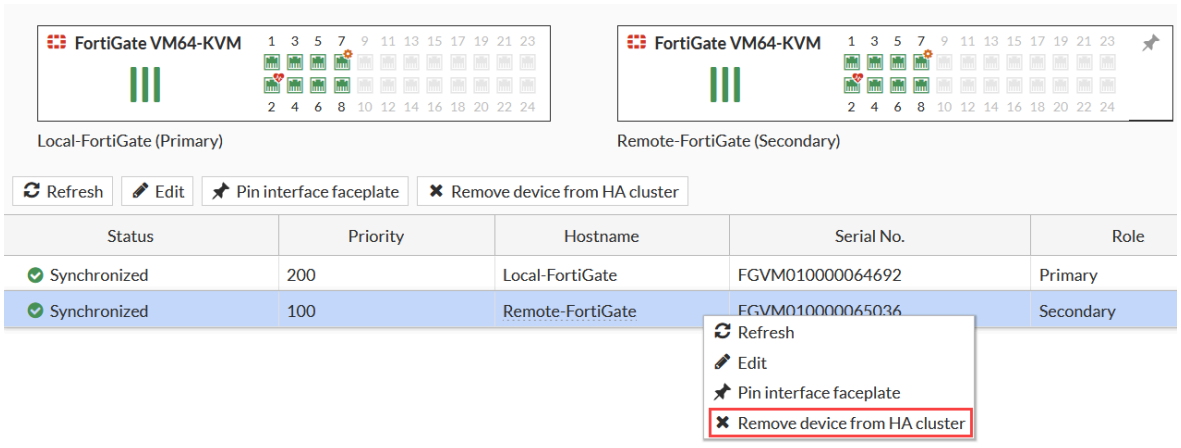
Each device in the cluster now has its own management IP address for monitoring purposes.

()Disconnect Remote-FortiGate From the Cluster

You will disconnect Remote-FortiGate from the cluster. Remote-FortiGate will prompt you to configure an IP address on any port on Remote-FortiGate so that you can access it after the disconnection.

To disconnect Remote-FortiGate from the cluster

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. Click **System** > **HA**.
3. Right-click **Remote-FortiGate**, and then click **Remove device from HA cluster**.



4. When prompted, configure the following settings:

Field	Value
Interface	port3
IP/Netmask	10.0.1.251/24

5. Click **OK**.

This removes the FortiGate from the HA cluster.

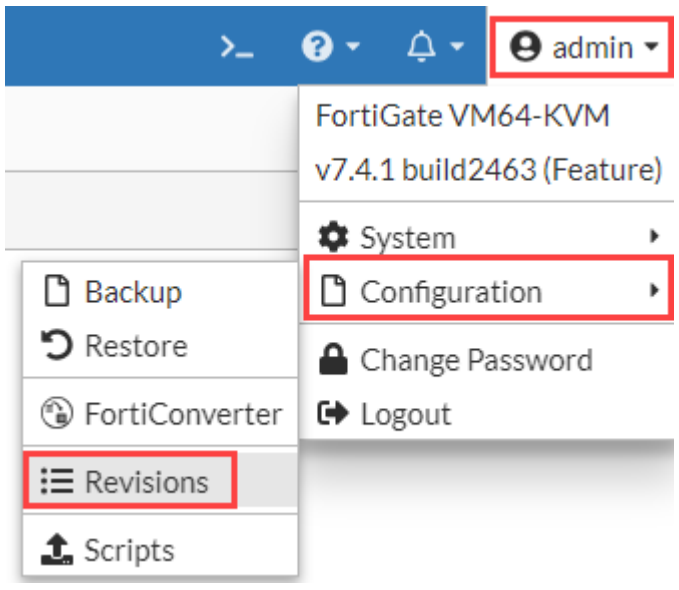
Restore the Remote-FortiGate Configuration

You will restore the Remote-FortiGate configuration, so that you can use Remote-FortiGate in the next labs.

