FORTINET

NSE Institute

FortiGate Security Lab Guide

for FortiOS 6.0

Fortinet Training

http://www.fortinet.com/training

Fortinet Document Library

http://docs.fortinet.com

Fortinet Knowledge Base

http://kb.fortinet.com

Fortinet Forums

https://forum.fortinet.com

Fortinet Support

https://support.fortinet.com

FortiGuard Labs

http://www.fortiguard.com

Fortinet Network Security Expert Program (NSE)

https://www.fortinet.com/support-and-training/training/network-security-expert-program.html

Feedback

Email: courseware@fortinet.com

11/7/2018

TABLE OF CONTENTS

Change Log

This table includes updates to the *FortiGate Security 6.0 Lab Guide* dated 5/13/2018 to the updated document version dated 8/9/2018.

Change	Location
Fixed FIT in the network topology diagram	Network Topology on page 10
Removed steps 1-13 after the lab prerequisites	Configure Central SNAT on page 65
Various formatting fixes	Entire guide

This table includes updates to the *FortiGate Security 6.0 Lab Guide* dated 8/9/2018 to this updated document version dated 11/7/2018.

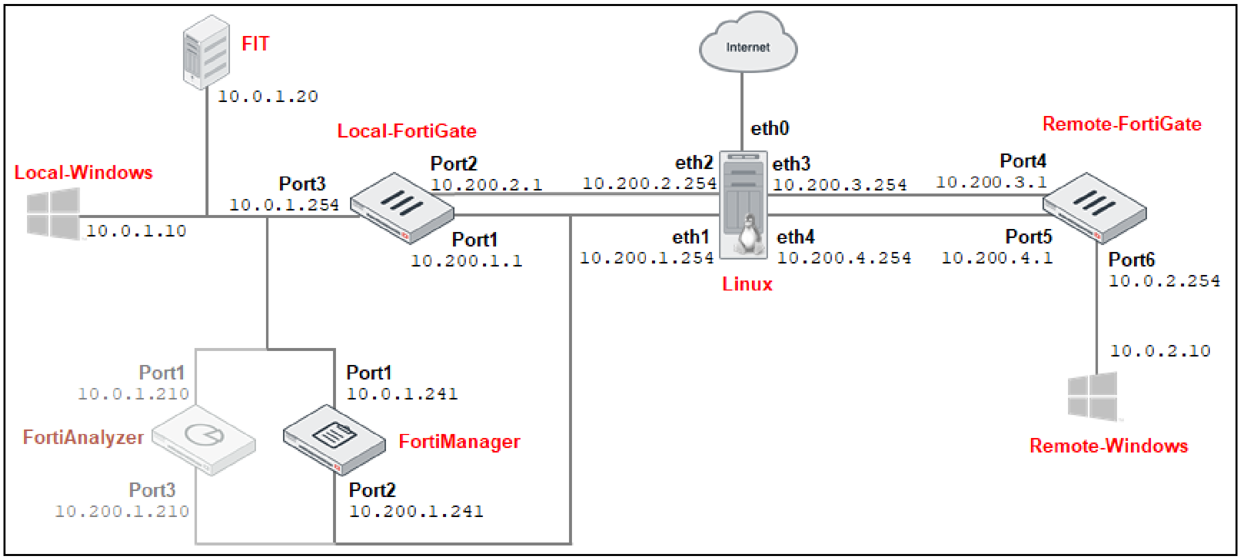
Change	Location
Updated the entire Virtual Lab Basics section	"Virtual Lab Basics" on page 10

Virtual Lab Basics

In this course, you will use a virtual lab for hands-on exercises. This section explains how to connect to the lab and its virtual machines. It also shows the topology of the virtual machines in the lab.

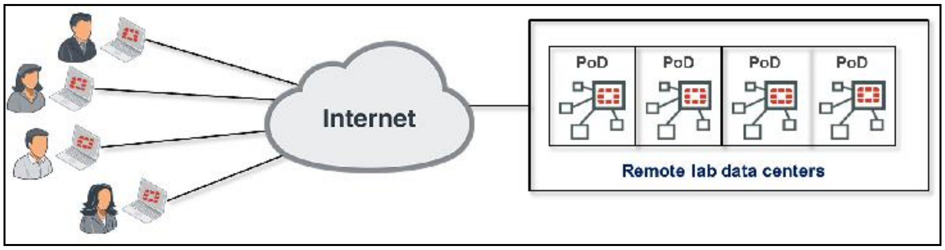
If your trainer asks you to use a different lab, such as devices physically located in your classroom, then ignore this section. This section applies only to the virtual lab accessed through the Internet. If you do not know which lab to use, please ask your trainer.

Network Topology



Lab Environment

Fortinet's virtual lab for hands-on exercises is hosted on remote data centers that allow each student to have their own training lab environment or point of deliveries (PoD).



Remote Access Test

Before starting any course, check if your computer can connect to the remote data center successfully. The remote access test fully verifies if your network connection and your web browser can support a reliable connection to the virtual lab.

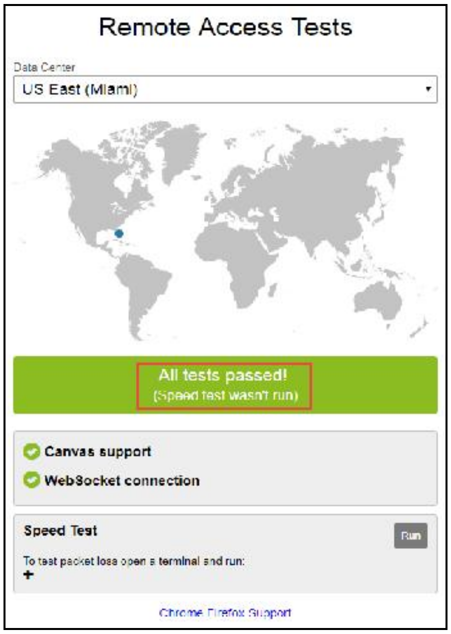
You do not have to be logged in to the lab portal in order to run the remote access test.

To run the remote access test

1. From a browser, access the following URL:

   ```
   https://use.cloudshare.com/test.mvc
   ```

   If your computer connects successfully to the virtual lab, you will see the message **All tests passed!**:



Remote Access Tests

Data Center: US East (Miami)

All tests passed!
(Speed test wasn't run)

Canvas support

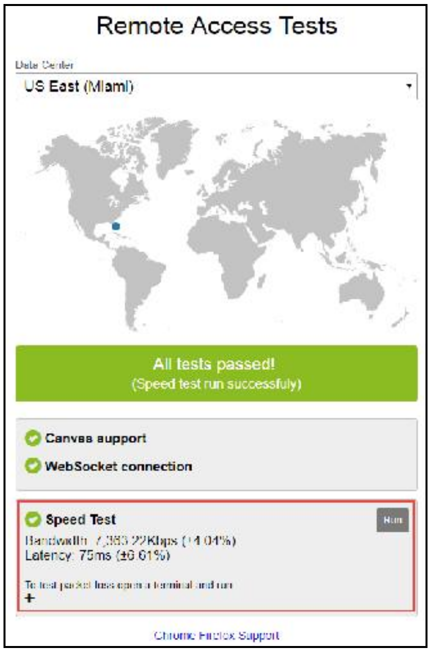
WebSocket connection

Speed Test

To test packet loss open a terminal and run:

2. Inside the **Speed Test** box, click **Run**.

   The speed test begins. Once complete, you will get an estimate for your bandwidth and latency. If those estimations are not within the recommended values, you will get any error message:



Remote Access Tests

Data Center

US East (Miami)

All tests passed!
(Speed test run successfuly)

Canvas support

WebSocket connection

Speed Test

Bandwidth: 7,363.22Kbps (±4.04%)
Latency: 75ms (±6.61%)

To test packet loss open a terminal and run

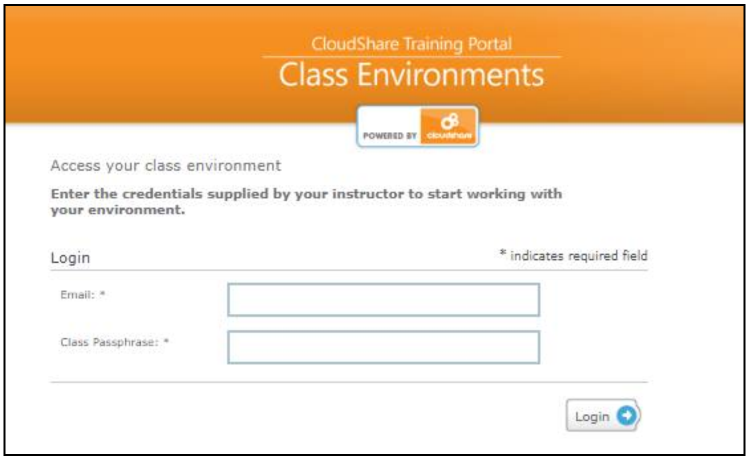
Logging In

After you run the remote access test to confirm that your system can run the labs successfully, you can proceed to log in.

You will receive an email from your trainer with an invitation to auto-enroll in the class. The email will contain a link and a passphrase.

To log in to the remote lab

1. Click the login link provided by your instructor over email.
2. Enter your email address and the class passphrase provided by your trainer over email, and then click **Login**.



CloudShare Training Portal

Class Environments

Access your class environment

Enter the credentials supplied by your instructor to start working with your environment.

Login

* indicates required field

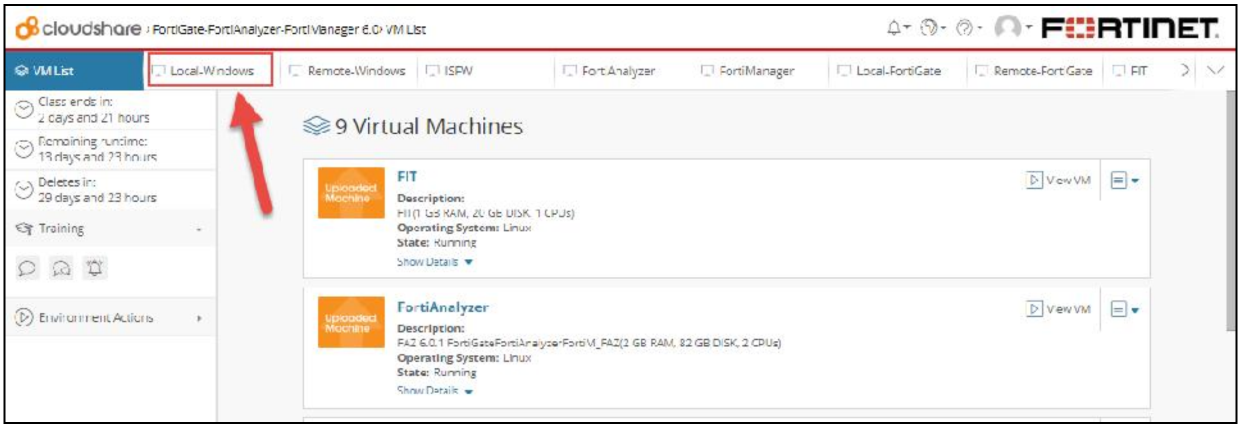
Email: *

Class Passphrase: *

3. Enter your first and last name.
4. Click **Register and Login**.

Your system dashboard appears, listing the virtual machines (VMs) in your lab topology.

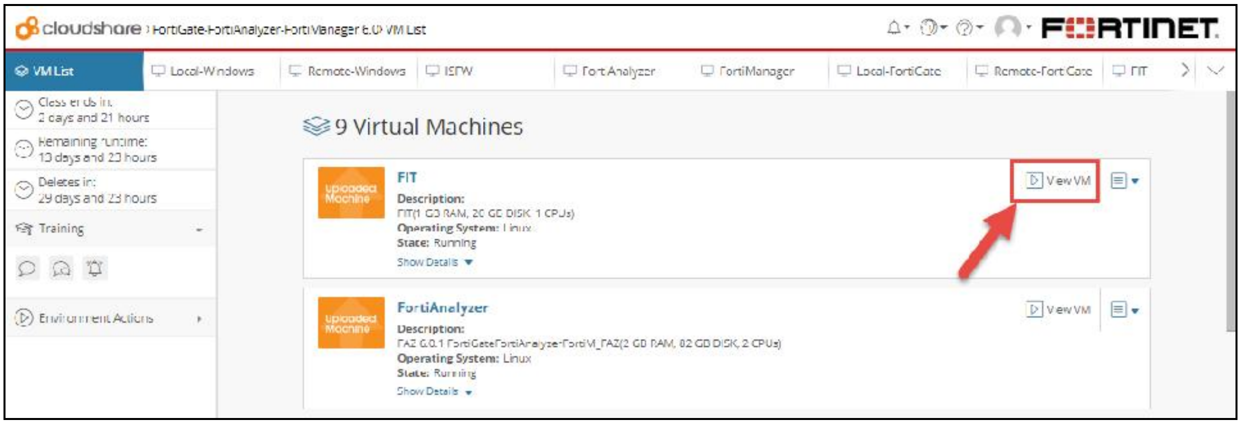
5. To open a VM from the dashboard, do one of the following:
   - From the top navigation bar, click a VM's tab.



FIT
Description: FIT(1 GB RAM, 20 GB DISK, 1 CPUs)
Operating System: Linux
State: Running

FortiAnalyzer
Description: FAZ 6.0.1 FortiGateFortiAnalyzerFortiM_FAZ(2 GB RAM, 82 GB DISK, 2 CPUs)
Operating System: Linux
State: Running

   - From the box of the VM you want to open, click **View VM**.

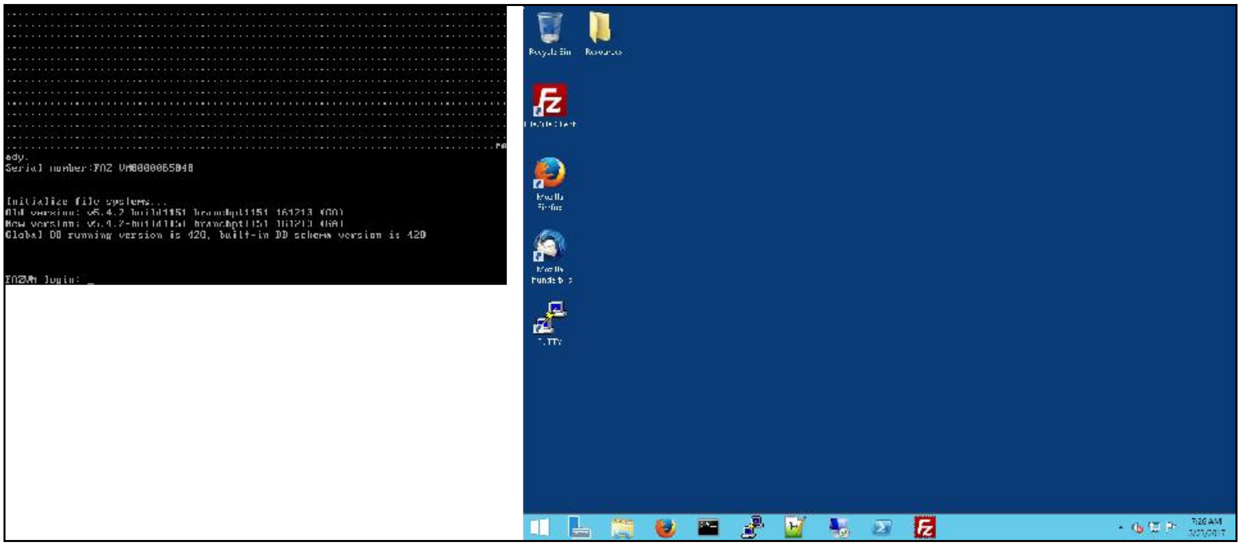


FIT
Description: FIT(1 GB RAM, 20 GB DISK, 1 CPUs)
Operating System: Linux
State: Running

FortiAnalyzer
Description: FAZ 6.0.1 FortiGateFortiAnalyzerFortiM_FAZ(2 GB RAM, 82 GB DISK, 2 CPUs)
Operating System: Linux
State: Running

Follow the same procedure to access any of your VMs.

When you open a VM, your browser uses HTML5 to connect to it. Depending on the VM you select, the web browser provides access to either the GUI of a Windows or Linux VM, or the CLI-based console access of a Fortinet VM.



```
ady.
Serial number:FAZ VM0000065048

Initialize file systems...
Old version: v5.4.2 build1151 branchpt1151 161213 (GA)
New version: v5.4.2-build1151 branchpt1151 161213 (GA)
Global DB running version is 420, built-in DB schema version is 420


FAZVM login: _
```

For most lab exercises, you will connect to a jumpbox VM, that could be either a Windows or a Linux VM. From the jumpbox VM, you will connect over HTTPS and SSH to all other Fortinet VMs in the lab environment.

Disconnections and Timeouts

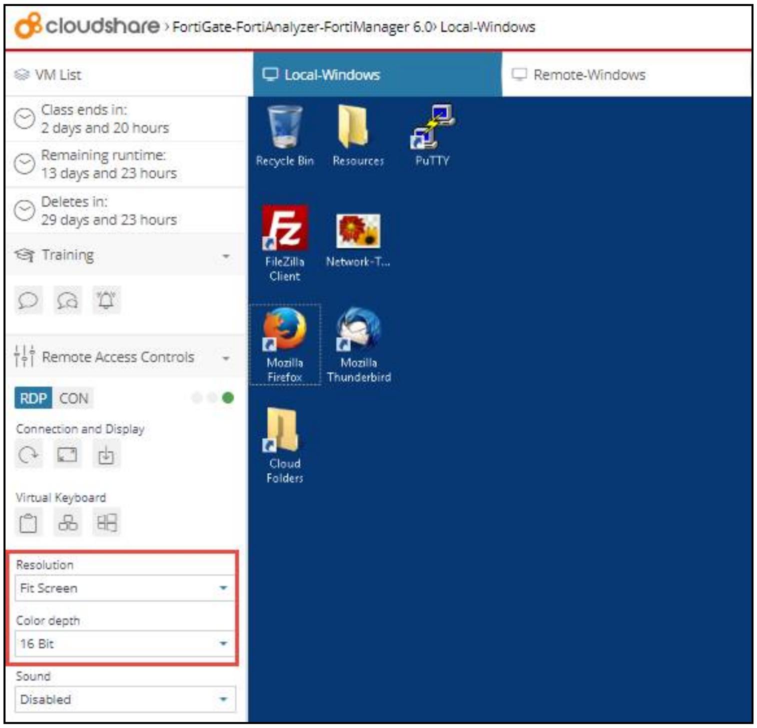
If your computer’s connection to the VM times out or closes, to regain access, return to the window or tab that contains the list of VMs for your session, and reopen the VM.

If that fails, see Troubleshooting Tips on page 16.

Screen Resolution

The GUIs of some Fortinet devices require a minimum screen size.

To configure screen resolution in the HTML5 client, use the **Resolution** drop-down list on the left. You can also change the color depth:



Class ends in: 2 days and 20 hours

Remaining runtime: 13 days and 23 hours

Deletes in: 29 days and 23 hours

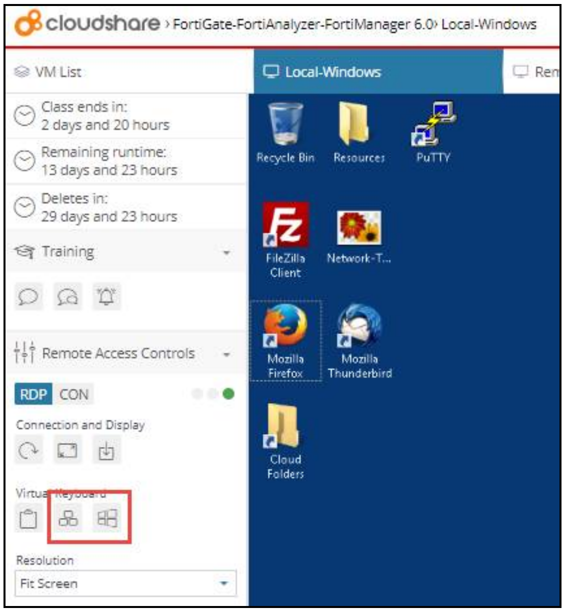
Resolution: Fit Screen

Color depth: 16 Bit

Sound: Disabled

Sending Special Keys

You can use the **Virtual Keyboard** panel to either send the Ctrl-Alt-Del combination, or the Windows key:



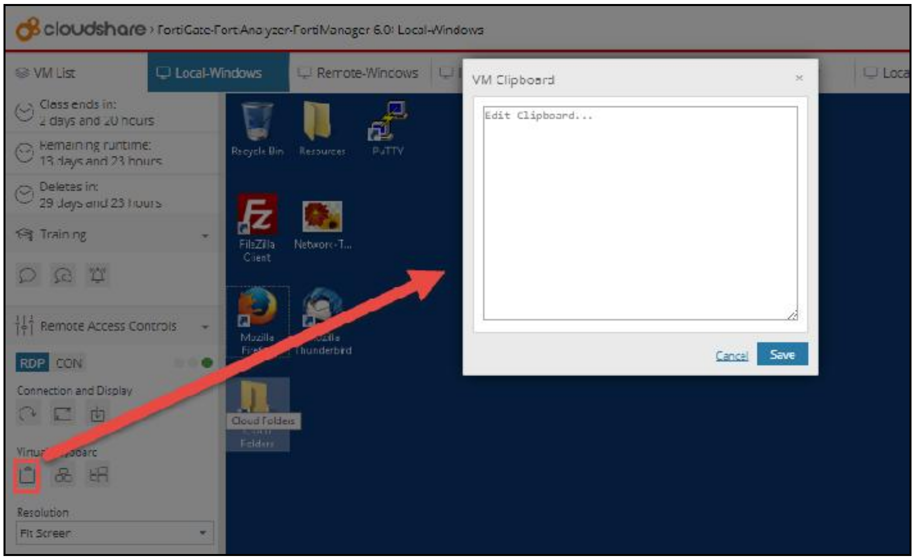
Class ends in: 2 days and 20 hours

Remaining runtime: 13 days and 23 hours

Deletes in: 29 days and 23 hours

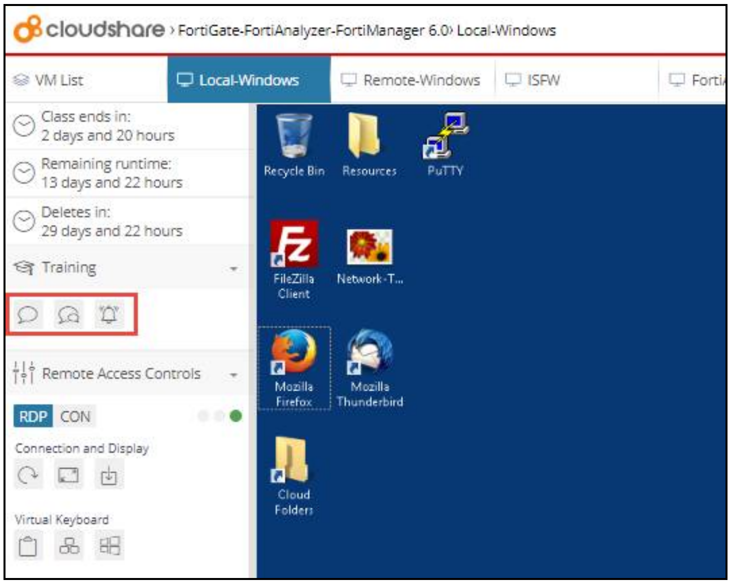
Resolution: Fit Screen

From the **Virtual Keyboard** panel, you can also copy text to the guest VM's clipboard:


cloudshare › FortiGate-FortiAnalyzer-FortiManager 6.0› Local-Windows
VM List
Local-Windows
Remote-Windows
VM Clipboard
Edit Clipboard...
Cancel
Save
Class ends in: 2 days and 20 hours
Remaining runtime: 13 days and 23 hours
Deletes in: 29 days and 23 hours
Training
Remote Access Controls
RDP
CON
Connection and Display
Virtual Keyboard
Resolution
Fit Screen

Student Tools

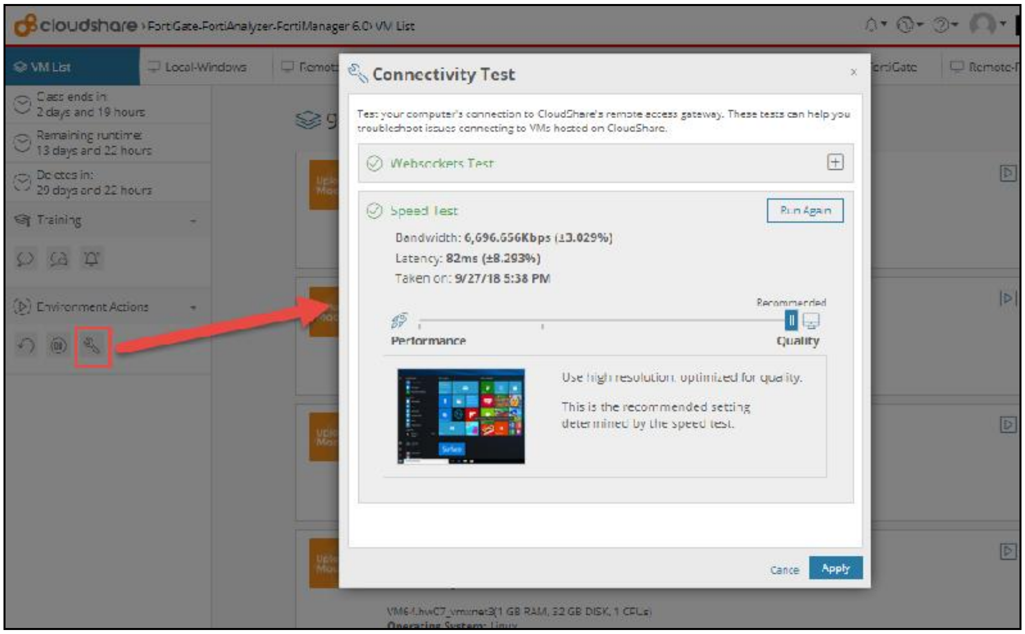
There are three icons on the left for messaging the instructor, chatting with the class, and requesting assistance:



Troubleshooting Tips

- *Do not* connect to the virtual lab environment through Wi-Fi, 3G, VPN tunnels, or other low-bandwidth or high-latency connections.
- Prepare your computer's settings by disabling screen savers and changing the power saving scheme so that your computer is always on, and does not go to sleep or hibernate.
- For best performance, use a stable broadband connection, such as a LAN.

- You can run a remote access test from within your lab dashboard. It will measure your bandwidth, latency and general performance:



cloudshare › FortiGate-FortiAnalyzer-FortiManager 6.0 › VM List
VM List
Local-Windows
Remote
FortiGate
Remote-
Class ends in: 2 days and 19 hours
Remaining runtime: 13 days and 22 hours
Deletes in: 29 days and 22 hours
Training
Environment Actions

Connectivity Test

Test your computer's connection to CloudShare's remote access gateway. These tests can help you troubleshoot issues connecting to VMs hosted on CloudShare.

Websockets Test

Speed Test

Run Again

Bandwidth: 6,696.656Kbps (±3.029%)
Latency: 82ms (±8.293%)
Taken on: 9/27/18 5:38 PM

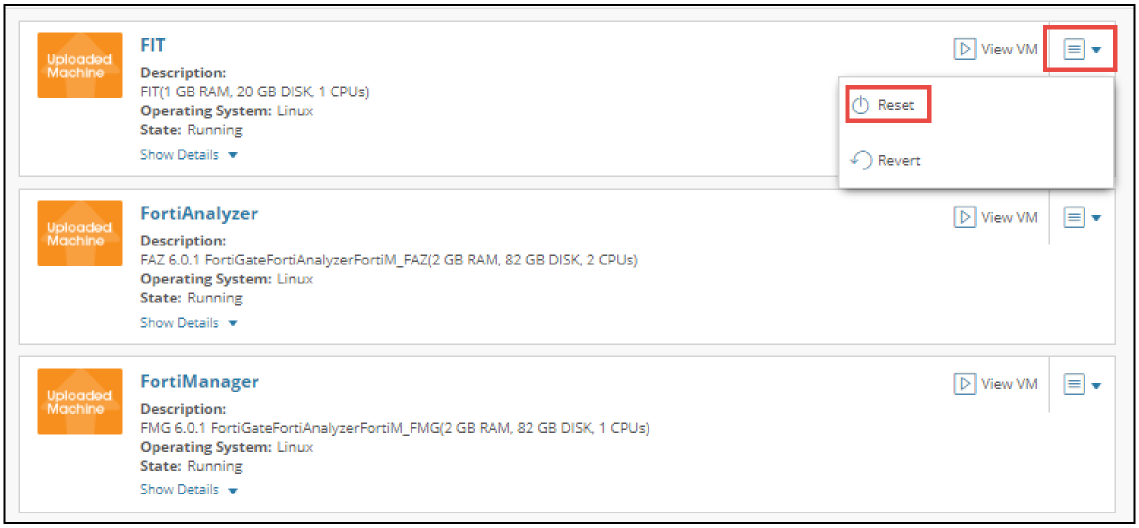
Recommended
Performance
Quality

Use high resolution, optimized for quality.

This is the recommended setting determined by the speed test.

VM64-hwC7_vmxnet3(1 GB RAM, 32 GB DISK, 1 CPUs)
Operating System: Linux

- If the connection to any VM or the virtual lab portal closes unexpectedly, try to reconnect. If you can't reconnect, notify the instructor.
- If you can't connect to a VM, on the dashboard, open the VM action menu, and select **Reset**:



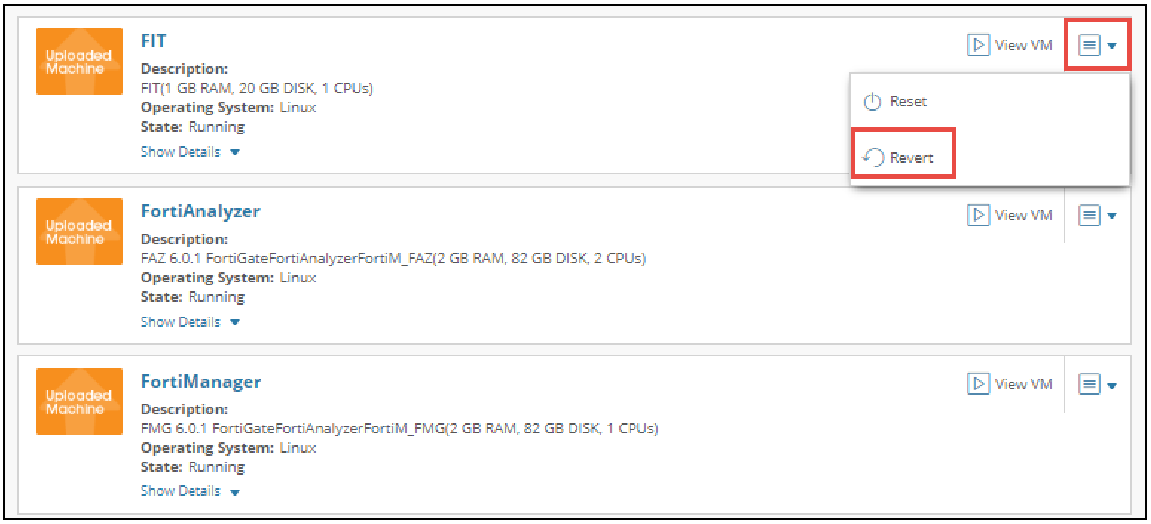
FIT
Description:
FIT(1 GB RAM, 20 GB DISK, 1 CPUs)
Operating System: Linux
State: Running
Show Details

FortiAnalyzer
Description:
FAZ 6.0.1 FortiGateFortiAnalyzerFortiM_FAZ(2 GB RAM, 82 GB DISK, 2 CPUs)
Operating System: Linux
State: Running
Show Details

FortiManager
Description:
FMG 6.0.1 FortiGateFortiAnalyzerFortiM_FMG(2 GB RAM, 82 GB DISK, 1 CPUs)
Operating System: Linux
State: Running
Show Details

- If that does not solve the access problem, you can try to revert the VM back to its initial state. Open the VM action menu, and select **Revert**:

Reverting to the VM's initial state will undo all of your work. Try other solutions first.



FIT

Description:
FIT(1 GB RAM, 20 GB DISK, 1 CPUs)
Operating System: Linux
State: Running

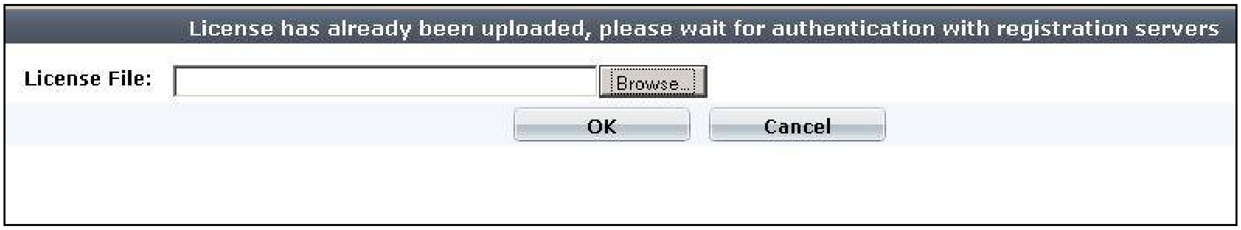
FortiAnalyzer

Description:
FAZ 6.0.1 FortiGateFortiAnalyzerFortiM_FAZ(2 GB RAM, 82 GB DISK, 2 CPUs)
Operating System: Linux
State: Running

FortiManager

Description:
FMG 6.0.1 FortiGateFortiAnalyzerFortiM_FMG(2 GB RAM, 82 GB DISK, 1 CPUs)
Operating System: Linux
State: Running

- During the labs, if the VM is waiting for a response from the authentication server, a license message similar to the following example appears:



License has already been uploaded, please wait for authentication with registration servers

License File:

To expedite the response, enter the following command in the CLI:

```
execute update-now
```

Lab 1: Introduction to FortiGate

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

Objectives

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

Time to Complete

Estimated: 25 minutes

Exercise 1: Working With the Command Line Interface

In this exercise, you will access a FortiGate device using the command line interface (CLI).

Explore the CLI

The next steps will help you get familiar with the FortiGate CLI.

To explore the CLI

1. In the VM List, from the box of the **Local-FortiGate**, click **View VM** to open the FortiGate console**.**
2. At the login prompt, enter `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 FortiGate's serial number, operation mode, and so on. When the `More` prompt appears on the CLI, do one of the following:

To continue scrolling	Space bar
To scroll one line at a time	Enter
To exit	Q

5. Enter the following command:

   ```
   get ?
   ```

   The ? character is not displayed on the screen.

   This command shows all of the 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 twice.

   This displays the previous `get system status` command.

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

Action	Command
Previous command	Up Arrow
Next command	Down Arrow
Beginning of line	CTRL+A
End of line	CTRL+E
Back one word	CTRL+B
Forward one word	CTRL+F
Delete current character	CTRL+D
Clear screen	CTRL+L
Abort command and exit	CTRL+C
Auto repeat history	CTRL+P

8. Enter the following command:

```
execute ?
```

   This command lists all options that the CLI will accept 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 presentations and labs, many of the commands that you see will be 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 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 fresh line, enter the following command to view the port3 interface configuration (hint: try using the shortcuts you just learned about):

```
show system interface port3
```

12. Enter the following command:

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

Stop and think!

Compare both outputs. How are they different?

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

Exercise 2: Configuration Backups

In this exercise, you will learn how to generate and restore clear-text and encrypted configuration backups. The configuration files produced by backups, allow you to restore to an earlier FortiGate configuration.

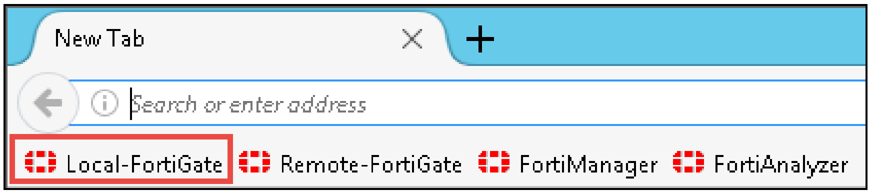
Restore Configuration From a Backup

Now, you will restore a configuration from a backup.

To restore a configuration from a backup

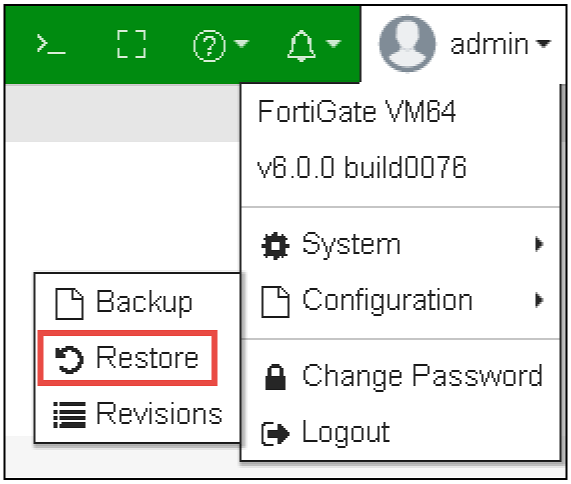
1. In the VM List, from the box of the **Local-Windows**, click **View VM.**
2. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.

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

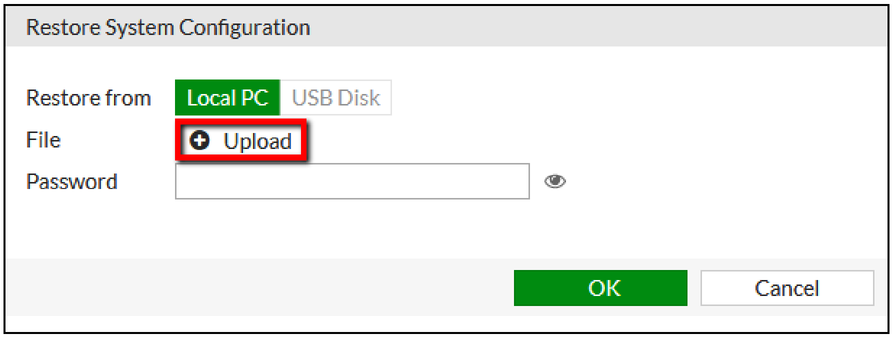


All the lab exercises were tested running Mozilla Firefox on the Local-Windows and Remote-Windows VMs. To get consistent results, you should use Firefox to access both the Internet and the FortiGate GUIs in this virtual environment.

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



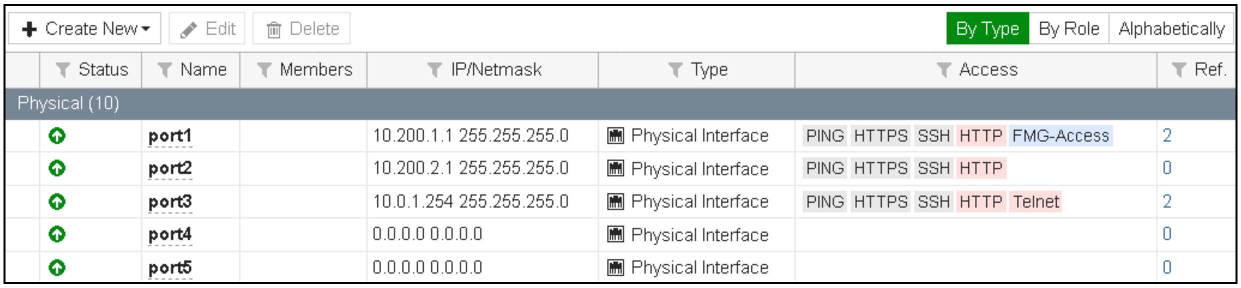
4. Click **Upload** to select the backup configuration file from your local PC.



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

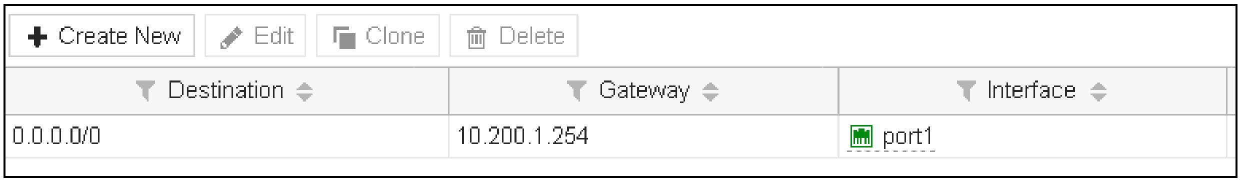
   After your browser uploads the configuration, FortiGate reboots automatically. This takes approximately 30 to 45 seconds.

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



Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (10)						
↑	port1		10.200.1.1 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access	2
↑	port2		10.200.2.1 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP	0
↑	port3		10.0.1.254 255.255.255.0	Physical Interface	PING HTTPS SSH HTTP Telnet	2
↑	port4		0.0.0.0 0.0.0.0	Physical Interface		0
↑	port5		0.0.0.0 0.0.0.0	Physical Interface		0

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



Destination	Gateway	Interface
0.0.0.0/0	10.200.1.254	port1

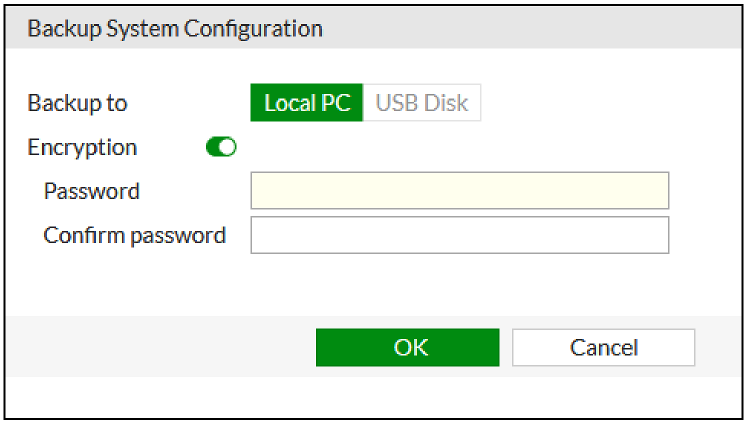
Back Up and Encrypt a Configuration File

Always back up the configuration file 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 plain-text and storing them in a secure place instead.

Now, you will create an encrypted file with the backup of the FortiGate's current configuration.

To save an encrypted configuration backup

1. Continuing on the Local-FortiGate GUI, in the upper-right corner, click **admin**, and then click **Configuration** > **Backup**.
2. On the **Backup System Configuration** page, enable **Encryption**.
3. In the **Password** field, enter `fortinet` and repeat in the **Confirm password** field.


Backup System Configuration

Backup to: Local PC | USB Disk

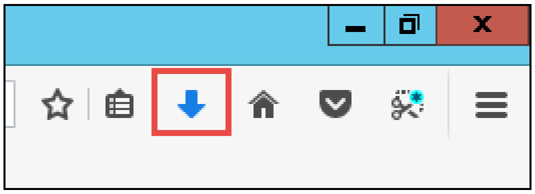
Encryption: ●

Password:

Confirm password:

4. Click **OK**.
5. Select **Save File** and click **OK**.
   The Firefox browser saves the encrypted configuration file in the **Downloads** folder, by default.

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



Restore an Encrypted Configuration Backup

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

Now, 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 26.

To restore an encrypted configuration backup

1. Continuing 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 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.

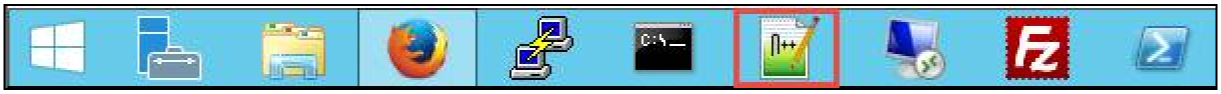
Compare the Headers of Two Configuration Files

When troubleshooting issues, or when having to restore FortiGate to an earlier OS version or build, it is useful to know where to find this information in a configuration file. This exercise will show you where to find the version and build number in a configuration file.

Now, you will open and compare two configuration files using Notepad++.

To compare the headers of two configuration files

1. On Local-Windows, in the Windows task bar, click the Notepad++ icon.



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

In both the clear-text and encrypted configuration files, the top line acts as a header, listing the firmware and model that this configuration belongs to.

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

Exercise 3: Configuring Administrator Accounts

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

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

Configure a User Administrator Profile

Now, 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. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `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**, but set all other permissions to **Read**.
6. Click **OK** to save the changes.

Create an Administrator Account

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

To create an administrator account

1. Continuing 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
User Name	Security
Type	Local User
Password	fortinet

Field	Value
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.

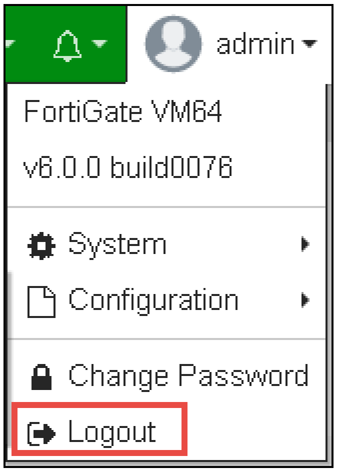
3. Click **OK** to save the changes.

Test the New Administrator Account

In this procedure, you will confirm that the new administrator account has read-write access to only the security profiles configuration.

To test the new administrator account

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



2. Log back in to the Local-FortiGate GUI with the user name `Security` and password `fortinet`.
3. Explore the permissions that you have in the GUI.

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

4. Log out of the GUI once done.

Restrict Administrator Access

Now, you will restrict access for FortiGate administrators. Only administrators connecting from a trusted subnet will be allowed access. This is useful if you need to restrict the access points from which administrators connect to FortiGate.

To restrict administrator access

1. Log back in to the Local-FortiGate GUI with the user name `admin` and password `password`.
2. Click **System** > **Administrators**.
3. Edit the **admin** account.
4. Enable **Restrict login to trusted hosts**, and set **Trusted Host 1** to the address `10.0.2.0/24`.
5. Click **OK** to save the changes.

Test the Restricted Access

Now, you will verify that administrators outside the subnet `10.0.2.0/24` can't access FortiGate.

To test the restricted access

1. Continuing on Local-Windows, log out of the Local-FortiGate GUI session as the admin user.
2. Try to log in to the `admin` account again with password `password`.

   What is the result this time?

> **Stop and think!**
>
> Why do you receive an authentication failure message?
>
> Because you are trying to connect from the `10.0.1.10` address, you shouldn't be able to connect. This is because you restricted logins to *only* the source IP addresses in the list of trusted hosts.

3. In the VM List, from the box of the **Local-FortiGate**, click **View VM** to open the FortiGate console**.**
4. Log in as `admin` with password `password`.
5. Enter the following CLI commands to add `10.0.1.0/24` as the second trusted IP subnet (**Trusted Host 2**) to the admin account:

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

6. Return to the Local-Windows VM.
7. Open a browser and try to log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.

   You should be able to log in.

Lab 2: Firewall Policies

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

Objectives

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

Time to Complete

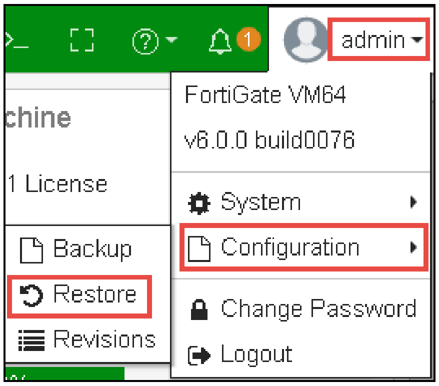
Estimated: 55 minutes

Prerequisites

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

To restore the Local-FortiGate configuration file

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**,and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **Firewall-Policies** > `local-firewall-policy.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Creating Firewall Address Objects and Firewall Policies

In this exercise, you will configure firewall address objects. You will also configure an IPv4 firewall policy to which you will apply firewall address objects along with 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. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Policy & Objects** > **Addresses**.
3. Click **Create New** > **Address**.
4. Configure the following settings:

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

5. Click **OK**.

Create a Firewall Policy

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

To disable an existing firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Right-click the **Full_Access** firewall policy from the **ID** column.
3. Select **Policy Status**, and then click **Disable**.