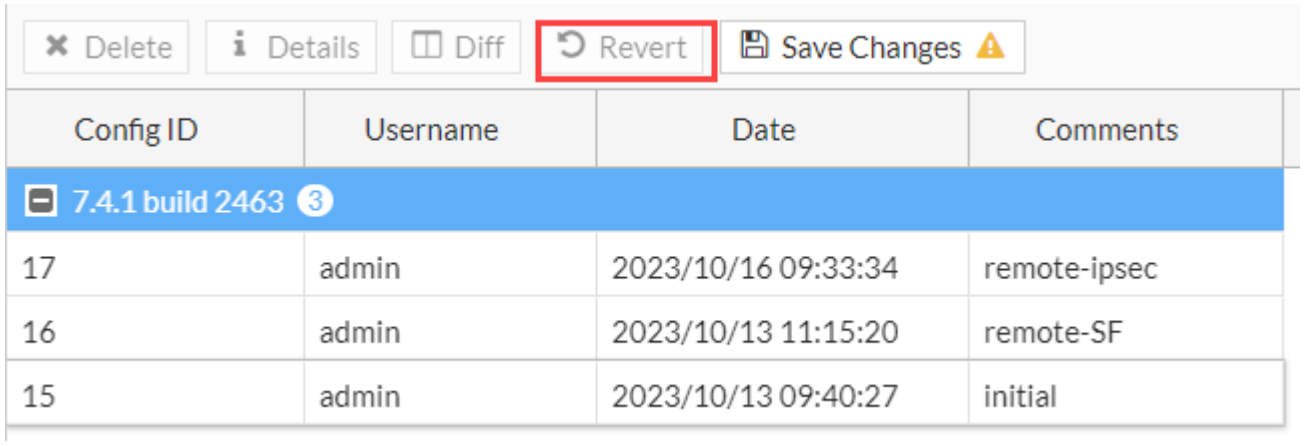
Failure to perform these steps will prevent you from doing the next exercises.

To restore the Remote-FortiGate configuration file

1. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI at `10.0.1.251` with the username `admin` and password `password`.
2. In the upper-right corner, 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**.



5. Click **OK** to reboot.

Failure to perform these steps will prevent you from doing the next exercises.

Lab 14: High Availability

In this lab, you will examine how to set up a FortiGate Clustering Protocol (FGCP) high availability (HA) cluster of FortiGate devices. You will explore active-passive HA mode and observe FortiGate HA behavior. You will also perform an HA failover and use diagnostic commands to observe the election of a new primary device in the cluster. Finally, you will configure management ports on FortiGate devices to reach each FortiGate individually for management purposes.