To create a firewall policy

1. Continuing in the **Policy & Objects** > **IPv4 Policy** section, click **Create New** to add a new firewall policy.
2. Configure the following settings:

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

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

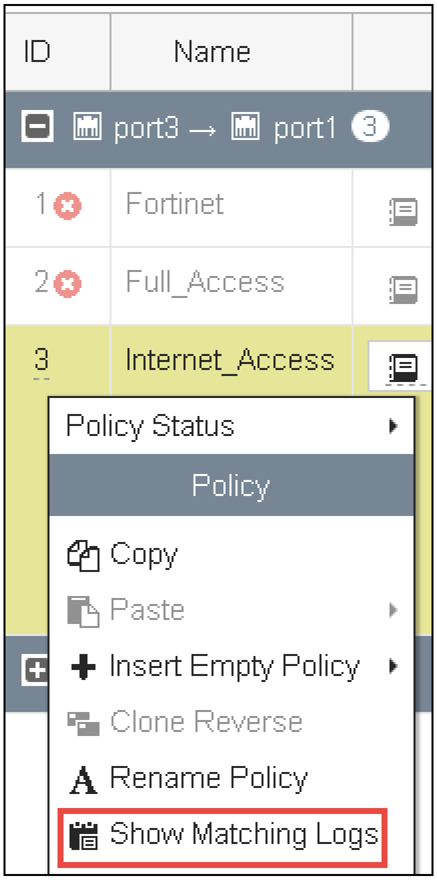
When creating firewall policies, remember that FortiGate is a stateful firewall. As a result, you need to create only one firewall policy that matches the direction of the traffic that initiates the session.

Test the Firewall Policy and View 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-Windows VM, open several web browser tabs and connect to several external web sites such as:
   - www.google.com
   - kb.fortinet.com
   - docs.fortinet.com
   - www.bbc.com
2. Return to your browser tab with the Local-FortiGate GUI, and click **Policy & Objects** > **IPv4 Policy**.
3. Right-click the **ID** column of the **Internet_Access** policy.
4. Click **Show Matching Logs**.



5. Identify the log entries for your Internet browsing traffic.

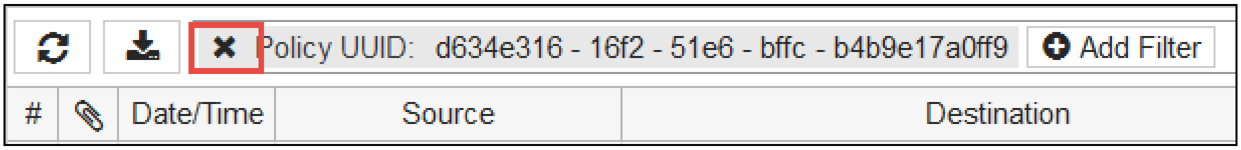
   With the current settings, you should have many log messages that have **Accept: session start** in the **Result** column. These are the session start logs.

   When sessions close, you will have a separate log entry for the amount of data 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 forward traffic logs.

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



Policy UUID: d634e316 - 16f2 - 51e6 - bffc - b4b9e17a0ff9

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

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

Exercise 2: Reordering Firewall Policies and Firewall Policy Actions

In the applicable interface pair's section, FortiGate will look 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 your more granular policies will never be applied.

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

Create a Firewall Policy

You will create a new firewall policy to match a specific source, destination, service, and action set 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 Local-FortiGate GUI using the following settings:

- Name the firewall policy **Block_Ping**.
- Incoming interface: port3, Outgoing interface: port1
- 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 37.

To create a firewall policy

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Policy & Objects** > **IPv4 Policy**, and then click **Create New**.
3. Configure the following settings:

Field	Value
Name	Block_Ping
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	LINUX_ETH1
Schedule	always
Service	PING **Tip**: Type the name in the search box on right hand side and click on services to add.
Action	DENY
Log Violation Traffic	<enable>
Enable this policy	<enable>

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

Test the Reordering of a Firewall Policy

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

- traffic is matched to a more specific firewall policy
- the policy ID remains same

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

1. Continuing on the Local-Windows VM, open a command prompt.
2. Ping the destination address (**LINUX_ETH1**) that you configured in the **Block_Ping** firewall policy.

```
ping -t 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 will look for a matching policy, beginning at the top.

3. Leave the command prompt window open and running.
4. Return to your browser where you are logging in to the Local-FortiGate GUI.
5. In **Policy & Objects** > **IPv4 Policy**, note the current **ID** values for both the **Internet_Access** and **Block_Ping** firewall policies.
6. From the **ID** column, drag the **Block_Ping** firewall policy and drop it above the **Internet_Access** firewall policy.

   When you move the **Block_Ping** policy up, the **ID** value remains the same.
7. Return to the command prompt window that is running the continuous ping.

   You should see that the traffic is now blocked and the replies appear as `Request timed out`.

Stop and think!

Why is the traffic now blocked`?`

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 action DENY, the traffic stops processing.

8. Close the command prompt window.

Exercise 3: Device Identification

FortiGate can match traffic by device type by selecting a device definition in the source field. There are two types of device identification:

- Agentless device identification, which uses traffic from the device and the device is indexed by its MAC address.
- Agent-based device identification, which uses FortiClient and sends its unique FortiClient ID to FortiGate.

In this lab, you will use the agentless device identification technique. You will add the device to the source field of the existing firewall policy and observe the firewall policy source-matching behavior.

Disable the Existing Firewall Policy

First, you will disable the **Block_Ping** firewall policy so that your traffic matches the **Internet_Access** firewall policy.

Take the Expert Challenge!

On the Local-FortiGate GUI, disable the **Policy Status** of the firewall policy named **Block_Ping**.

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

After you have performed these steps, see Configure and Test Device Identification on page 39.

To disable the existing firewall policy

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Policy & Objects** > **IPv4 Policy**.
3. Right-click the **ID** column for the **Block_Ping** firewall policy.
4. Select **Policy Status**, and then click **Disable**.

Configure and Test Device Identification

Now, you will run a continuous ping to an IP address. To test the firewall policy source matching behavior, you will add a non-matching device, such as a Linux PC, to the source field.

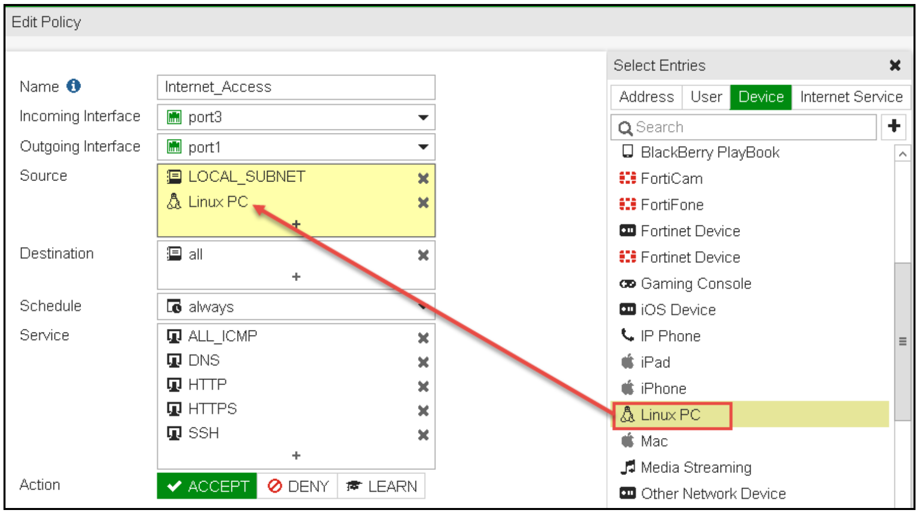
To configure and test device identification

1. Continuing on the Local-Windows VM, open a command prompt.
2. Enter the following command to run a continuous ping to `10.200.1.254`:

```
ping -t 10.200.1.254
```

3. Return to your browser where you are logged in to the Local-FortiGate GUI, and click **Policy & Objects** > **IPv4 Policy**.
4. Right-click the **ID** column for the **Internet_Access** firewall policy and click **Edit**.
5. Click **Source** and in the right pane, click **Device**.
6. Click **Linux PC**.

   You are choosing a device type that doesn't match your device (Windows).



Edit Policy

Name	Internet_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET Linux PC
Destination	all
Schedule	always
Service	ALL_ICMP DNS HTTP HTTPS SSH
Action	✓ ACCEPT / DENY / LEARN

7. Click **OK**.

   FortiGate notifies you that this action enables device identification on the source interface.

8. Click **OK**.

If you enable a source device type in the firewall policy, FortiGate enables device detection on the source interface(s) of the policy.

9. Return to the command prompt on the Local-Windows VM where you are running the continuous ping.

   You should see that traffic is blocked.

10. On the Local-Windows VM, open a few browser tabs and try connecting to various external websites such as:

    - kb.fortinet.com
    - docs.fortinet.com

    The firewall blocks this traffic.

    The traffic is blocked because the source device type in the firewall policy is set to Linux PC, which does not match the Windows device from which the traffic is generated.

11. Close all other browser tabs except Local-FortiGate GUI.

Do not close the command prompt. Keep the continuous ping running until you are notified to stop it.

Modify the Implicit Deny Firewall Policy

FortiGate checks from top to bottom to find a firewall policy that matches the traffic. If none of the firewall policies match the traffic, the default implicit deny firewall policy drops the traffic.

To confirm that the traffic is dropped by the implicit deny policy, you will enable logging on the implicit firewall policy and then check the logs.

Take the Expert Challenge!

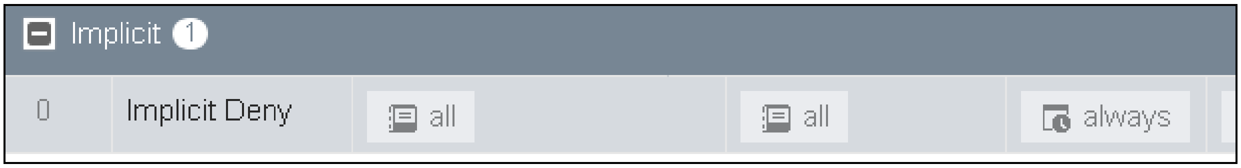
- On Local-FortiGate GUI, enable **Log Violation Traffic** on the **Implicit Deny** firewall policy.
- Check the logs to confirm that traffic is dropped by the **Implicit Deny** firewall policy for ping traffic.

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

After you have performed these steps, see Reconfigure Device Identification on page 41.

To enable logging on the implicit deny firewall policy

1. Continuing on Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Click the **+** sign to expand the **Implicit** section.



3. Right-click the **ID** column for the **Implicit Deny** firewall policy and click **Edit**.
4. Enable **Log Violation Traffic**.
5. Click **OK**.

To confirm traffic is dropped by the implicit deny firewall policy

1. Continuing on the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.
2. Confirm that there are logging entries for the denied ping traffic.

   The **Policy** column shows **Implicit Deny**.

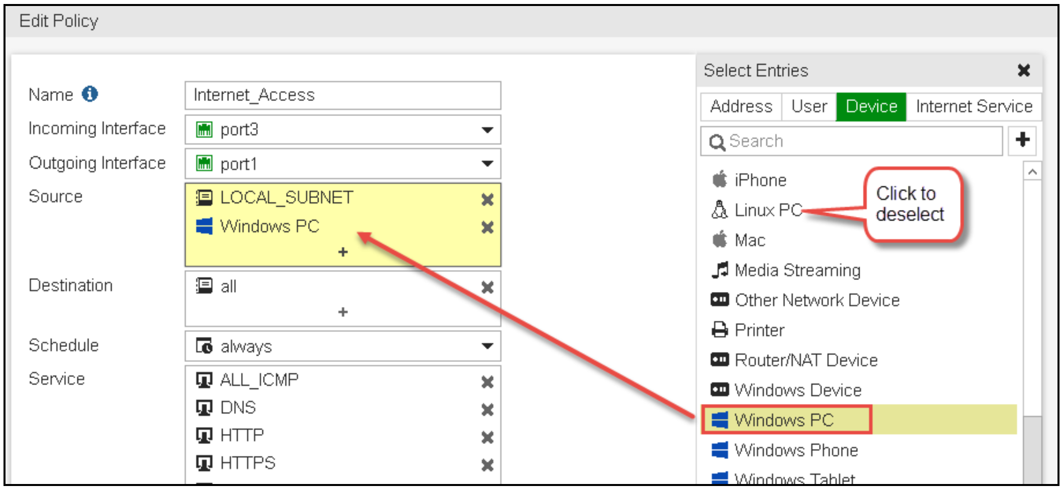
Reconfigure Device Identification

Now you will edit the **Internet_Access** firewall policy and add a Windows PC to match your Local-Windows VM. You will see that the traffic will be allowed by this policy after you add a matching source device.

To reconfigure device identification

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Right-click the **ID** column for the **Internet_Access** firewall policy and click **Edit.**

3. Click **Source** and in the right pane, click **Device**.
4. Click **Windows PC** to select it.
5. Click **Linux PC** to deselect it.



Edit Policy

Name: Internet_Access
Incoming Interface: port3
Outgoing Interface: port1
Source: LOCAL_SUBNET, Windows PC
Destination: all
Schedule: always
Service: ALL_ICMP, DNS, HTTP, HTTPS

Click to deselect

4. Click **OK**.

To confirm traffic is allowed by a firewall policy

1. On the Local-Windows VM, return to the continuous ping that you started earlier.

   You should see that traffic is allowed.

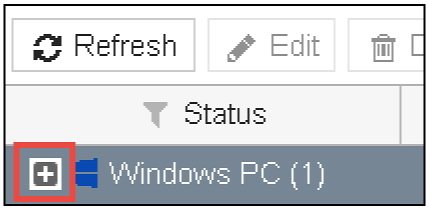
2. Close the command prompt window.
3. On the Local-Windows VM, try browsing the Internet by opening a few browser tabs and connecting to external websites such as:
   - kb.fortinet.com
   - docs.fortinet.com
4. Confirm that the firewall allows this traffic.
5. Close all browser tabs expect for the FortiGate GUI.

View the Details of an Identified Device

After a device is identified, FortiGate updates its list of devices and caches the list on the flash disk to speed up detection. You can view the details of an identified device, which include device type, detection method, IP address, and so on.

To view the details of an identified device

1. Continuing on the Local-FortiGate GUI, click **User & Device** > **Device Inventory**.
2. Click the **+** sign associated with **Windows PC** to expand the section.

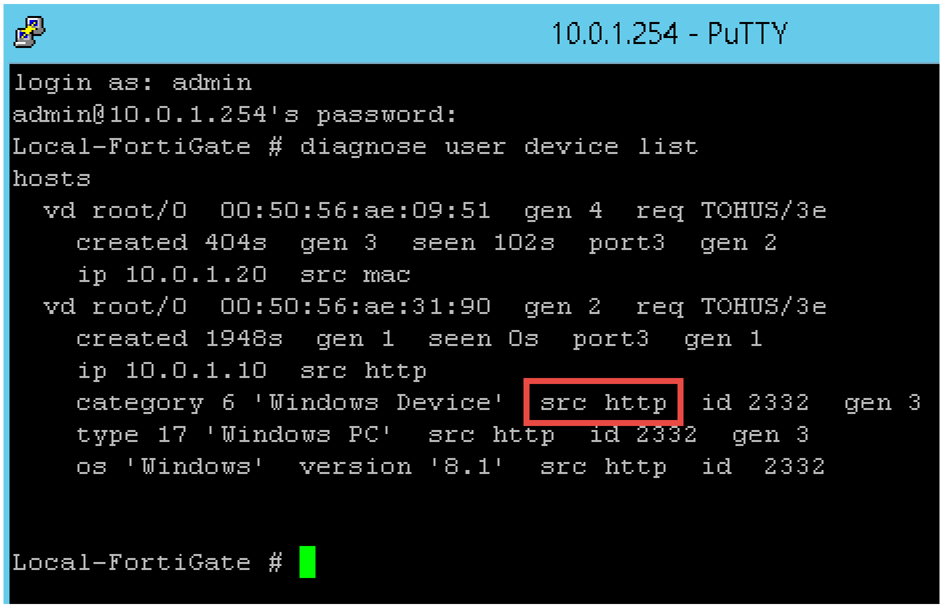


3. Review the details of your detected host device.

   You can see the device details, such as IP address, interface, status, and so on.

4. On the Local-Windows VM, open PuTTY and connect over SSH to the **LOCAL-FORTIGATE** saved session.
5. At the login prompt, enter the user name `admin` and password `password`.
6. Run the following command to view the detection method and other device details:

```
diagnose user device list
```



```
login as: admin
admin@10.0.1.254's password:
Local-FortiGate # diagnose user device list
hosts
  vd root/0  00:50:56:ae:09:51  gen 4  req TOHUS/3e
    created 404s  gen 3  seen 102s  port3  gen 2
    ip 10.0.1.20  src mac
  vd root/0  00:50:56:ae:31:90  gen 2  req TOHUS/3e
    created 1948s  gen 1  seen 0s  port3  gen 1
    ip 10.0.1.10  src http
    category 6 'Windows Device'  src http  id 2332  gen 3
    type 17 'Windows PC'  src http  id 2332  gen 3
    os 'Windows'  version '8.1'  src http  id  2332


Local-FortiGate #
```

7. Leave your PuTTY session open.

Add an Identified Device to the Configuration File

The identified device is cached on FortiGate and is not added to the configuration file. You will add the identified device to the configuration file by adding an alias to the device.

To add an identified device to the configuration file

1. Continuing on the Local-FortiGate PuTTY session, run the following command to confirm that there are no devices in the configuration file:

```
show user device
```

2. Return to your browser where you are logged in to the Local-FortiGate GUI, and click **User & Device** > **Device Inventory**.
3. Click your Windows PC device and click **Edit.**
4. Configure the following settings:

Field	Value
Alias	MyDevice

   This creates a static device in the configuration file.

5. Click **OK**.
6. Return to the Local-FortiGate PuTTY session, and run the following command to confirm that the device now appears in the configuration file as a permanent device:

```
show user device
```

8. Return to your browser where you are logged in to the Local-FortiGate GUI, and click **User & Device** > **Custom Devices & Groups**.
   Your device is now listed under **Custom Devices**.

Add a Custom Device to the Firewall Policy

Now that you've added your device as a custom device, you will add it to the firewall policy.

To add a custom device to the firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Click the **Source** column for the **Internet_Access** firewall policy.
4. In the right pane, click **Device.**
5. Click **Windows PC** to deselect.
6. Under **CUSTOM DEVICE**, click **MyDevice** to select it.
7. Click **OK**.

To confirm that traffic is allowed by the firewall policy

1. Continuing on the Local-Windows VM, try browsing the Internet by opening a few browser tabs and connecting to various external websites, such as:
   - www.yahoo.com
   - www.google.com
2. Confirm that the firewall allows this traffic.
3. Close all browser tabs except the Local-FortiGate GUI.

Exercise 4: Internet Service Database (ISDB) Objects as Destination

FortiGate can match the traffic using address objects or ISDB objects as destinations. ISDB objects are predefined entries that are regularly updated by FortiGuard and contains a database of IP addresses, protocols, and port numbers used by the most common Internet services.

ISDB objects can be used to allow or deny traffic to well-known Internet destinations, without worrying about configuring IP addresses, protocols, or ports used by those destinations in the firewall policy.

In this lab, you will apply an ISDB object as a destination criteria on a firewall policy to block traffic to a well-known Internet service.

Review the Internet Service Database

You will now review the entries in the Internet Service Database.

To review the Internet Service Database

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Policy & Objects** > **Internet Service Database**.
3. Double-click any entry.

   You will see the corresponding IP addresses, ports, and protocols used by that Internet service.
4. Click **Return**.

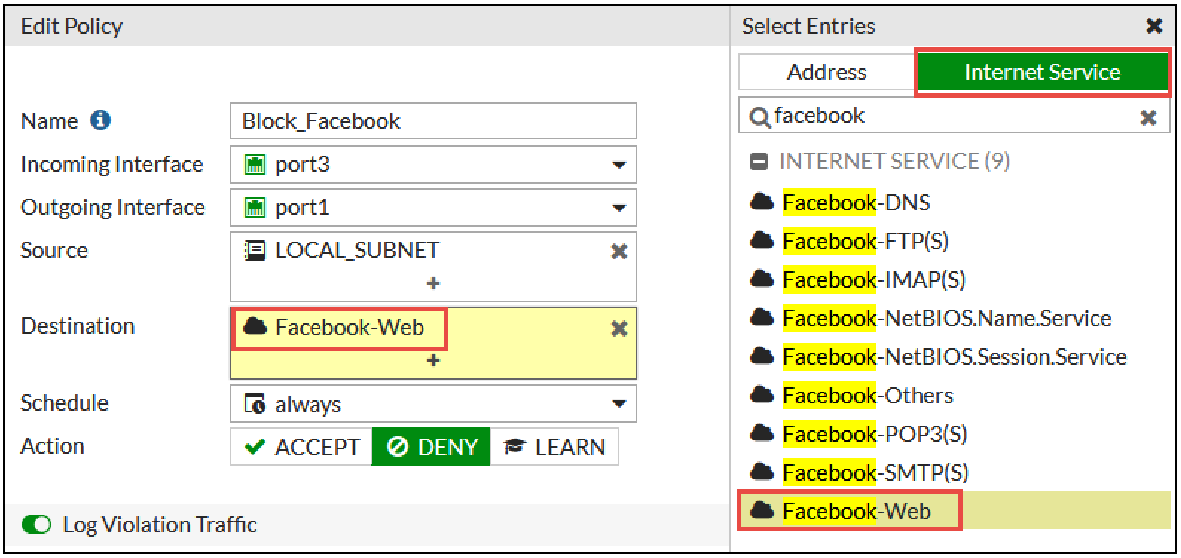
Configure a Firewall Policy Destination as an Internet Service Database Object

Now, you will now modify an existing firewall policy and use an ISDB object as a destination.

To configure a destination as an Internet Service

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Right-click the **ID** column for the **Block_Ping** firewall policy, and click **Edit**.
3. Change the **Name** to **Block_Facebook**.
4. Click **Destination** and in the right pane, click **LINUX_EHT1** to deselect.
5. Click **Internet Service**.
6. Select **Facebook-Web**.

   Tip: Type the name in the search box and click a service to add it.



Edit Policy

Name	Block_Facebook
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	Facebook-Web
Schedule	always
Action	✓ ACCEPT / ⊘ DENY / LEARN

● Log Violation Traffic

Select Entries

Address | Internet Service

facebook

INTERNET SERVICE (9)

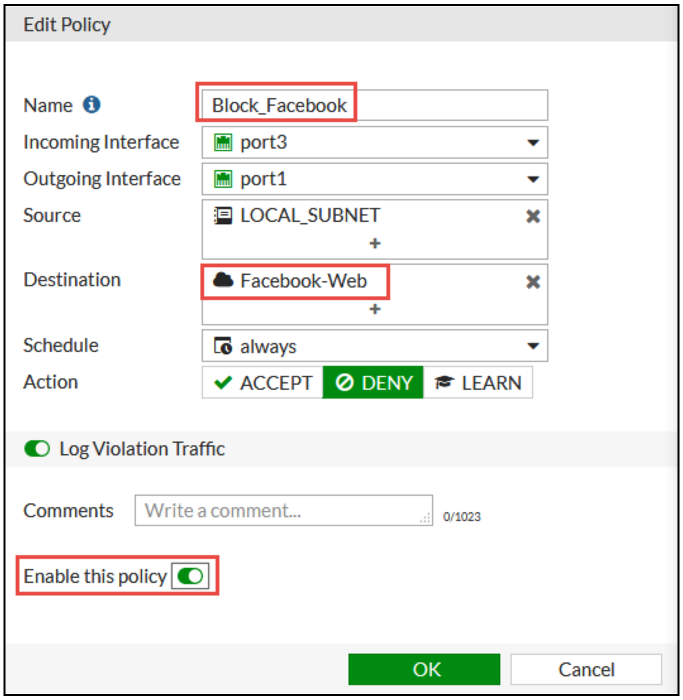
- Facebook-DNS
- Facebook-FTP(S)
- Facebook-IMAP(S)
- Facebook-NetBIOS.Name.Service
- Facebook-NetBIOS.Session.Service
- Facebook-Others
- Facebook-POP3(S)
- Facebook-SMTP(S)
- Facebook-Web

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

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

7. Turn on the **Enable this policy** switch.

   Your configuration should look like the following example:



Edit Policy

Name	Block_Facebook
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	Facebook-Web
Schedule	always
Action	✓ ACCEPT / ⊘ DENY / LEARN

● Log Violation Traffic

Comments: Write a comment... 0/1023

Enable this policy ●

8. Click **OK**.

Test the Internet Service Firewall Policy

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

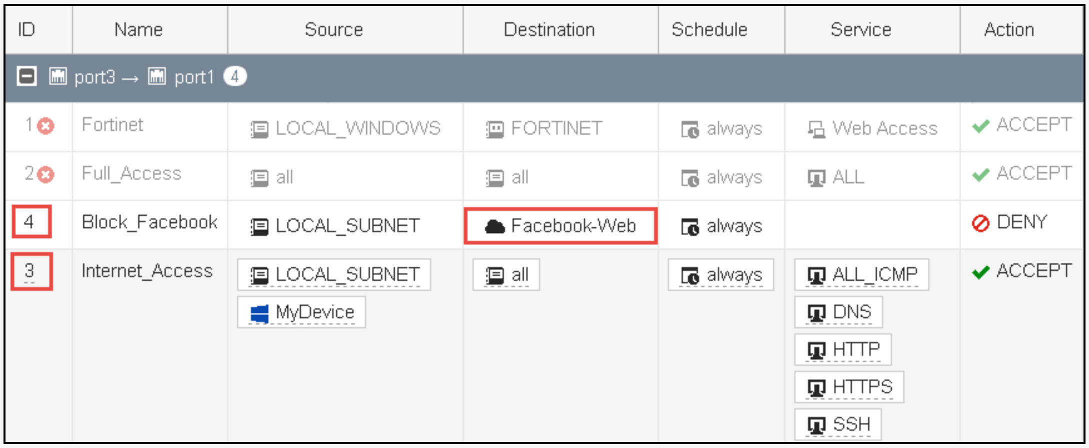
To test the Internet Service firewall policy

1. Continuing on the Local-Windows VM, open few browser tabs and go to the following websites:
   - www.facebook.com
   - www.twitter.com

Stop and think!

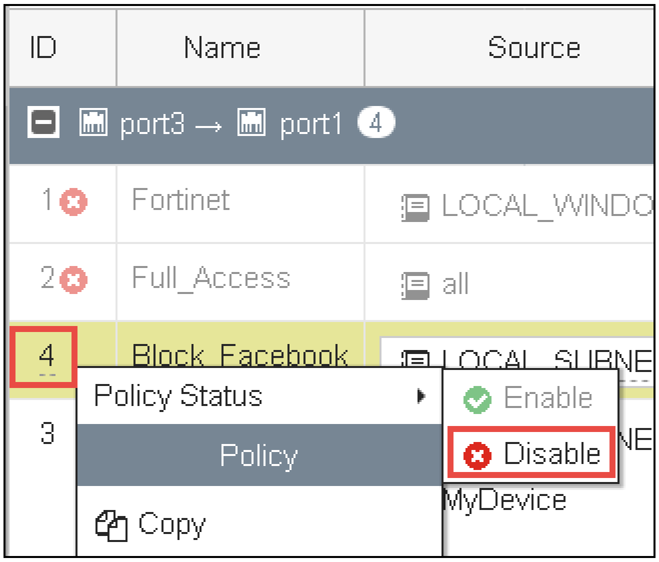
Why is Facebook blocked but Twitter is allowed?

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



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

2. Return to the browser where you are logged into the Local-FortiGate GUI, and right-click the **ID** column for the **Block_Facebook** firewall policy.
3. Select **Policy Status**, and then click **Disable**.



4. Close all browser tabs except for the Local-FortiGate GUI.

Exercise 5: Policy Lookup

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

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

Enable Existing Firewall Policies

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

Take the Expert Challenge!

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

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

After you have performed these steps, see Set Up and Test the Policy Lookup Criteria on page 49.

To enable existing firewall policies

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Policy & Objects** > **IPv4 Policy**.
3. Right-click the **ID** column for the **Fortinet** firewall policy, click **Policy Status**, and then click **Enable**.
4. Right-click the **ID** column for the **Full_Access** firewall policy, click **Policy Status**, and then click **Enable**.

Set Up and Test the Policy Lookup Criteria

Now, you will set up the policy lookup criteria. FortiGate will search and highlight the matching firewall policy based on your input criteria.

To set up and test the policy lookup criteria

1. Continuing on the Local-FortiGate GUI in the **Policy & Objects** > **IPv4 Policy**, click **Policy Lookup**.
2. Configure the following settings:

Field	Value
Source Interface	port3
Protocol	TCP
Source	10.0.1.100
Source Port	<Leave it empty>
Destination	fortinet.com
Destination Port	443

3. Click **Search**.

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

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

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

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

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

5. Click **Search**.

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

Reorder the Firewall Policies

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

Take the Expert Challenge!

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

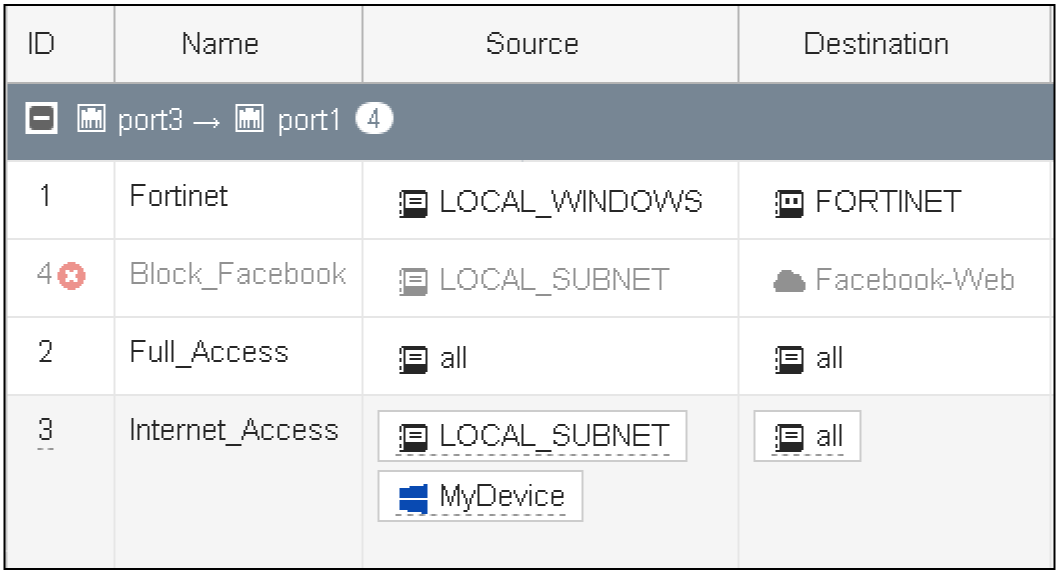
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you have performed these steps, see Retest Policy Lookup After Reordering the Firewall Policies on page 51.

To reorder the firewall policies

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. From the **ID** column, drag the **Block_Facebook** firewall policy above the **Full_Access** firewall policy.

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



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

Retest Policy Lookup After Reordering the Firewall Policies

Now, you will test the policy lookup feature after reordering the firewall policies.

To retest the policy lookup after reordering the firewall policies

1. Continuing on the Local-FortiGate GUI in **Policy & Objects** > **IPv4 Policy**, click **Policy Lookup**.
2. Set the following values:

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

3. Click **Search**.

Stop and think!

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

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

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

4. Right-click the **ID** column of the **Block_Facebook** policy and set the **Policy Status** to **Enable**.
5. Click **Policy Lookup**.
6. Click **Search**.

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

Lab 3: Network Address Translation (NAT)

NAT is used to perform source NAT (SNAT) and destination NAT (DNAT) for the traffic passing through FortiGate. There are two ways to configure source NAT and destination NAT:

- Firewall policy NAT
- Central NAT

In this lab, you will configure and test firewall policy NAT for SNAT using IP pool, and for DNAT using virtual IP (VIP).

You will configure and test SNAT using the central SNAT policy and DNAT using the DNAT policy and VIPs.

Objectives

- Configure destination NAT settings using a VIP.
- Configure the source NAT settings using overload IP pools.
- Configure a central NAT policy for the source NAT.
- Configure DNAT and VIPs for the destination NAT.

Time to Complete

Estimated: 50 minutes

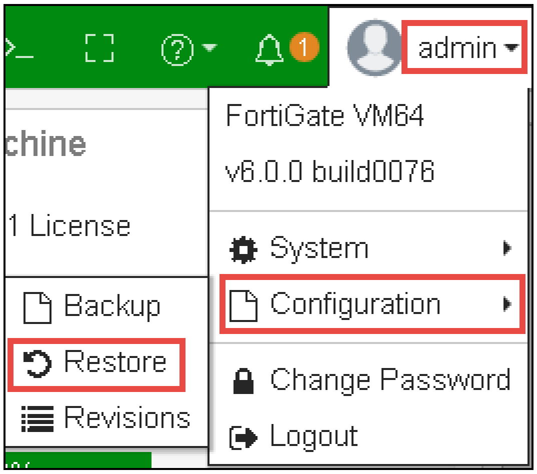
Prerequisites

Before starting the procedures in this lab, you must restore a configuration file on each FortiGate.

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

To restore the Remote-FortiGate configuration file

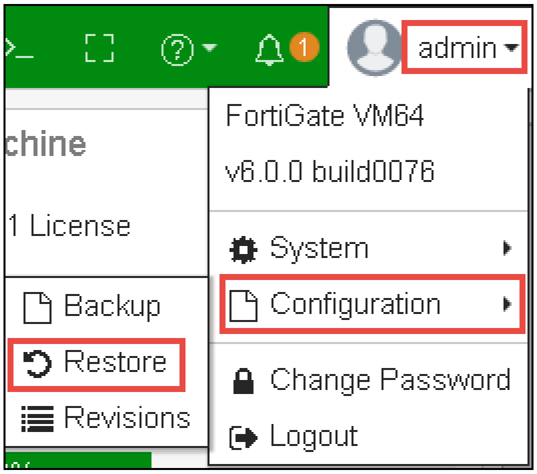
1. On the Local-Windows VM, open a browser and log in to the Remote-FortiGate GUI at `10.200.3.1`with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**,and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **NAT** > `remote-nat.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**,and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **NAT** > `local-nat.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Access Through VIPs

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

In this exercise, you will configure a VIP address for the Local-Windows VM. Then, you will create an egress-to-ingress firewall policy and apply a VIP address. This will allow Internet connections to the Local-Windows VM. You will also verify the destination NAT (DNAT) and source NAT (SNAT) behavior using CLI commands.

Create a VIP

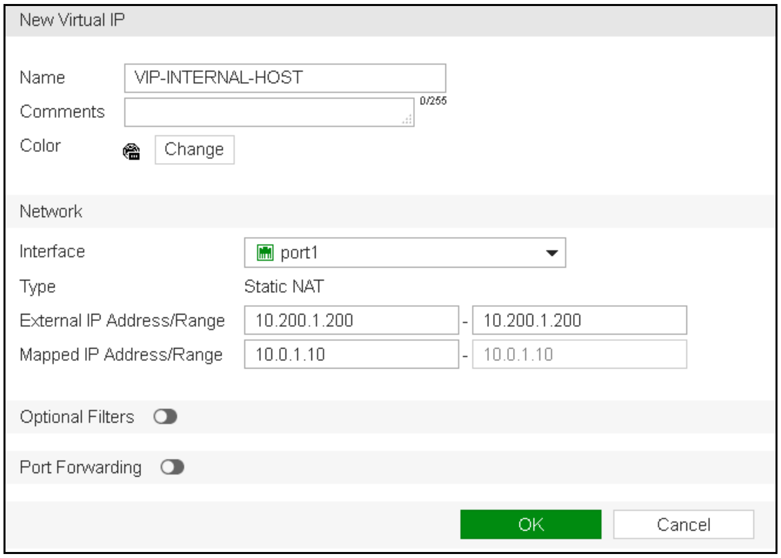
On FortiGate, a VIP is a destination NAT (DNAT), which you can select only in a firewall policy's destination address field.

In this procedure, you will configure the VIP to map the Local-Windows VM (`10.0.1.10`) to `10.200.1.200`, which is a part of the port1 subnet. You can refer to the lab Network Topology on page 10 diagram.

To create a VIP

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Policy & Objects** > **Virtual IPs**.
3. Click **Create New**, and then select **Virtual IP**.
4. Configure the following settings:

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


New Virtual IP

Name: VIP-INTERNAL-HOST

Comments: 0/255

Color: Change

Network

Interface: port1

Type: Static NAT

External IP Address/Range: 10.200.1.200 - 10.200.1.200

Mapped IP Address/Range: 10.0.1.10 - 10.0.1.10

Optional Filters

Port Forwarding

5. Click **OK**.

Create a Firewall Policy

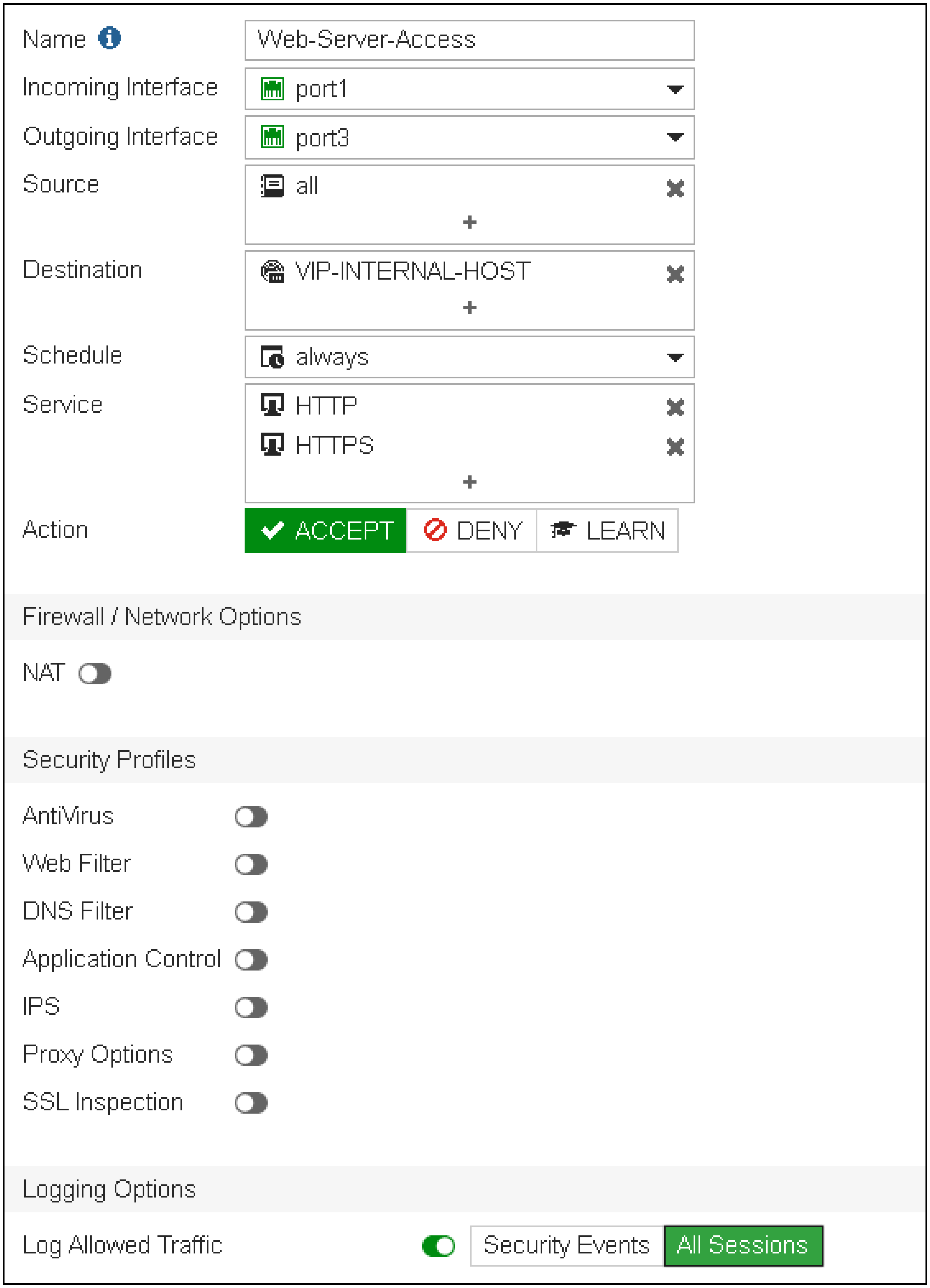
You will configure a new firewall policy using the VIP that you just created as the destination address.

To create a firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Click **Create New**.
3. Configure the following settings:

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

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



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

Firewall / Network Options

NAT ○

Security Profiles

AntiVirus	○
Web Filter	○
DNS Filter	○
Application Control	○
IPS	○
Proxy Options	○
SSL Inspection	○

Logging Options

Log Allowed Traffic ● Security Events [✓ All Sessions]

Test the VIP Firewall Policy

Now that you've configured a firewall policy with the VIP address as the destination, you can test your VIP by accessing it from the Remote-Windows VM, which is behind the Remote-FortiGate internal network. Traffic is routed from the Remote-FortiGate to the Local-FortiGate by a Linux machine, which acts as a router between these two FortiGate devices. For more information, see Network Topology on page 10.

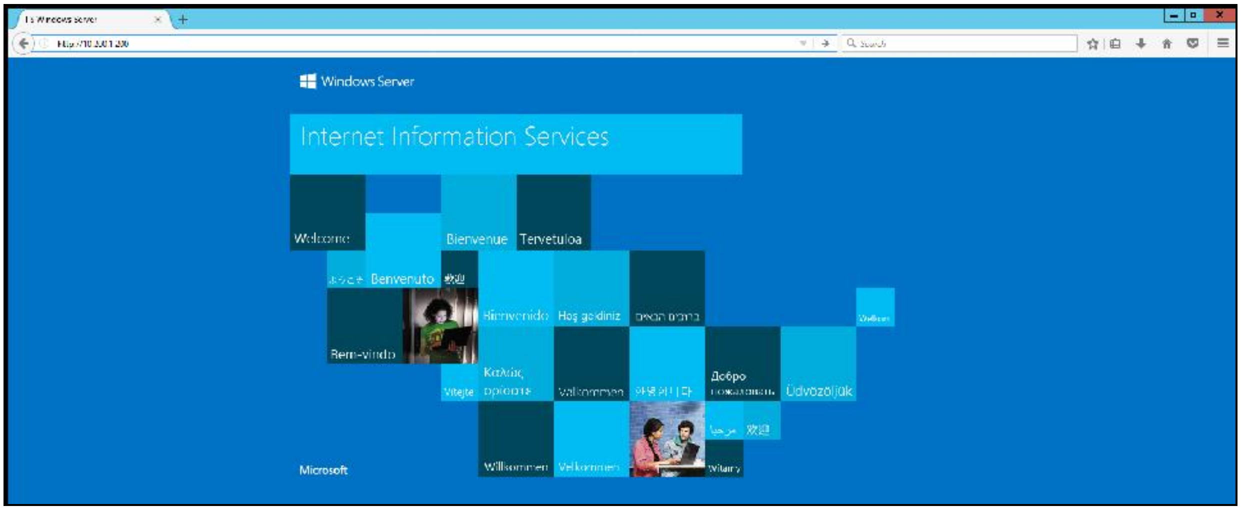
You will also test how the source address is translated by the VIP when traffic is leaving from the Local-Windows VM.

To test VIPs (DNAT)

1. On the Remote-Windows VM, open a web browser and go to the following URL:

    ```
    http://10.200.1.200
    ```

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



2. On the Local-Windows VM, open PuTTY and connect over SSH to the **LOCAL-FORTIGATE** saved session.
3. At the login prompt, enter the user name `admin` and password `password`.
4. Enter the following command to check the destination NAT entries in the session table:

    ```
    get system session list
    ```

    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.

Test the Source NAT

As a result of the VIP (which is a static NAT), all translated outgoing connections from the Local-Windows VM (IP address `10.0.1.10`) will use the VIP address to source NAT for the ingress-to-egress firewall policy and *not* the egress interface IP address.

To test SNAT

1. Continuing on Local-Windows, return to the Local-FortiGate PuTTY session and run the following command to clear any existing sessions:

```
diagnose sys session clear
```

The CLI command `diagnose sys session clear` will clear all sessions including SSH session you created using PuTTY. This is expected behavior.

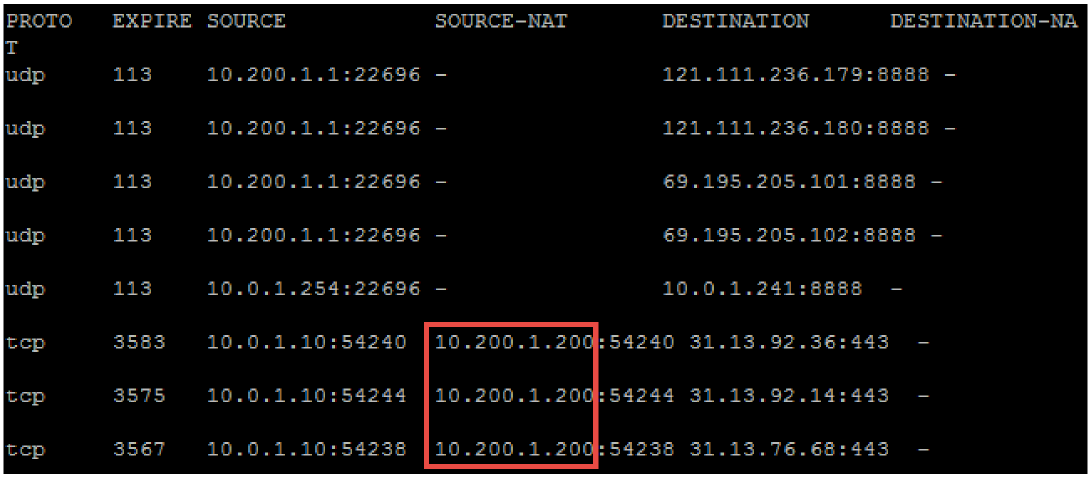
The firewall is stateful, so any existing sessions will not use this new firewall policy until they time out or are cleared for ingress-to-egress traffic.

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

2. Close the PuTTY window.
3. Open a web browser tab and connect to a few websites, for example:
   - www.fortinet.com
   - www.yahoo.com
   - www.bbc.com
4. Open PuTTY, and connect over SSH to the **LOCAL-FORTIGATE** saved session.
5. At the login prompt, enter the user name `admin` and password `password`.
6. Run the following command to view the session information:

```
get system session list
```

Sample output:



```
PROTO    EXPIRE SOURCE           SOURCE-NAT        DESTINATION       DESTINATION-NA
T
udp      113    10.200.1.1:22696 -                 121.111.236.179:8888 -

udp      113    10.200.1.1:22696 -                 121.111.236.180:8888 -

udp      113    10.200.1.1:22696 -                 69.195.205.101:8888 -

udp      113    10.200.1.1:22696 -                 69.195.205.102:8888 -

udp      113    10.0.1.254:22696 -                 10.0.1.241:8888  -

tcp      3583   10.0.1.10:54240  10.200.1.200:54240 31.13.92.36:443  -

tcp      3575   10.0.1.10:54244  10.200.1.200:54244 31.13.92.14:443  -

tcp      3567   10.0.1.10:54238  10.200.1.200:54238 31.13.76.68:443  -
```

The outgoing connections from the Local-Windows VM are now being 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 of the SNAT VIP. That is, when you enable SNAT on a policy, a VIP static NAT takes priority over the destination interface IP address.

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

Exercise 2: 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, the Local-FortiGate translates the source IP address of all traffic generated from the Local-Windows VM to `10.200.1.200` because of the SNAT translation in the VIP.

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

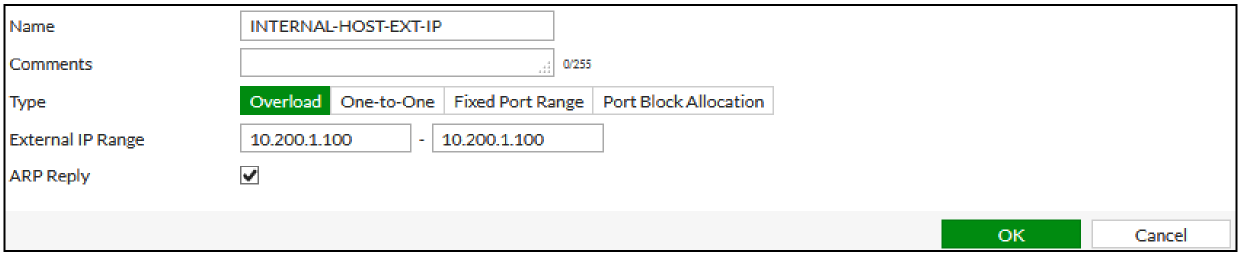
Create an IP Pool

In this procedure, 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. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Policy & Objects** > **IP Pools**.
3. Click **Create New** and configure the following settings:

Field	Value
Name	INTERNAL-HOST-EXT-IP
Type	Overload
External IP Range/Subnet	10.200.1.100 - 10.200.1.100



Name	INTERNAL-HOST-EXT-IP
Comments	0/255
Type	[✓ Overload] One-to-One Fixed Port Range Port Block Allocation
External IP Range	10.200.1.100 - 10.200.1.100
ARP Reply	☑

4. Click **OK**.

Edit a Firewall Policy to Use the IP Pool

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

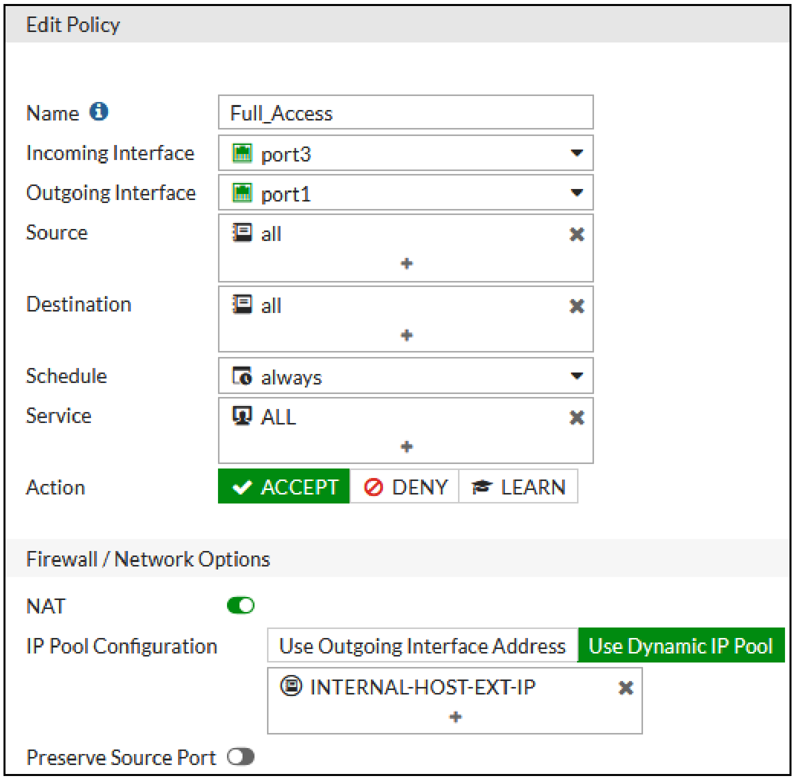
To edit the firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Right-click the **ID** column for the **Full_Access** firewall policy and click **Edit**.
3. In the **Firewall / Network Options** section, configure the following settings:

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

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

   Your configuration will look similar to the following example:



Edit Policy

Name	Full_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	ALL
Action	[✓ ACCEPT] DENY LEARN

Firewall / Network Options

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

5. Click **OK**.

Test Dynamic NAT with IP Pools

Now that your configuration is ready, you can test dynamic NAT with IP pools by browsing to a few external sites on the Internet. If successful, you will see that the Local-Windows 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. Continuing on the Local-Windows VM, open PuTTY and connect over SSH to the **LOCAL-FORTIGATE** saved session.
2. At the login prompt, enter the user name `admin` and password `password`.
3. Run the following command to clear any existing sessions:

```
diagnose sys session clear
```

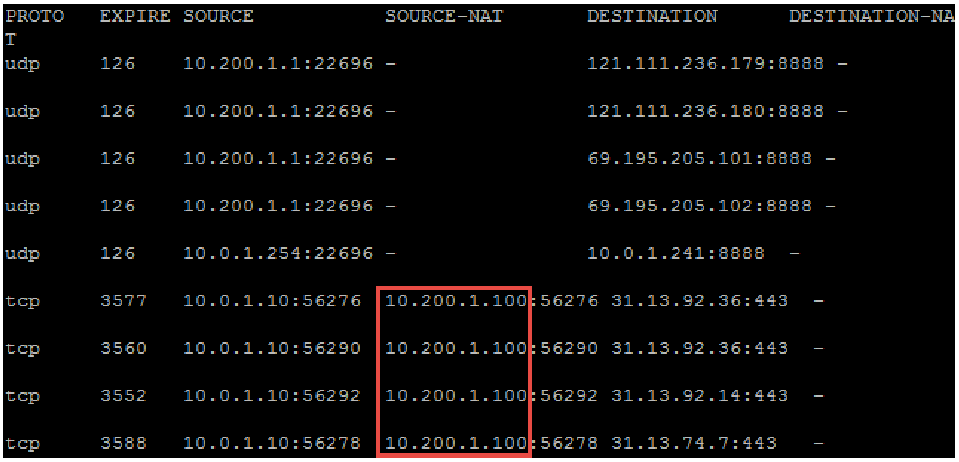
The CLI command `diagnose sys session clear` will clear all sessions including the SSH session you created using PuTTY. This is expected behavior.

The firewall is stateful, so any existing sessions will not use this updated firewall policy until they time out or are cleared for ingress-to-egress traffic.

4. Close the PuTTY window.
5. Open several broswer tabs and connect to a few websites. For example:
   - www.fortinet.com
   - www.yahoo.com
   - www.bbc.com
5. Open PuTTY and connect over SSH to the **LOCAL-FORTIGATE** saved session.
6. At the login prompt, enter the user name `admin` and password `password`.
7. Run the following command to verify the source NAT IP address that those sessions are using:

```
get system session list
```

Sample output:



```
PROTO    EXPIRE SOURCE           SOURCE-NAT       DESTINATION      DESTINATION-NA
T
udp      126    10.200.1.1:22696 -                121.111.236.179:8888 -

udp      126    10.200.1.1:22696 -                121.111.236.180:8888 -

udp      126    10.200.1.1:22696 -                69.195.205.101:8888 -

udp      126    10.200.1.1:22696 -                69.195.205.102:8888 -

udp      126    10.0.1.254:22696 -                10.0.1.241:8888  -

tcp      3577   10.0.1.10:56276  10.200.1.100:56276 31.13.92.36:443  -

tcp      3560   10.0.1.10:56290  10.200.1.100:56290 31.13.92.36:443  -

tcp      3552   10.0.1.10:56292  10.200.1.100:56292 31.13.92.14:443  -

tcp      3588   10.0.1.10:56278  10.200.1.100:56278 31.13.74.7:443   -
```

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

8. Close PuTTY.
9. Close all browser tabs except the Local-FortiGate GUI.

Exercise 3: Configure Central SNAT

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

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

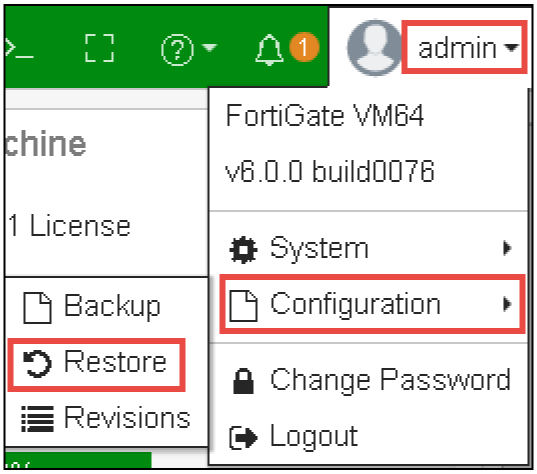
Prerequisites

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

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

To restore the Local-FortiGate configuration file

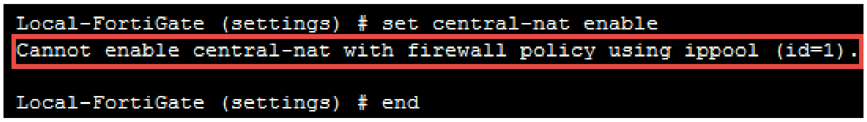
1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**,and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **NAT**> `local-central-nat.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

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

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



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

Local-FortiGate (settings) # end
```

To prevent this error from occurring during this exercise, the VIP and IP pool references must be removed from the firewall policies.

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

Configure Central SNAT Policy

In this procedure, you will configure a central SNAT policy using the IP pool you created in the previous exercise.

To review IP Pool Configuration

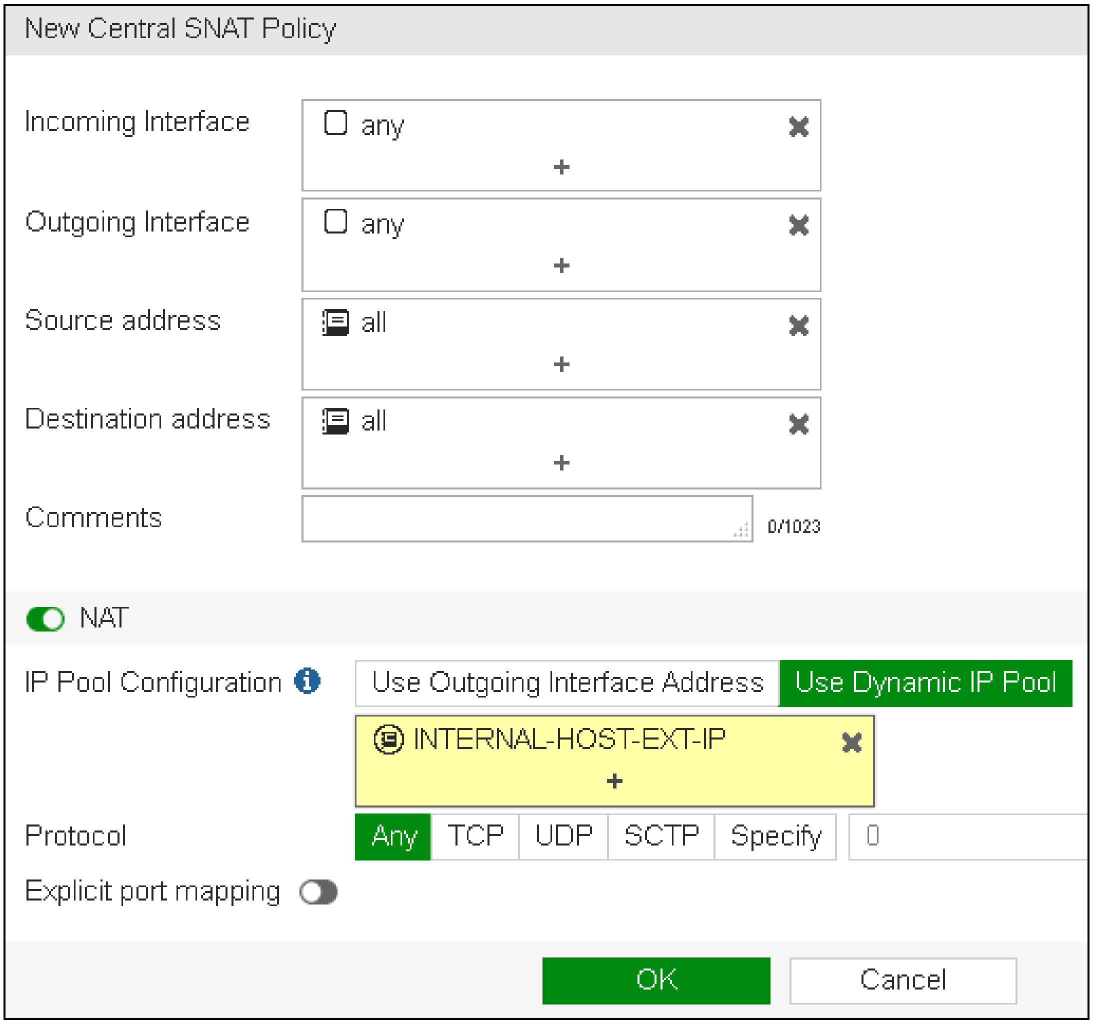
1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Policy & Objects** > **IP Pools**.
3. Review the settings of **INTERNAL-HOST-EXT-IP**.

To configure a central NAT policy

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

Field	Value
Incoming Interface	any
Outgoing Interface	any
Source address	all
Destination address	all
NAT	<enable>

Field	Value
IP Pool Configuration	Use Dynamic IP Pool Click + and select INTERNAL-HOST-EXT-IP
Protocol	ANY



New Central SNAT Policy

Incoming Interface: □ any ✖ +

Outgoing Interface: □ any ✖ +

Source address: all ✖ +

Destination address: all ✖ +

Comments: 0/1023

● NAT

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

INTERNAL-HOST-EXT-IP ✖ +

Protocol: **Any** | TCP | UDP | SCTP | Specify | 0

Explicit port mapping ○

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

NAT is enabled on the central SNAT policy.

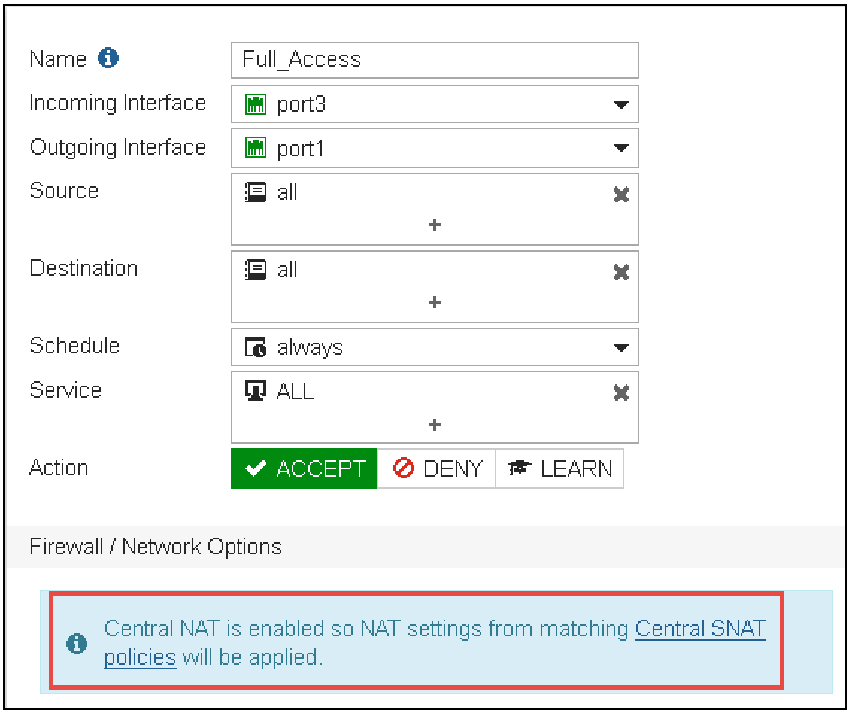
If no central SNAT or matching central SNAT rule exists, FortiGate drops the traffic.

Review the Firewall Policy

In this procedure, you will review the firewall policy.

To verify that NAT is enabled on firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Right-click the **ID** column for the **Full_Access** firewall policy and click **Edit**.
3. Review the **Firewall / Network Options** of the **Full_Access** policy.



Name	Full_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	ALL
Action	✓ ACCEPT DENY LEARN

Firewall / Network Options

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

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

4. Click **Cancel**.

Test Central SNAT

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

To test central SNAT

1. On the Local-Windows VM, open PuTTY and connect over SSH to the **LOCAL-FORTIGATE** saved session.
2. At the login prompt, enter the user name `admin` and password `password`.

3. Run the following command to clear the existing sessions:

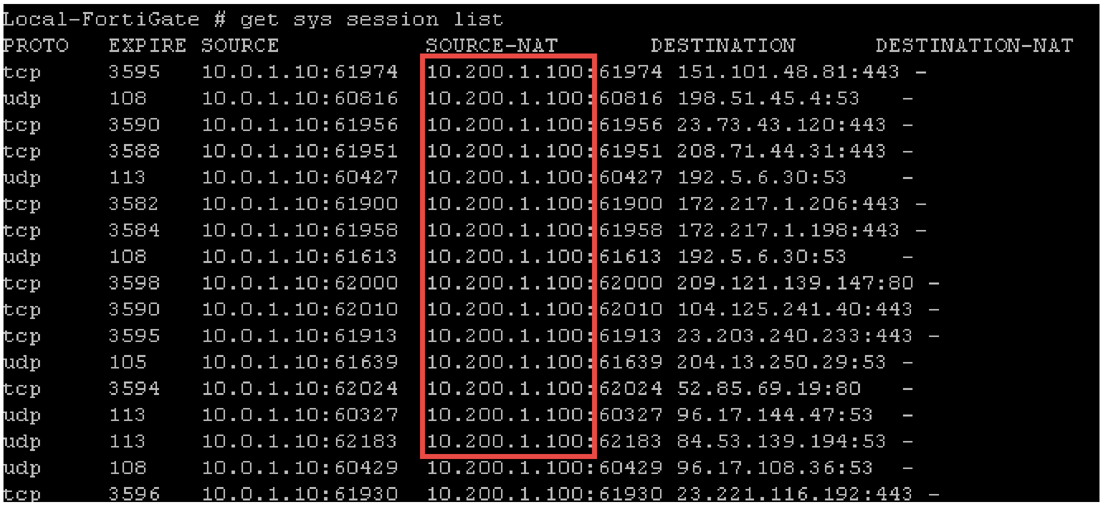
```
diagnose sys session clear
```

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

4. Close the PuTTY window.
5. Open multiple browser tabs and connect to a few websites. For example:
   - www.fortinet.com
   - www.yahoo.com
   - www.bbc.com
6. Open PuTTY and connect over SSH to the **LOCAL-FORTIGATE** saved session.
7. At the login prompt, enter the user name `admin` and password `password`.
8. Run the following command to verify the source NAT IP address that those sessions are using:

```
get system session list
```

Sample output:



```
Local-FortiGate # get sys session list
PROTO   EXPIRE SOURCE            SOURCE-NAT         DESTINATION        DESTINATION-NAT
tcp     3595   10.0.1.10:61974   10.200.1.100:61974 151.101.48.81:443 -
udp     108    10.0.1.10:60816   10.200.1.100:60816 198.51.45.4:53    -
tcp     3590   10.0.1.10:61956   10.200.1.100:61956 23.73.43.120:443 -
tcp     3588   10.0.1.10:61951   10.200.1.100:61951 208.71.44.31:443 -
udp     113    10.0.1.10:60427   10.200.1.100:60427 192.5.6.30:53    -
tcp     3582   10.0.1.10:61900   10.200.1.100:61900 172.217.1.206:443 -
tcp     3584   10.0.1.10:61958   10.200.1.100:61958 172.217.1.198:443 -
udp     108    10.0.1.10:61613   10.200.1.100:61613 192.5.6.30:53    -
tcp     3598   10.0.1.10:62000   10.200.1.100:62000 209.121.139.147:80 -
tcp     3590   10.0.1.10:62010   10.200.1.100:62010 104.125.241.40:443 -
tcp     3595   10.0.1.10:61913   10.200.1.100:61913 23.203.240.233:443 -
udp     105    10.0.1.10:61639   10.200.1.100:61639 204.13.250.29:53 -
tcp     3594   10.0.1.10:62024   10.200.1.100:62024 52.85.69.19:80   -
udp     113    10.0.1.10:60327   10.200.1.100:60327 96.17.144.47:53  -
udp     113    10.0.1.10:62183   10.200.1.100:62183 84.53.139.194:53 -
udp     108    10.0.1.10:60429   10.200.1.100:60429 96.17.108.36:53  -
tcp     3596   10.0.1.10:61930   10.200.1.100:61930 23.221.116.192:443 -
```

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

9. Close PuTTY.
10. Close all browser tabs except the Local-FortiGate GUI.

Create a Second IP Pool

Now you will create a second IP Pool, which you will use later when creating a second central SNAT policy.

Take the Expert Challenge!

On the Local-FortiGate GUI, create a second IP Pool named `SNAT-Pool` with IP range `10.200.1.50` - `10.200.1.50` and the type as **Overload**.

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

After you complete the challenge, see Create a Second SNAT Policy on page 70

To create a second IP Pool

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

Field	Value
Name	SNAT-Pool
Type	Overload
External IP Range	10.200.1.50 - 10.200.1.50

3. Click **OK**.

Create a Second SNAT Policy

Now you will create a more granular SNAT policy by selecting a specific destination address and protocol to match specific traffic.

Take the Expert Challenge!

On the Local-FortiGate GUI, create a second SNAT policy for **REMOTE_FORTIGATE** as a destination to allow only the TCP protocol using **SNAT_Pool** for traffic from port3 to port1.

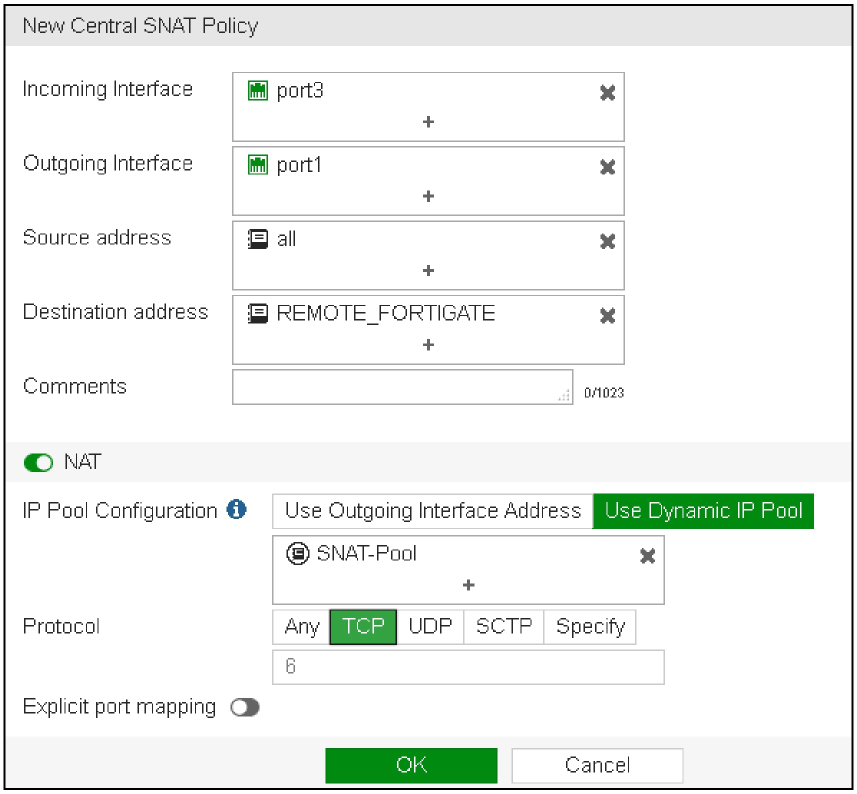
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Reorder Central SNAT Policies on page 71

To create second SNAT policy

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

Field	Value
Incoming Interface	port3
Outgoing Interface	port1
Source address	all
Destination address	REMOTE_FORTIGATE
NAT	<enable>
IP Pool Configuration	Use Dynamic IP Pool Click + and select SNAT-Pool
Protocol	TCP



New Central SNAT Policy

Incoming Interface: port3

Outgoing Interface: port1

Source address: all

Destination address: REMOTE_FORTIGATE

Comments: 0/1023

NAT: enabled

IP Pool Configuration: Use Outgoing Interface Address | [✓ Use Dynamic IP Pool]

SNAT-Pool

Protocol: Any | [✓ TCP] | UDP | SCTP | Specify

6

Explicit port mapping: disabled

3. Click **OK**.

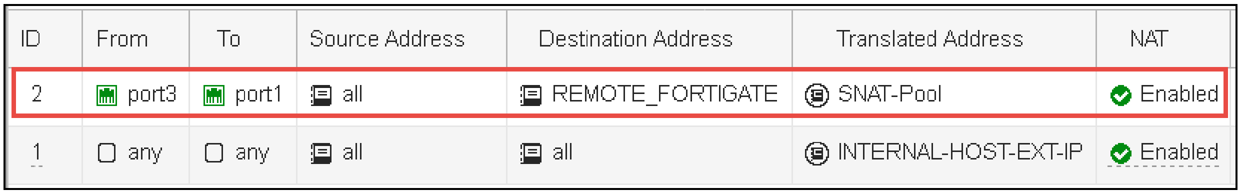
Reorder Central SNAT Policies

Now you will reorder the central NAT policies to put the more granular rule at the top.

Similar to firewall policies, a central SNAT policy is processed from *top to bottom* and, if a match is found, the source address and source port translate based on that central SNAT policy.

To reorder central SNAT policies

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **Central SNAT**.
2. Drag the newly created central SNAT policy above the previously created central SNAT policy.



ID	From	To	Source Address	Destination Address	Translated Address	NAT
2	port3	port1	all	REMOTE_FORTIGATE	SNAT-Pool	✓ Enabled
1	any	any	all	all	INTERNAL-HOST-EXT-IP	✓ Enabled

Test Central SNAT

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

To test central SNAT

1. On the Local-Windows VM, open PuTTY and connect over SSH to the **LOCAL-FORTIGATE** saved session.
2. At the login prompt, enter the user name `admin` and password `password`.
3. Run the following command to clear the existing sessions:

```
diagnose sys session clear
```

4. Close the PuTTY window.
5. Open a new browser tab and log in to the Remote-FortiGate GUI at `10.200.3.1`with the user name `admin` and password `password`.
6. Open a command prompt and run a continuous ping to the Remote-FortiGate IP.

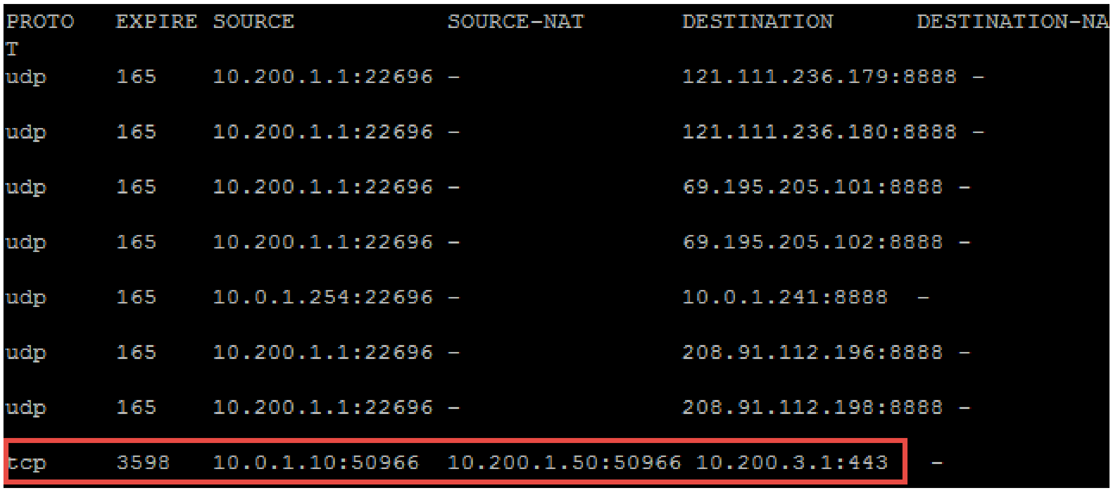
```
ping -t 10.200.3.1
```

8. Open PuTTY and connect over SSH to the **LOCAL-FORTIGATE** saved session.
9. At the login prompt, enter the user name `admin` and password `password`.
10. Run the following command:

```
get system session list
```

Notice that the TCP sessions to destination `10.200.3.1` are translated to `10.200.1.50`, because that address matches the central SNAT policy.

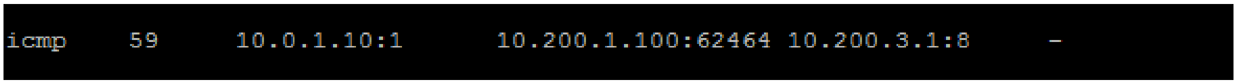
Sample output:



```
PROTO    EXPIRE SOURCE            SOURCE-NAT         DESTINATION        DESTINATION-NA
T
udp      165    10.200.1.1:22696 -                  121.111.236.179:8888 -

udp      165    10.200.1.1:22696 -                  121.111.236.180:8888 -

udp      165    10.200.1.1:22696 -                  69.195.205.101:8888 -

udp      165    10.200.1.1:22696 -                  69.195.205.102:8888 -

udp      165    10.0.1.254:22696 -                  10.0.1.241:8888   -

udp      165    10.200.1.1:22696 -                  208.91.112.196:8888 -

udp      165    10.200.1.1:22696 -                  208.91.112.198:8888 -

tcp      3598   10.0.1.10:50966  10.200.1.50:50966 10.200.3.1:443    -
```

ICMP sessions to destination `10.200.3.1` are translated to `10.200.1.100`, which matches the central SNAT policy at the bottom.

Sample output:



```
icmp     59      10.0.1.10:1       10.200.1.100:62464 10.200.3.1:8     -
```

11. Open several browser tabs and connect to a few websites. For example:
    - www.fortinet.com
    - www.yahoo.com
    - www.bbc.com
12. Return to **LOCAL-FORTIGATE** PuTTY session.
13. Run the following command:

    ```
    get system session list
    ```

    Also, other TCP sessions to different destinations are translated to `10.200.1.100,` based on the matching central SNAT policy at the bottom.

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

14. Close the command prompt and PuTTY.
15. Close all browser tabs except the Local-FortiGate GUI.

Exercise 4: DNAT and VIPs

In firewall policy NAT, **Virtual IPs** is selected in the firewall policy as the destination address. In central NAT, as soon as **DNAT & Virtual IPs** is configured, FortiGate automatically creates a rule in the kernel to allow DNAT to occur, and no additional configuration is required.

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

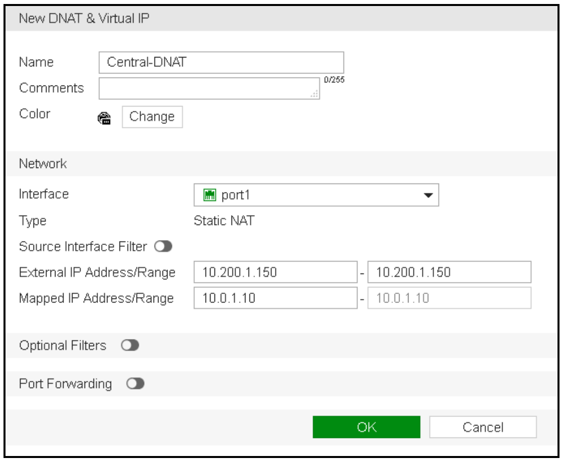
Create DNAT and VIPs

In this procedure, you will configure DNAT and VIPs.

To create DNAT and VIPs

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Policy & Objects** > **DNAT & Virtual IPs**.
3. Click **Create New**, and then select **DNAT & Virtual IP**.
4. Configure the following settings:

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



New DNAT & Virtual IP

Name: Central-DNAT
Comments: 0/255
Color

Network

Interface: port1
Type: Static NAT
Source Interface Filter
External IP Address/Range: 10.200.1.150 - 10.200.1.150
Mapped IP Address/Range: 10.0.1.10 - 10.0.1.10

Optional Filters

Port Forwarding

5. Click **OK**.

Verify the Firewall Policy Settings

Now, you will verify the firewall policy settings for the egress-to-ingress firewall policy.

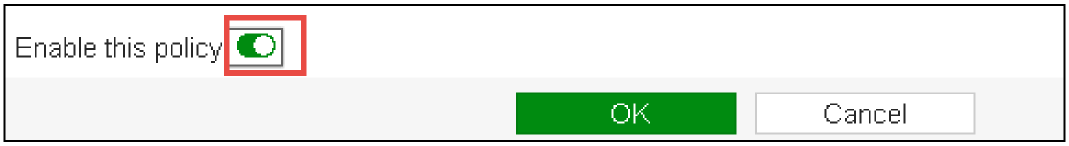
To verify the firewall policy settings

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Right click **ID** column of the **Web-Server-Access** firewall policy, and then click **Edit**.
3. Review the settings of the firewall policy.
4. Try to select the **DNAT & Virtual IPs** address in the firewall destination address.

   You will be not able to do so.

You can't select VIPs previously created in a firewall policy as a destination address. As soon as a VIP object is created, FortiGate automatically creates a rule in the kernel for DNAT to occur.

5. Scroll to the bottom of the page and ensure the **Enable this policy** switch is turned on.



6. Click **OK**.

Testing DNAT and VIPs

In this procedure, you will test DNAT and VIPs by accessing the Local-Windows VM.

To test DNAT and VIPs

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

   ```
   http://10.200.1.150
   ```

   If the VIP operation is successful, a simple web page opens.
2. Return to the Local-Windows VM.
3. Open PuTTY and connect over SSH to the **LOCAL-FORTIGATE** saved session.
4. At the login prompt, enter the user name `admin` and password `password`.
5. Run the following command to check the destination NAT entries in the session table:

   ```
   get system session list
   ```

   Sample output:

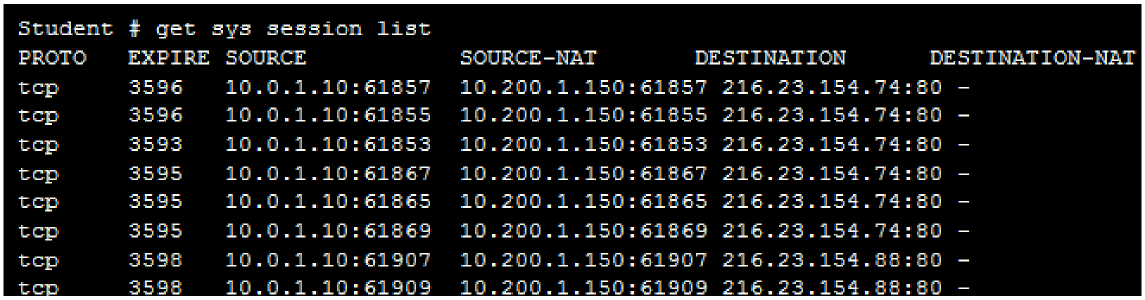
   ```
   Local-FortiGate # get system session list
   PROTO EXPIRE    SOURCE    SOURCE-NAT  DESTINATION    DESTINATION-NAT
   ```

```
    tcp   3599  10.200.3.1:49183 10.200.1.100 10.200.1.150:80  10.0.1.10:80
```

6. Open additional web browser tabs and try to access few websites. For example:
    - www.fortinet.com
    - www.yahoo.com
    - www.bbc.com
7. Return to the Local-FortiGate PuTTY session and verify the SNAT IP address those sessions are using:

    ```
    get system session list
    ```

    Sample output:

    ```
    Student # get sys session list
    PROTO   EXPIRE SOURCE           SOURCE-NAT        DESTINATION      DESTINATION-NAT
    tcp     3596   10.0.1.10:61857  10.200.1.150:61857 216.23.154.74:80 -
    tcp     3596   10.0.1.10:61855  10.200.1.150:61855 216.23.154.74:80 -
    tcp     3593   10.0.1.10:61853  10.200.1.150:61853 216.23.154.74:80 -
    tcp     3595   10.0.1.10:61867  10.200.1.150:61867 216.23.154.74:80 -
    tcp     3595   10.0.1.10:61865  10.200.1.150:61865 216.23.154.74:80 -
    tcp     3595   10.0.1.10:61869  10.200.1.150:61869 216.23.154.74:80 -
    tcp     3598   10.0.1.10:61907  10.200.1.150:61907 216.23.154.88:80 -
    tcp     3598   10.0.1.10:61909  10.200.1.150:61909 216.23.154.88:80 -
    ```

    Notice that the session originating from source IP, `10.0.1.10,` is translated to `10.200.1.150` (VIP) as opposed to the central SNAT policy pool IP of `10.200.1.100`. This is expected behavior in central NAT.

If both the SNAT and DNAT are defined, the egress traffic will source NAT to the DNAT/VIP address, as opposed to the configured source SNAT policy.

8. Close PuTTY.
9. Close all browser tabs except the Local-FortiGate GUI.

Lab 4: Firewall Authentication

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

You will also configure captive portal, so that any user connecting to the network is prompted for their login credentials (active authentication).

Objectives

- Configure server-based password authentication with an LDAP server.
- Configure captive portal so users connecting to the network are forced to authenticate.

Time to Complete

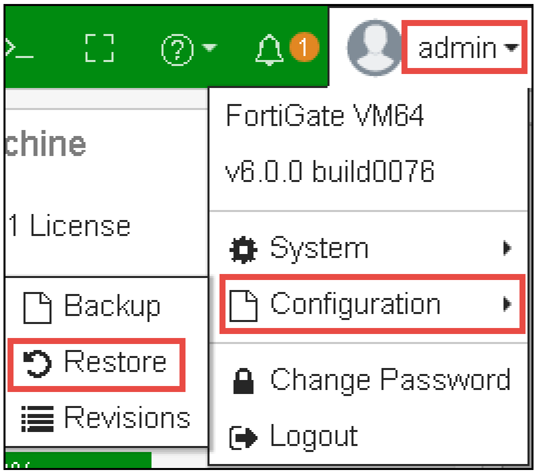
Estimated: 20 minutes

Prerequisites

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

To restore the Local-FortiGate configuration file

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then select **Configuration** > **Restore**.



3. Click **Local PC**,and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **Firewall-Authentication** > `local-firewall-authentication.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring Remote Authentication

In this exercise, you will configure an LDAP server on FortiGate for remote authentication, create a remote authentication group for remote users, and add that group as a source in a firewall policy.

Finally, you will authenticate over SSL-VPN as one of the remote users, and then monitor the login as the administrator.

Configure an LDAP Server on FortiGate

You can configure FortiGate to point to an LDAP server for server-based password authentication using the preconfigured Active Directory service located on the Local-Windows VM. Active Directory already has users available to use in this lab.

To configure an LDAP server on FortiGate

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **User & Device** > **LDAP Servers**, and then click **Create New**.
3. Configure a server using the following settings:

Field	Value
Name	ADserver
Server IP/Name	10.0.1.10 This is the IP address of the Windows Server, Local-Windows VM. For more information, see Network Topology on page 10.
Server Port	389 This is the default port for LDAP.
Common Name Identifier	cn This is the attribute name used to find the user name. Active Directory calls this cn.
Distinguished Name	ou=Training,dc=trainingAD,dc=training,dc=lab This is the domain name for Active Directory on the Windows Server. Active Directory has already been preconfigured, with all users located in the Training organizational unit (ou).
Bind Type	Regular

Field	Value
Username	ADadmin We are using the credentials of an Active Directory user called ADadmin to authenticate to Active Directory. ADadmin is located in the Users organizational unit (ou).
Password	Training! This is the password pre-configured 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 to a Firewall Group

Now, 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.

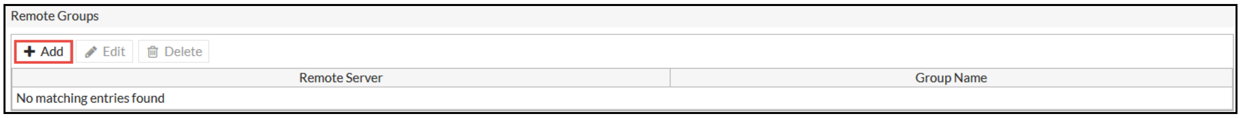
After you have completed this exercise, see Add the Remote User Group to Your Firewall Policy on page 81.

To assign a user to a user group

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

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

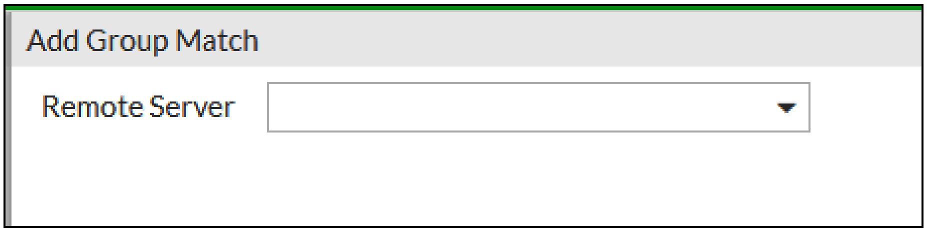
2. To add users from the remote LDAP server, in the **Remote Groups** table, click **Add**.



Remote Groups

Remote Server	Group Name
No matching entries found	

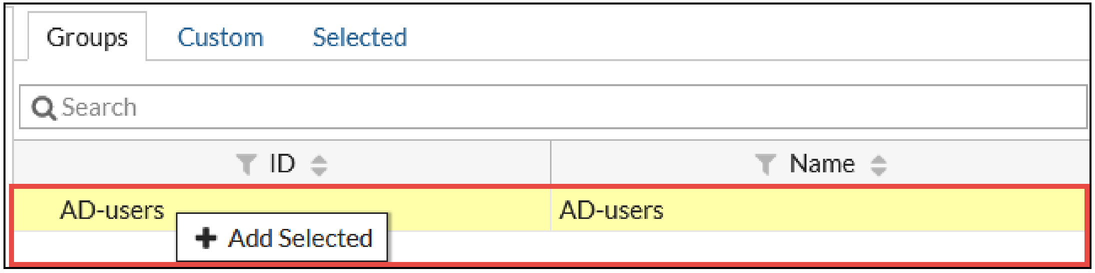
The **Add Group Match** dialog box opens.



Add Group Match

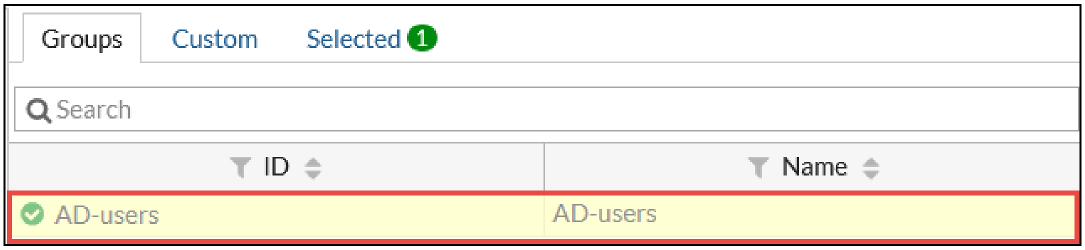
Remote Server

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



ID	Name
AD-users	AD-users

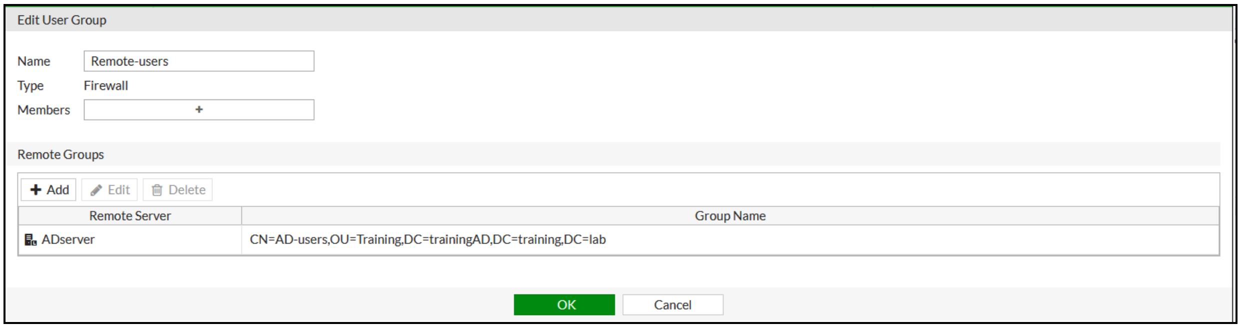
The AD-users group is disabled and has a green checkmark beside it, indicating it has been added.



ID	Name
✓ AD-users	AD-users

5. Click **OK**.

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



Edit User Group

Name Remote-users
Type Firewall
Members +

Remote Groups

Remote Server	Group Name
ADserver	CN=AD-users,OU=Training,DC=trainingAD,DC=training,DC=lab

6. Click **OK**.

Add the Remote User Group to Your Firewall Policy

Now that the LDAP server is added 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.

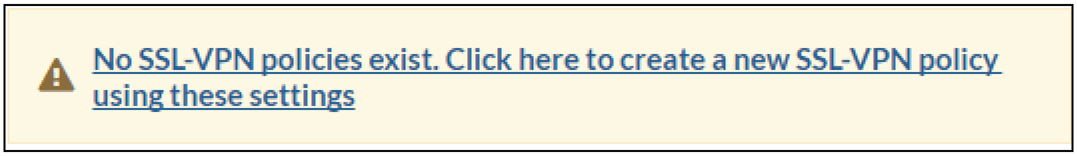
Because a remote user on your LDAP server will authenticate over SSL-VPN, you will add the group to an SSL-VPN firewall policy.

Configuring SSL-VPN is out of scope for this lab, so the SSL-VPN settings are preconfigured. However, you still need to configure an SSL-VPN firewall policy and add the **Remote-user** group to it.

To add the remote user group to your firewall policy

1. Continuing on the Local-FortiGate GUI, click **VPN** > **SSL-VPN Settings**, and then click the warning message that opens at the top of the page.

   Clicking this warning message will create a new SSL-VPN policy using the preconfigured settings.



⚠ No SSL-VPN policies exist. Click here to create a new SSL-VPN policy using these settings

2. Configure the following settings:

Field	Value
Name	SSL-VPN
Outgoing Interface	port1
Source	LOCAL_SUBNET Remote-users (located under **User**)
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT

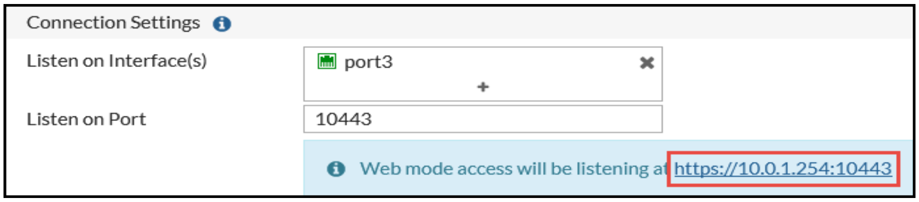
3. In the **Security Profiles** section, enable **Web Filter**, and then select **Category_Monitor**.

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

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

6. Click **OK**.

   The **SSL_VPN Settings** page reopens. Note that web mode access for SSL VPN is listening at `https://10.0.1.254:10443`.