Objectives

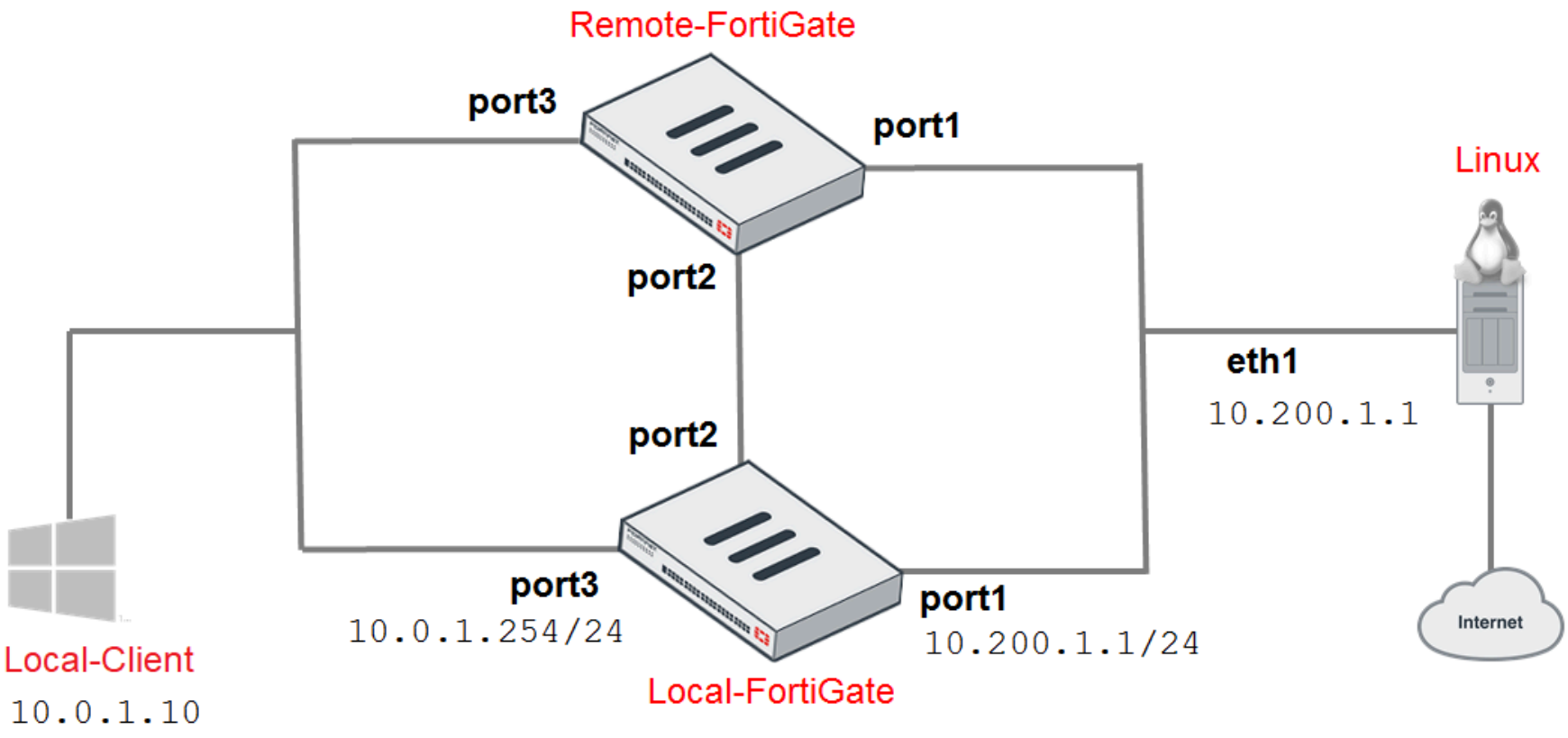
- Set up an HA cluster using FortiGate devices
- Observe HA synchronization and interpret diagnostic output
- Perform an HA failover
- Manage individual cluster members by configuring a reserved management interface

Time to Complete

Estimated: 40 minutes

Lab HA Topology

After you upload the required configurations to each FortiGate, the logical topology will change to the following:



Lab 15: Diagnostics Performance

In this lab, you will run diagnostic commands to learn about the current status of FortiGate. You will also use the sniffer and debug flow tools to troubleshoot and fix a connectivity problem.

Objectives

- Monitor for abnormal behavior, such as traffic spikes
- Diagnose problems at the physical and network layers
- Diagnose connectivity problems using the GUI debug flow tool
- Diagnose resource problems, such as high CPU or memory usage

Time to Complete

Estimated: 30 minutes
LAB-15 > Diagnostics Performance

Exercise 1: Determining What Is Happening Now

In this exercise, you will use CLI commands to get information about FortiGate, such as traffic volume, CPU usage, memory usage, and the ARP table.

Run Diagnostic Commands

You will run some diagnostic commands and make a note of some of the information displayed.

To run diagnostic commands

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Find the following information and write down your answers in the space provided—refer to the list of commands that follows to get the answers:

Field	Value
Firmware branch point	
Current HA mode	
Host name	
CPU utilization	
Memory utilization	
Average network usage	
Average session setup rate	
Negotiated speed and duplex mode for interface port1	
MTU for port1	
MAC address for the IP address 10.200.1.254	
Name of the process consuming the most CPU (if any)	
Name of the process consuming the most memory	

Enter the following CLI commands to find the information requested above:

get system status

get system performance status

get hardware nic port1

get system arp

diagnose sys top 1

(Press `Shift` + `P` to order the processes by CPU usage, `Shift` + `M` to order them by memory usage, or `Q` to stop.)