Connection Settings

Listen on Interface(s): port3

Listen on Port: 10443

Web mode access will be listening at https://10.0.1.254:10443

To test whether aduser1 will be able to successfully authenticate

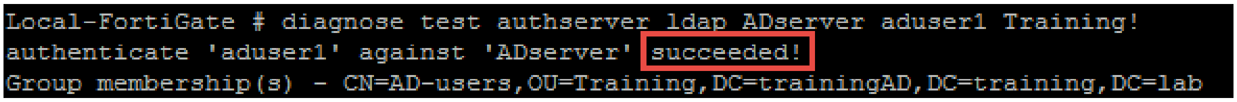
1. Continuing on the Local-Windows VM, open PuTTY and connect over SSH to the **LOCAL-FORTIGATE** saved session.
2. At the login prompt, enter the user name `admin` and password `password`.
3. Type the following command:

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

   Where:

- `<LDAP server name>` is ADserver (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 ADserver aduser1 Training!
authenticate 'aduser1' against 'ADserver' succeeded!
Group membership(s) - CN=AD-users,OU=Training,DC=trainingAD,DC=training,DC=lab
```

4. Close PuTTY.

Authenticate and Monitor

Now, you will authenticate through the preconfigured SSL VPN as aduser1. This user is a member of the **Remote_users** group on FortiGate. Then, you will monitor the authentication.

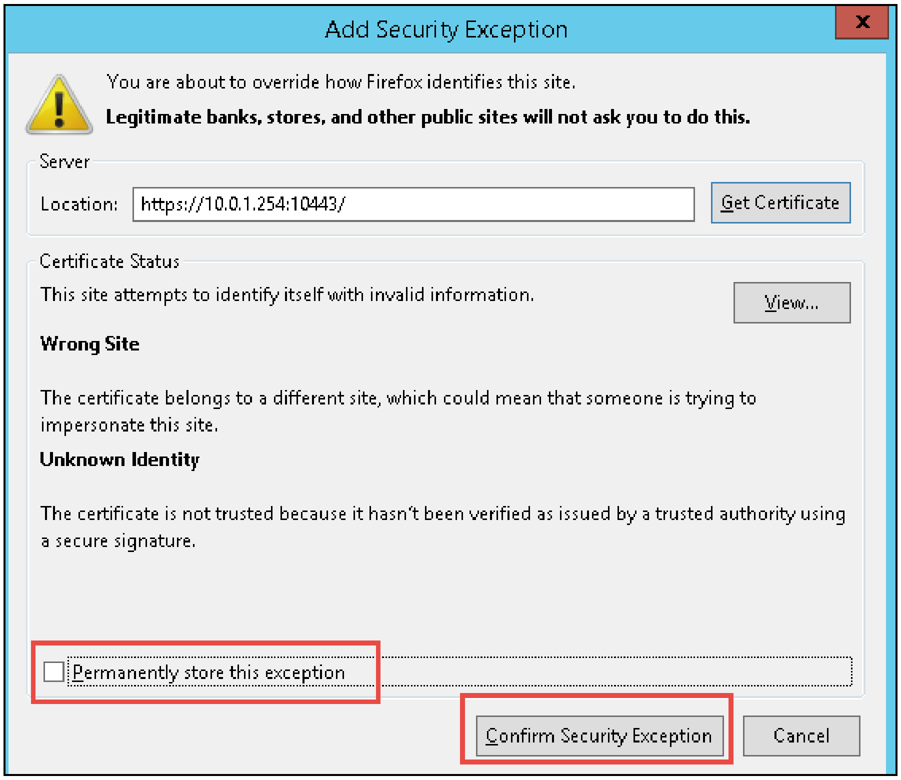
To authenticate as a remote user

1. Continuing on the Local-Windows VM, open a new browser tab and go to `https://10.0.1.254:10443`.

   This is the web mode access for SSL VPN.

   If you receive an error that indicates your connection is not secure, click **Advanced**, and then select **Add Exception**.

2. Clear the **Permanently store this exception** check box and click **Confirm Security Exception**.



Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://10.0.1.254:10443/

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

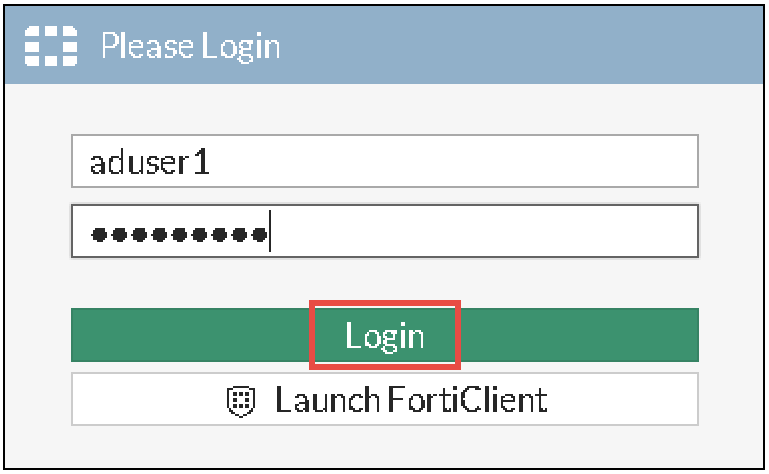
The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

☐ Permanently store this exception

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

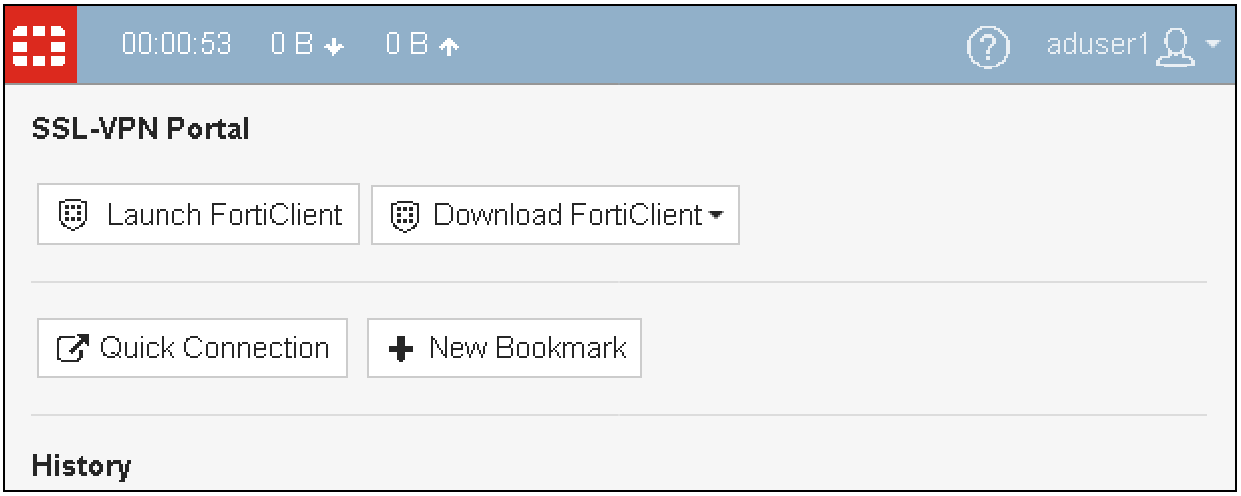


Please Login

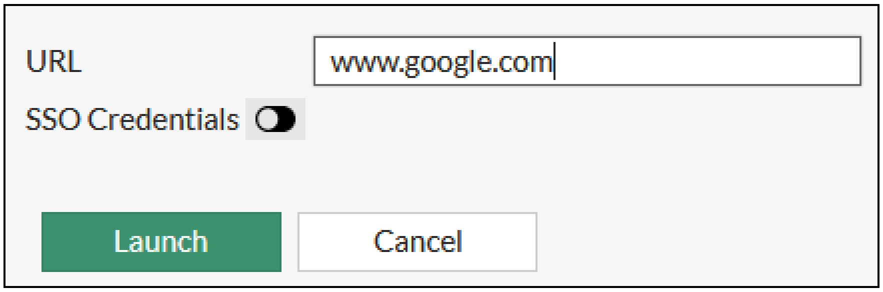
aduser1

●●●●●●●●●

The SSL VPN Web portal opens.



4. Click **Quick Connection**.
5. In the **URL** field, type `www.google.com`, and then click **Launch**.



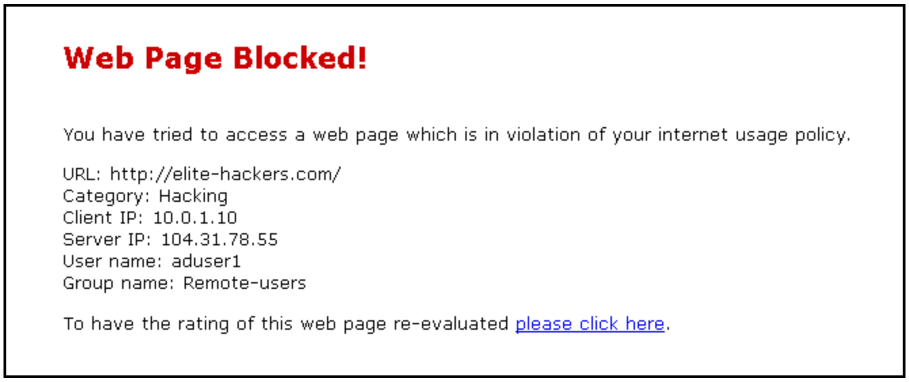
URL www.google.com

SSO Credentials

The site launches successfully.

6. Return to your browser tab with the SSL-VPN portal and click **Quick Connection** again. This time, in the **URL** field, type `elite-hackers.com` and then click **Launch**.

   This URL is set to be blocked by the Web Filter security profile you enabled in the SSL VPN firewall policy.



Web Page Blocked!

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

URL: http://elite-hackers.com/
Category: Hacking
Client IP: 10.0.1.10
Server IP: 104.31.78.55
User name: aduser1
Group name: Remote-users

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

7. Remain logged in to the SSL VPN portal and continue to the next procedure.

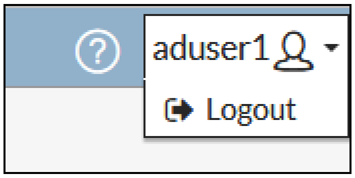
To monitor user authentications

1. Return to the browser tab where you are logged in to Local-FortiGate as `admin`.
2. To monitor aduser1, click **Monitor** > **SSL-VPN Monitor**.
3. To view the activity of aduser1, do one of the following:

- Click **FortiView** > **All Sessions**.
- Click **Log & Report** > **Forward Traffic**.
- Click **Log & Report** > **Web Filter**.

If you do not see a **Web Filter** menu item, refresh your browser tab.

4. Return to the browser tab where you are logged in to the SSL VPN portal and log out.



5. Return to the browser tab with the Local-FortiGate GUI, and go to **Monitor** > **SSL-VPN Monitor**.

Stop and think!

Why does aduser1 no longer appear in the SSL-VPN monitor?

The user no longer appears in the SSL-VPN monitor because the connection is no longer active.

6. Close your browser.

Exercise 2: Configuring Captive Portal

In this exercise, you will configure captive portal and restrict access to a specific user group. Captive portal is a convenient way to authenticate web users on wired or Wi-Fi networks using an HTML form that requests a user name and password (active authentication).

This exercise involves creating a user group (and adding a user to it), enabling captive portal and restricting access based on that group, and enabling the disclaimer message.

Finally, you will authenticate through captive portal and monitor the authentication.

Create a User Group for Captive Portal

Because the goal is to enable captive portal based on a specific group, you must first create a user group and then add a user to the group. For the purposes of this exercise, you will add the user **student** to the group. Student is a local user on FortiGate that was preconfigured.

To create a user group for captive portal

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **User & Device** > **User Groups**, and then click **Create New**.
3. Create a captive portal user group using the following settings:

Field	Value
Name	CP-group
Type	Firewall
Members	student

4. Click **OK**.

Enable Captive Portal

Now, you will enable captive portal on a wired network.

To enable captive portal

1. Continuing on the Local-FortiGate GUI, click **Network** > **Interfaces**, and then edit **port3**.
   This port is your incoming traffic. For more information, see Network Topology on page 10.
2. In the **Admission Control** section, enable captive portal using the following settings:

Field	Value
Security Mode	Captive Portal
Authentication Portal	Local
User Access	Restricted to Groups
User Groups	CP-group

3. Click **OK**.

Enable the Disclaimer Message

To provide a disclaimer message to users who are logging in through captive portal, you must enable disclaimers. Because you are enabling captive portal through a wired interface, you can enable disclaimers only using the CLI.

If you enable captive portal using Wi-Fi, you can enable disclaimers using the GUI (**WiFi & Switch Controller** > **SSID**). You are using a wired interface in this lab.

To enable the disclaimer message

1. Continuing on the Local-Windows VM, open PuTTY and connect over SSH to the **LOCAL-FORTIGATE** saved session.
2. At the login prompt, enter the user name `admin` and password `password`.
3. Type the following commands:

```
config firewall policy
edit 1
set disclaimer enable
end
```

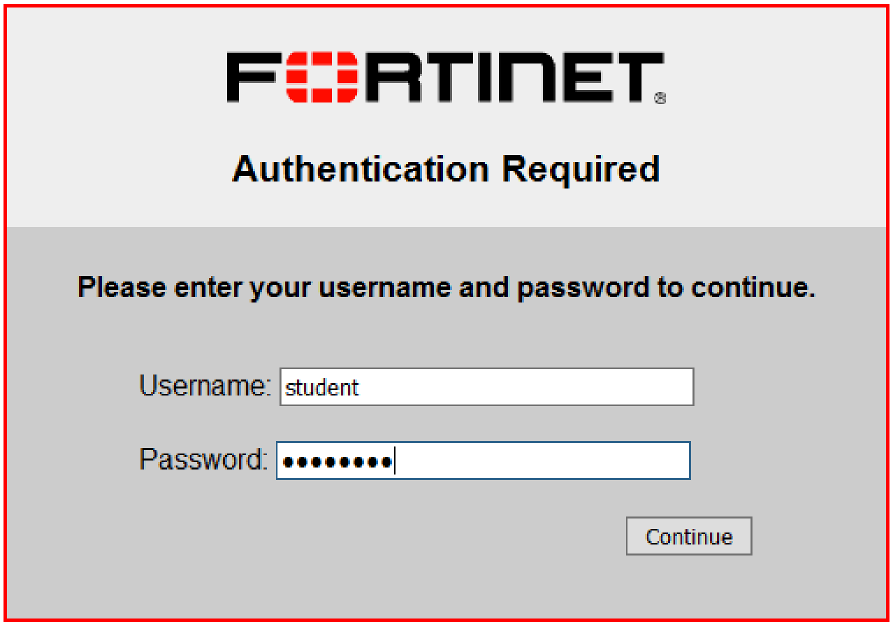
4. Close PuTTY.

Authenticate and Monitor

Now that captive portal is configured and the disclaimer is enabled, you can test the configuration by authenticating through captive portal as the **student** user. Then, you will monitor the authentication as the **admin** user.

To authenticate through captive portal

1. Continuing on the Local-Windows VM, open a new browser tab and go to a website, such as www.bbc.com.
2. When prompted, log in with the username `student` and password `fortinet`.



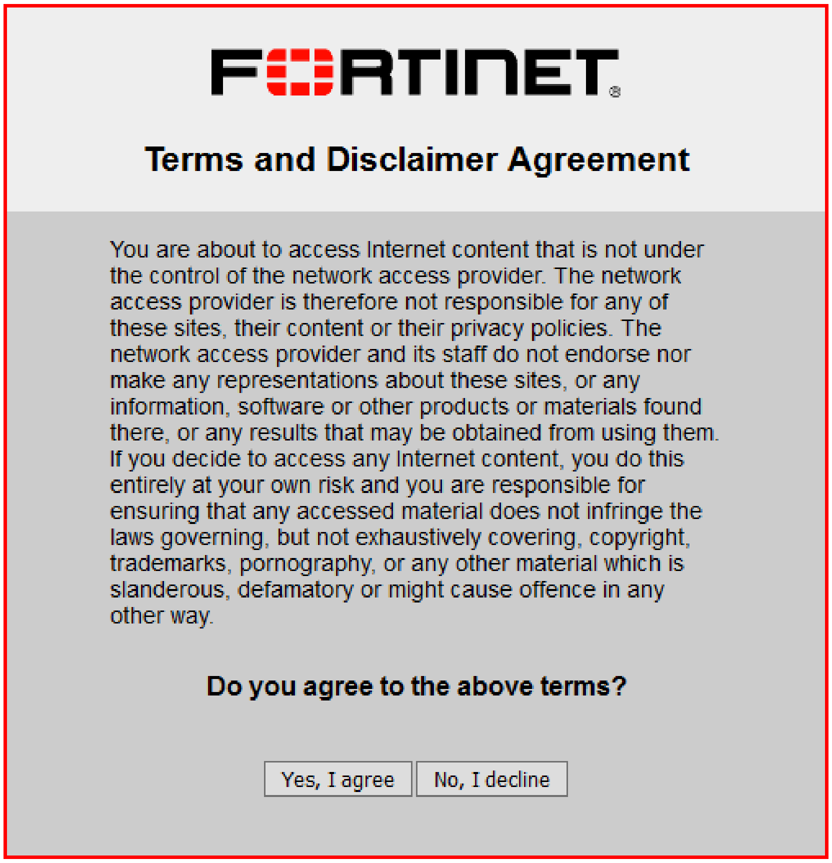
Authentication Required

Please enter your username and password to continue.

Username: student

Password: ●●●●●●●●●

The **Terms and Disclaimer Agreement** dialog opens.



Terms and Disclaimer Agreement

You are about to access Internet content that is not under the control of the network access provider. The network access provider is therefore not responsible for any of these sites, their content or their privacy policies. The network access provider and its staff do not endorse nor make any representations about these sites, or any information, software or other products or materials found there, or any results that may be obtained from using them. If you decide to access any Internet content, you do this entirely at your own risk and you are responsible for ensuring that any accessed material does not infringe the laws governing, but not exhaustively covering, copyright, trademarks, pornography, or any other material which is slanderous, defamatory or might cause offence in any other way.

Do you agree to the above terms?

3. Click **Yes, I agree**.

   After you agree to the terms, you are redirected to the website you originally requested.

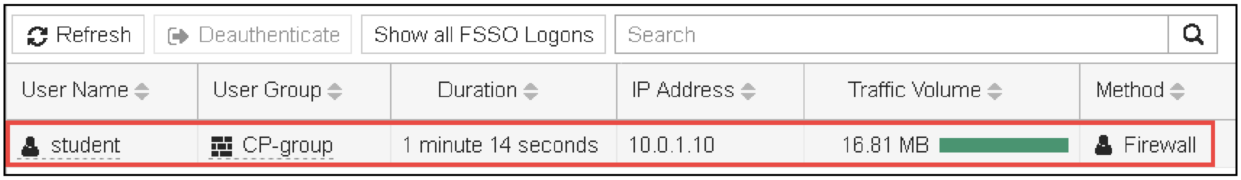
4. Open additional browser tabs and access a few more websites through captive portal, for example:

- www.youtube.com
- www.cnn.com

5. Leave all browser tabs open and continue to the next procedure.

To monitor active captive portal authentications

1. Continuing on the Local-Windows VM, return to the browser tab where you are logged in to the Local-FortiGate GUI as `admin`.
2. Monitor the student user. To view this login authentication, click **Monitor** > **Firewall User Monitor**.



User Name	User Group	Duration	IP Address	Traffic Volume	Method
student	CP-group	1 minute 14 seconds	10.0.1.10	16.81 MB	Firewall

While the CLI `config user setting` dictates how long a user authenticating through captive portal can remain authenticated, you can choose to manually revoke a captive portal user's authentication by selecting the user in the **Firewall User Monitor** list and clicking **De-authenticate**. Once deauthenticated, the user disappears from the list, because it is reserved for active users only.

3. Select **student** and click **De-authenticate** to manually end the user's session.
4. Click **OK**.
5. Close the browser.

Lab 5: Logging and Monitoring

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

Objectives

- Configure logging on FortiGate so FortiGate understands how to log traffic.
- Configure threat weight.
- Monitor logs through alert emails.
- View logs on the Local-FortiGate GUI.

Time to Complete

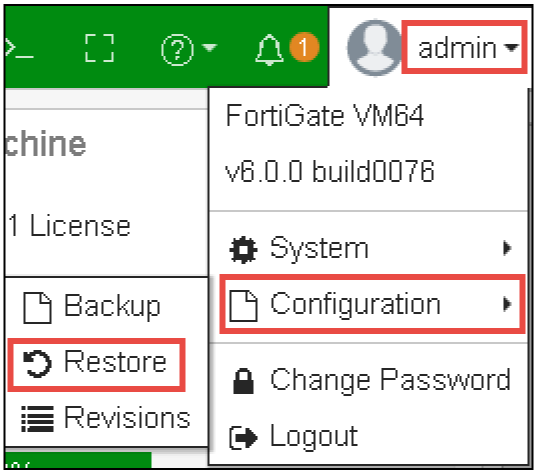
Estimated: 35 minutes

Prerequisites

Before beginning this lab, you must restore a configuration file to Local-FortiGate. After the reboot, you must also check your web filter license status, because you will be using web filtering in this lab and it must show as licensed.

To restore the Local-FortiGate configuration file

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **Logging** > `local-logging.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

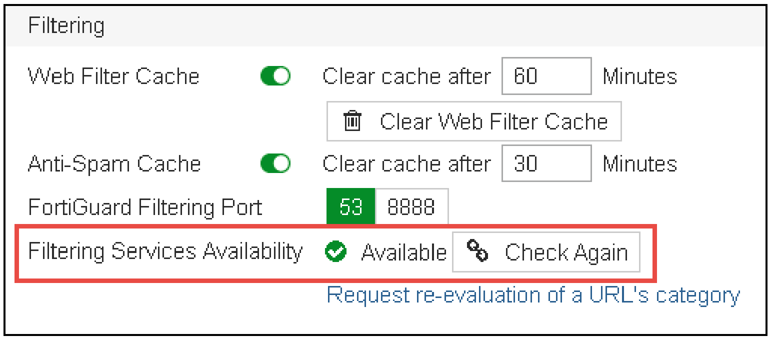
To check the web filter license status upon reboot

1. Continuing on the Local-Windows VM, log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Select **Dashboard**, and in the **Licenses** widget, verify that there is a green check mark next to **Web Filtering**, indicating the service is licensed and active.

   If it is licensed, continue to Configuring Log Settings on page 92
3. If there is a grey **?** icon next to **Web Filtering**, indicating the license status is unavailable, complete the following:

   a. Click **System** > **FortiGuard**.

   b. Scroll to the bottom of the page, and then, next to **Filtering Services Availability**, click **Check Again** to force an update.



Filtering

Web Filter Cache ● Clear cache after 60 Minutes

Anti-Spam Cache ● Clear cache after 30 Minutes

FortiGuard Filtering Port 53 8888

Filtering Services Availability ✓ Available

   c. Click **OK** to confirm.

   You should see a confirmation message indicating that the web filtering service is available.

Exercise 1: Configuring Log Settings

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

Configure Log Settings

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

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

- Enabling disk logging, so that logs are stored locally on FortiGate.
- Enabling **Historical FortiView**, so that more than just real-time information is captured in the FortiView dashboards.
- Configuring event logging for all activity, to track and monitor events that occur on FortiGate.
- Disabling **Local Traffic** logging, to prevent filling up your disk too quickly with traffic going directly to and from FortiGate.
- Configuring FortiGate to resolve hostnames, so that FortiGate performs reverse DNS lookups for all the IPs and makes searching logs easier.

Take the Expert Challenge!

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

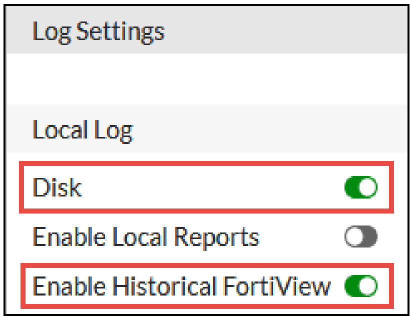
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure Threat Weight on page 94.

To configure the log settings

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Log & Report** > **Log Settings**.
3. In the **Local Log** section, enable the following:

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



Log Settings

Local Log

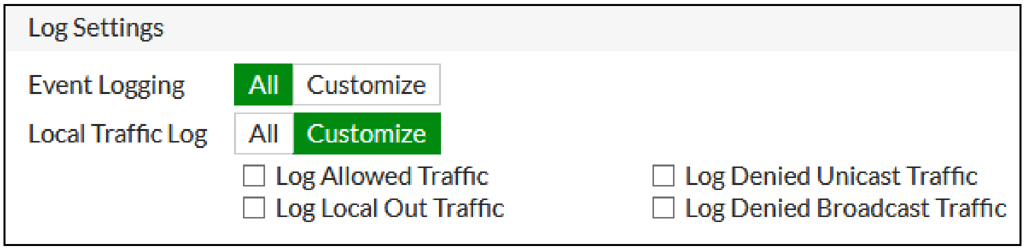
Disk

Enable Local Reports

Enable Historical FortiView

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

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



Log Settings

Event Logging [✓ All] Customize

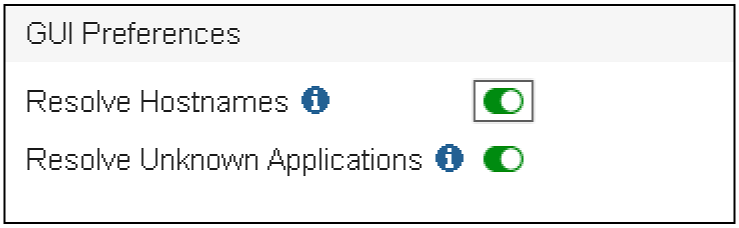
Local Traffic Log All [✓ Customize]

□ Log Allowed Traffic □ Log Denied Unicast Traffic

□ Log Local Out Traffic □ Log Denied Broadcast Traffic

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

Field	Value
Resolve Hostnames	<enable> Resolving hostnames requires FortiGate to perform reverse DNS lookups for all the IPs and makes searching logs easier.



GUI Preferences

Resolve Hostnames

Resolve Unknown Applications

6. Click **Apply**.

Configure Threat Weight

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

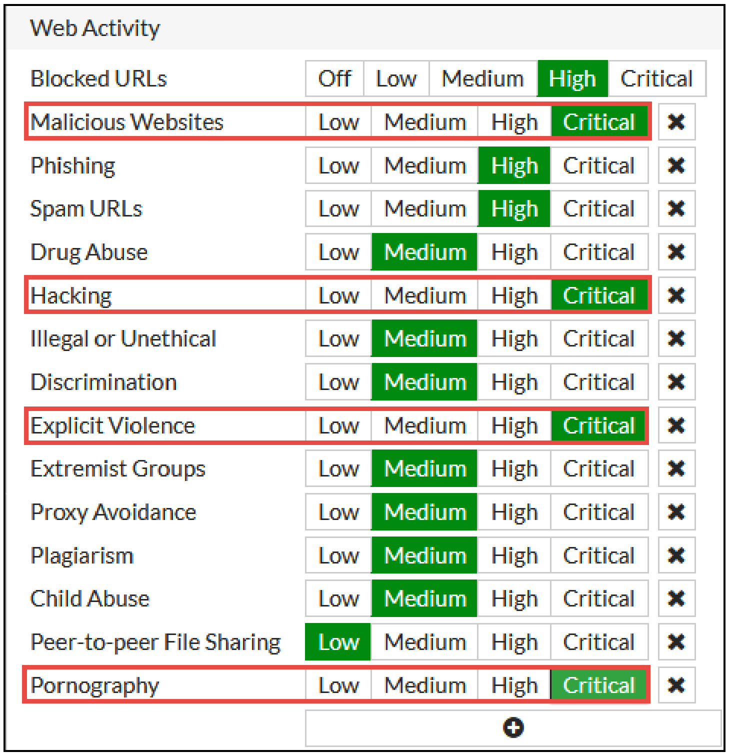
The objective of this task is to set the following categories to critical status:

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

You will use threat weight later when searching for logs at a specific threat weight.

To configure threat weight

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



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

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

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

Risk Level	Value
Critical	

4. Click **Apply**.

Exercise 2: Enabling Logging on Firewall Policies

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

Enable Logging on a Firewall Policy

For the purposes of this lab, two firewall policies have been created for you. However, you will now need to configure these firewall polices for logging.

The two firewall policies are:

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

Take the Expert Challenge!

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

IPS

- IPS | default

Full Access

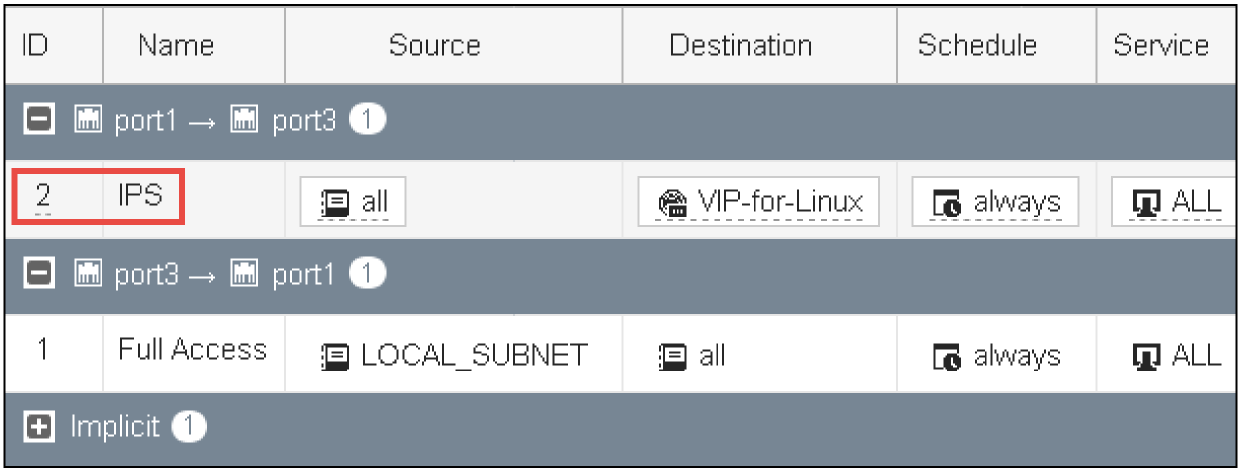
- AntiVirus | default
- Web Filter | Category-block-and-warning
- DNS Filter | default
- Application Control | block-high-risk

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

After you complete the challenge, see Monitoring Logs Through Alert Email on page 98.

To enable logging on the IPS firewall policy

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Policy & Objects** > **IPv4 Policy**, and then edit the **IPS** firewall policy.

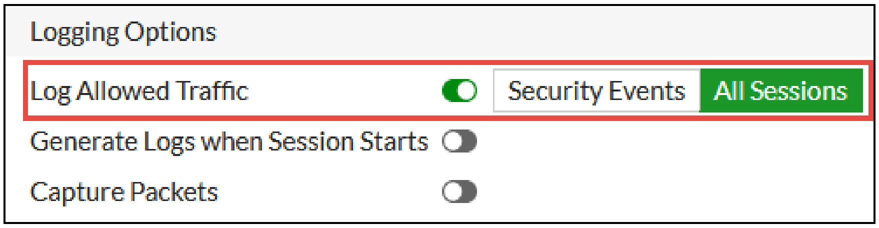


ID	Name	Source	Destination	Schedule	Service
port1 → port3 1					
2	IPS	all	VIP-for-Linux	always	ALL
port3 → port1 1					
1	Full Access	LOCAL_SUBNET	all	always	ALL
Implicit 1					

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

Security Profile	Profile
IPS	default

3. In the **Logging Options** section, enable **Log Allowed Traffic**, and then select **All Sessions**.
Remember, you will not get logs of any kind if **Log Allowed Traffic** is not enabled.



Logging Options

Log Allowed Traffic ● Security Events **All Sessions**

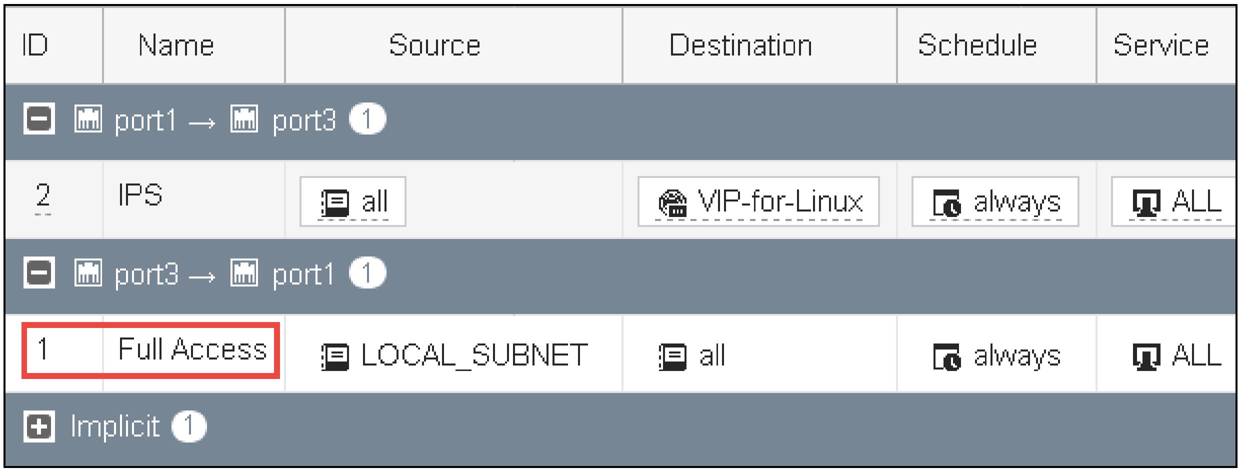
Generate Logs when Session Starts ○

Capture Packets ○

4. Click **OK**.
You've successfully enabled logging on your firewall policy. Later in this lab, you will test these log settings.

To enable logging on the Full Access firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**, and then edit the **Full Access** firewall policy.

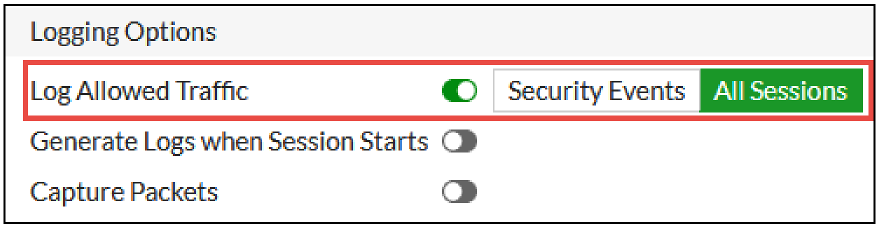


ID	Name	Source	Destination	Schedule	Service
⊟ port1 → port3 1					
2	IPS	all	VIP-for-Linux	always	ALL
⊟ port3 → port1 1					
1	Full Access	LOCAL_SUBNET	all	always	ALL
⊞ Implicit 1					

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

Security Profile	Profile
AntiVirus	default
Web Filter	Category-block-and-warning
DNS Filter	default
Application Control	block-high-risk

3. In the **Logging Options** section, enable **Log Allowed Traffic**, and then select **All Sessions**. Remember, you will not get logs of any kind if **Log Allowed Traffic** is not enabled.



Logging Options

Log Allowed Traffic ● Security Events [✓ All Sessions]

Generate Logs when Session Starts ○

Capture Packets ○

4. Click **OK**.
You've successfully enabled logging on your firewall policy. Later in this lab, you will test these log settings.

Exercise 3: Monitoring Logs Through Alert Email

In this exercise, you will configure alert emails, run some traffic through the Local-FortiGate, and view alert emails.

Configure Alert Emails

Because you can’t always be physically at the FortiGate device, you can monitor events by setting up alert emails. Alert emails provide an efficient and direct method of notifying an administrator of events.

An SMTP mail server is required for alert email to operate. Because configuring a mail server is out of scope for this lab, it has been preconfigured for you. You can view the email service configuration on the Local-FortiGate GUI by clicking **System** > **Advanced**.

To configure email alerts

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Log & Report** > **Email Alert Settings**.
3. Turn on the **Enabled** switch.

   The page loads with configuration options.
4. In the **Email Alert Settings** section, configure the following:

Field	Value
From	FortiGate@training.lab
To	admin@training.lab
Alert parameter	Events
Interval	1

5. In the **Security** section, enable the following:
   - **Intrusion detected**
   - **Web Filter blocked traffic**
6. Click **Apply**.

Generate Traffic

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

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

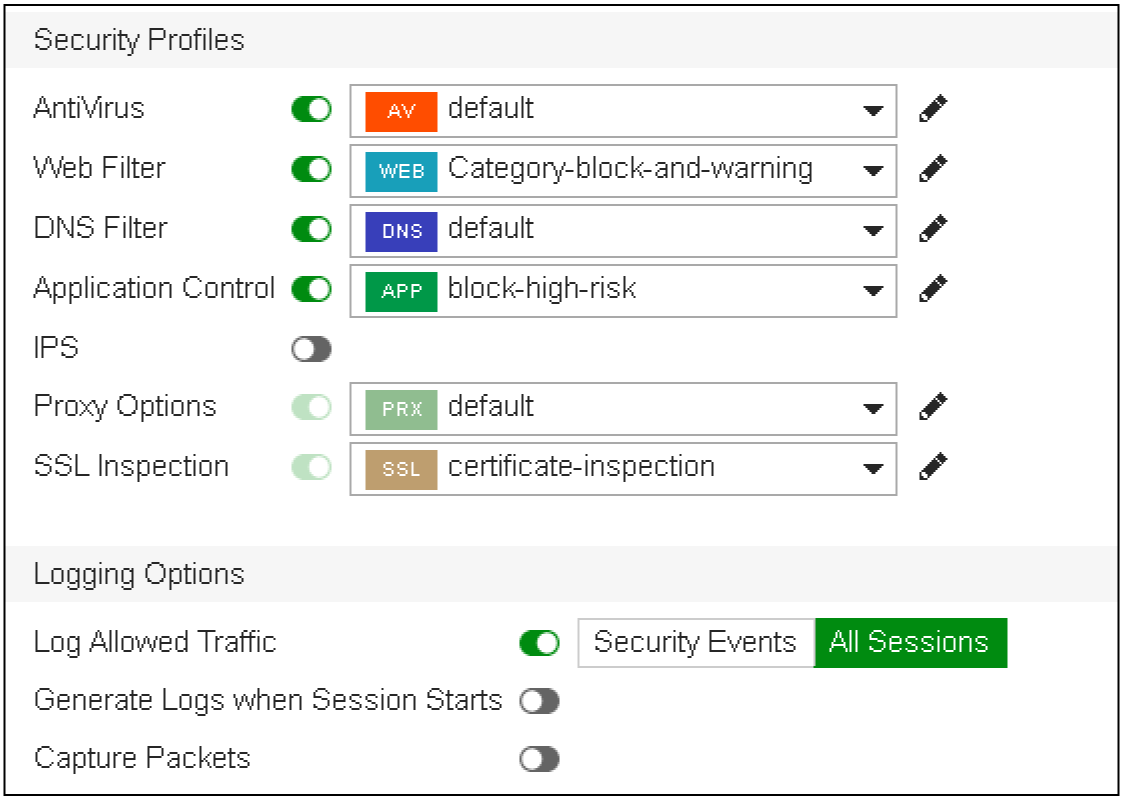
You will use two different tools to create different types of traffic.

Generate Traffic Through FIT

The Firewall Inspection Tester (FIT) program on the FIT VM generates web browsing traffic, application control, botnet IP hits, malware URLs, and malware downloads.

In this lab, you will direct FIT-generated traffic through the Local-FortiGate. The FIT is behind port3 on the Local-FortiGate. The traffic from FIT will go through the **Full Access** firewall policy. For more information, see Network Topology on page 10.

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



Security Profiles

AntiVirus ● AV default

Web Filter ● WEB Category-block-and-warning

DNS Filter ● DNS default

Application Control ● APP block-high-risk

IPS ○

Proxy Options ● PRX default

SSL Inspection ● SSL certificate-inspection

Logging Options

Log Allowed Traffic ● Security Events [✓ All Sessions]

Generate Logs when Session Starts ○

Capture Packets ○

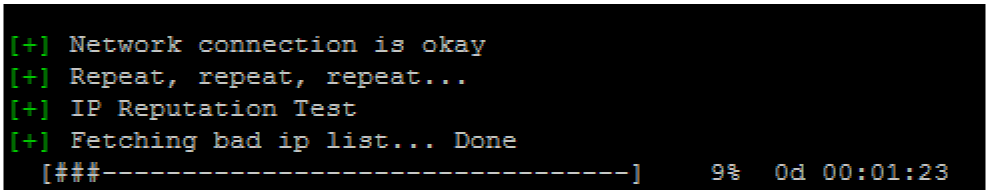
Because FIT-generated traffic will originate from the IP of the FIT VM (`10.0.1.20`), all these logs will show the same source IP in the logs. This is a limitation of the lab environment. In a real-world scenario, you will likely see many different source IPs for your traffic.

To generate traffic through FIT

1. Continuing on the Local-Windows VM, open PuTTY and connect over SSH to the **FIT** saved session.
2. At the login prompt, enter `student` with the password `password`.
3. Type the following commands:

   ```
   cd FIT

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

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

   ```
   [+] Network connection is okay
   [+] Repeat, repeat, repeat...
   [+] IP Reputation Test
   [+] Fetching bad ip list... Done
     [###---------------------------------]     9%   0d 00:01:23
   ```

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

   This will run throughout the remainder of this lab.

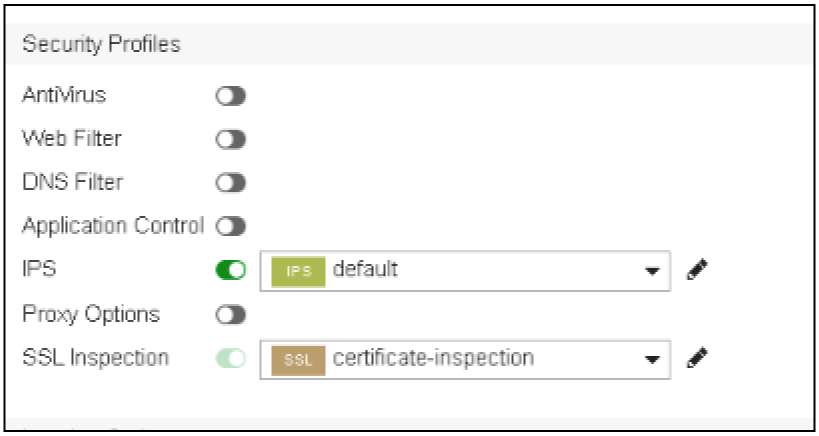
Do not close the FIT PuTTY session or traffic will stop generating.

Generate Traffic Through Nikto

Nikto generates intrusion prevention system (IPS) traffic.

You will direct the Nikto-generated traffic through Local-FortiGate. Nitko is running on the Linux VM, and the traffic will go through the egress to ingress firewall policy named **IPS**. For more information, see Network Topology on page 10.

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



Security Profiles

AntiVirus ○

Web Filter ○

DNS Filter ○

Application Control ○

IPS ● IPS default

Proxy Options ○

SSL Inspection ● SSL certificate-inspection

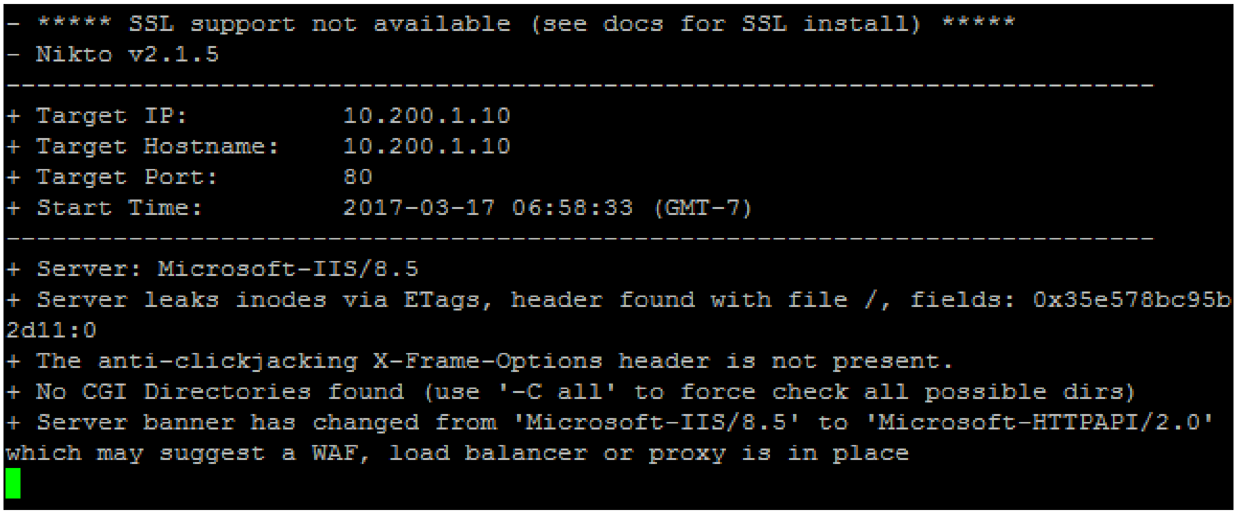
Because Nikto-generated traffic will originate from the IP of the Linux VM where Nikto is installed (`10.200.1.254`), all these logs will show the same source IP in the FortiGate logs. This is a limitation of the lab environment. In a real-world scenario, you will likely see many different source IPs for your traffic.

To generate traffic through Nikto

1. Continuing on the Local-Windows VM, open a second PuTTY application and connect over SSH to the **LINUX** saved session.
2. Log in as `student` with password `password`.
3. Type the following command:

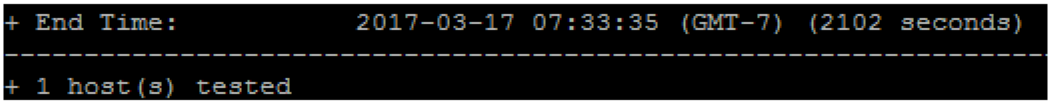
   ```
   nikto.pl -host 10.200.1.10
   ```

   The vulnerability scanning will result in traffic beginning to generate.

   ```
   - ***** SSL support not available (see docs for SSL install) *****
   - Nikto v2.1.5
   ---------------------------------------------------------------------------
   + Target IP:          10.200.1.10
   + Target Hostname:    10.200.1.10
   + Target Port:        80
   + Start Time:         2017-03-17 06:58:33 (GMT-7)
   ---------------------------------------------------------------------------
   + Server: Microsoft-IIS/8.5
   + Server leaks inodes via ETags, header found with file /, fields: 0x35e578bc95b
   2d11:0
   + The anti-clickjacking X-Frame-Options header is not present.
   + No CGI Directories found (use '-C all' to force check all possible dirs)
   + Server banner has changed from 'Microsoft-IIS/8.5' to 'Microsoft-HTTPAPI/2.0'
   which may suggest a WAF, load balancer or proxy is in place
   ```

   The scan will continue for approximately 25 minutes. The dialog displays an **End Time** and indication that **1** host is tested when complete.

   ```
   + End Time:           2017-03-17 07:33:35 (GMT-7) (2102 seconds)
   ---------------------------------------------------------------------
   + 1 host(s) tested
   ```

   You can run the command again after the scan completes (press the up arrow and then press Enter) to generate more logs, but it's not required. One cycle will provide enough logs for the purposes of this lab.

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

   This will run for the remainder of the lab.

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

View Alert Emails

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

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

To view your alert emails

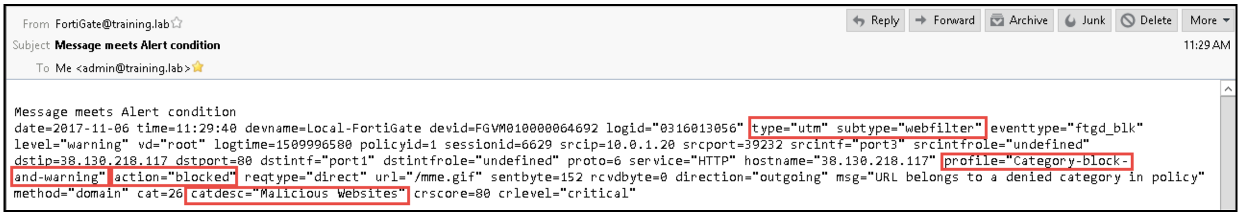
1. Continuing on Local-Windows, on the desktop, open Mozilla Thunderbird.

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

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

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

   As you can see, the log message is in raw format. In the web filter example below (you may receive a different log message), the log message header provides the `type` (utm) and `subtype` (webfilter). The log message body provides information about the web filter security profile that was applied to the traffic (Category_block-and-warning), the action it took (blocked), and the category description of the traffic (Malicious Websites).



From FortiGate@training.lab
Subject **Message meets Alert condition**
To Me <admin@training.lab>
11:29 AM

```
Message meets Alert condition
date=2017-11-06 time=11:29:40 devname=Local-FortiGate devid=FGVM010000064692 logid="0316013056" type="utm" subtype="webfilter" eventtype="ftgd_blk"
level="warning" vd="root" logtime=1509996580 policyid=1 sessionid=6629 srcip=10.0.1.20 srcport=39232 srcintf="port3" srcintfrole="undefined"
dstip=38.130.218.117 dstport=80 dstintf="port1" dstintfrole="undefined" proto=6 service="HTTP" hostname="38.130.218.117" profile="Category-block-
and-warning" action="blocked" reqtype="direct" url="/mme.gif" sentbyte=152 rcvdbyte=0 direction="outgoing" msg="URL belongs to a denied category in policy"
method="domain" cat=26 catdesc="Malicious Websites" crscore=80 crlevel="critical"
```

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

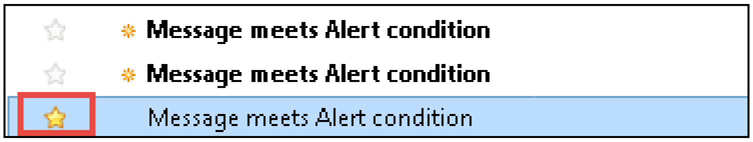
Field	Value
date	
time	
logid	
subtype	
level	

Field	Value
sessionid	
profile	
catdesc	
crscore	

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

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

   The star icon turns yellow.



Message meets Alert condition
Message meets Alert condition
Message meets Alert condition

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

6. Close the Thunderbird email client when you are finished.

Exercise 4: Viewing Logs on the FortiGate GUI

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

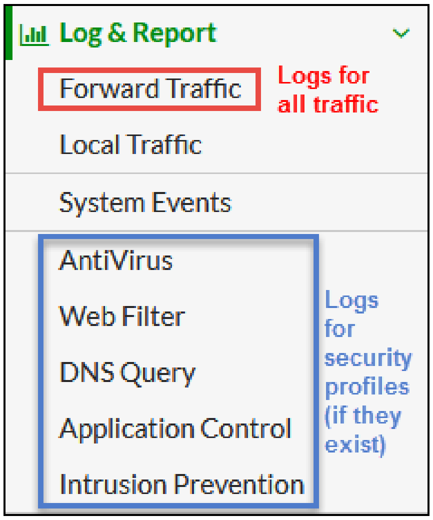
View Logs from Log & Report

In this exercise, you will examine the logs on the Local-FortiGate GUI, based on the traffic you generated from the FIT VM and Nikto.

Forward Traffic

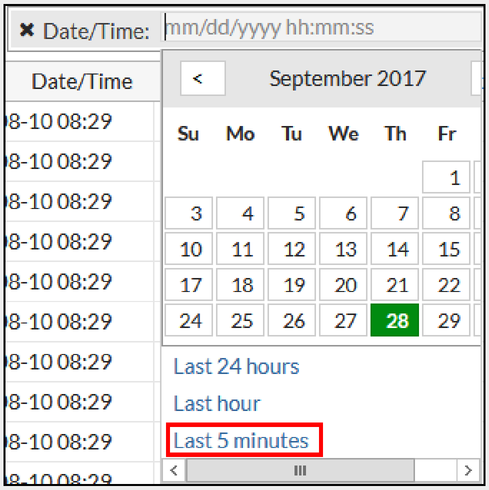
The first place you will examine logs is on the **Forward Traffic** page.

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



To view and filter forward traffic logs

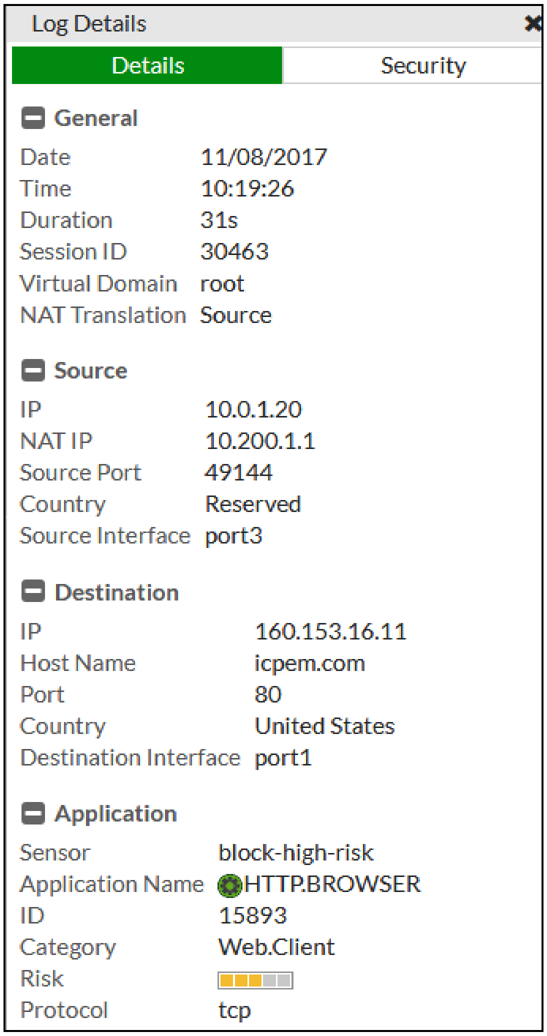
1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Log & Report** > **Forward Traffic**.
3. To narrow down the logs (results), on the search bar, click **Add Filter**, and then add some filters. For example:

Filter	Value
Date/Time	Last 5 Minutes This filters on all logs from the last 5 minutes.  ✖ Date/Time: mm/dd/yyyy hh:mm:ss Date/Time 8-10 08:29 September 2017 Su Mo Tu We Th Fr Last 24 hours Last hour Last 5 minutes
Result	Deny (all) This filters on all blocked traffic.
Threat Score	>=50 This filters on all Web activity greater than or equal to the Critical (50) risk level. Remember, you set Malicious Websites, Hacking, Explicit Violence, and Pornography to the critical risk level.

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

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

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



General

Date	11/08/2017
Time	10:19:26
Duration	31s
Session ID	30463
Virtual Domain	root
NAT Translation	Source

Source

IP	10.0.1.20
NAT IP	10.200.1.1
Source Port	49144
Country	Reserved
Source Interface	port3

Destination

IP	160.153.16.11
Host Name	icpem.com
Port	80
Country	United States
Destination Interface	port1

Application

Sensor	block-high-risk
Application Name	HTTP.BROWSER
ID	15893
Category	Web.Client
Risk	🟨🟨🟨⬜⬜
Protocol	tcp

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

Security Profile Logs

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

To view web filter logs

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

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

2. Locate the log in the alert email that you recorded in To view your alert emails on page 102 by using log filters.

Stop and think!

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

Answer: **Log original timestamp** or **Session ID**.

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

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

View and Filter IPS Logs

In this exercise, you will view and filter IPS logs.

Take the Expert Challenge!

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

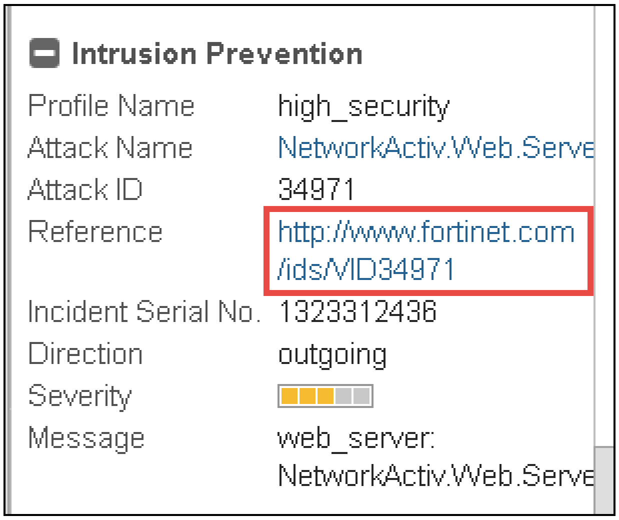
- View the GUI page that shows intrusion prevention logs only.
- Filter for a log with the attack name **NetworkActiv.Web.Server.XSS**.
- View information about the attack on FortiGuard.

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

After you complete the challenge, see View Logs in FortiView on page 108.

To view and filter IPS logs

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



Intrusion Prevention

Profile Name	high_security
Attack Name	NetworkActiv.Web.Serve
Attack ID	34971
Reference	http://www.fortinet.com /ids/VID34971
Incident Serial No.	1323312436
Direction	outgoing
Severity	🟨🟨🟨⬜⬜
Message	web_server: NetworkActiv.Web.Serve

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

4. After you finish, close the FortiGuard tab.

View Logs in FortiView

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

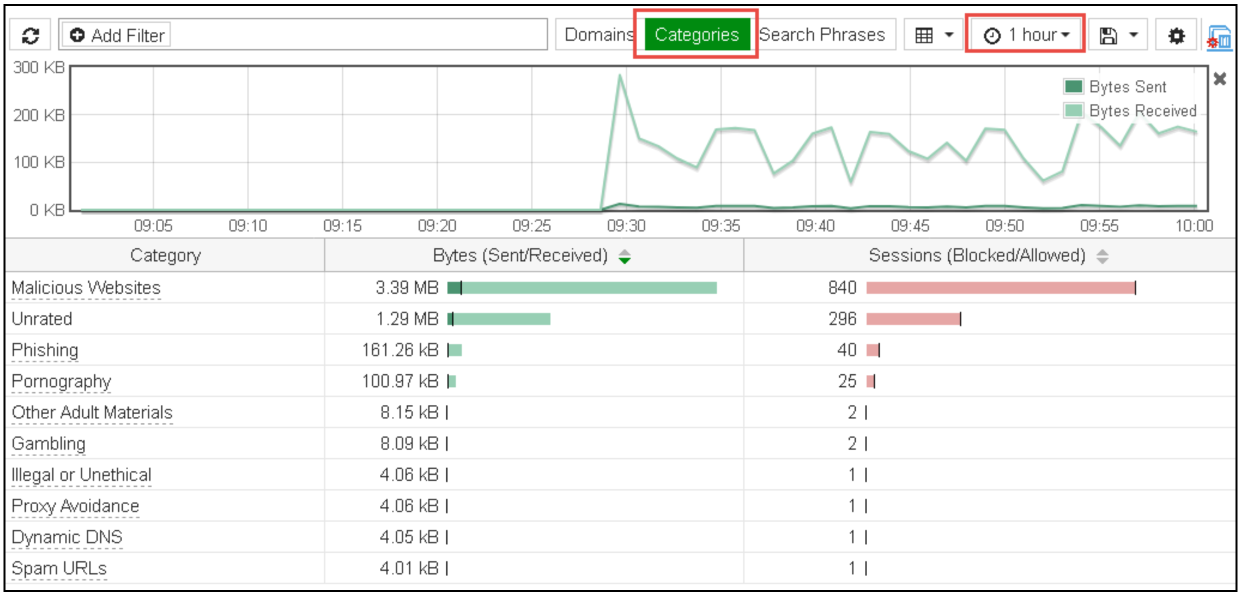
Now, you will view your logs in FortiView.

To view logs in FortiView

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

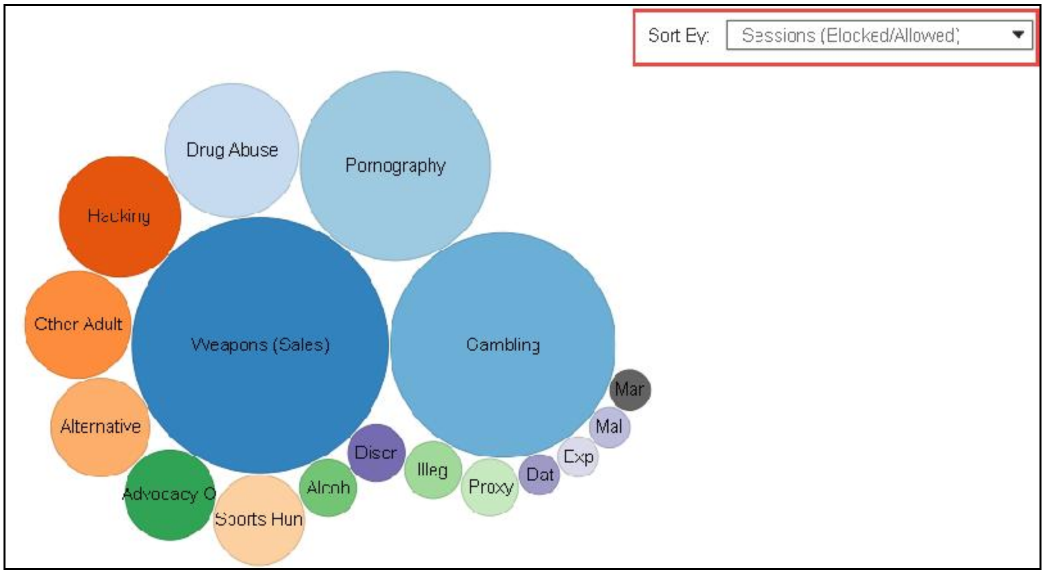
   By default, the search settings are set to display logs being created **now**. If no logs are being created currently, the page will be blank. This is expected.

2. Use the search settings to display the Web activity in a different way. For example:
   - Select **Categories** and **1 hour** to see the Web categories most accessed in the last hour.



Category	Bytes (Sent/Received)	Sessions (Blocked/Allowed)
Malicious Websites	3.39 MB	840
Unrated	1.29 MB	296
Phishing	161.26 kB	40
Pornography	100.97 kB	25
Other Adult Materials	8.15 kB	2
Gambling	8.09 kB	2
Illegal or Unethical	4.06 kB	1
Proxy Avoidance	4.06 kB	1
Dynamic DNS	4.05 kB	1
Spam URLs	4.01 kB	1

- Click the table icon (▦ ▾), and then select **Bubble Chart**.
- Use the **Sort By** drop-down menu to display the information by **Threat Score**, **Sessions**, **Browsing Time** or **Bytes**.


Sort By: Sessions (Blocked/Allowed)

3. Click **FortiView** > **Threats**.
4. Use the filters and sort options to examine different ways you can view the threats to the network.

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

Lab 6: Certificate Operations

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

Objectives

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

Time to Complete

Estimated: 40 minutes

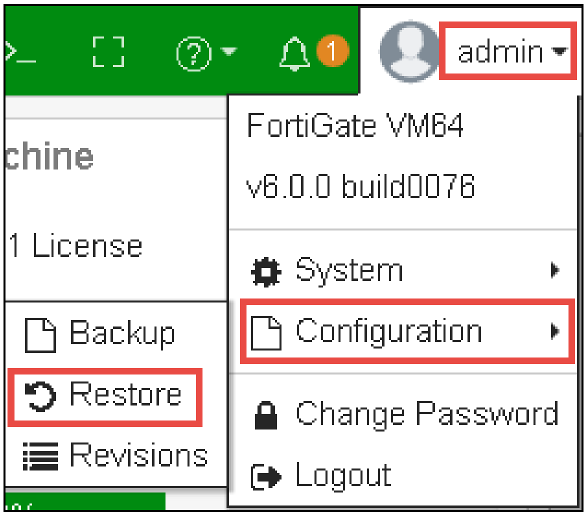
Prerequisites

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

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

To restore the Remote-FortiGate configuration file

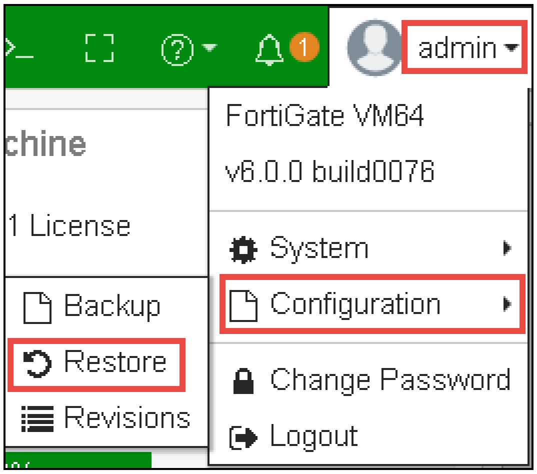
1. On the Local-Windows VM, open a browser and log in to the Remote-FortiGate GUI at `10.200.3.1` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **Certificate-Operations** > `remote-certificate-operations.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **Certificate-Operations** > `local-certificate-operations.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring SSL Deep Inspection on Outbound Traffic

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

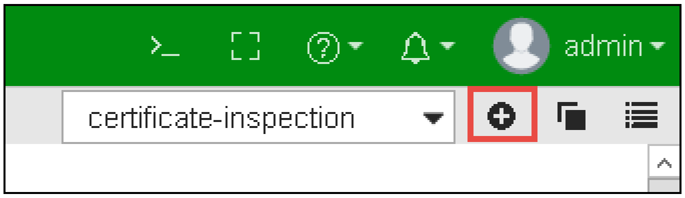
In this exercise, you will configure and enable SSL inspection on all outbound traffic.

Configure SSL Inspection

By default, FortiGate includes two security profiles for SSL/SSH inspection: **certificate-inspection** and **deep-inspection**, which you cannot modify. Because this exercise involves configuring FortiGate for SSL full inspection, you will configure a new SSL/SSH inspection profile for full SSL inspection.

To configure SSL inspection

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Security Profiles** > **SSL/SSH Inspection**.
3. In the upper-right corner, click the plus (+) icon to create a new profile.



4. In the **Name** field, type `Custom_Full_Inspection`.
5. At the bottom of the page, in the **Common Options** section, enable **Allow Invalid SSL Certificates**.
6. Click **OK**.

Enable SSL Inspection on a Firewall Policy

You must enable SSL inspection on a firewall policy to start inspecting traffic. However, you cannot enable SSL inspection by itself. The firewall policy must have one or more other security profiles enabled, because enabling SSL inspection tells FortiGate only how to handle encrypted traffic—you still need to tell FortiGate which traffic to inspect. For the purposes of this lab, you will enable the default web filter security profile.

To enable SSL inspection on a firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Double-click the **Full_Access** firewall policy to edit it.

3. In the **Security Profiles** section, enable the following security profiles:

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

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

Install the Fortinet_CA_SSL Certificate

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

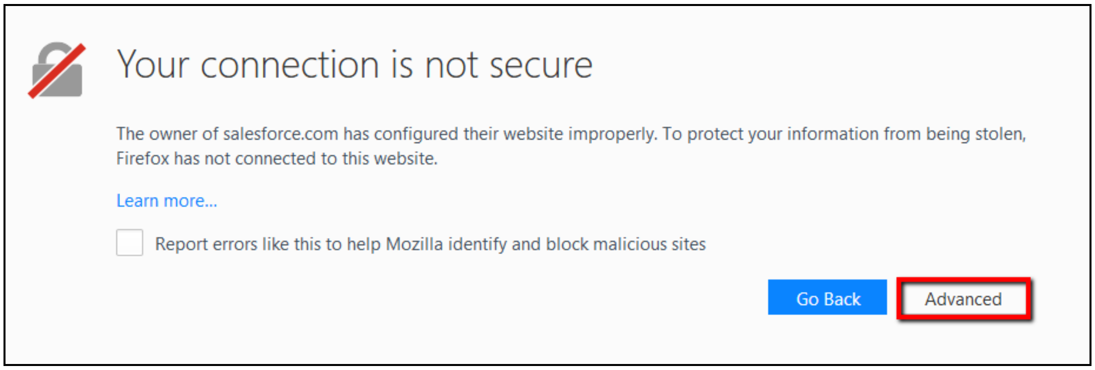
In this procedure, you will first test access to an HTTPS site *without* the Fortinet_CA_SSL certificate installed. Then, you will install the Fortinet_CA_SSL certificate and test again.

To test SSL deep inspection without a trusted CA

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

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

2. Click **Advanced**.
Notice the certificate warning. This appears because the browser is receiving certificates signed by the FortiGate CA's private key, and the corresponding CA certificate is not in the Local-Windows certificate store.



Your connection is not secure

The owner of salesforce.com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

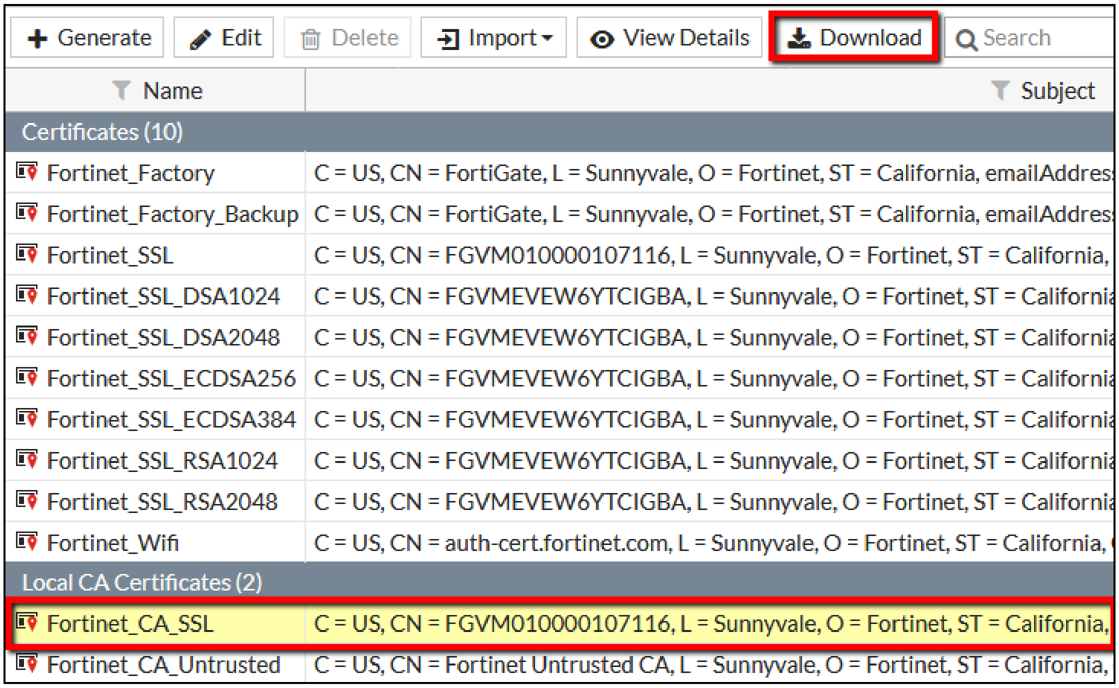
Learn more...

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

3. Leave the browser tab open and continue to the next procedure. *Do not add the exception.*

To install the Fortinet_CA_SSL certificate in the browser

1. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and click **System** > **Certificates**.
2. In the **Local CA Certificates** section, click **Fortinet_CA_SSL**, and then click **Download**.

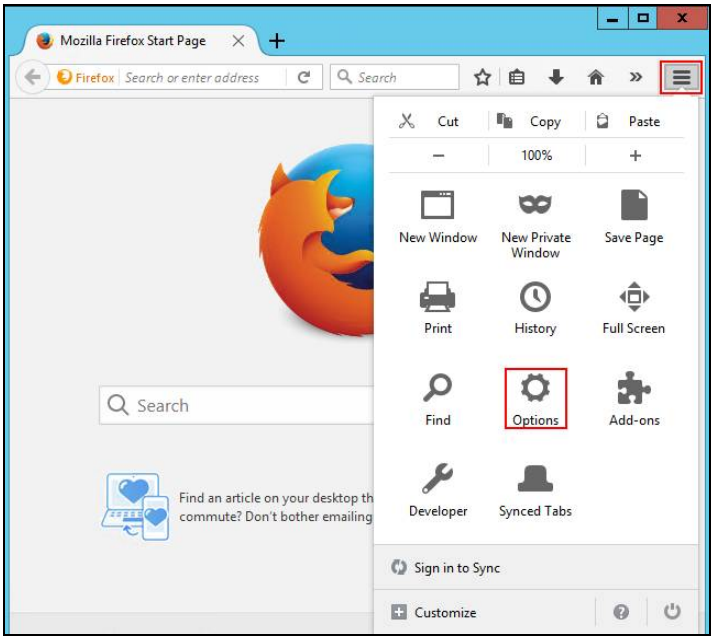


Name	Subject
Certificates (10)	
Fortinet_Factory	C = US, CN = FortiGate, L = Sunnyvale, O = Fortinet, ST = California, emailAddres
Fortinet_Factory_Backup	C = US, CN = FortiGate, L = Sunnyvale, O = Fortinet, ST = California, emailAddres
Fortinet_SSL	C = US, CN = FGVM010000107116, L = Sunnyvale, O = Fortinet, ST = California,
Fortinet_SSL_DSA1024	C = US, CN = FGVMEVEW6YTCIGBA, L = Sunnyvale, O = Fortinet, ST = Californi
Fortinet_SSL_DSA2048	C = US, CN = FGVMEVEW6YTCIGBA, L = Sunnyvale, O = Fortinet, ST = Californi
Fortinet_SSL_ECDSA256	C = US, CN = FGVMEVEW6YTCIGBA, L = Sunnyvale, O = Fortinet, ST = Californi
Fortinet_SSL_ECDSA384	C = US, CN = FGVMEVEW6YTCIGBA, L = Sunnyvale, O = Fortinet, ST = Californi
Fortinet_SSL_RSA1024	C = US, CN = FGVMEVEW6YTCIGBA, L = Sunnyvale, O = Fortinet, ST = Californi
Fortinet_SSL_RSA2048	C = US, CN = FGVMEVEW6YTCIGBA, L = Sunnyvale, O = Fortinet, ST = Californi
Fortinet_Wifi	C = US, CN = auth-cert.fortinet.com, L = Sunnyvale, O = Fortinet, ST = California,
Local CA Certificates (2)	
Fortinet_CA_SSL	C = US, CN = FGVM010000107116, L = Sunnyvale, O = Fortinet, ST = California,
Fortinet_CA_Untrusted	C = US, CN = Fortinet Untrusted CA, L = Sunnyvale, O = Fortinet, ST = California,

3. Click **Save File**.

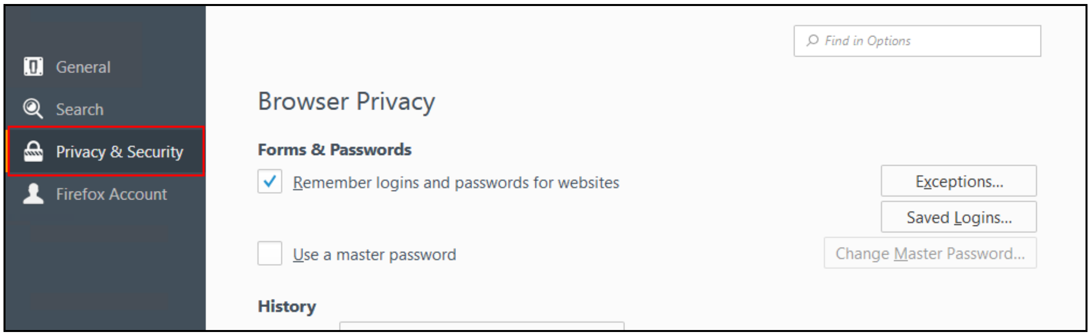
   The certificate downloads to your **Downloads** folder.

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



Find an article on your desktop th commute? Don't bother emailing

5. Click **Privacy & Security**.



Browser Privacy

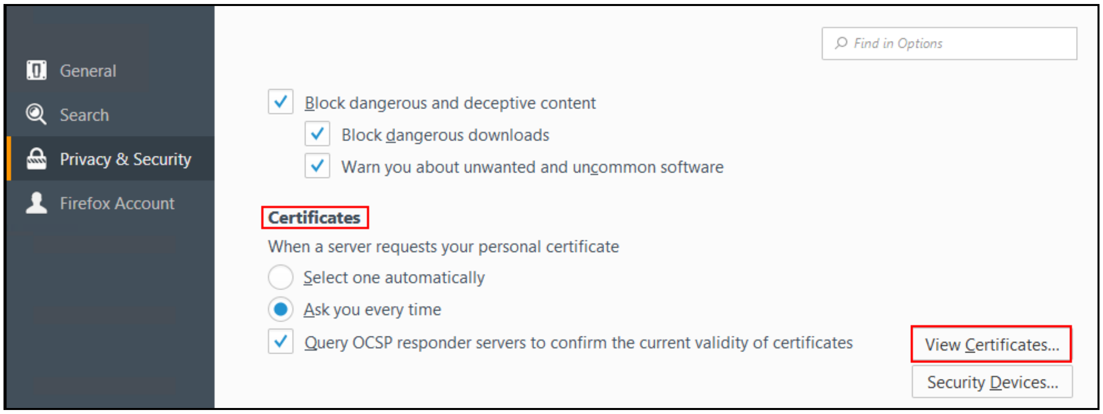
Forms & Passwords

☑ Remember logins and passwords for websites

□ Use a master password

History

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



☑ Block dangerous and deceptive content

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

Certificates

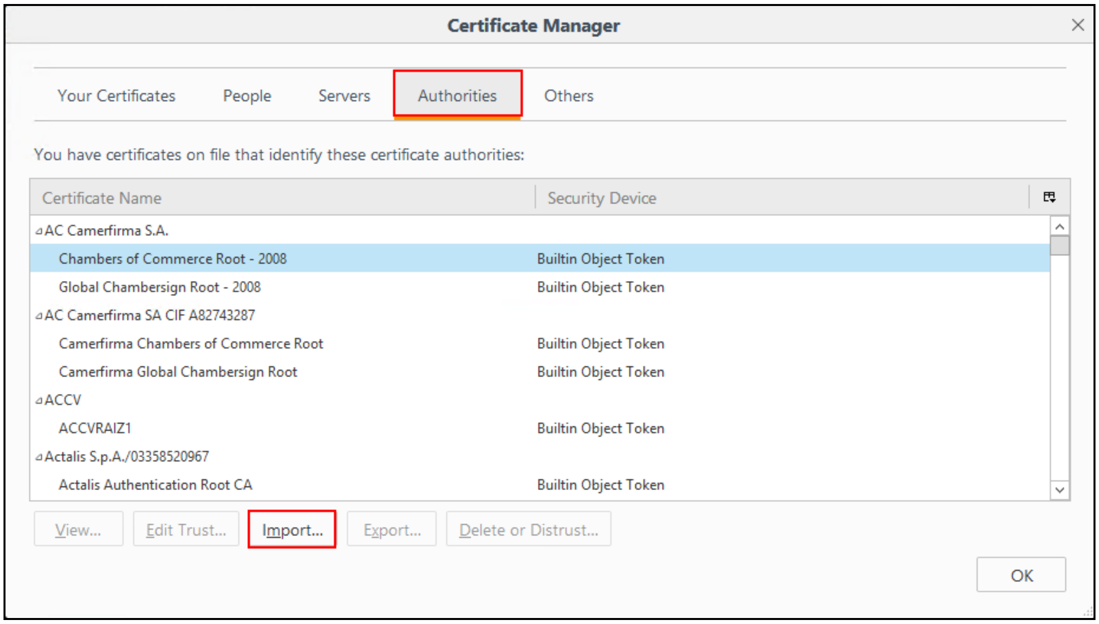
When a server requests your personal certificate

○ Select one automatically

● Ask you every time

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

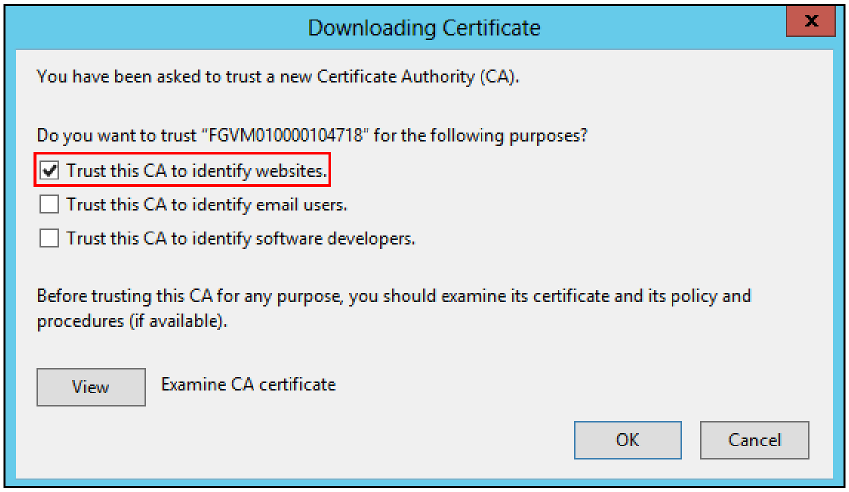
7. In the **Certificate Manager** window, click the **Authorities** tab, and then click **Import**.



You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
⊿AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
⊿AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
⊿ACCV	
ACCVRAIZ1	Builtin Object Token
⊿Actalis S.p.A./03358520967	
Actalis Authentication Root CA	Builtin Object Token

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



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

Do you want to trust "FGVM010000104718" for the following purposes?

☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

□ Trust this CA to identify software developers.

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

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

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

Test Full SSL Inspection

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

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

To test SSL full inspection

1. Continuing on the Local-Windows VM, open a new browser and go to a secure site, such as:

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

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

2. Close the browser.

Exercise 2: Configuring SSL Deep Inspection on Inbound Traffic

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

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

Configure a Virtual IP and Firewall Policy

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

Take the Expert Challenge!

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

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

After you complete the challenge, see Install the Training CA Certificate on page 118.

To configure a virtual IP

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Policy & Objects** > **Virtual IPs**.
3. Click **Create New**, and select **Virtual IP**.
4. Configure the following settings:

Field	Value
Name	VIP-WEB-SERVER
Interface	port1

Field	Value
External IP Address/Range	10.200.1.200
Mapped IP Address/Range	10.0.1.10

5. Click **OK**.

To configure a firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Click **Create New**, and then create a new firewall policy using the following settings:

Field	Value
Name	Web_Server_Access
Incoming Interface	port1
Outgoing Interface	port3
Source	all
Destination	VIP-WEB-SERVER
Schedule	always
Service	ALL
Action	ACCEPT
NAT	<disable>

3. Click **OK**.

Install the Training CA Certificate

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

Take the Expert Challenge!

- On the Remote-Windows VM, verify that you have access to the web server using `https://10.200.1.200`.
- Using Firefox, review the web server certificate details and identify the certificate issuer.
- Install the Training CA certificate in Firefox's **Authorities** certificate store. The certificate file is located on **Desktop** > **Resources** > **FortiGate-Security** > `Training.crt`.
- Make sure certificate-related warning messages no longer appear before proceeding to the next section.

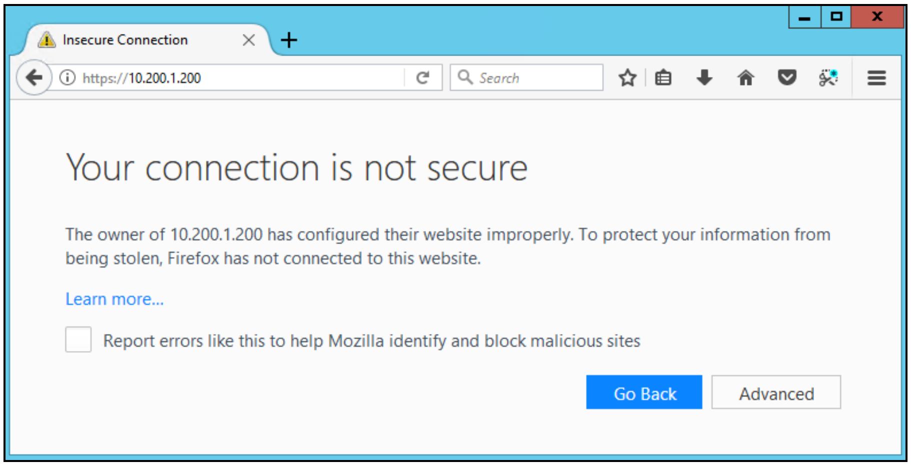
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Configure Inbound SSL Deep Inspection on page 123.

To verify access

1. On the virtual lab portal, click the Remote-Windows VM.
2. Open Firefox and access the web server using `https://10.200.1.200`.

   A security warning opens.



Your connection is not secure

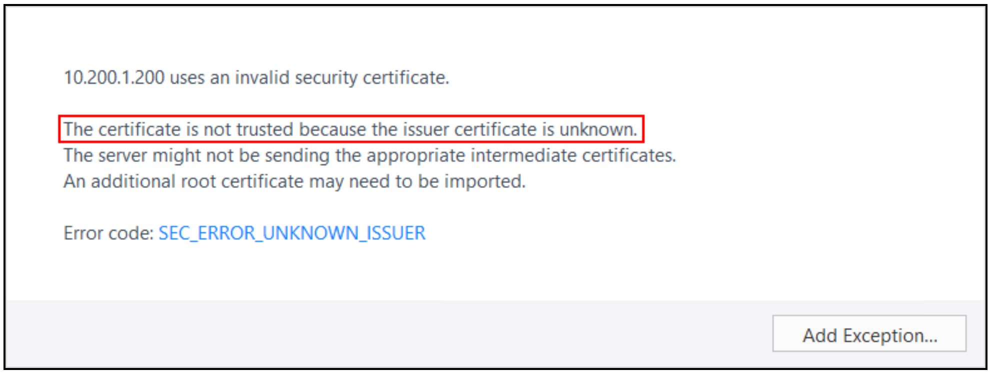
The owner of 10.200.1.200 has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more...

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

Go Back Advanced

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



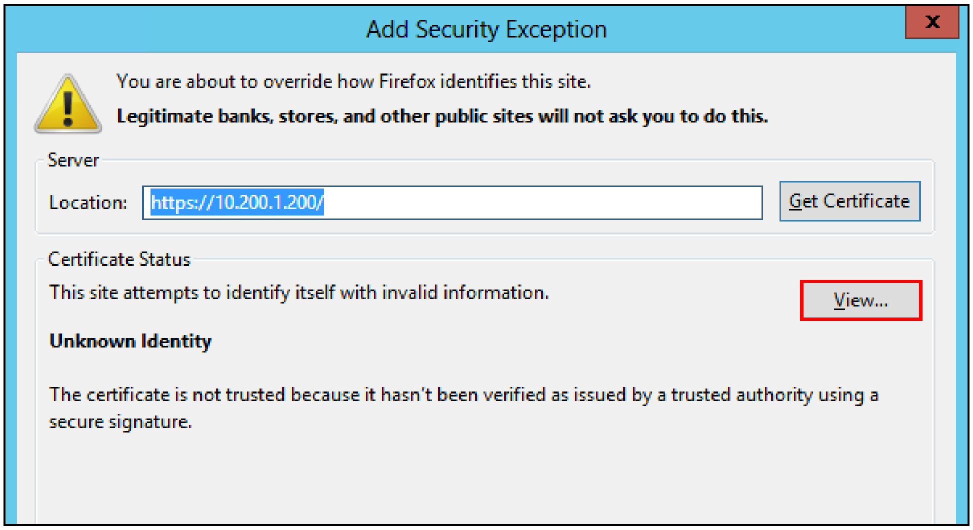
10.200.1.200 uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.

Error code: SEC_ERROR_UNKNOWN_ISSUER

Add Exception...

4. Click **Add Exception**.
5. Click **View**.



You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://10.200.1.200/

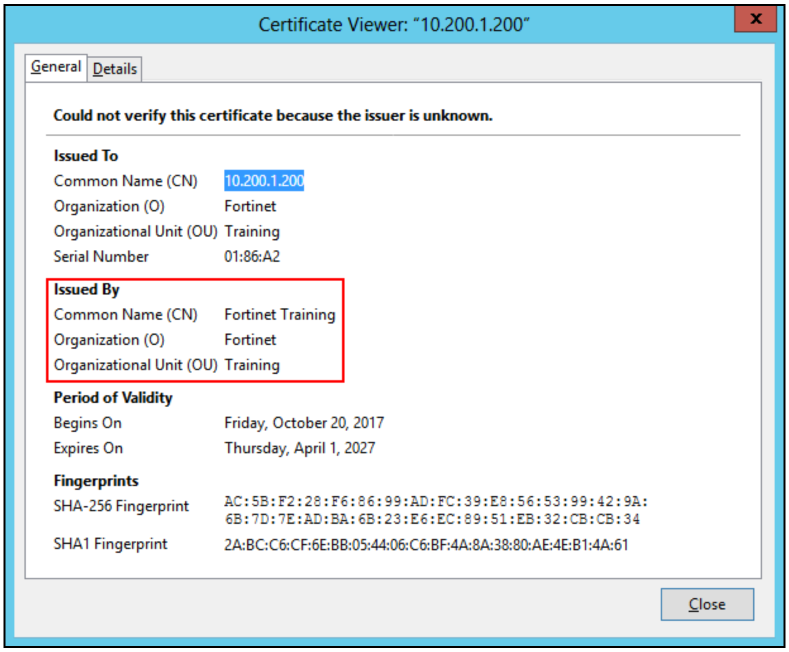
Certificate Status

This site attempts to identify itself with invalid information.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

6. In the **Issued By** section, review the information.



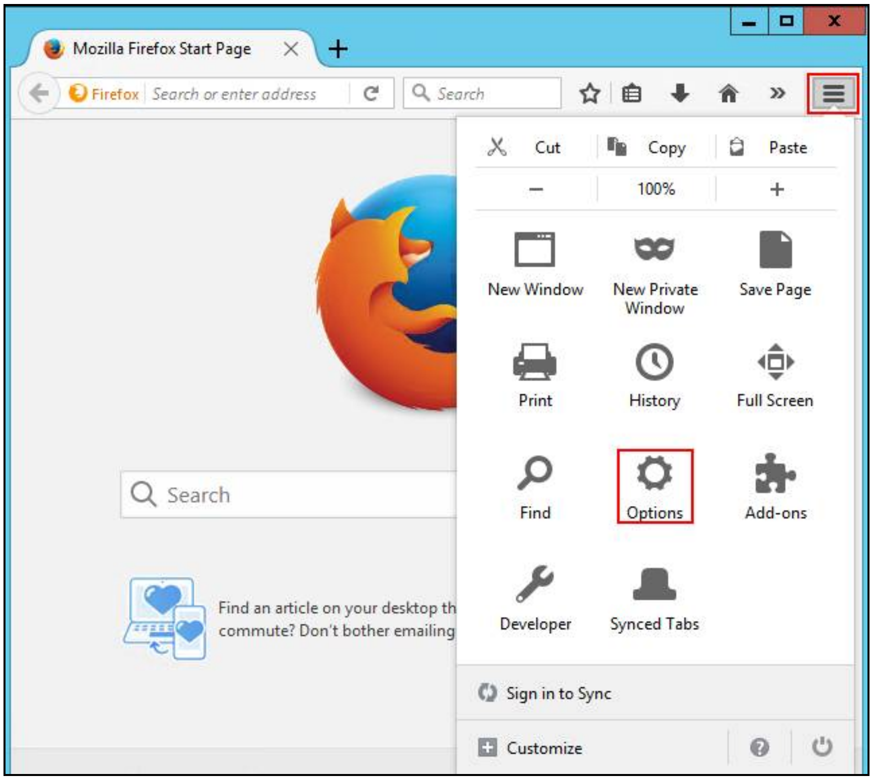
Could not verify this certificate because the issuer is unknown.

Issued To	
Common Name (CN)	10.200.1.200
Organization (O)	Fortinet
Organizational Unit (OU)	Training
Serial Number	01:86:A2
Issued By	
Common Name (CN)	Fortinet Training
Organization (O)	Fortinet
Organizational Unit (OU)	Training
Period of Validity	
Begins On	Friday, October 20, 2017
Expires On	Thursday, April 1, 2027
Fingerprints	
SHA-256 Fingerprint	AC:5B:F2:28:F6:86:99:AD:FC:39:E8:56:53:99:42:9A: 6B:7D:7E:AD:BA:6B:23:E6:EC:89:51:EB:32:CB:CB:34
SHA1 Fingerprint	2A:BC:C6:CF:6E:BB:05:44:06:C6:BF:4A:8A:38:80:AE:4E:B1:4A:61

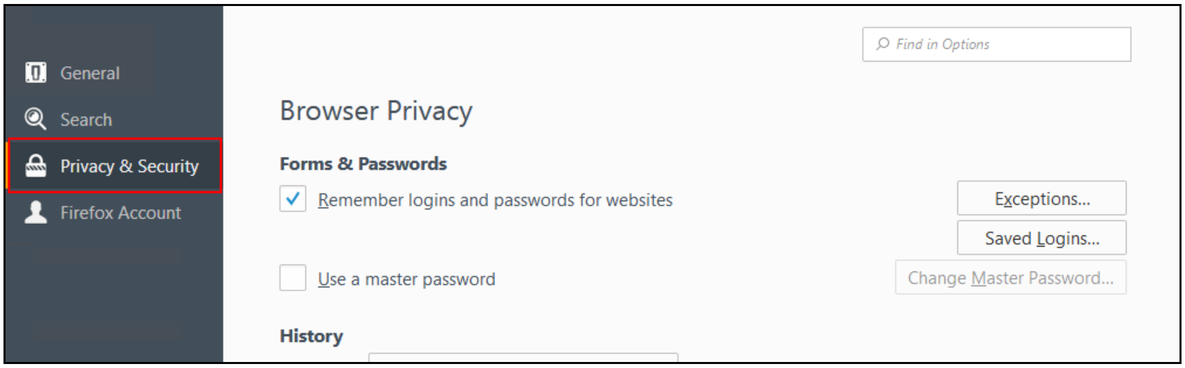
7. Click **Close**.
8. Click **Cancel**.

To install the Training CA certificate

1. Continuing on the Remote-Windows VM, in the upper-right corner of theFirefox browser, click the **Open menu** icon, and then select **Options**.