3. Close the Local-FortiGate CLI session.

Exercise 2: Troubleshooting a Connectivity Problem

In this exercise, you will use the sniffer and debug flow tool to troubleshoot a network connectivity problem.

Identify the Problem

As you will see in this procedure, there is a network connectivity problem between the Local-Client VM and the Linux server.

To identify the problem

1. On the Local-Client VM, open a terminal window.
2. Enter the following command to start a continuous ping to the Linux server (IP address `10.200.1.254`):

```
ping 10.200.1.254
```

The ping is failing. You will use the sniffer and debug flow tool on Local-FortiGate to find out why.

3. Do not close the terminal window—keep the ping running.

Use the Sniffer

> **Take the Expert Challenge!**
>
> Now that you understand what the problem is, try to fix it without looking at the FortiGate configuration. Use the built-in sniffer and debug flow tool to troubleshoot the problem.
>
> 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 Fix on page 1 (#Testing).

You will start troubleshooting by sniffing the ICMP traffic going to the Linux server.

To use the sniffer

1. On the Local-FortiGate CLI, log in with the username `admin` and password `password`.
2. Enter the following command to sniff the ICMP traffic to `10.200.1.254`:

```
diagnose sniffer packet any "icmp and host 10.200.1.254" 4
```

3. Observe the output.

```
interfaces=[any]
filters=[icmp and host 10.200.1.254]
5.439019 port3 in 10.0.1.10 → 10.200.1.254: icmp: echo request
10.442347 port3 in 10.0.1.10 → 10.200.1.254: icmp: echo request
15.444343 port3 in 10.0.1.10 → 10.200.1.254: icmp: echo request
20.545397 port3 in 10.0.1.10 → 10.200.1.254: icmp: echo request
```

The packets are arriving on FortiGate, but FortiGate is not routing them.

4. Press `Ctrl` + `C` to stop the sniffer.

Use the GUI Debug Flow Tool

You will run the GUI debug flow tool to get information about why FortiGate is dropping the packets.

To use the GUI debug flow tool

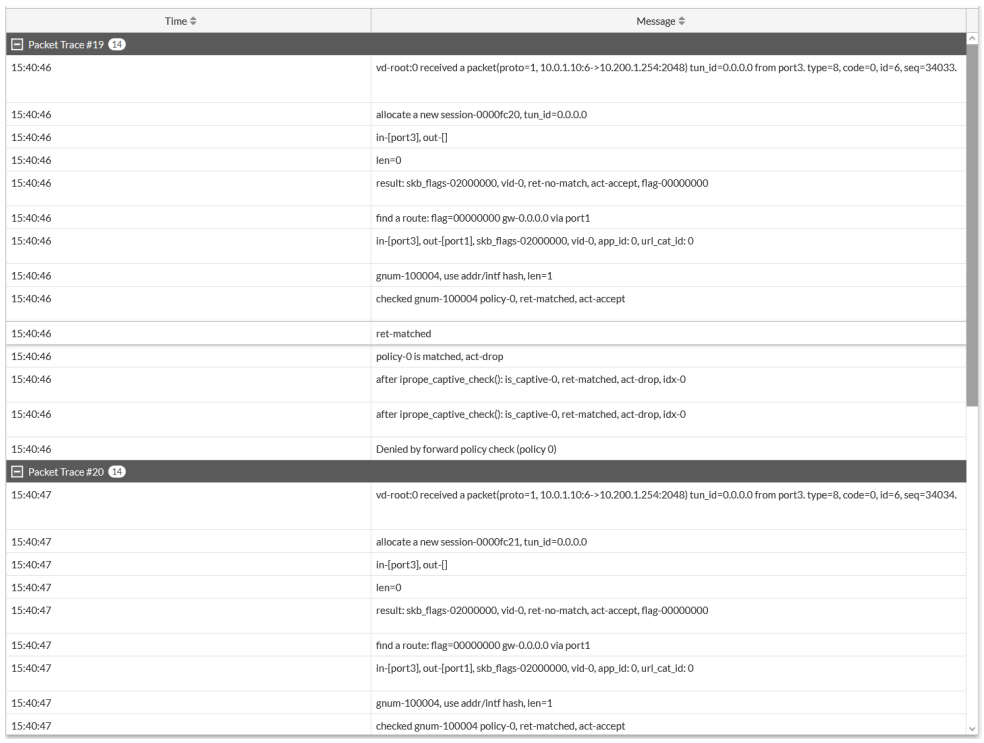
1. Connect to the Local-FortiGate GUI, and then log in with the username `admin` and password `password`.

2. Click **Network** > **Diagnostics**, and then click the **Debug Flow** tab.
3. In the **Number of packets** field, change the value to `3` packets.
4. Enable **Filters**, and then configure the following settings:

Field	Value
IP address	10.200.1.254
Protocol	ICMP

5. Click **Start debug flow**.

The output should be similar to the following example:



Time	Message
Packet Trace #19 14	
15:40:46	vd-root:0 received a packet(proto=1, 10.0.1.10:6->10.200.1.254:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=6, seq=34033.
15:40:46	allocate a new session-0000fc20, tun_id=0.0.0.0
15:40:46	in-[port3], out-[]
15:40:46	len=0
15:40:46	result: skb_flags-02000000, vid-0, ret-no-match, act-accept, flag-00000000
15:40:46	find a route: flag=00000000 gw-0.0.0.0 via port1
15:40:46	in-[port3], out-[port1], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0
15:40:46	gnum-100004, use addr/intf hash, len=1
15:40:46	checked gnum-100004 policy-0, ret-matched, act-accept
15:40:46	ret-matched
15:40:46	policy-0 is matched, act-drop
15:40:46	after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-0
15:40:46	after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-0
15:40:46	Denied by forward policy check (policy 0)
Packet Trace #20 14	
15:40:47	vd-root:0 received a packet(proto=1, 10.0.1.10:6->10.200.1.254:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=6, seq=34034.
15:40:47	allocate a new session-0000fc21, tun_id=0.0.0.0
15:40:47	in-[port3], out-[]
15:40:47	len=0
15:40:47	result: skb_flags-02000000, vid-0, ret-no-match, act-accept, flag-00000000
15:40:47	find a route: flag=00000000 gw-0.0.0.0 via port1
15:40:47	in-[port3], out-[port1], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0
15:40:47	gnum-100004, use addr/intf hash, len=1
15:40:47	checked gnum-100004 policy-0, ret-matched, act-accept

FortiGate receives the ICMP packet from `10.0.1.10` to `10.200.1.254` from `port3`.

vd-root:0 received a packet(proto=1, 10.0.1.10:6→10.200.1.254:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=6, seq=34033.

It creates a new session.

allocate a new session-0000fc20, tun_id=0.0.0.0

It finds a route for the destination `10.200.1.254` through `port1`.

find a route: flag=00000000 gw-0.0.0.0 via port1

It drops the packet. The debug flow shows the error message.

Denied by forward policy check (policy 0)

The `Denied by forward policy check` message indicates that a firewall policy denied the traffic. It could be either a denied policy that the administrator explicitly configured, or the implicit denied policy for traffic that does not match a configured policy.

The `policy 0` indicates that the default implicit policy denied the traffic. If an explicitly configured policy blocked the traffic, its policy ID number would be indicated in this output, instead of `0`.

Fix the Problem

Now that you have found the cause of the problem, you will fix it.

To fix the problem

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Look at the firewall policies.

The **Full_Access** firewall policy does not allow ICMP traffic (only HTTP)—this is why FortiGate is dropping the ping packets.