2. Click **Privacy & Security**.



Browser Privacy

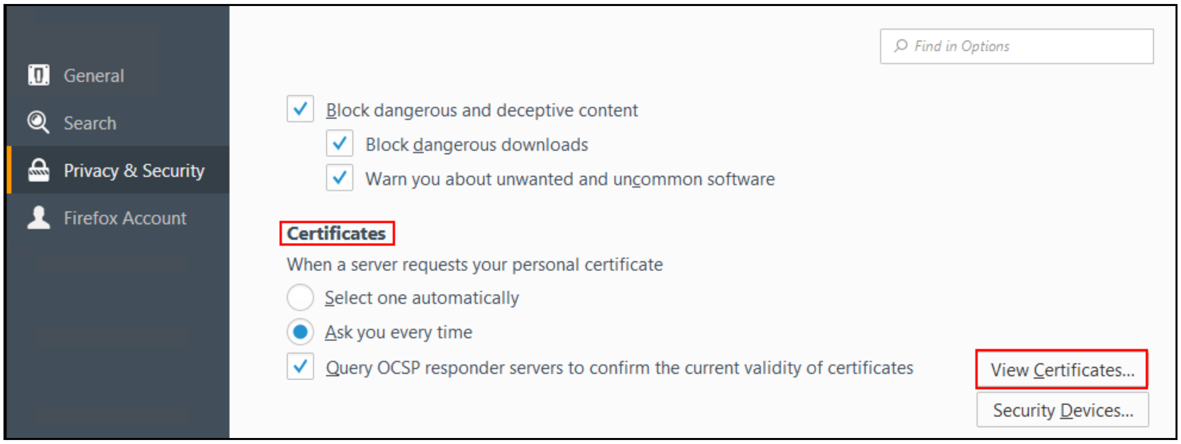
Forms & Passwords

☑ Remember logins and passwords for websites

□ Use a master password

History

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



☑ Block dangerous and deceptive content

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

Certificates

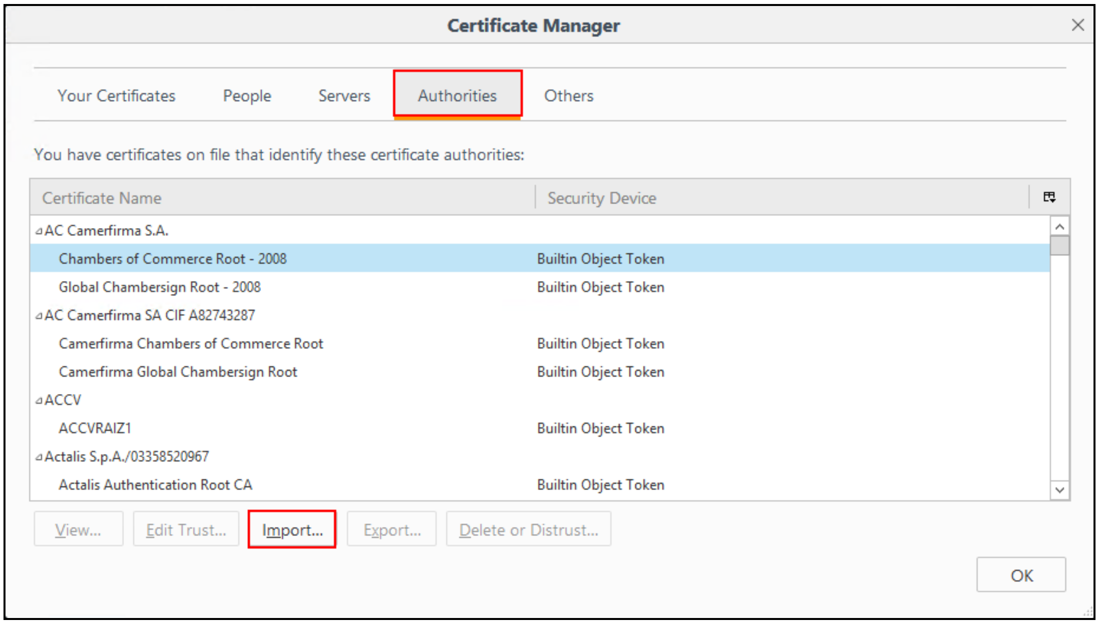
When a server requests your personal certificate

○ Select one automatically

● Ask you every time

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

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



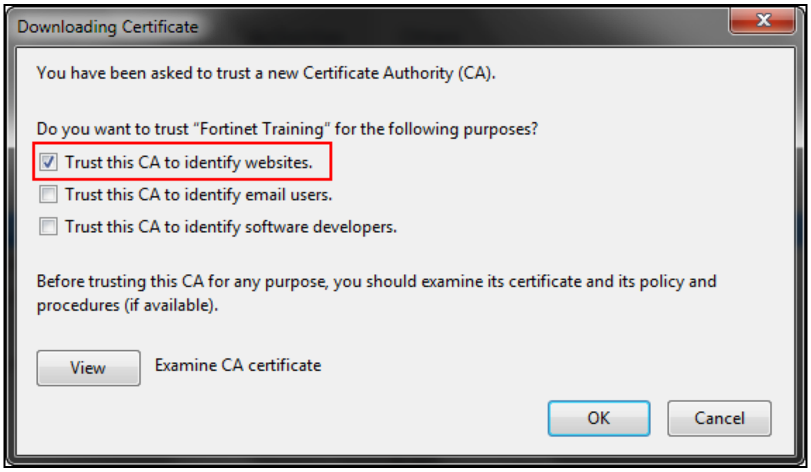
You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
⊿AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
⊿AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
⊿ACCV	
ACCVRAIZ1	Builtin Object Token
⊿Actalis S.p.A./03358520967	
Actalis Authentication Root CA	Builtin Object Token

5. Click **Desktop** > **Resources** > **FortiGate-Security** > **Certificate-Operations** > **Training.crt**, and then click **Open**.

   The **Downloading Certificate** window opens.

6. Click **Trust this CA to identify websites**.



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

Do you want to trust "Fortinet Training" for the following purposes?

☑ Trust this CA to identify websites.

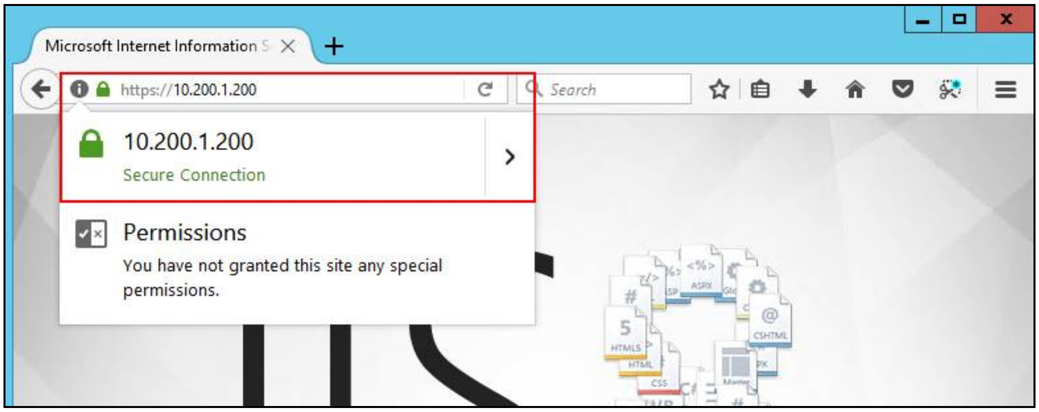
□ Trust this CA to identify email users.

□ Trust this CA to identify software developers.

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

Examine CA certificate

7. Click **OK**.
8. Click **OK**.
9. Restart Firefox.
10. Go to `https://10.200.1.200`, and then verify that the security warning is no longer displayed.


Microsoft Internet Information S
https://10.200.1.200
Search
10.200.1.200
Secure Connection
Permissions
You have not granted this site any special permissions.

Configure Inbound SSL Deep Inspection

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

To configure inbound SSL deep inspection

1. Return to the Local-Windows VM, and on the Local-Fortigate GUI, click **Security Profiles** > **SSL/SSH Inspection**.
2. In the upper-right corner, click the plus (**+**) icon to create a new profile.
3. Configure the following settings:

Field	Value
Name	Inbound_SSL_Inspection
Enable SSL Inspection of	Protecting SSL Server
Server Certificate	Fortinet_SSL

4. Click **OK**.
5. Click **Policy & Objects** > **IPv4 Policy**.
6. Edit the **Web_Server_Access** policy.
7. In the **Security Profiles** section, enable the following security profiles:

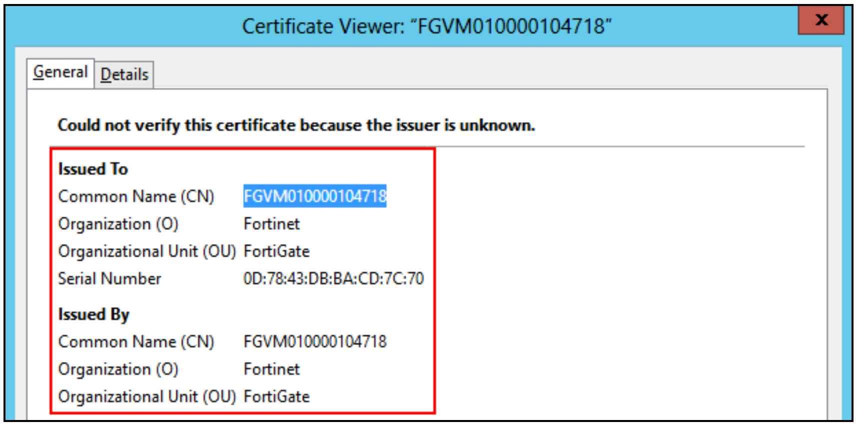
Security Profile	Value
AntiVirus	default
SSL/SSH Inspection	Inbound_SSL_Inspection

8. Click **OK**.

To verify inbound SSL deep inspection

1. Return to the Remote-Windows VM, and close any existing instances of Firefox.
2. Open Firefox again, and go to `https://10.200.1.200`.

   A security warning opens. If you do not receive a security warning, refresh the page (F5). This forces Firefox to update its local cache.
3. Click **Advanced**, and review the error message.
4. Click **Add Exception**.
5. Click **View**.
6. Review the certificate information.



Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	FGVM010000104718
Organization (O)	Fortinet
Organizational Unit (OU)	FortiGate
Serial Number	0D:78:43:DB:BA:CD:7C:70

Issued By

Common Name (CN)	FGVM010000104718
Organization (O)	Fortinet
Organizational Unit (OU)	FortiGate

Stop and think!

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

7. Click **Close**.
8. Click **Cancel**.

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

1. Return to the Local-Windows VM.
2. On the Local-FortiGate GUI, click **System** > **Certificates**.
3. Click **Import**, and then select **Local Certificate**.
4. In the **Type** drop-down list, select **PKCS # 12 Certificate**.
5. Click **Upload**.
6. Click **Desktop** > **Resources** > **FortiGate-Security** > **Certificate-Operations** > **webserver.p12**, and then click **Open**.

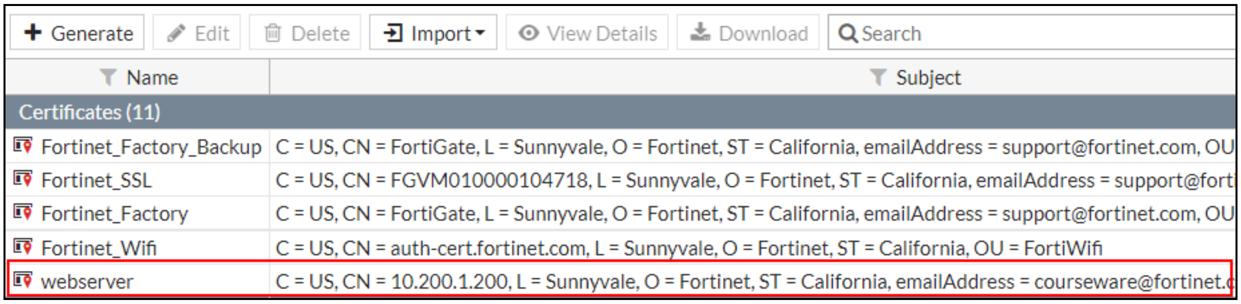
   The **Certificate Name** field is auto-populated from the certificate file name.

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

The `webserver.p12` file contains the web server's certificate and private key.

7. In the **Password** field, enter `fortinet`.
8. Click **OK**.

   The certificate and key are imported.



Name	Subject
Certificates (11)	
Fortinet_Factory_Backup	C = US, CN = FortiGate, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU
Fortinet_SSL	C = US, CN = FGVM010000104718, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fort
Fortinet_Factory	C = US, CN = FortiGate, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU
Fortinet_Wifi	C = US, CN = auth-cert.fortinet.com, L = Sunnyvale, O = Fortinet, ST = California, OU = FortiWifi
webserver	C = US, CN = 10.200.1.200, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = courseware@fortinet.c

To modify the inbound SSL inspection profile

1. Continuing on the Local-FortiGate GUI, click **Security Profiles** > **SSL/SSH Inspection**.
2. In the upper-right corner, in the profile drop-down list, select **Inbound_SSL_Inspection**.
3. In the **Server Certificate** drop-down list, select **webserver**.
4. Click **Apply**.

To verify the SSL inspection profile change

1. Return to the Remote-Windows VM, and close any existing instances of Firefox.
2. Open Firefox again, and go to `https://10.200.1.200`.

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

Lab 7: Web Filtering

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

You will also apply overrides to FortiGuard website categories and perform overrides on the web filtering profile. The web filtering overrides allow you to execute different actions, rather than the configured actions on the web filter security profile.

Objectives

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

Time to Complete

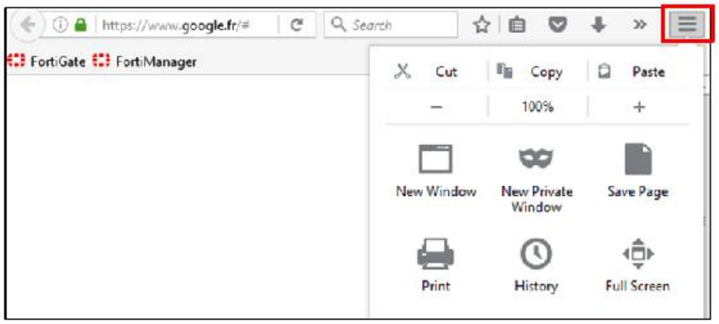
Estimated: 25 minutes

Prerequisites

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

To clear the web browser history

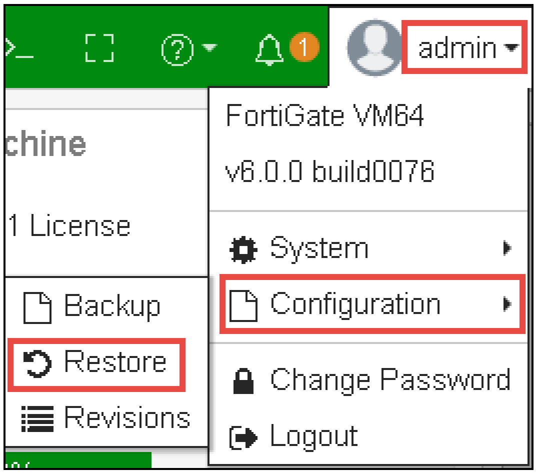
1. On the Local-Windows VM, open the browser and click the menu icon in the upper-right corner.



2. Click **History** > **Clear Recent History**, and ensure the time range to clear is set to **Everything**.
3. Click **Clear Now**.

To restore the FortiGate configuration file

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then select **Configuration** > **Restore**.



3. Select **Restore** from **Local PC**, and then click **Upload**.
4. Browse to **Desktop** > **Resources** > **FortiGate-Security** > **Web-Filtering** > `local-web-filtering.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring FortiGuard Web Filtering

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

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

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

Review the FortiGate Settings

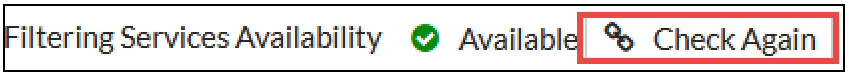
You will review the inspection mode and the license status according to the uploaded settings. You will also list the FortiGuard distribution servers (FDS) that your FortiGate will use to send the web filtering requests.

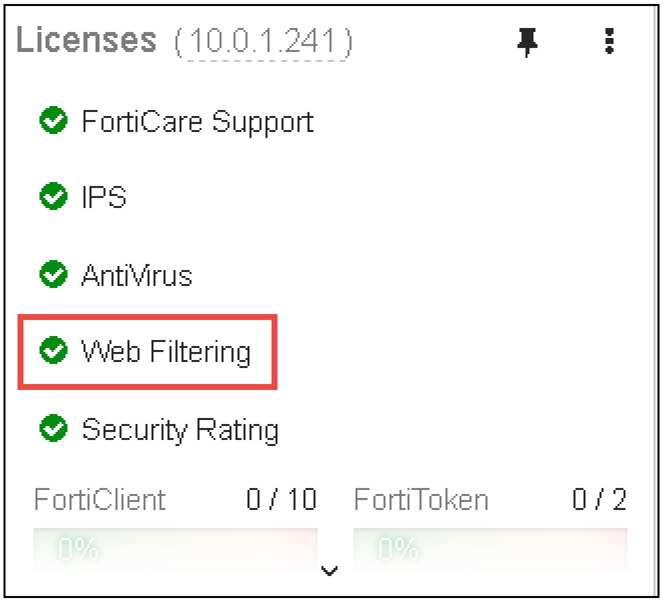
To review the restored settings on FortiGate

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. On the **Dashboard**, locate the **Licenses** widget and confirm that the **FortiGuard Web Filtering** service is licensed and active.

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

Because of the reboot following the restoration of the configuration file, the web filter license status may show "Unavailable". In this case, navigate to **System** > **FortiGuard**, click **Check Again** to force an update, and **OK** to confirm.


Filtering Services Availability ✓ Available Check Again



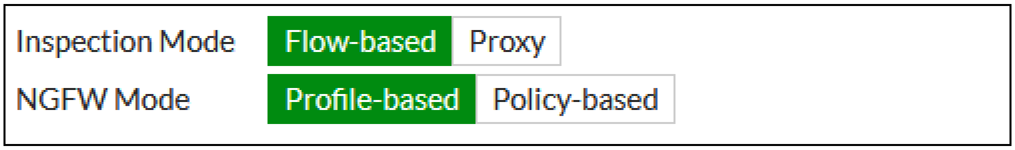
Licenses (10.0.1.241)

- ✓ FortiCare Support
- ✓ IPS
- ✓ AntiVirus
- ✓ Web Filtering
- ✓ Security Rating

FortiClient 0 / 10 0%

FortiToken 0 / 2 0%

3. Click **System** > **Settings** to verify the **Inspection Mode** setting.



Inspection Mode [✓ Flow-based] Proxy

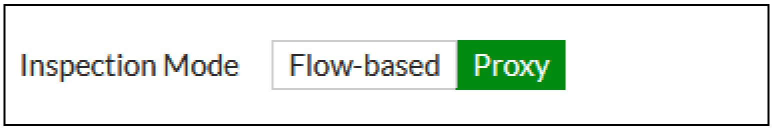
NGFW Mode [✓ Profile-based] Policy-based

Notice that the setting is **Flow-based**, which is the default setting.

4. Open PuTTY and connect over SSH to the **LOCAL-FORTIGATE** saved session.
5. At the login prompt, enter the user name `admin` and password `password`.
6. Enter the following commands to change from **Flow-based** to **Proxy** inspection mode.

```
config system settings
set inspection-mode proxy
end
```

7. Return to your browser where you are logged into the Local-FortiGate GUI and refresh the browser. (Alternatively, you can log out of the Local-FortiGate GUI and log back in.)
8. Click **System** > **Settings** to verify that the **Inspection Mode** is now set to **Proxy**.



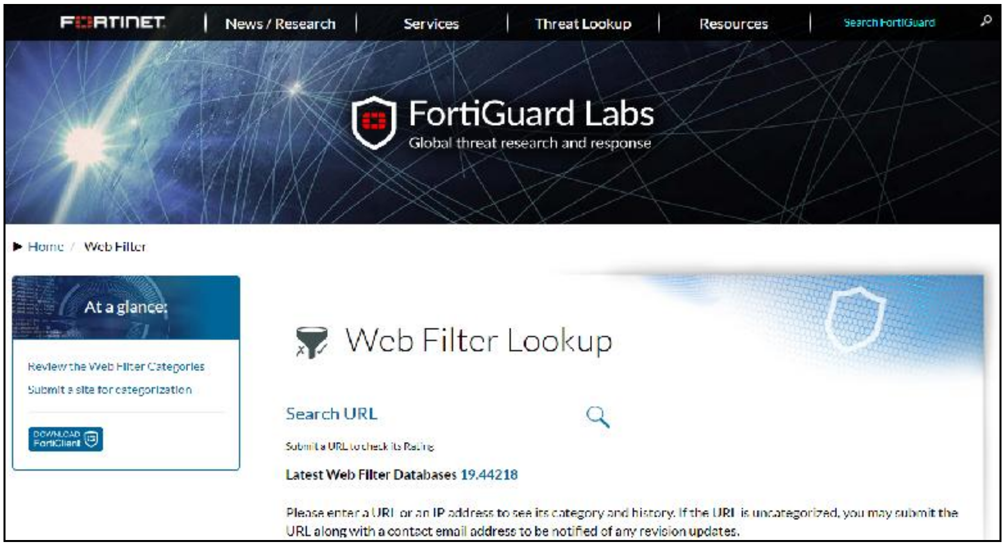
Inspection Mode Flow-based [✓ Proxy]

Determine Web Filter Categories

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

To determine web filter categories

1. Continuing on the Local-Windows VM, open a new browser tab and go to http://www.fortiguard.com/webfilter.

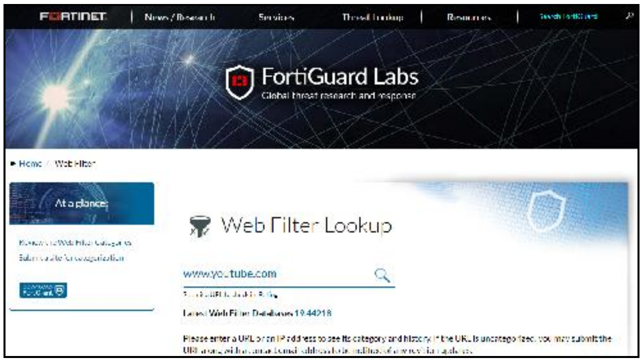


Latest Web Filter Databases 19.44218

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

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

```
http://www.youtube.com
```



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

As you can see, YouTube is listed in the **Steaming Media and Download** category.

3. Use the **Web Filter Lookup** tool again to find the web filter category for the following websites:
   - http://www.skype.com/
   - http://www.ask.com/
   - http://www.bing.com/

You will test your web filter using these websites as well.

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

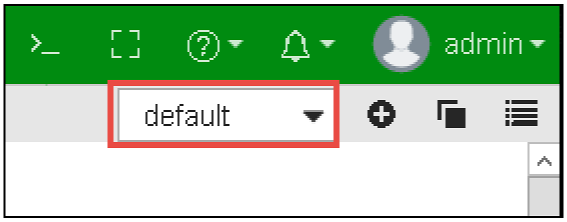
Website	Category	Action
http://www.youtube.com/	Streaming Media and Download	Block
http://www.skype.com/	Internet Telephony	Warning
http://www.bing.com/	Search Engines and Portals	Allow
http://www.ask.com	Search Engines and Portals	Allow

Configure a FortiGuard Category-Based Web Filter

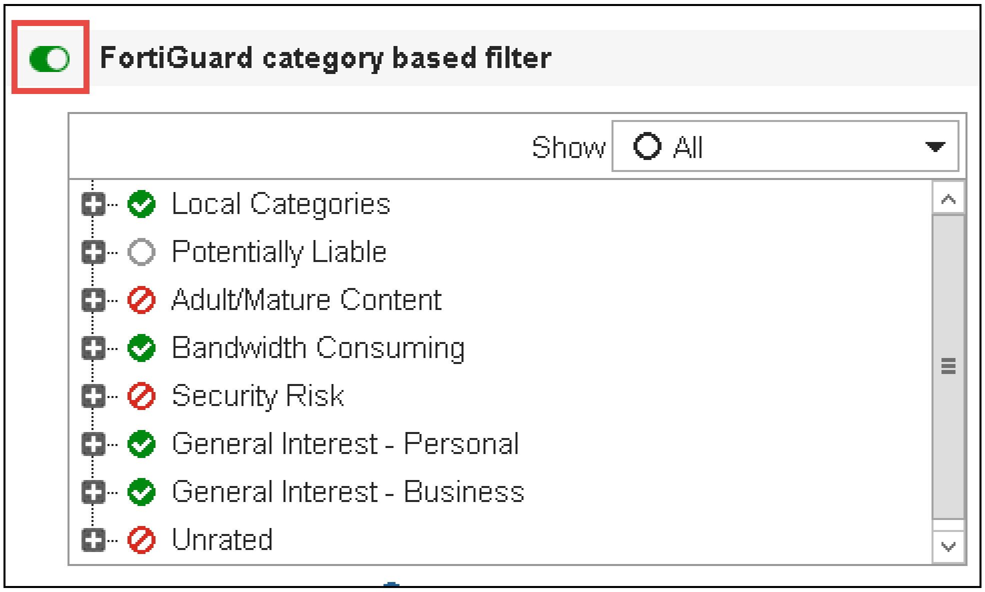
You will review the default web filtering profile and configure the FortiGuard category-based filter.

To configure the web filter security profile

1. Return to your browser tab where you are logged into the Local-FortiGate GUI, and click **Security Profiles** > **Web Filter**.
2. In the drop-down list in the upper-right corner of the screen, ensure **default** is selected as your web filter profile.



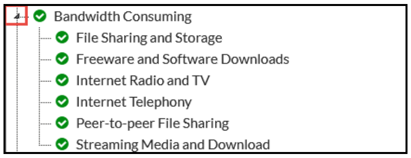
3. Verify that **FortiGuard category based filter** is enabled.



4. Review the default actions for each category.

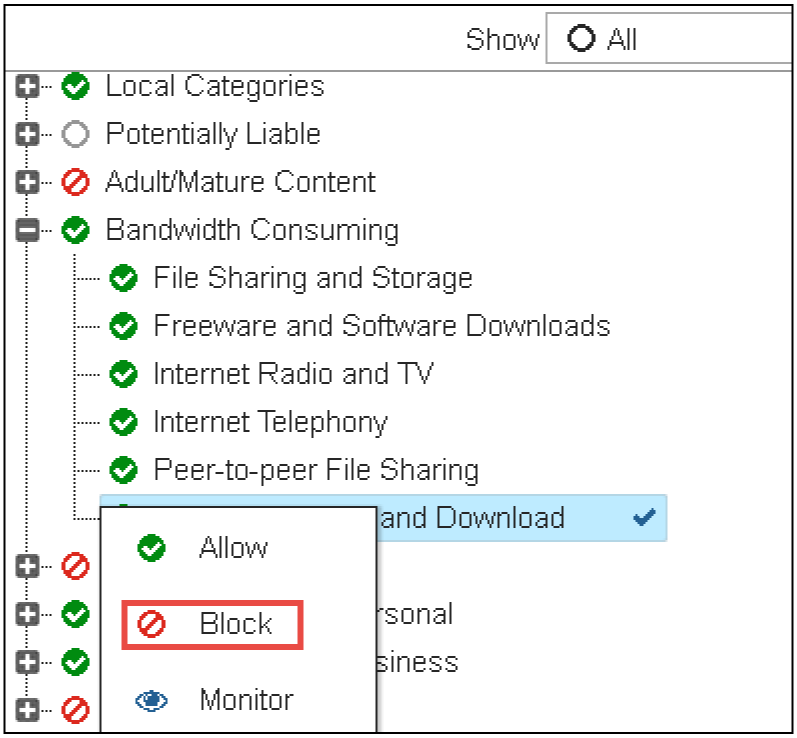
Category	Action
Local Categories	Enable
Potentially Liable	Block: **Extremist Group** Allow: all other sub-categories **Tip**: Expand **Potentially Liable** to view the subcategories.
Adult/Mature Content	Block
Bandwidth Consuming	Allow
Security Risk	Block
General Interest - Personal	Allow
General Interest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

5. Expand **Bandwidth Consuming** to view the subcategories.

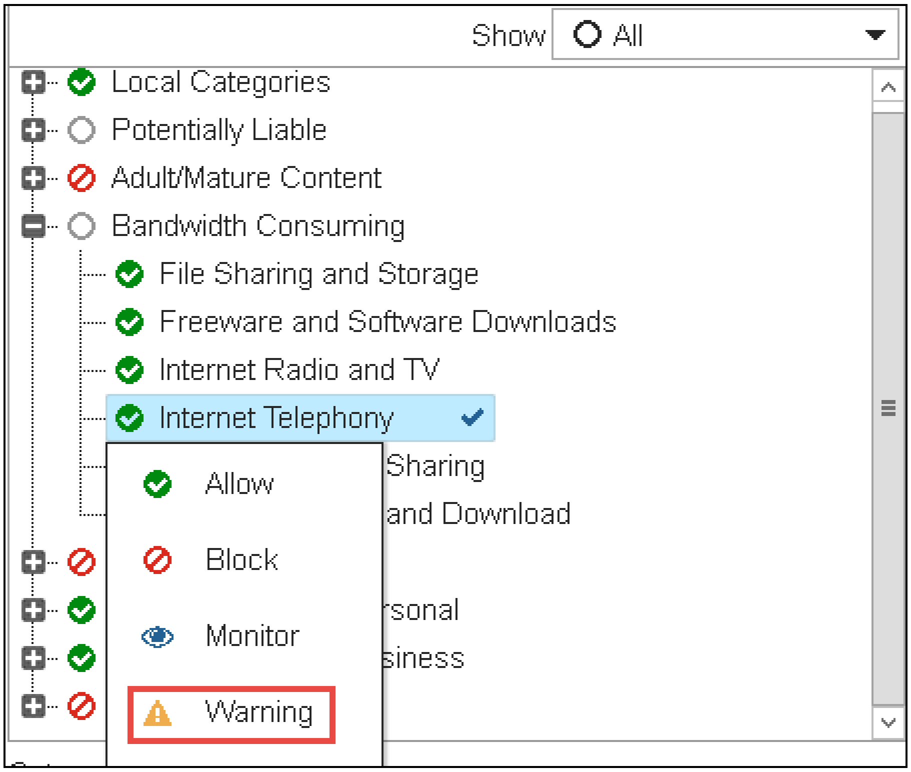


Bandwidth Consuming
File Sharing and Storage
Freeware and Software Downloads
Internet Radio and TV
Internet Telephony
Peer-to-peer File Sharing
Streaming Media and Download

6. Right-click **Streaming Media and Download** and select **Block**.



7. Right-click **Internet Telephony**, and then select **Warning**.



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

8. Keep the default setting of 5 minutes and click **OK**.
9. Click **Apply**.

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 generated by the web traffic.

Take the Expert Challenge!

On the Local-FortiGate GUI (`10.0.1.254`),apply the web filter profile to the existing **Full_Access** firewall policy. Make sure that logging is also enabled and set to **Security Events**.

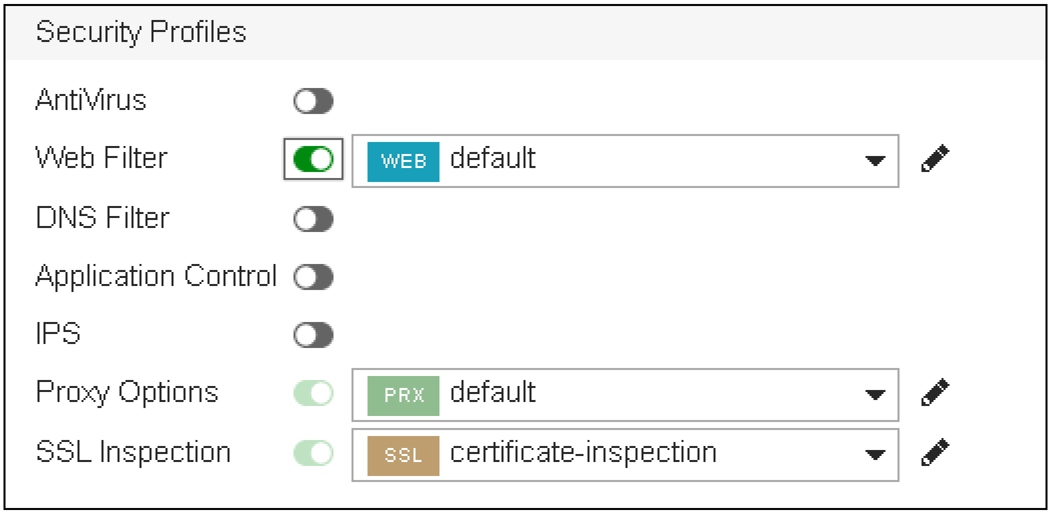
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Test the Web Filter on page 134.

To apply a security profile on a firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Double-click the **Full_Access** policy to edit it.
3. In the **Security Profiles** section, enable **Web Filter**, and from the drop-down menu select **default**.

   Note that this action enables the **Proxy Options** profile.



Security Profiles

AntiVirus ○
Web Filter ● WEB default
DNS Filter ○
Application Control ○
IPS ○
Proxy Options ● PRX default
SSL Inspection ● SSL certificate-inspection

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

Test the Web Filter

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

To test the web filter

1. Continuing on the Local-Windows VM, open PuTTY and connect over SSH to the **LOCAL-FORTIGATE** saved session.
2. At the login prompt, enter the user name `admin` and password `password`.
3. 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 FortiGuard FDS that your FortiGate uses to send web filtering requests. In normal operations, FortiGate sends the rating requests only to the server at the top of the list. Each server is probed for round-trip time (RTT) every two minutes.

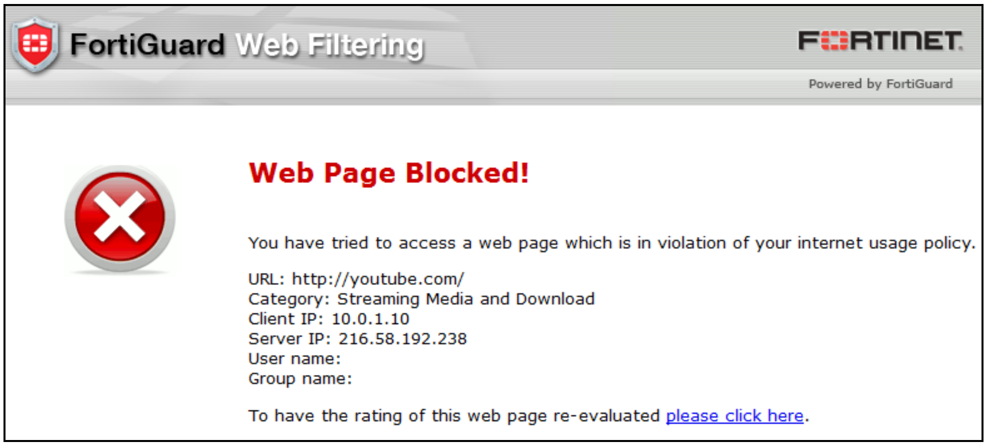
   Stop and think!

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

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

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

4. Open a new web browser tab and go to `http://www.youtube.com`.
   A warning displays, according to the predefined action for this website category.



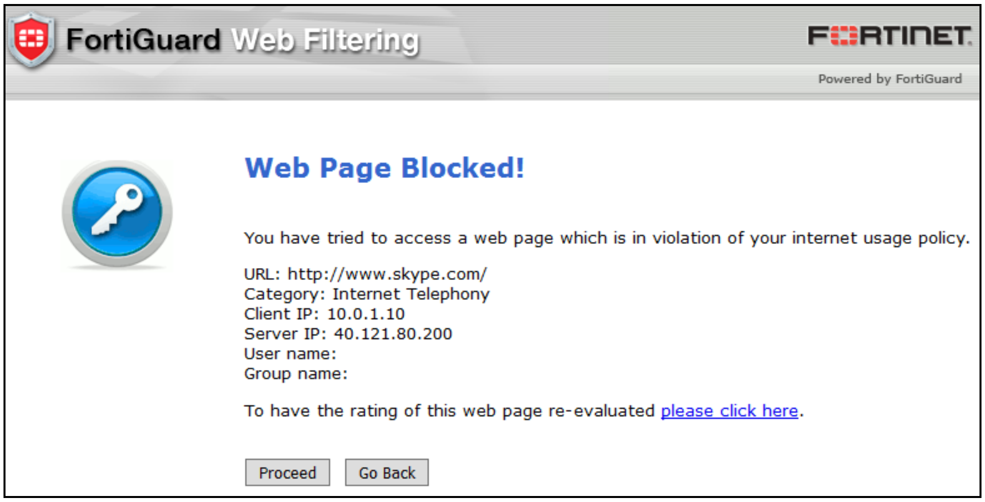
Web Page Blocked!

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

URL: http://youtube.com/
Category: Streaming Media and Download
Client IP: 10.0.1.10
Server IP: 216.58.192.238
User name:
Group name:

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

5. Open a new web browser tab and go to `http://www.skype.com/`.
   A warning displays, according to the predefined action for this website category.



Web Page Blocked!

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

URL: http://www.skype.com/
Category: Internet Telephony
Client IP: 10.0.1.10
Server IP: 40.121.80.200
User name:
Group name:

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

6. Click **Proceed** to accept the warning and access the website.

   You are presented with a certificate warning.

7. Click **Advanced** and then **Add Exception**.
8. Click **Confirm Security Exception**.
9. Open a new web browser tab and go to `http://www.bing.com/`.

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

Create a Web Rating Override

In this procedure you will override the category for www.bing.com.

To create a web rating override

1. Return to your browser tab where you are logged in to the Local-FortiGate GUI, and 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**.

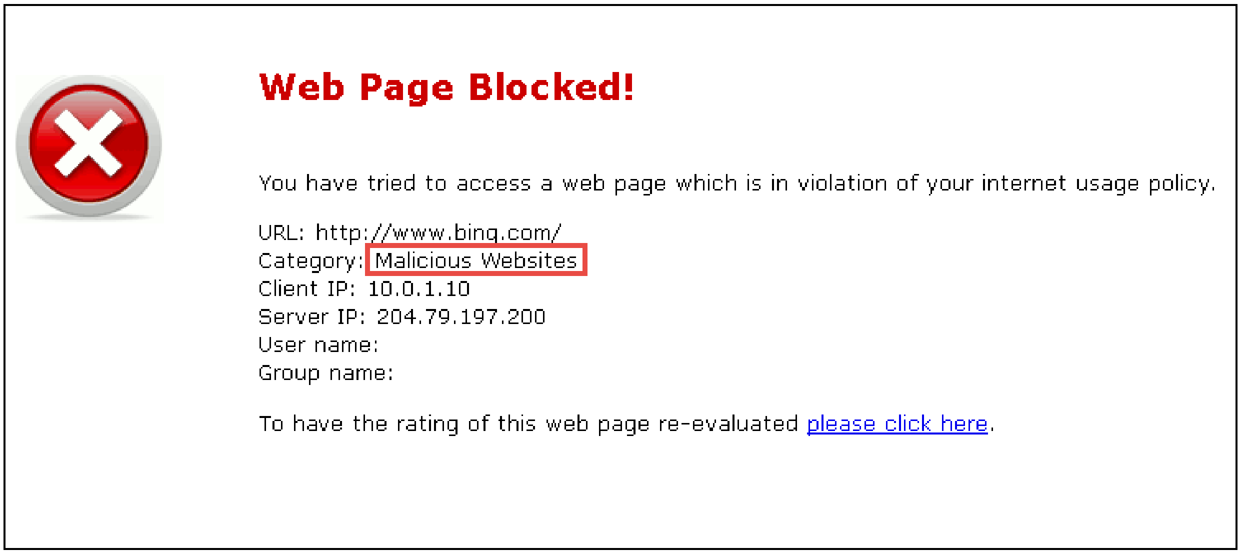
Test the Web Rating Override

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

To test the Web Rating Override

1. Continuing on the Local-Windows VM, open a new browser tab, and try again to access the website `www.bing.com`.

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



Web Page Blocked!

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

URL: http://www.bing.com/
Category: Malicious Websites
Client IP: 10.0.1.10
Server IP: 204.79.197.200
User name:
Group name:

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

Exercise 2: Setting Up Web Filtering Authentication

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

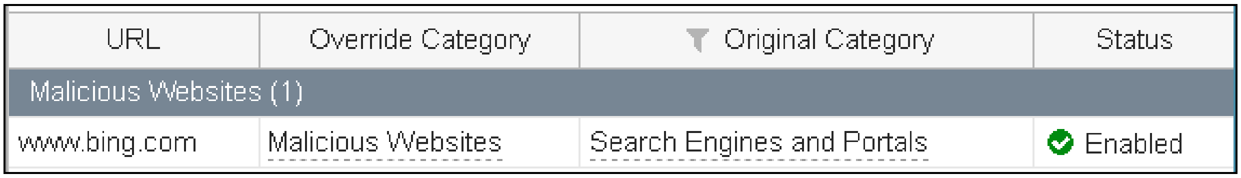
Set Up the Authenticate Action

First, you will override the category for www.bing.com to **Proxy Avoidance**. Then, you will set the action for this FortiGuard category to **Authenticate**.

To override the category

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Security Profiles** > **Web Rating Overrides**.

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



URL	Override Category	Original Category	Status
Malicious Websites (1)			
www.bing.com	Malicious Websites	Search Engines and Portals	✓ Enabled

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

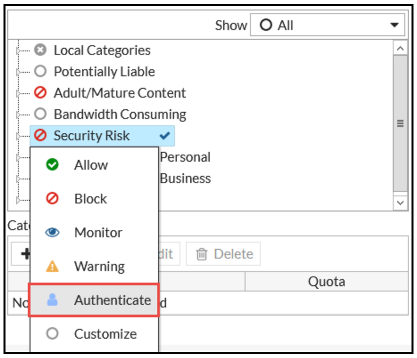
Field	Value
Category	Security Risk
Sub-Category	Malicious Websites

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

4. Click **Cancel**.

To set up the authenticate action

1. Continuing on the Local-FortiGate GUI, click **Security Profiles** > **Web Filter**.
2. Under **FortiGuard category based filter**, right-click **Security Risk**, and then select **Authenticate**.



The **Edit Filter** widget appears.

3. Use the following settings:

Field	Value
Warning Interval	5 minutes
Selected User Groups	Override_Permissions

4. Click **OK**.
5. Click **Apply**.

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

Define Users and Groups

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

To create a user

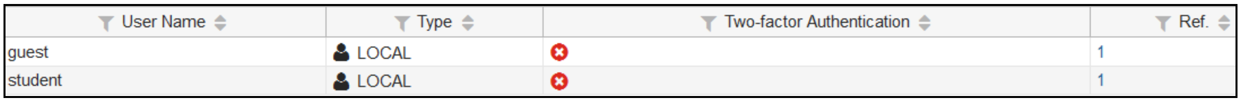
1. Continuing on the Local-FortiGate GUI, click **User & Device** > **User Definition**.
2. Click **Create New**.
3. Select **Local User** as the **User Type**.
4. Click **Next**, and then configure the following settings:

Field	Value
User Name	student
Password	fortinet

5. Click **Next**.
6. Click **Next**.

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

   The **student** user is created.



User Name	Type	Two-factor Authentication	Ref.
guest	LOCAL	✖	1
student	LOCAL	✖	1

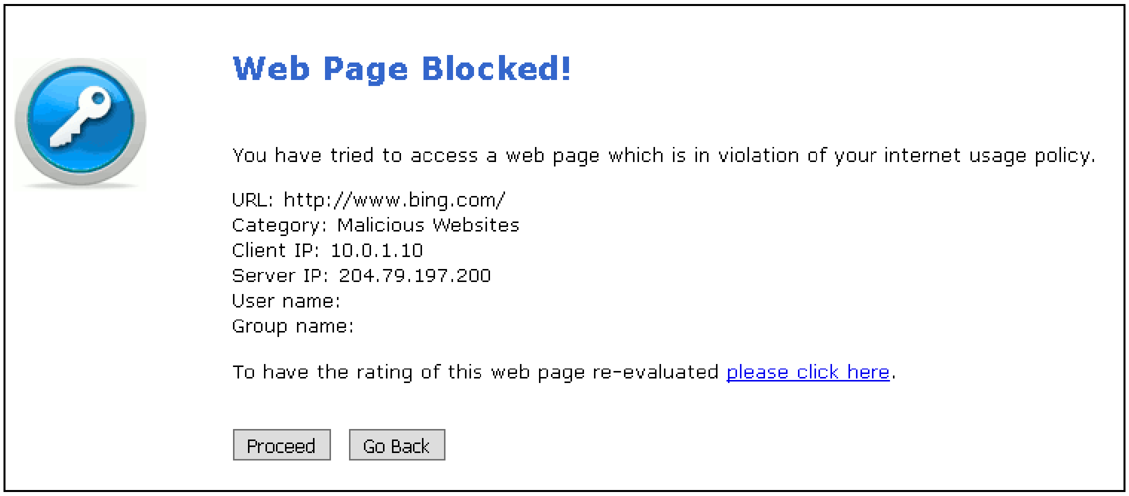
Test the Authenticate Action

In this section, you will test access to a website using the authenticate action, and then analyze the logs made by the security events.

To test the web rating override

1. Continuing in the Local-Windows VM, open a new browser tab, and try to access `http://www.bing.com`.

   A warning displays. Note that it is a different message from the one that appeared before.



Web Page Blocked!

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

URL: http://www.bing.com/
Category: Malicious Websites
Client IP: 10.0.1.10
Server IP: 204.79.197.200
User name:
Group name:

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

2. Click **Proceed**.

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

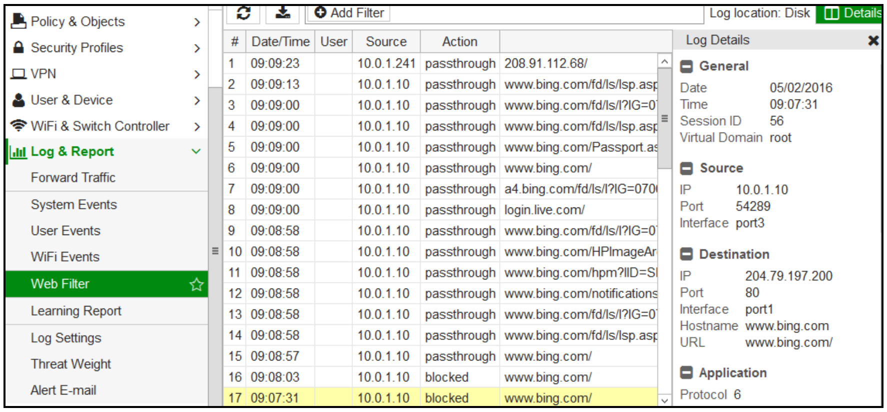
3. Enter the following credentials:

Field	Value
Username	student
Password	fortinet

   This website now displays correctly.

To review the web filter logs for web rating overrides

1. Return to your browser tab where you are logged into the Local-FortiGate GUI, and click **Log & Report** > **Web Filter**.



#	Date/Time	User	Source	Action	
1	09:09:23		10.0.1.241	passthrough	208.91.112.68/
2	09:09:13		10.0.1.10	passthrough	www.bing.com/fd/ls/lsp.asp
3	09:09:00		10.0.1.10	passthrough	www.bing.com/fd/ls/l?IG=07
4	09:09:00		10.0.1.10	passthrough	www.bing.com/fd/ls/lsp.asp
5	09:09:00		10.0.1.10	passthrough	www.bing.com/Passport.as
6	09:09:00		10.0.1.10	passthrough	www.bing.com/
7	09:09:00		10.0.1.10	passthrough	a4.bing.com/fd/ls/l?IG=070
8	09:09:00		10.0.1.10	passthrough	login.live.com/
9	09:08:58		10.0.1.10	passthrough	www.bing.com/fd/ls/l?IG=07
10	09:08:58		10.0.1.10	passthrough	www.bing.com/HPImageAr
11	09:08:58		10.0.1.10	passthrough	www.bing.com/hpm?IID=SI
12	09:08:58		10.0.1.10	passthrough	www.bing.com/notifications
13	09:08:58		10.0.1.10	passthrough	www.bing.com/fd/ls/l?IG=07
14	09:08:58		10.0.1.10	passthrough	www.bing.com/fd/ls/lsp.asp
15	09:08:57		10.0.1.10	passthrough	www.bing.com/
16	09:08:03		10.0.1.10	blocked	www.bing.com/
17	09:07:31		10.0.1.10	blocked	www.bing.com/

Log Details

General

Date 05/02/2016
Time 09:07:31
Session ID 56
Virtual Domain root

Source

IP 10.0.1.10
Port 54289
Interface port3

Destination

IP 204.79.197.200
Port 80
Interface port1
Hostname www.bing.com
URL www.bing.com/

Application

Protocol 6

The **Web Filter** logs section won't display if there are no web filtering logs. FortiGate displays the section after creating logs. If the **Web Filter** menu does not appear in the GUI, refresh your browser or log out of the Local-FortiGate GUI and log back in.

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

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

However, for this website, you changed the category to **Security Risk**.

Exercise 3: Web Profile Overrides

As you have tested the web rating overrides, you will now test web profile overrides.

The web profile overrides feature changes the rules applied to inspected traffic. It authorizes some users, user groups, or predefined source IPs, to use a different web filter profile.

Configure Web Profile Overrides

In this procedure, you will allow users to override blocked categories. Those users must authenticate in order to apply a different web filter profile.

To configure a web profile override

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Security Profiles** > **Web Filter**.
3. In the drop-down list in the upper-right corner of the screen, ensure **default** is selected as your web filter profile.
4. Enable **Allow users to override blocked categories**, and then enter the following values:

Field	Value
Group that can override	Override_Permissions
Profile can switch to	monitor-all
Switch applies to	IP
Switch duration	Predefined 0 Day(s) | 0 Hour(s) | 15 Minute(s)

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

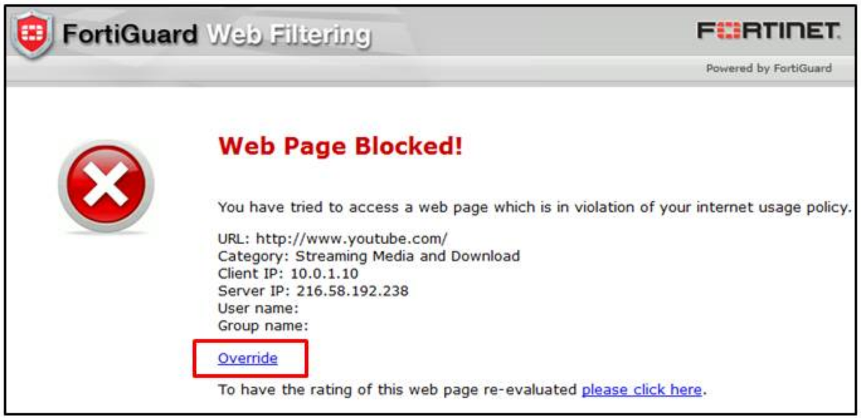
Test the Web Profile Override

Finally, you will test the global access for a blocked category, and authenticate to apply a new web filter profile. You will also review the web filter logs to verify how actions change after the new web profile is applied.

To test the web profile override

1. Continuing on the Local-Windows VM, open a new browser tab, and try to access `www.youtube.com`.

   A warning displays according to the action for this website category. However, this warning is different from the one that appeared in To test the web filter on page 135. This warning includes an override link at the bottom.



Web Page Blocked!

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

URL: http://www.youtube.com/
Category: Streaming Media and Download
Client IP: 10.0.1.10
Server IP: 216.58.192.238
User name:
Group name:

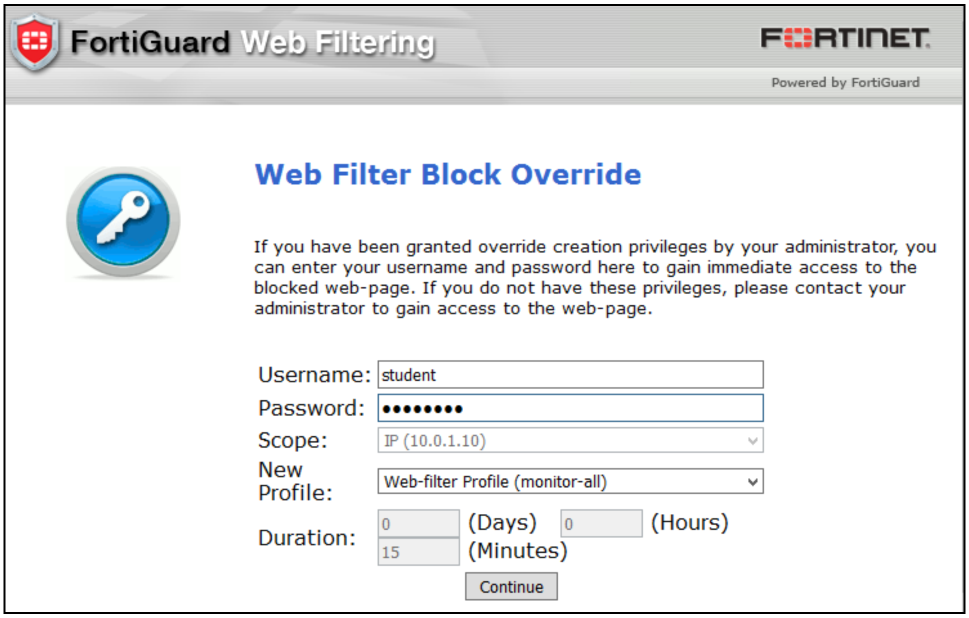
Override

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

2. Click **Override**.

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

A block override message appears:



Web Filter Block Override

If you have been granted override creation privileges by your administrator, you can enter your username and password here to gain immediate access to the blocked web-page. If you do not have these privileges, please contact your administrator to gain access to the web-page.

Username: student
Password: ••••••••
Scope: IP (10.0.1.10)
New Profile: Web-filter Profile (monitor-all)
Duration: 0 (Days) 0 (Hours) 15 (Minutes)

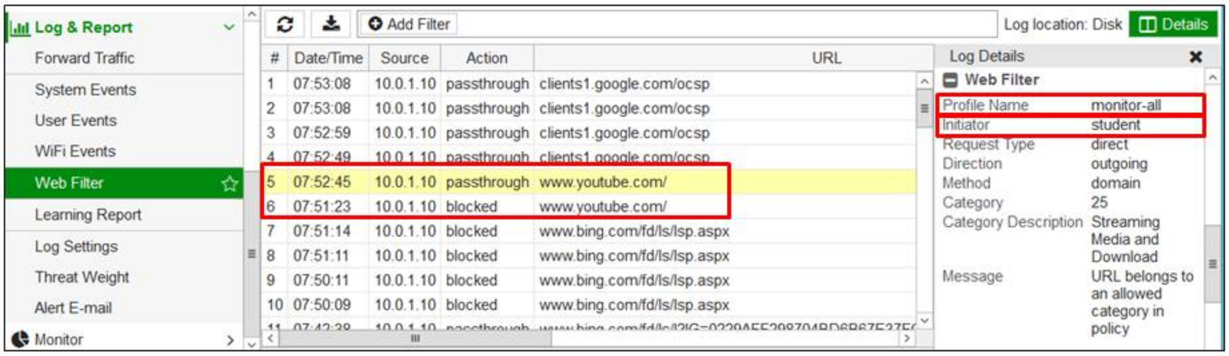
3. Enter the following values, and then click **Continue**:

Field	Value
Username	student
Password	fortinet

FortiGate overrides the default profile and allows you to access the website.

To review the web filter logs for web profile overrides

1. Return to your browser tab where you are logged in to the **Local-FortiGate** GUI, and click **Log & Report** > **Web Filter**.
2. Compare the current **passthrough** entries with the older **blocked** logs.



#	Date/Time	Source	Action	URL
1	07:53:08	10.0.1.10	passthrough	clients1.google.com/ocsp
2	07:53:08	10.0.1.10	passthrough	clients1.google.com/ocsp
3	07:52:59	10.0.1.10	passthrough	clients1.google.com/ocsp
4	07:52:49	10.0.1.10	passthrough	clients1.google.com/ocsp
5	07:52:45	10.0.1.10	passthrough	www.youtube.com/
6	07:51:23	10.0.1.10	blocked	www.youtube.com/
7	07:51:14	10.0.1.10	blocked	www.bing.com/fd/ls/lsp.aspx
8	07:51:11	10.0.1.10	blocked	www.bing.com/fd/ls/lsp.aspx
9	07:50:11	10.0.1.10	blocked	www.bing.com/fd/ls/lsp.aspx
10	07:50:09	10.0.1.10	blocked	www.bing.com/fd/ls/lsp.aspx
11	07:42:38	10.0.1.10	passthrough	www.bing.com/fd/ls/l?IG=0229AEE209704BD6B67E27E

Log Details

Web Filter

Profile Name	monitor-all
Initiator	student
Request Type	direct
Direction	outgoing
Method	domain
Category	25
Category Description	Streaming Media and Download
Message	URL belongs to an allowed category in policy

3. Select a blocked entry and in the upper-right corner of the screen, click **Details**.
4. Now, select a passthrough entry and click **Details**.

   Notice that the web profile used is different.

Lab 8: Application Control

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

Objectives

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

Time to Complete

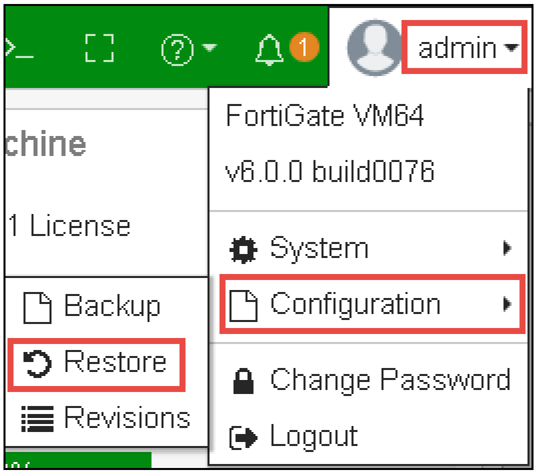
Estimated: 15 minutes

Prerequisites

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

To restore the FortiGate configuration file

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**,and then click **Upload**.
4. Click **Desktop** > **Resources** > **FGT-Security** > **Application Control** > `Local-App-Control-Policy.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Implementing Application Control in NGFW Policy-Based Mode

In NGFW policy-based mode, application control is applied directly on a firewall policy, without the use of an application control profile.

The following settings are configured on the configuration file:

- NGFW policy-mode enabled
- Central SNAT policy allowing traffic in NGFW policy-mode to pass
- Firewall policy allowing all traffic to pass

In this exercise, you will configure application control on a FortiGate operating in NGFW policy-based mode.

Apply Application Control in NGFW Policy-Based Mode

You will be configuring a new firewall policy and applying application control on the policy.

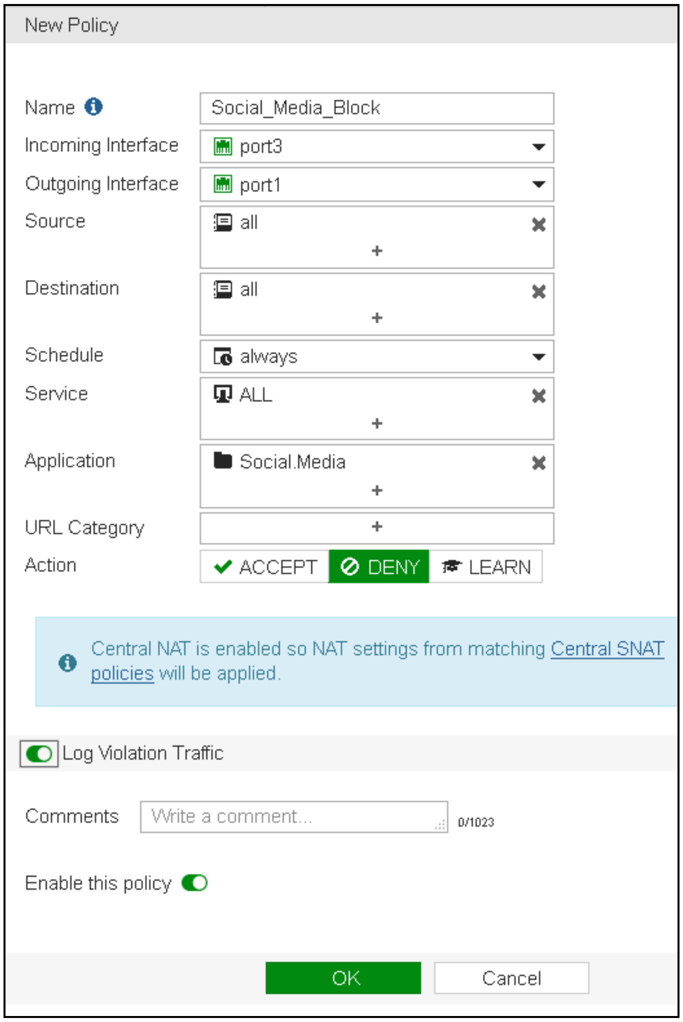
To configure an application control firewall policy

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Policy & Objects** > **IPv4 Policy**.
3. Click **Create New**.
4. Configure the following settings:

Field	Value
Name	Social_Media_Block
Incoming Interface	port3
Outgoing Interface	port1
Source	all
Destination	all
Service	ALL
Application	Social.Media **Tip**: From the right pane, click **Category** and then search for **Social.Media**.

Field	Value
Action	DENY
Log Violation Traffic	<enable>
Enable this policy	<enable>

5. Keep the default values for the remaining settings.



New Policy

Name	Social_Media_Block
Incoming Interface	port3
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	ALL
Application	Social.Media
URL Category	+
Action	ACCEPT [✓ DENY] LEARN

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

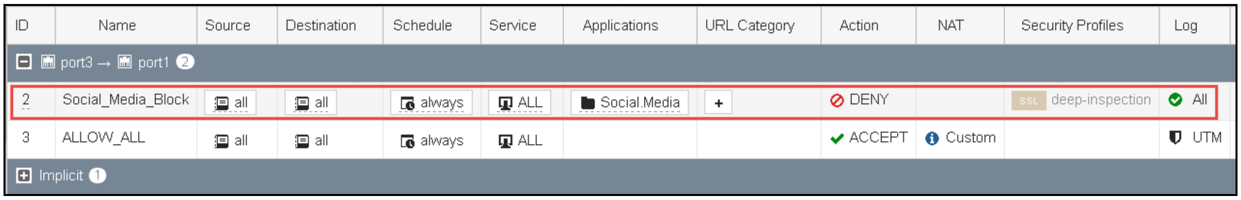
● Log Violation Traffic

Comments: Write a comment... 0/1023

Enable this policy ●

6. Click **OK**.

7. From the **ID** column, drag the **Social_Media_Block** firewall policy above the **ALLOW_ALL** firewall policy. Your firewall policy order should look like this:



ID	Name	Source	Destination	Schedule	Service	Applications	URL Category	Action	NAT	Security Profiles	Log
⊟ port3 → port1 2											
2	Social_Media_Block	all	all	always	ALL	Social.Media	+	DENY		SSL deep-inspection	All
3	ALLOW_ALL	all	all	always	ALL			ACCEPT	Custom		UTM
⊞ Implicit 1											

When applying application control, you should have a policy that allows all applications. Otherwise, you allow only specific applications and all other applications (including web browsers) will be blocked.

Test Application Control

Now that your configuration is complete, you will test application control by going to the application that you have configured.

To test the application control firewall policy

1. Continuing on the Local-Windows VM, open new web browser tabs and go to one or more of the following URLs:
   - https://www.linkedin.com
   - https://facebook.com
   - https://plus.google.com

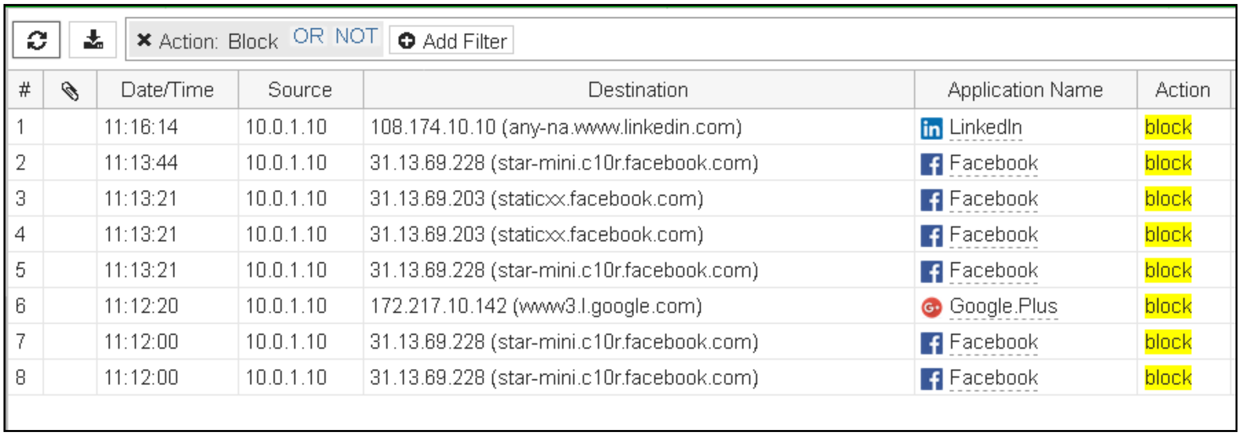
   None of the pages load.
2. Try to visit websites that fall under application categories other than social media, such as http://dailymotion.com.

   The pages load.
3. Return to your browser tab where you are logged in to the Local-FortiGate GUI, and click **Log & Report** > **Application Control**.

The **Application Control** logs section will not display if there are no application control logs. FortiGate will show the section after creating logs. If the **Application Control** menu item does not display in the GUI, refresh your browser or log out of the Local-FortiGate GUI and log back in.

4. Search the logs for LinkedIn, Facebook, and Google Plus.

   You will see logs similar to the following example:



#		Date/Time	Source	Destination	Application Name	Action
1		11:16:14	10.0.1.10	108.174.10.10 (any-na.www.linkedin.com)	LinkedIn	block
2		11:13:44	10.0.1.10	31.13.69.228 (star-mini.c10r.facebook.com)	Facebook	block
3		11:13:21	10.0.1.10	31.13.69.203 (staticxx.facebook.com)	Facebook	block
4		11:13:21	10.0.1.10	31.13.69.203 (staticxx.facebook.com)	Facebook	block
5		11:13:21	10.0.1.10	31.13.69.228 (star-mini.c10r.facebook.com)	Facebook	block
6		11:12:20	10.0.1.10	172.217.10.142 (www3.l.google.com)	Google.Plus	block
7		11:12:00	10.0.1.10	31.13.69.228 (star-mini.c10r.facebook.com)	Facebook	block
8		11:12:00	10.0.1.10	31.13.69.228 (star-mini.c10r.facebook.com)	Facebook	block

5. Close your browser.

Lab 9: Antivirus

In this lab, you will 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 inspection modes.
- Understand FortiGate antivirus scanning behavior.
- Scan multiple protocols.
- Read and understand antivirus logs.

Time to Complete

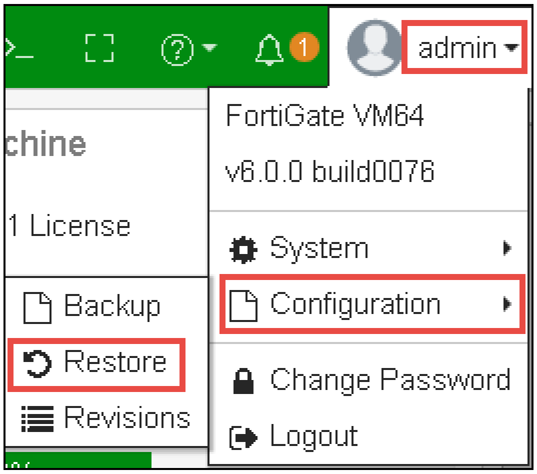
Estimated: 20 minutes

Prerequisites

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

To restore the FortiGate configuration file

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**,and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **Antivirus** > `local-AV-flow-based.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Using Antivirus Scanning in Flow-Based Inspection Mode

There are two antivirus scanning modes in flow-based inspection mode:

- Quick scan uses a compact antivirus database and performs faster scanning because it doesn’t buffer the file in memory.
- Full scan uses the full antivirus database. It buffers the file locally, but transmits it simultaneously to the end client. Everything is transmitted except the last packet. The last packet is delayed, and the whole file is sent to the antivirus engine for scanning.

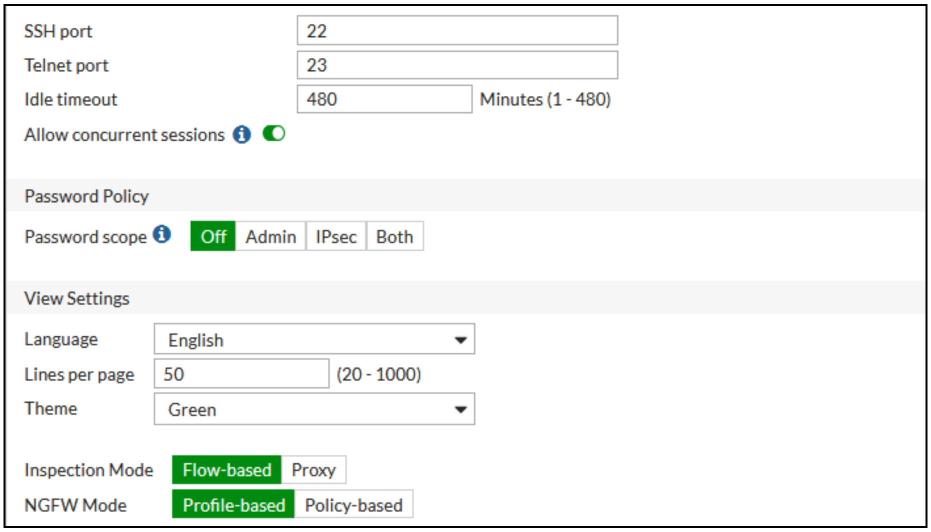
In this exercise, you will use antivirus in flow-based inspection mode to understand how FortiGate performs antivirus scanning. You will use full-scan mode with and without deep inspection. You will observe the behavior of antivirus scanning, with and without deep inspection, to understand the importance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

Configure the Antivirus Profile in Flow-Based Inspection Mode

By default, the FortiGate inspection mode is set to flow-based, so all the security profiles will also be set to flow-based inspection mode. In this procedure, you will verify the antivirus profile settings, and apply the antivirus profile to a firewall policy.

To view the current FortiGate inspection mode

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **System** > **Settings**.
3. At the bottom of the page, verify that **Inspection Mode** is set to **Flow-based**, and that **NGFW Mode** is set to **Profile-based**.



SSH port	22	
Telnet port	23	
Idle timeout	480	Minutes (1 - 480)
Allow concurrent sessions	☑	

Password Policy

Password scope	[✓ Off] Admin IPsec Both

View Settings

Language	English	
Lines per page	50	(20 - 1000)
Theme	Green	

Inspection Mode	[✓ Flow-based] Proxy
NGFW Mode	[✓ Profile-based] Policy-based

Review the Flow-Based Antivirus Profile

Now that you've verified that the inspection mode is set to flow-based, you will review the antivirus profile to view the settings.

To review the flow-based antivirus profile

1. Continuing on the Local-FortiGate GUI, click **Security Profiles** > **AntiVirus**.
2. Review the **default** antivirus profile.

Because the inspection mode is set to flow-based, by default, all the security profiles will be set to flow-based as well.

Enable the Antivirus Profile on a Firewall Policy

Now that you have reviewed the antivirus profile, you must enable the antivirus profile on your firewall policy. After you enable the antivirus profile on a firewall policy, it can scan for viruses and generate logs (based on configured log settings).

Take the Expert Challenge!

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

- Edit the **Full_Access** firewall policy and enable the **default** antivirus profile.
- Use **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 152.

To enable the antivirus profile on a firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Right-click the **ID** column for the **Full_Access** firewall policy and click **Edit**.
3. Under the **Security Profiles** section, enable **AntiVirus**, and select **default** from the drop-down menu.
4. In the **SSL/SSH Inspection** drop-down menu, keep the default **certificate-inspection** profile.

When selecting an antivirus profile, **SSL/SSH Inspection** is enabled by default. You can't disable it, but you can select any preconfigured SSL/SSH inspection profile in the associated drop-down menu. You will use the **certificate-inspection** profile for this section of the lab.

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

Test the Antivirus Configuration

In this procedure, you will download the EICAR test file to your Local-Windows VM. The EICAR test file is an industry-standard virus used to test antivirus detection without causing damage. The file contains the following characters:

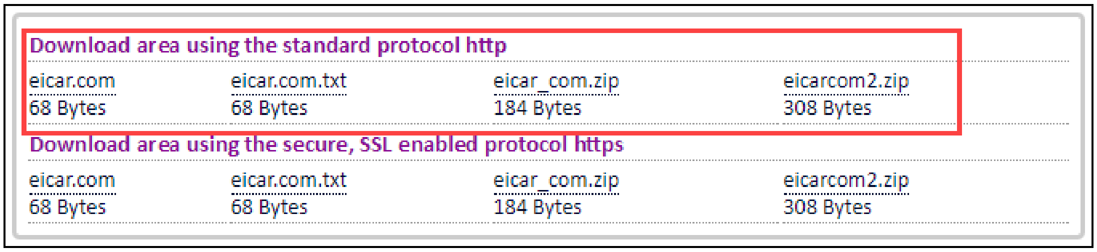
```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

To test the antivirus configuration

1. Continuing on the Local-Windows VM, open a new web browser tab and access the following website:

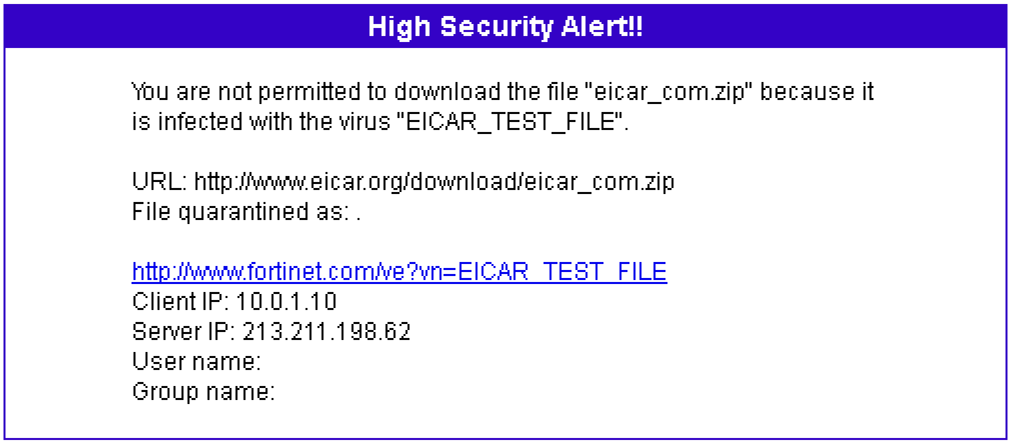
   `http://eicar.org`

2. In the upper-right corner of the EICAR webpage, click **DOWNLOAD ANTI MALWARE TESTFILE**.
3. Click the **Download** link on the left.
4. In the **Download area using the standard protocol http** section, download any EICAR sample file**.**



Download area using the standard protocol http			
eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes
Download area using the secure, SSL enabled protocol https			
eicar.com	eicar.com.txt	eicar_com.zip	eicarcom2.zip
68 Bytes	68 Bytes	184 Bytes	308 Bytes

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



High Security Alert!!

You are not permitted to download the file "eicar_com.zip" because it is infected with the virus "EICAR_TEST_FILE".

URL: http://www.eicar.org/download/eicar_com.zip
File quarantined as: .

http://www.fortinet.com/ve?vn=EICAR_TEST_FILE
Client IP: 10.0.1.10
Server IP: 213.211.198.62
User name:
Group name:

FortiGate shows the HTTP virus message when it blocks or quarantines infected files.

Test an alternate download method

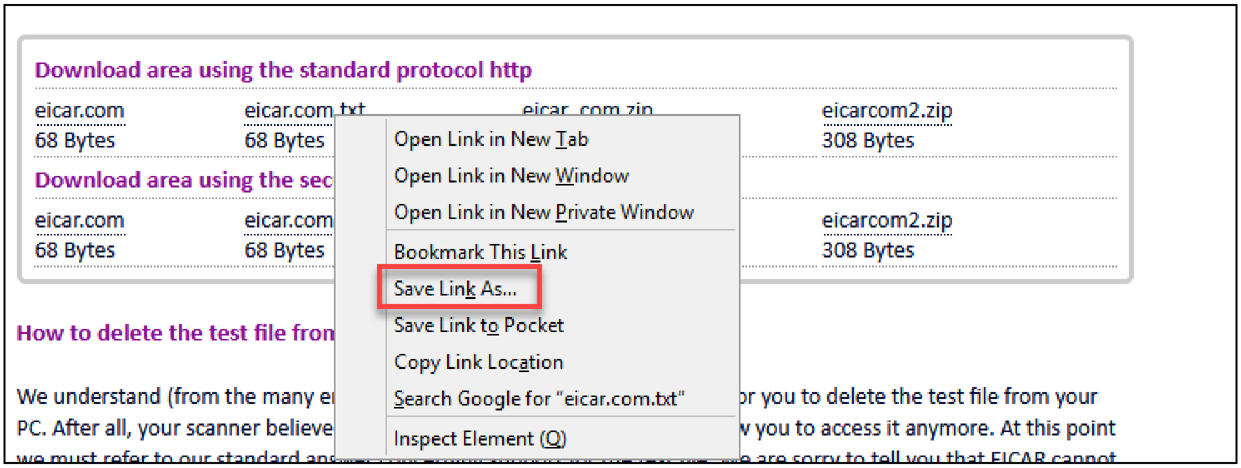
In this section, you will test the flow-based antivirus configuration using the **Save Link As** method to download the EICAR text file.

To test the antivirus configuration

1. Continuing on the Local-Windows VM, open a new web browser tab and go to the following website:

   `http://eicar.org`

2. On the EICAR website, in the upper-right corner of the page, click **DOWNLOAD ANTI MALWARE TESTFILE**.
3. Click the **Download** link on the left.
4. In the **Download area using the standard protocol http** section, right-click **eicar.com.txt** and select **Save Link As**.


Download area using the standard protocol http
eicar.com
68 Bytes
eicar.com.txt
68 Bytes
eicar_com.zip
eicarcom2.zip
308 Bytes
Download area using the sec
eicar.com
68 Bytes
eicar.com
68 Bytes
eicarcom2.zip
308 Bytes
How to delete the test file fron
We understand (from the many e
PC. After all, your scanner believe
or you to delete the test file from your
v you to access it anymore. At this point
Open Link in New Tab
Open Link in New Window
Open Link in New Private Window
Bookmark This Link
Save Link As...
Save Link to Pocket
Copy Link Location
Search Google for "eicar.com.txt"
Inspect Element (Q)

5. 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?

6. On your desktop, right-click the `eicar.com` downloaded file, and click **Edit with Notepad++** to open the file you downloaded.

   Is the content of the file what it's supposed to be?

Stop and think!

Remember, you are using flow-based inspection mode. Using this method, the client sends a request and starts receiving the packets immediately, but FortiGate is also buffering those packets at the same time.

When the last packet arrives, FortiGate buffers it and puts it on hold. Then, it sends the whole buffered file to the IPS engine where rule match is checked and passed to the antivirus engine for scanning. If the antivirus scan does not detect any viruses, and the result comes back clean, the last buffered packet is regenerated and delivered to the client.

However, if a virus is found, the last packet is dropped. Even if the client has received most of the file, the file will be truncated and the client will be not able to open a truncated file. FortiGate injects the block message into the partially download file. The client can use Notepad to open and view the file.

7. Delete the downloaded `eicar.com` file from the **Desktop**.

View the Antivirus Logs

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

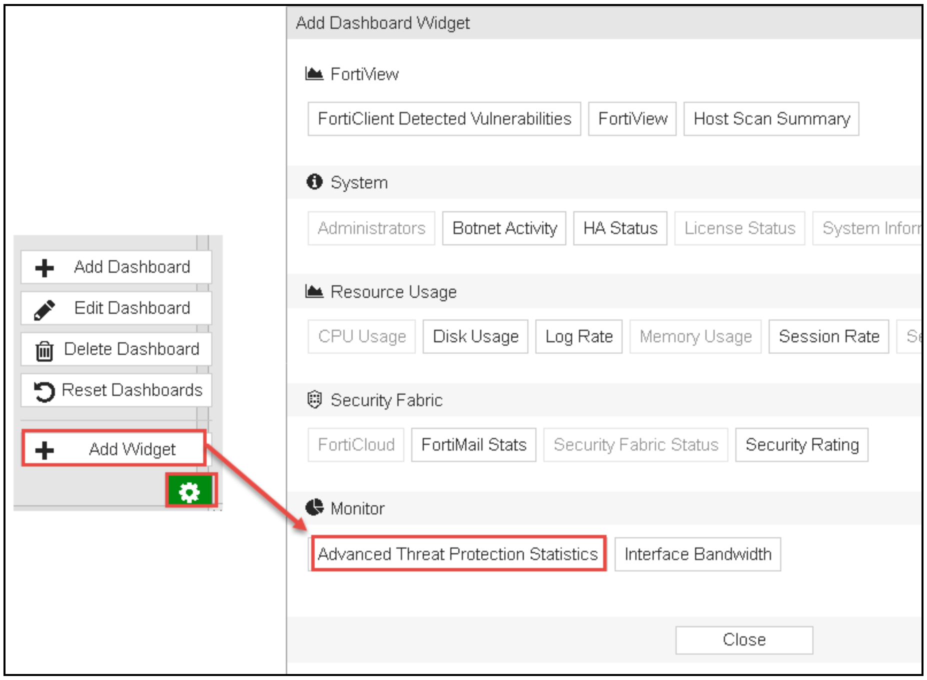
To view the antivirus logs

1. Return to your browser where you are logged in to the Local-FortiGate GUI, and click **Log & Report** > **Forward Traffic**. You may need to remove any log filters you have set.
2. Locate the antivirus log message and double-click it.

   The **Details** tab shows forward traffic log information along with the action taken.
3. Select the**Security** tab to view security logs, which provide information more specific to security events, such as file name, virus or botnet, and reference.
4. To view antivirus security logs, click **Log & Report** > **AntiVirus**.

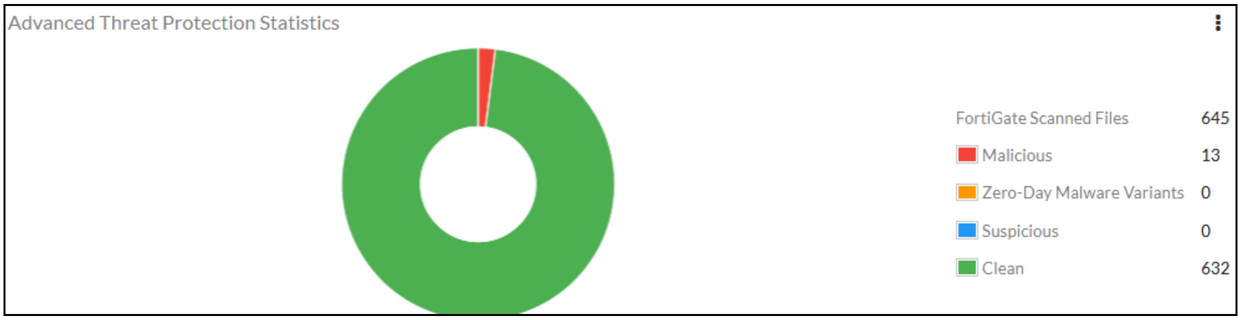
The **AntiVirus** section won't display if there are no antivirus logs. FortiGate displays the **AntiVirus** section after creating logs. If the **AntiVirus** menu item does not display in the GUI, refresh your browser or log out of the FortiGate GUI and log back in again.

5. Click **Dashboard** > **Main**.
6. Scroll to the bottom of the page, and in the bottom right, click the settings icon.
7. Click **Add Widget** and add the **Advanced Threat Protection Statistics** widget to view the summary statistics of the antivirus activity.



8. Click **Close**.

The **Advanced Threat Protection Statistics** widget provides statistics about the number of files submitted and the results of those scans.



Advanced Threat Protection Statistics

FortiGate Scanned Files	645
🟥 Malicious	13
🟧 Zero-Day Malware Variants	0
🟦 Suspicious	0
🟩 Clean	632

The Advance Threat Protection Statistics widget displays malware statistics stored on the device by the antivirus process. Statistics on the widget can be cleared by formatting the log disk.

Enable SSL Inspection on a Firewall Policy

So far, you have tested unencrypted traffic for antivirus scanning. In order for FortiGate to inspect the encrypted traffic, you must enable deep inspection on the firewall policy. After you enable this feature, FortiGate will filter for traffic that is using the SSL encrypted protocol, which is very similar to a man-in-the-middle (MITM) attack.

Take the Expert Challenge!

- On Local-Windows, test the configuration by downloading the `eicar.com` file using HTTPS without enabling the **deep-inspection** profile on the **Full Access** firewall policy.
- Configure Local-FortiGate to scan secure protocols by enabling **SSH/SSL Inspection** using the **deep-inspection** profile on the **Full Access** firewall policy.
- Test the configuration by downloading the `eicar.com` file using HTTPS.

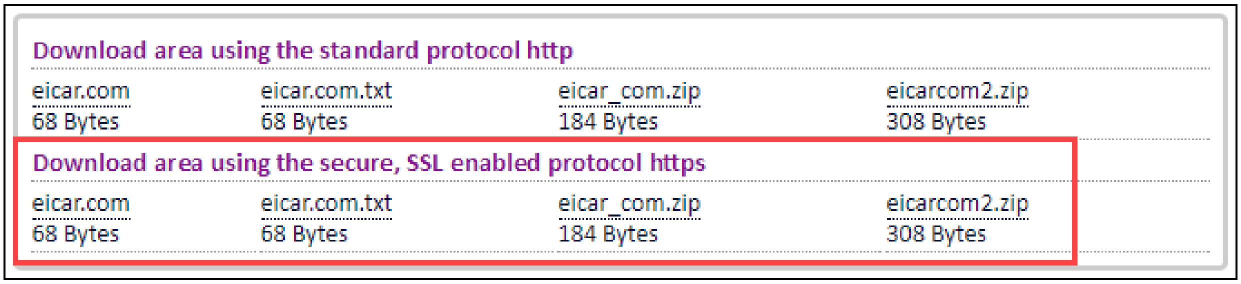
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

To test antivirus scanning without SSL Inspection enabled on the firewall policy

1. Continuing on the Local-Windows VM, open a web browser and go to the following website:

   `http://eicar.org`

2. On the EICAR webpage, click **DOWNLOAD ANTI MALWARE TESTFILE**.
3. Click the **Download** link that appears on the left side.
4. In the **Download area using the secure, SSL enabled protocol https** section, download **eicar.com** sample file.



Download area using the standard protocol http

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

Download area using the secure, SSL enabled protocol https

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

FortiGate should not block the file, because you have not enabled full SSL inspection.

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

1. Return to your browser tab where you are logged in to the Local-FortiGate GUI, and click **Policy& Objects** > **IPv4Policy**.
2. Right-click the **ID** column for the **Full Access** firewall policy and click **Edit**.
3. Under the **Security Profiles** section, in the **SSL/SSH Inspection** drop-down menu, select **deep-inspection**.
4. Keep the remaining default settings, and then click **OK** to save the changes.
5. On the EICAR web page, in the **Download area using the secure, SSL enabled protocol https** section, try to download the same `eicar.com` file again.

If the FortiGate self-signed, full-inspection certificate is not installed on the browser, end users will see a certificate warning message. In this environment, the FortiGate self-signed SSL inspection certificate is installed on the browser.

FortiGate should block the download and replace it with a message. If it doesn't, you may need to clear your cache. In Firefox, click **History** > **Clear Recent History** > **Everything**.

Exercise 2: Configuring Proxy-Based Antivirus Scanning

In proxy-based inspection mode, each protocol's proxy buffers the entire file (or waits for oversize limit) and scans it. The client must wait for the scan to finish.

In this exercise, you will configure antivirus scanning in proxy-based inspection mode, including associated security features, such as proxy options with deep-inspection. Then, you will apply antivirus scanning to the firewall policy. Finally, you will view the logs and summary information for the antivirus activity.

Change the FortiGate Inspection Mode

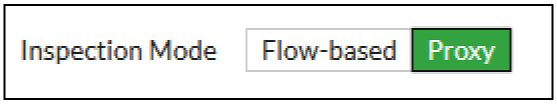
By default, flow-based inspection mode is enabled on FortiGate. You will change the inspection mode from flow-based to proxy-based.

To change the FortiGate inspection mode

1. On the Local-Windows VM, open PuTTY and connect over SSH to the LOCAL-FORTIGATE saved session.
2. At the login prompt, enter the user name `admin` and password `password`.
3. Enter the following commands to change from **Flow-based** to **Proxy** inspection mode:

```
config system settings
   set inspection-mode proxy
end
```

4. Open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
5. Click **System** > **Settings** to verify that the **Inspection Mode** is now set to **Proxy**.



Inspection Mode Flow-based [✓ Proxy]

Changing from one inspection mode to another will result in the conversion of profiles and removal or addition of security features, based on the selected mode.

Review the Antivirus Profile in Proxy-Based Inspection Mode

Now that you've changed the inspection mode to proxy-based, you will view the antivirus profile to see the changes.

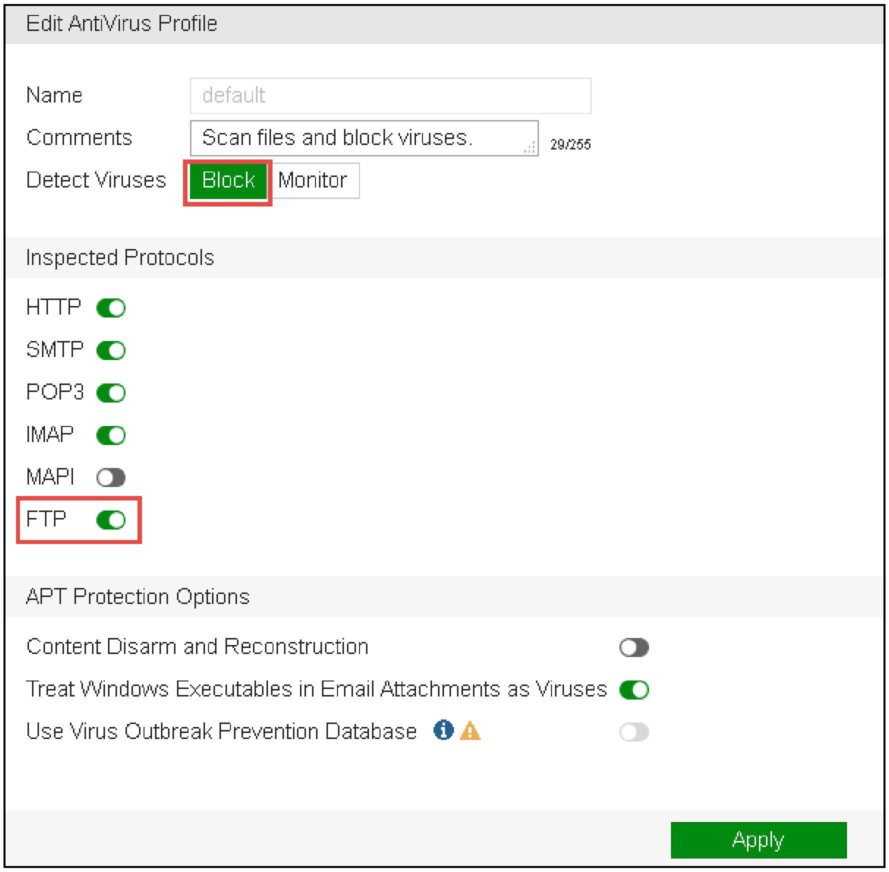
To review the antivirus profile in proxy-based inspection mode

1. Continuing on the Local-FortiGate GUI, click **Dashboard** > **Main**.
   You will notice that in **System Information** widget, the **Mode** is set to **NAT (Proxy-based)**.

If you do not see the mode set to **NAT (Proxy-based)** in the system information widget, please refresh your browser.

2. Click **Security Profiles** > **AntiVirus**, and select the **default** antivirus profile.
3. Verify that **Detect Viruses** is set to **Block** and, in the **Inspected Protocols** section, make sure the **FTP** switch is turned on.

   This profile defines the behavior for virus scanning on the traffic that matches policies using that profile.



Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

Detect Viruses: Block | Monitor

Inspected Protocols

HTTP: on

SMTP: on

POP3: on

IMAP: on

MAPI: off

FTP: on

APT Protection Options

Content Disarm and Reconstruction: off

Treat Windows Executables in Email Attachments as Viruses: on

Use Virus Outbreak Prevention Database: off

Enable the Antivirus Profile on a Firewall Policy

Now that the antivirus profile is configured, you must enable the antivirus profile on the firewall policy. After you enable the antivirus profile on a firewall policy, it can scan for viruses and generate logs (based on configured log settings).

To enable an antivirus profile on a firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Right-click the **ID** column for the **Full_Access** firewall policy and click **Edit**.
3. Under the **Security Profiles** section, verify that the default profile for **AntiVirus** is applied.

When selecting an antivirus profile, **Proxy Options** and **SSL/SSH Inspection** are automatically enabled. You can't disable **Proxy Options** or **SSL/SSH Inspection**, but you can select any preconfigured profiles in the **Proxy Options** and **SSL/SSH Inspection** drop-down menus.

4. Beside the **Proxy Options** profile, click the pencil icon to view the profile on the firewall policy tab.

   Alternatively, click **Security Profiles** > **Proxy Options** to see the **default** proxy options profile selected in the firewall policy.

   This profile specifies how FortiGate's proxies pick up protocols. For example, The FTP listening port is set to port 21.

Test the Proxy-Based Antivirus Profile

Now, you will test the proxy-based antivirus profile using FTP file transfer.

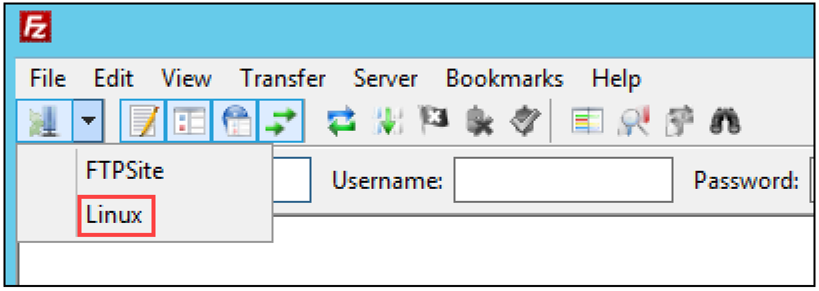
Take the Expert Challenge!

- On the Local-Windows VM desktop, use the FileZilla FTP client to connect to the **Linux** preconfigured profile under Site Manager.
- Leave the username and password fields empty.
- Download the `eicar.com` file from the FTP server.
- View the relevant logs on the Local-FortiGate GUI, and identify the action taken as a result of the scanning.

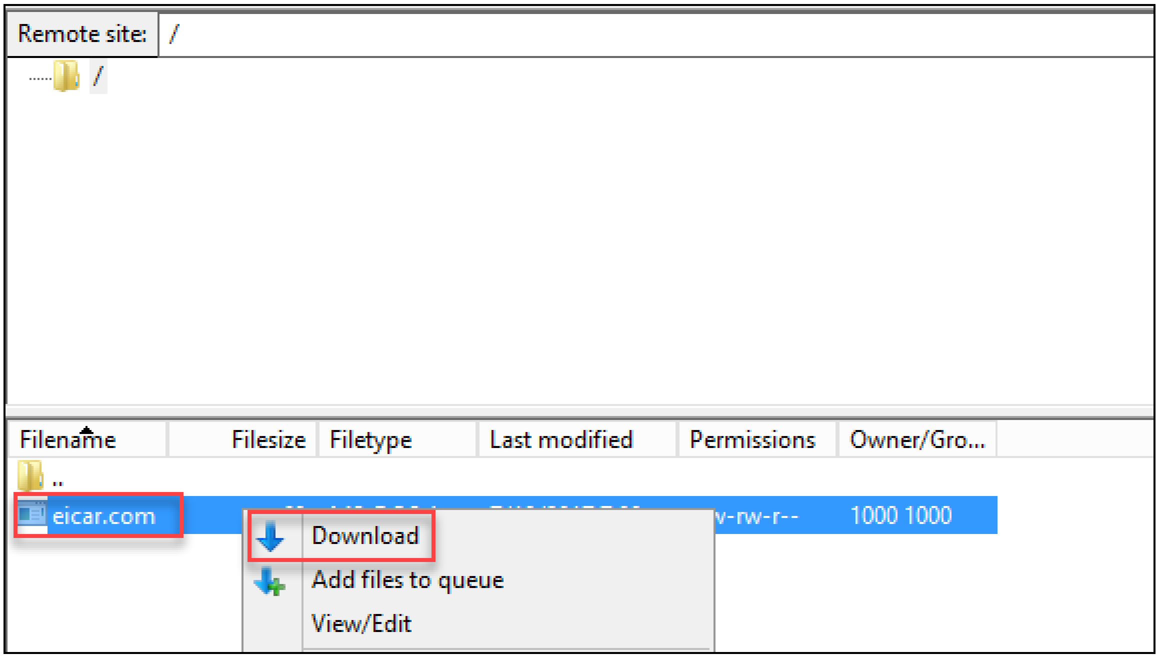
If you require assistance, or to verify your work, the step-by-step instructions are provided below.

To test the antivirus configuration

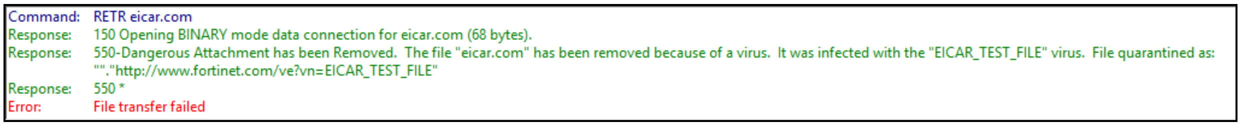
1. Continuing on the Local-Windows VM, open the FileZilla FTP client software from the desktop.
2. Click the Site Manager icon in the upper-left corner and Select **Linux**.



3. On the **Remote site** side of the application (right), right-click the **eicar.com** file, and then select **Download**.



The client should display an error message that the server aborted the connection. FortiGate sends the replacement message as a server response.