3. Edit the **Full_Access** firewall policy.
4. Change the service from **HTTP** to **ALL**.
5. Click **OK**.

()Test the Fix

You will test to confirm that the configuration change fixed the problem.

To test the fix

1. On the Local-Client VM, check the terminal window to see if the continuous ping is working now.
2. Press `Ctrl` + `C` to stop the ping, but leave the terminal open.
3. On the Local-FortiGate CLI session where you are running debug commands, clear all the ICMP sessions from the session table, using the following commands:

diagnose sys session filter clear

diagnose sys session filter proto 1

diagnose sys session clear

4. Continuing on the Local-FortiGate GUI, click **Network** > **Diagnostics**, and then click the **Debug Flow** tab.
5. In the **Number of packets** field, change the value to `3` packets.
6. Enable **Filters**, and then configure the following settings:

Field	Value
IP address	10.200.1.254
Protocol	ICMP

7. Click **Start debug flow**.

There should not be any output yet, because the ping is not running.

8. Return to the terminal window, and then start the ping again.

ping 10.200.1.254

9. Check the debug flow output.

Packet Trace #22 24

16:32:41	vd-root:0 received a packet(proto=1, 10.0.1.10:7->10.200.1.254:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=7, seq=1.
16:32:41	allocate a new session-00010feb, tun_id=0.0.0.0
16:32:41	in-[port3], out-[]
16:32:41	len=0
16:32:41	result: skb_flags-02000000, vid-0, ret-no-match, act-accept, flag-00000000
16:32:41	find a route: flag=00000000 gw-0.0.0.0 via port1
16:32:41	in-[port3], out-[port1], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0
16:32:41	gnum-100004, use addr/intf hash, len=2
16:32:41	checked gnum-100004 policy-1, ret-matched, act-accept
16:32:41	ret-matched
16:32:41	gnum-4e20, check-000000003d334358
16:32:41	checked gnum-4e20 policy-6, ret-no-match, act-accept
16:32:41	checked gnum-4e20 policy-6, ret-no-match, act-accept
16:32:41	checked gnum-4e20 policy-6, ret-no-match, act-accept
16:32:41	gnum-4e20 check result: ret-no-match, act-accept, flag-00000000, flag2-00000000
16:32:41	find SNAT: IP-10.200.1.1(from IPPOOL), port-60424
16:32:41	policy-1 is matched, act-accept
16:32:41	after iprope_captive_check(): is_captive-0, ret-matched, act-accept, idx-1
16:32:41	after iprope_captive_check(): is_captive-0, ret-matched, act-accept, idx-1
16:32:41	in-[port3], out-[port1], skb_flags-02000000, vid-0
16:32:41	len=0
16:32:41	Allowed by Policy-1: SNAT
16:32:41	npu_state=0x100, hook=4
16:32:41	SNAT 10.0.1.10->10.200.1.1:60424

Packet Trace #23 6

It is a bit different now. The error message is not displayed and you can see a few new logs.

The firewall policy with the ID 1 is allowing traffic.

Allowed by Policy-1: SNAT

FortiGate applies source NAT (SNAT).

SNAT 10.0.1.10→10.200.1.1:60424

Additionally, you can see the debug flow logs from the return (ping reply) packets.

vd-root:0 received a packet(proto=1, 10.200.1.254:60424→10.200.1.1:0) tun_id=0.0.0.0 from port1. type=0, code=0, id=60424, seq=1.

Find an existing session, id-00010feb, reply direction

DNAT 10.200.1.1:0→10.0.1.10:7

find a route: flag=00000000 gw-0.0.0.0 via port3

The procedure in this exercise describes what you should usually do when troubleshooting connectivity problems on FortiGate. Sniff the traffic first to check that the packets are arriving on FortiGate and that FortiGate is routing them correctly. If the sniffer shows that FortiGate is dropping the traffic, use the debug flow tool to find out why.

LAB-15 > Troubleshooting a Connectivity Problem