```
Command:   RETR eicar.com
Response:  150 Opening BINARY mode data connection for eicar.com (68 bytes).
Response:  550-Dangerous Attachment has been Removed.  The file "eicar.com" has been removed because of a virus.  It was infected with the "EICAR_TEST_FILE" virus.  File quarantined as:
           ""."http://www.fortinet.com/ve?vn=EICAR_TEST_FILE"
Response:  550 *
Error:     File transfer failed
```

In proxy-based inspection mode, FortiGate buffers the file to scan the content before sending the file or a replacement message to the client.

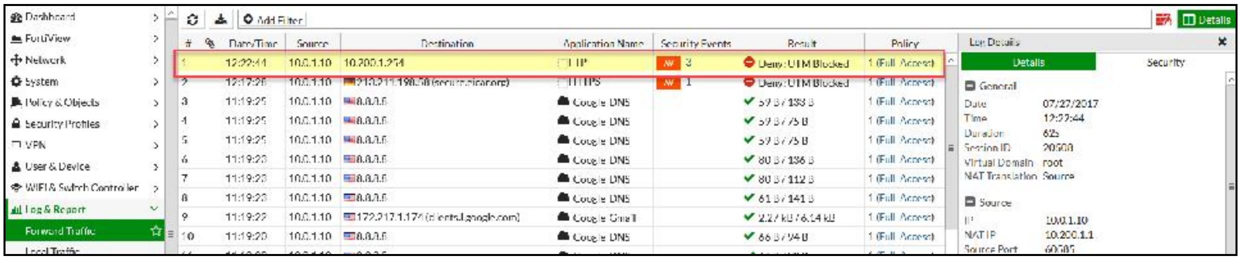
4. Close the FileZilla FTP client.

View the Antivirus Logs

Now, you will check and confirm the logs for the test you just performed.

To view the antivirus logs

1. Return to your browser tab where you are logged in to the Local-FortiGate GUI, and click **Log & Report** > **Forward Traffic**.
2. Locate the antivirus logs message from when you tried to access the file from the FTP, and double-click the log entry to view the details.



#	Date/Time	Source	Destination	Application Name	Security Events	Result	Policy
1	12:22:44	10.0.1.10	10.200.1.254	FTP	AV 3	Deny: UTM Blocked	1 (Full Access)
2	12:17:26	10.0.1.10	213.211.198.58 (secure.eicar.org)	HTTPS	AV 1	Deny: UTM Blocked	1 (Full Access)
3	11:19:25	10.0.1.10	8.8.8.8	Google DNS		✓ 59 B / 133 B	1 (Full Access)
4	11:19:25	10.0.1.10	8.8.8.8	Google DNS		✓ 59 B / 75 B	1 (Full Access)
5	11:19:25	10.0.1.10	8.8.8.8	Google DNS		✓ 59 B / 75 B	1 (Full Access)
6	11:19:23	10.0.1.10	8.8.8.8	Google DNS		✓ 80 B / 136 B	1 (Full Access)
7	11:19:23	10.0.1.10	8.8.8.8	Google DNS		✓ 80 B / 112 B	1 (Full Access)
8	11:19:23	10.0.1.10	8.8.8.8	Google DNS		✓ 61 B / 141 B	1 (Full Access)
9	11:19:22	10.0.1.10	172.217.1.174 (clients1.google.com)	Google Gmail		✓ 2.27 kB / 76.14 kB	1 (Full Access)
10	11:19:20	10.0.1.10	8.8.8.8	Google DNS		✓ 66 B / 94 B	1 (Full Access)

General

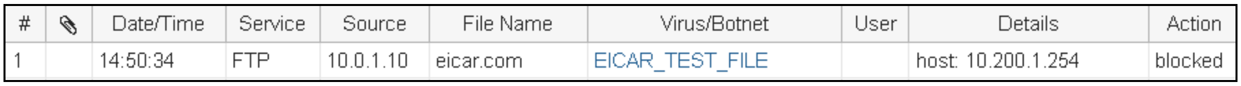
Date	07/27/2017
Time	12:22:44
Duration	62s
Session ID	20900
Virtual Domain	root
NAT Translation	Source

Source

IP	10.0.1.10
NAT IP	10.200.1.1
Source Port	60505

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

3. To view security log information, do one of the following:
   - Select the **Security** tab. This includes information more specific to the security event, such as file name, virus/botnet, reference, and so on.
   - Click **Log & Report** > **AntiVirus**.



#	📎	Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action
1		14:50:34	FTP	10.0.1.10	eicar.com	EICAR_TEST_FILE		host: 10.200.1.254	blocked

Lab 10: Intrusion Prevention System (IPS) and Denial of Service (DoS)

In this lab, you will set up IPS profiles and denial of service (DoS) policies. You will also use a vulnerability scanner and a custom script to generate attacks on Local-FortiGate.

Objectives

- Protect your network against known attacks using IPS signatures.
- Use rate based signatures to block brute force attacks.
- Mitigate and block DoS attacks.

Time to Complete

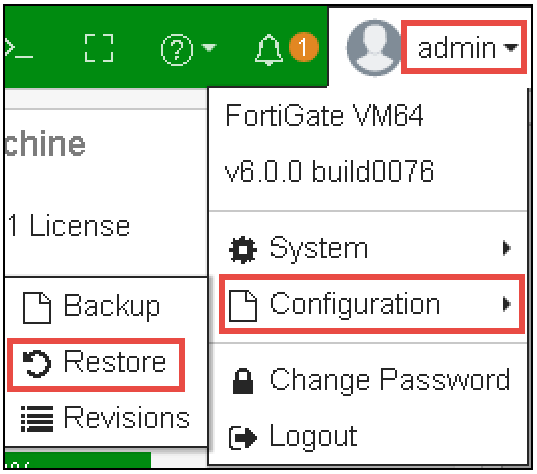
Estimated: 30 minutes

Prerequisites

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

To restore the Local-FortiGate configuration file

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, in the **admin** drop-down menu, select **Configuration** > **Restore**.



3. Select **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **Intrusion-Prevention-System** > `local-intrusion-prevention-system.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Blocking Known Exploits

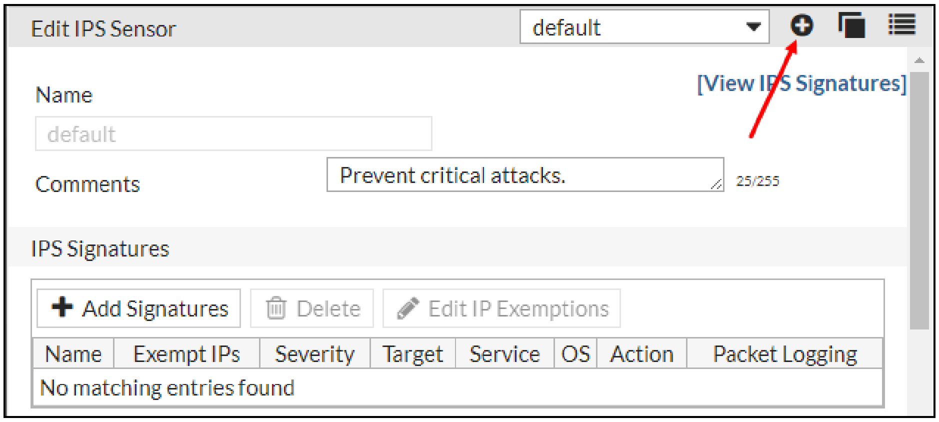
During this exercise, you will configure IPS inspection on Local-FortiGate.

Configure IPS Inspection

First, you will configure an IPS sensor that includes the signatures for known attacks on Windows operating systems.

To configure IPS

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Security Profiles** > **Intrusion Prevention**.
3. In the upper-right corner, click the plus (**+**) icon to create a new sensor.



Edit IPS Sensor — default

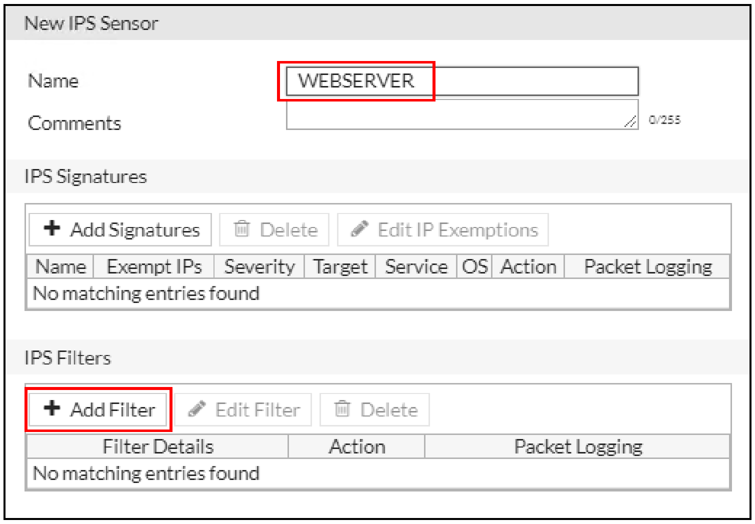
Name: default

Comments: Prevent critical attacks. 25/255

IPS Signatures

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
No matching entries found							

4. In the **Name** field, type `WEBSERVER` for the new sensor name.
5. In the **IPS Filters** section, click **Add Filter**.



New IPS Sensor

Name: WEBSERVER

Comments: 0/255

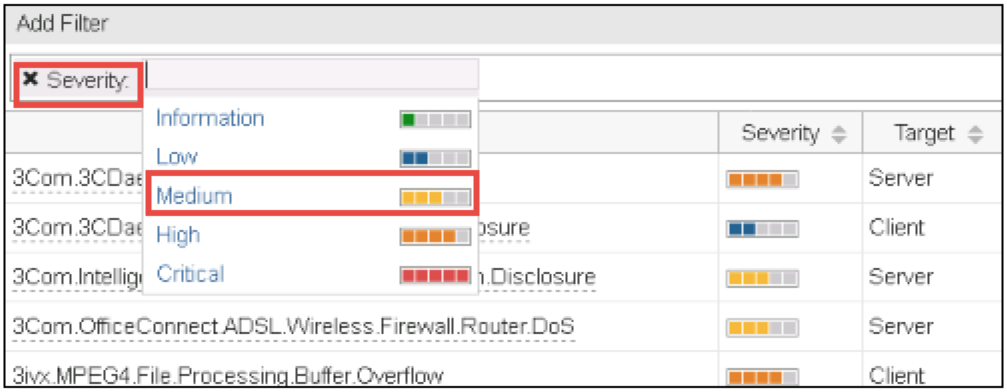
IPS Signatures

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
No matching entries found							

IPS Filters

Filter Details	Action	Packet Logging
No matching entries found		

6. In the **Add Filter** window, click **Add Filter**.
7. Click **Severity** and then click **Medium**:



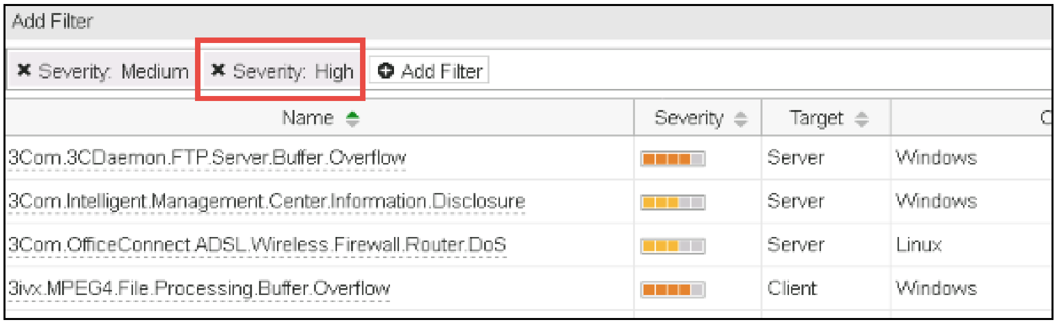
Add Filter

✖ Severity:

- Information 🟩⬜⬜⬜⬜
- Low 🟦🟦⬜⬜⬜
- Medium 🟨🟨🟨⬜⬜
- High 🟧🟧🟧🟧⬜
- Critical 🟥🟥🟥🟥🟥

	Severity	Target
3Com.3CDae	🟧🟧🟧🟧⬜	Server
3Com.3CDae osure	🟦🟦⬜⬜⬜	Client
3Com.Intellig n.Disclosure	🟨🟨🟨⬜⬜	Server
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	🟨🟨🟨⬜⬜	Server
3ivx.MPEG4.File.Processing.Buffer.Overflow	🟧🟧🟧🟧⬜	Client

8. Click **Add Filter** again.
9. Click **Severity** and then click **High:**

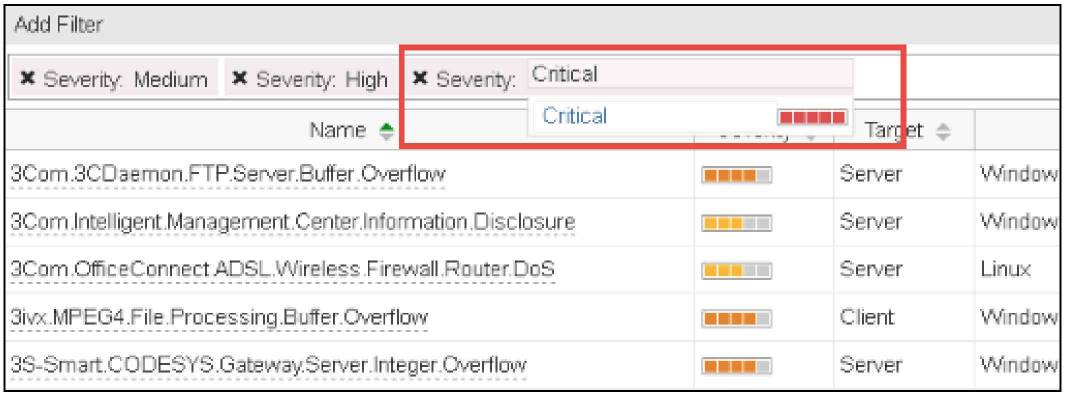


Add Filter

✖ Severity: Medium ✖ Severity: High ⊕ Add Filter

Name	Severity	Target	O
3Com.3CDaemon.FTP.Server.Buffer.Overflow	🟧🟧🟧🟧⬜	Server	Windows
3Com.Intelligent.Management.Center.Information.Disclosure	🟨🟨🟨⬜⬜	Server	Windows
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	🟨🟨🟨⬜⬜	Server	Linux
3ivx.MPEG4.File.Processing.Buffer.Overflow	🟧🟧🟧🟧⬜	Client	Windows

10. Click **Add Filter** one more time.
11. Click **Severity** and then click **Critical**:



Add Filter

✖ Severity: Medium ✖ Severity: High ✖ Severity: Critical

- Critical 🟥🟥🟥🟥🟥

Name	Severity	Target	
3Com.3CDaemon.FTP.Server.Buffer.Overflow	🟧🟧🟧🟧⬜	Server	Window
3Com.Intelligent.Management.Center.Information.Disclosure	🟨🟨🟨⬜⬜	Server	Window
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	🟨🟨🟨⬜⬜	Server	Linux
3ivx.MPEG4.File.Processing.Buffer.Overflow	🟧🟧🟧🟧⬜	Client	Window
3S-Smart.CODESYS.Gateway.Server.Integer.Overflow	🟧🟧🟧🟧⬜	Server	Window

12. Click **Use Filters**.

    All the signatures matching the filter are added to the IPS sensor and FortiGate will take the default action for these signatures.

13. Click **OK**.
14. Click **Apply**.

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 Local-Windows.

Take the Expert Challenge!

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

- Configure a new virtual IP to map the external IP `10.200.1.200` to the internal IP `10.0.1.10`, using **port1** as the external interface. Name the virtual IP `VIP-WEB-SERVER`.
- Create a new firewall policy to allow all inbound traffic to the virtual IP and enable the **WEBSERVER** IPS sensor. Name the firewall policy `Web_Server_Access_IPS`.

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

After you complete the challenge, see Generate Attacks from the Linux Server on page 167

To create a virtual IP

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

Field	Value
Name	VIP-WEB-SERVER
Interface	port1
External IP Address/Range	10.200.1.200
Mapped IP Address/Range	10.0.1.10

4. Click **OK**.

To configure a firewall policy

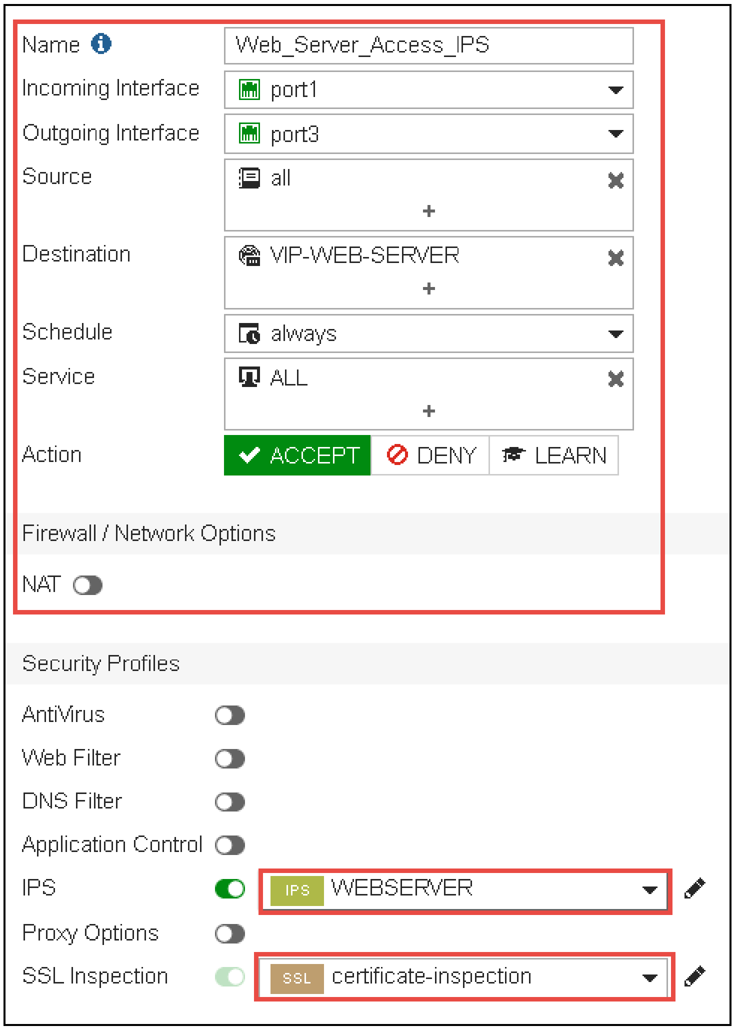
1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Click **Create New** and create a new firewall policy using the following settings:

Field	Value
Name	Web_Server_Access_IPS
Incoming Interface	port1

Field	Value
Outgoing Interface	port3
Source	all
Destination	VIP-WEB-SERVER
Schedule	always
Service	ALL
Action	ACCEPT
NAT	disabled

3. In the **Security Profiles** section, enable **IPS**, and from the drop-down list, select **WEBSERVER**.

   The policy should look like the following example:



Name: Web_Server_Access_IPS

Incoming Interface: port1

Outgoing Interface: port3

Source: all

Destination: VIP-WEB-SERVER

Schedule: always

Service: ALL

Action: ✓ ACCEPT | DENY | LEARN

Firewall / Network Options

NAT ○

Security Profiles

AntiVirus ○

Web Filter ○

DNS Filter ○

Application Control ○

IPS ● IPS WEBSERVER

Proxy Options ○

SSL Inspection ● SSL certificate-inspection

Configuring full SSL inspection would significantly increase the time required to complete this lab. Therefore, for the purposes of this exercise, you will not configure full SSL inspection.

4. Click **OK**.

Generate Attacks from the Linux Server

You will run a Perl script to generate attacks from the Linux server located in front of the Local-FortiGate.

To generate attacks from the Linux server

1. Continuing on Local-Windows, open PuTTY and connect over SSH to the **LINUX** saved session.
2. At the login prompt, enter the user name `student` with the password `password`.
3. Run the following script to start the attacks:
   ```
   nikto.pl -host 10.200.1.200
   ```
4. Leave the PuTTY session open (you can minimize it) so traffic continues to generate.

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

Monitor the IPS

You will check the IPS logs to monitor for known attacks being detected and dropped by Local-FortiGate.

Take the Expert Challenge!

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

- Review the IPS logs for all detected and dropped attacks.
- Review the FortiGuard encyclopedia pages.

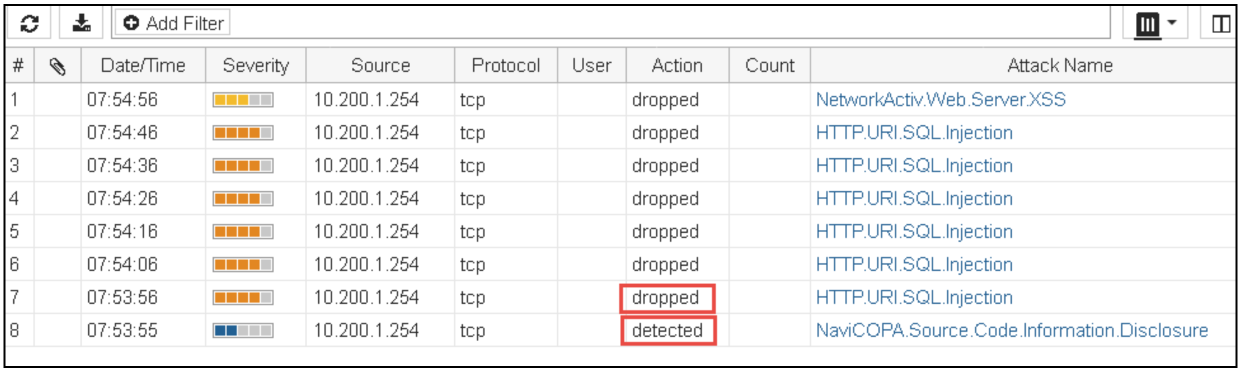
If you require assistance, or to verify your work, use the step-by-step instructions that follow.

To monitor the IPS

1. Return to your browser tab where you are logged in to the Local-FortiGate GUI, and click **Log & Report** > **Intrusion Prevention**.

The IPS logs section will not display if there are no IPS logs. FortiGate displays this section only after creating logs. After the attacks, if the Intrustion Prevention menu item does not display in the GUI, refresh your browser or log out of the Local-FortiGate GUI and log back in again.

2. Locate and review the relevant log entries for the detected and dropped attacks.

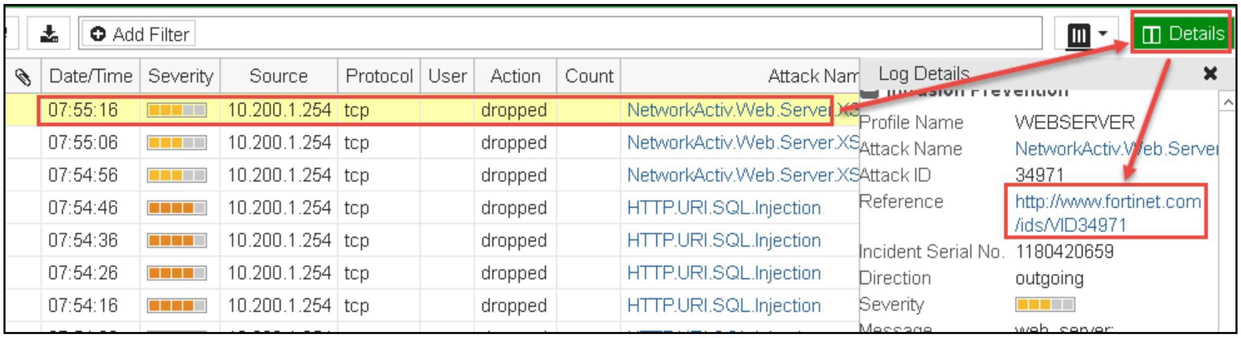


#		Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
1		07:54:56	■■■□□	10.200.1.254	tcp		dropped		NetworkActiv.Web.Server.XSS
2		07:54:46	■■■■□	10.200.1.254	tcp		dropped		HTTP.URI.SQL.Injection
3		07:54:36	■■■■□	10.200.1.254	tcp		dropped		HTTP.URI.SQL.Injection
4		07:54:26	■■■■□	10.200.1.254	tcp		dropped		HTTP.URI.SQL.Injection
5		07:54:16	■■■■□	10.200.1.254	tcp		dropped		HTTP.URI.SQL.Injection
6		07:54:06	■■■■□	10.200.1.254	tcp		dropped		HTTP.URI.SQL.Injection
7		07:53:56	■■■■□	10.200.1.254	tcp		dropped		HTTP.URI.SQL.Injection
8		07:53:55	■■□□□	10.200.1.254	tcp		detected		NaviCOPA.Source.Code.Information.Disclosure

FortiGate will create an intrusion prevention log entry for each:

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

3. Click a log entry, and then click **Details**.
4. Click the **Reference** link:



	Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Narr
	07:55:16	■■■□□	10.200.1.254	tcp		dropped		NetworkActiv.Web.Server.XS
	07:55:06	■■■□□	10.200.1.254	tcp		dropped		NetworkActiv.Web.Server.XS
	07:54:56	■■■□□	10.200.1.254	tcp		dropped		NetworkActiv.Web.Server.XS
	07:54:46	■■■■□	10.200.1.254	tcp		dropped		HTTP.URI.SQL.Injection
	07:54:36	■■■■□	10.200.1.254	tcp		dropped		HTTP.URI.SQL.Injection
	07:54:26	■■■■□	10.200.1.254	tcp		dropped		HTTP.URI.SQL.Injection
	07:54:16	■■■■□	10.200.1.254	tcp		dropped		HTTP.URI.SQL.Injection

Profile Name	WEBSERVER
Attack Name	NetworkActiv.Web.Server
Attack ID	34971
Reference	http://www.fortinet.com /ids/VID34971
Incident Serial No.	1180420659
Direction	outgoing
Severity	■■■□□
Message	web_server:

5. Review the FortiGuard encyclopedia pages for the signatures.

The FortiGuard encyclopedia provides information about that signature such as severity, coverage, affected products, impact, and recommended actions that you can take.

None of the affected products are currently installed on Local-Windows. This information is important to make note of before you tune the **WEBSERVER** IPS sensor. If the affected products aren't installed, is it really necessary to inspect those packets?

Exercise 2: Using Rate Based IPS Signatures

In this exercise you will configure a rate based signature to detect and block a brute force FTP attack.

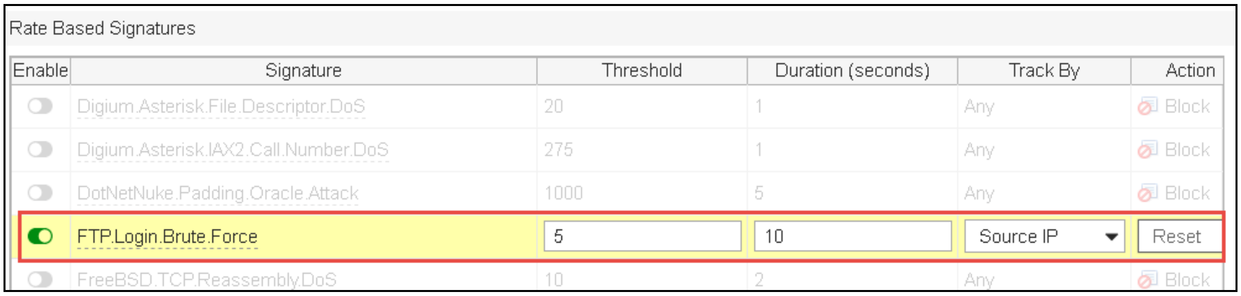
Apply Rate Based Signatures

You will create a new IPS sensor, then enable and configure the appropriate signature to detect and block FTP brute-force attacks. You will then apply the IPS sensor to all outbound traffic on Local-FortiGate.

To create an IPS sensor

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Security Profiles** > **Intrusion Prevention**.
3. Click the plus (**+**) icon in the top right of the page to create a new sensor.
4. In the **Name** field, type `FTP_BRUTE_FORCE`.
5. In the **Rate Based Signatures** table, enable the **FTP.Login.Brute.Force** signature.
6. Double-click the signature and configure the following values:

Field	Value
Threshold	5
Track By	Source IP
Action	Reset



Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action
○	Digium.Asterisk.File.Descriptor.DoS	20	1	Any	Block
○	Digium.Asterisk.IAX2.Call.Number.DoS	275	1	Any	Block
○	DotNetNuke.Padding.Oracle.Attack	1000	5	Any	Block
●	FTP.Login.Brute.Force	5	10	Source IP	Reset
○	FreeBSD.TCP.Reassembly.DoS	10	2	Any	Block

7. Click **OK**.

To apply IPS on outbound traffic

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Double-click the existing **Full_Access** policy to edit it.
3. In the **Security Profiles** section, enable **IPS**, and in the drop-down list, select **FTP_BRUTE_FORCE**.
4. Click **OK**.

Test the Rate Based Signature

You will use a custom Windows batch script to generate invalid login attempts to the FTP server located on the Linux VM. You will then verify your configuration using the IPS logs.

A typical brute-force attack makes use of a dictionary of usernames and passwords. In this scenario, the script is using an incorrect username and password to flood the FTP server with invalid login attempts. The `530 Login incorrect` responses from the FTP server should be enough to trigger the signature.

To run the Windows batch script

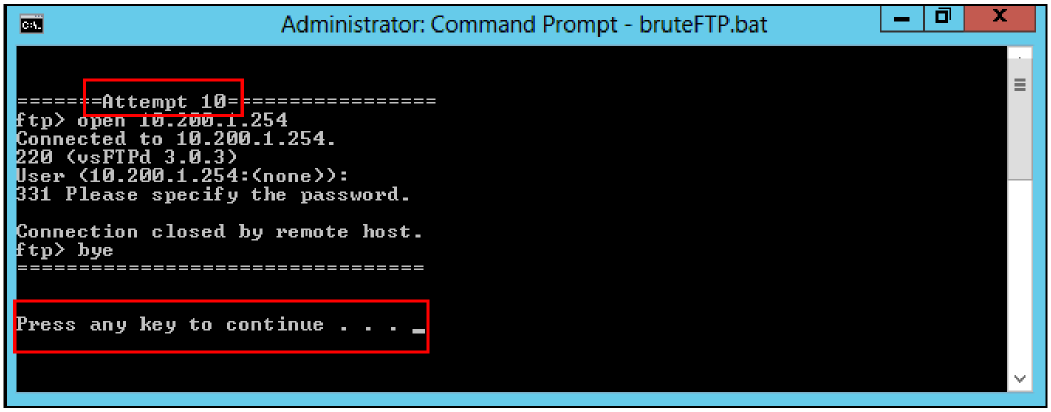
1. Continuing on the Local-Windows VM, open a command prompt window.
2. Change the working directory to `Resources\FortiGate-Security\Intrusion-Prevention-System`:

```
>cd Desktop
>cd Resources
>cd FortiGate-Security
>cd Intrusion-Prevention-System
```

3. Execute the Windows batch script:

```
bruteFTP
```

4. Wait for the script to finish running all 10 attempts, and then press any key to stop the script.

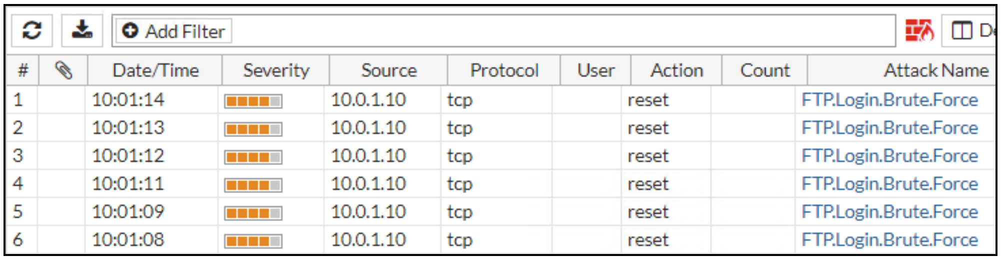


```
=======Attempt 10=================
ftp> open 10.200.1.254
Connected to 10.200.1.254.
220 (vsFTPd 3.0.3)
User (10.200.1.254:(none)):
331 Please specify the password.

Connection closed by remote host.
ftp> bye
================================

Press any key to continue . . . _
```

5. Leave the command prompt window open in the background.

To view the IPS logs

1. Return to the browser tab where you are logged in to the Local-FortiGate GUI, and click **Log & Report** > **Intrusion Prevention**.
2. Locate the logs for the FTP brute force attacks:



#	📎	Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
1		10:01:14	■■■■	10.0.1.10	tcp		reset		FTP.Login.Brute.Force
2		10:01:13	■■■■	10.0.1.10	tcp		reset		FTP.Login.Brute.Force
3		10:01:12	■■■■	10.0.1.10	tcp		reset		FTP.Login.Brute.Force
4		10:01:11	■■■■	10.0.1.10	tcp		reset		FTP.Login.Brute.Force
5		10:01:09	■■■■	10.0.1.10	tcp		reset		FTP.Login.Brute.Force
6		10:01:08	■■■■	10.0.1.10	tcp		reset		FTP.Login.Brute.Force

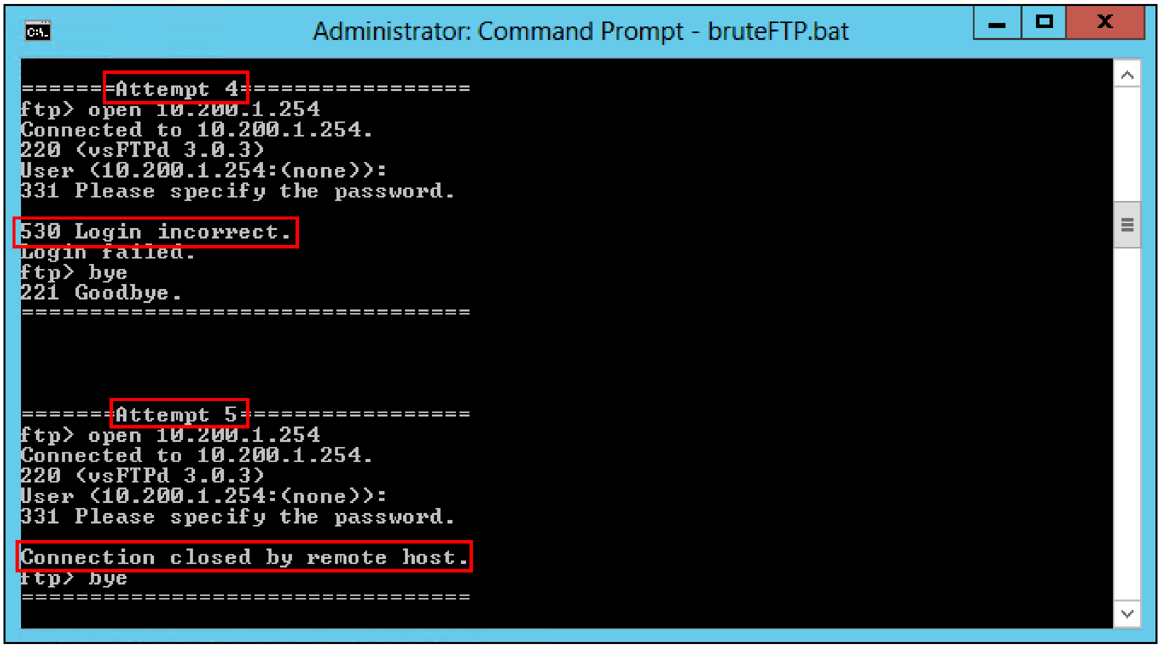
Why are there only six log entries, when the script generated 10 login attempts?

Stop and think!

The **FTP.Login.Brute.Force** rate based signature was configured with a threshold of five. The IPS signature action only triggered after the threshold was met.

To verify the IPS signature action

1. Continuing on the Local-Windows VM, go back to the command prompt window.
2. Scroll up and locate **Attempt 4** and **Attempt 5**.



```
======Attempt 4=================
ftp> open 10.200.1.254
Connected to 10.200.1.254.
220 (vsFTPd 3.0.3)
User (10.200.1.254:(none)):
331 Please specify the password.

530 Login incorrect.
Login failed.
ftp> bye
221 Goodbye.
=================================



======Attempt 5=================
ftp> open 10.200.1.254
Connected to 10.200.1.254.
220 (vsFTPd 3.0.3)
User (10.200.1.254:(none)):
331 Please specify the password.

Connection closed by remote host.
ftp> bye
=================================
```

Note that for **Attempt 4**, the server response is `530 Login incorrect`. However, for **Attempt 5**, the error message is `Connection closed by remote host`. This is where the rate based signature's action triggers, and the FTP client's connections are reset. This `Connection closed by remote host` message repeats until the script ends with **Attempt 10**.

3. Close the command prompt window.

Exercise 3: Mitigating a DoS Attack

In this exercise, you will configure the Local-FortiGate for DoS protection.

Create a DoS Policy

You will create a DoS policy to detect and block an icmp flood attack

Take the Expert Challenge!

On the Local-FortiGate GUI (`10.0.1.254` | `admin`/ **password**), do the following:

- Create a new IPv4 DoS policy for **port1**.
- Configure the policy to block ICMP floods with a threshold of 200.
- Enable logging.

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

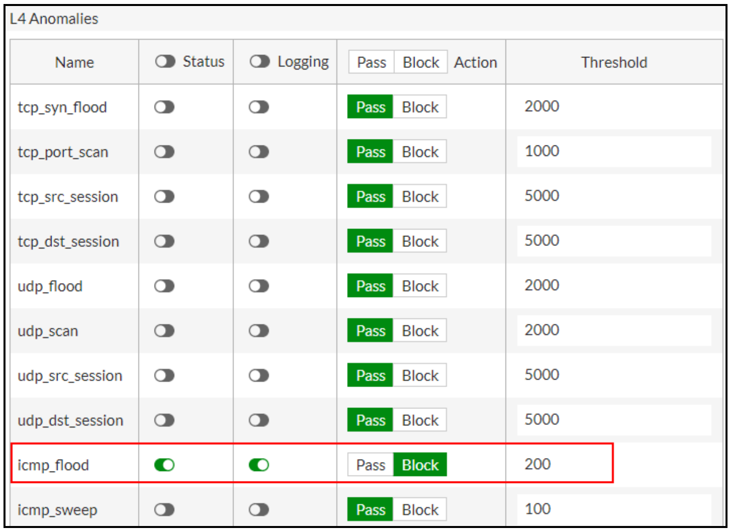
After you complete the challenge, see Test the DoS Policy on page 173.

To create a DoS policy

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Policy & Objects** > **IPv4 DoS Policy**.
3. Click **Create New**.
4. Configure the following settings:

Field	Value
Incoming Interface	port1
Source Address	all
Destination Address	all
Services	ALL

5. Locate **icmp_flood**, and enable **Status** and **Logging**.
6. Set the **Action** to **Block** and the **Threshold** to `200`.



L4 Anomalies

Name	○ Status	○ Logging	Pass Block Action	Threshold
tcp_syn_flood	○	○	[✓ Pass] Block	2000
tcp_port_scan	○	○	[✓ Pass] Block	1000
tcp_src_session	○	○	[✓ Pass] Block	5000
tcp_dst_session	○	○	[✓ Pass] Block	5000
udp_flood	○	○	[✓ Pass] Block	2000
udp_scan	○	○	[✓ Pass] Block	2000
udp_src_session	○	○	[✓ Pass] Block	5000
udp_dst_session	○	○	[✓ Pass] Block	5000
icmp_flood	●	●	Pass [✓ Block]	200
icmp_sweep	○	○	[✓ Pass] Block	100

7. Click **OK**.

Test the DoS Policy

You will generate an ICMP flood from the Linux VM. This will trigger the DoS policy on Local-FortiGate.

To test the DoS policy

1. Continuing on the Local-Windows VM, open PuTTY and connect over SSH to the **LINUX** saved session.
2. At the login prompt, enter the user name `student` with a password of `password`.
3. Execute the following command to generate an ICMP flood to Local-FortiGate:

```
sudo ping -f 10.200.1.1
```

   A password prompt for the `student` account is displayed

The command option `-f` causes the ping utility to run continuously, and not wait for replies between ICMP echo requests. It also requires super-user privilege.

4. Enter `password`.

   For every ping sent, the SSH session will display a period.

5. Leave the SSH connection open with the ping running (you can minimize the window).

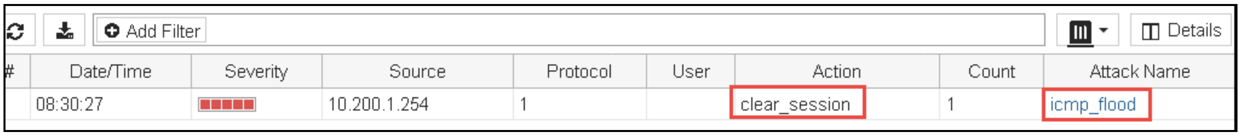
To view the anomaly logs

1. Return to the browser where you are logged in to the Local-FortiGate GUI, and press F5 to refresh the browser (or log out and log in).
2. Click **Log & Report** > **Anomaly**.

The **Anomaly** logs section will not display if there are no anomaly logs. If the **Anomaly** menu item does not display in the GUI, refresh the browser or log out from the Local-FortiGate GUI and log back in again.

3. Examine the logs.

   Note that the ICMP flood has been blocked. This is indicated by the entry **clear_session** in the **Action** field.



#	Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
	08:30:27	■■■■■	10.200.1.254	1		clear_session	1	icmp_flood

4. Go back to the PuTTY window and press Ctrl+C to stop the ping.
5. Close the PuTTY session.

Lab 11: SSL-VPN

In this lab, you will configure an SSL-VPN connection in tunnel and web modes. 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.
- Customize the SSL-VPN portal for web mode.
- Configure FortiClient for the SSL-VPN connection in tunnel mode.

Time to Complete

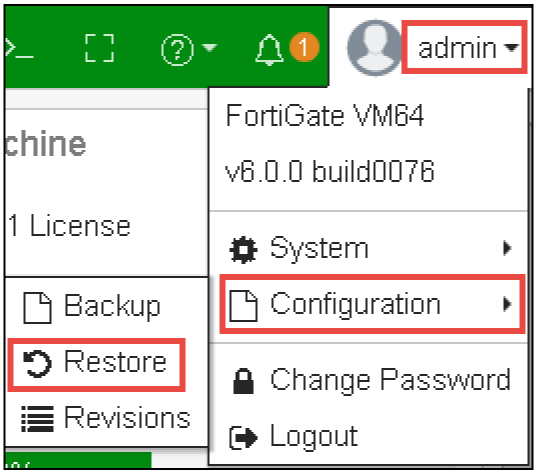
Estimated: 25 minutes

Prerequisites

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

To restore the Local-FortiGate configuration file

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **SSL-VPN** > **local-SSL-VPN.conf**, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

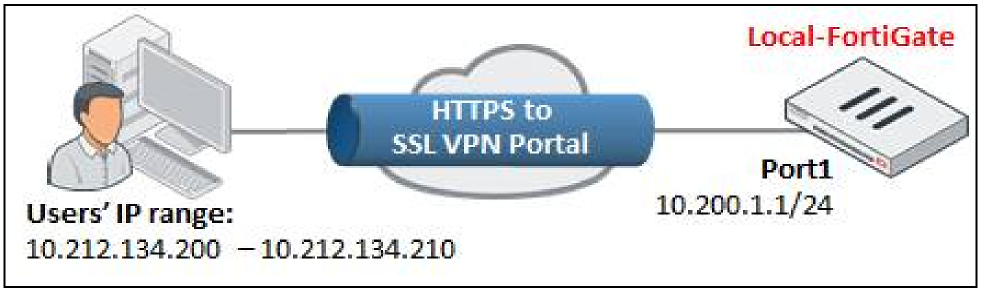
Exercise 1: Configuring Web Mode SSL-VPN

On FortiGate, there are two modes you can configure to allow remote access through SSL-VPN: web mode and tunnel.

In this exercise, you will test web mode, which will allow SSL-VPN users to connect from the Remote-Windows VM, to resources located in the local subnet (`10.0.1.0/24`).

Configure the SSL-VPN Settings

Now, you will configure the SSL-VPN settings to allow the remote connection shown in the following example:



To create a user for SSL-VPN connections

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **User & Device** > **User Definition**.
3. Click **Create New**.
4. Click **Local User**, and then click **Next**.
5. Enter the following credentials for the remote user, and then click **Next**:

Username	student
Password	fortinet

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

The group **SSL_VPN_USERS** has been preconfigured for the purpose of this lab.

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

To configure the SSL-VPN settings for web access

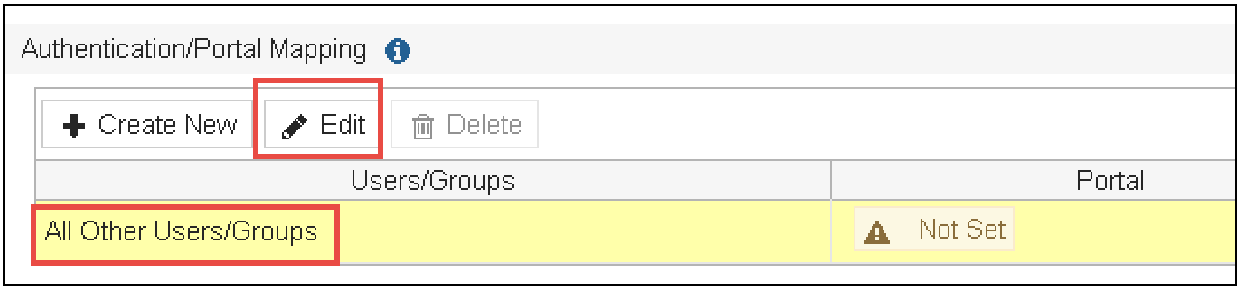
1. Continuing on the Local-FortiGate GUI, click **VPN** > **SSL-VPN Settings**.
2. In the **Connection Settings** section, configure the following settings:

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

3. In the **Tunnel Mode Client Settings** section, configure the following settings:

Field	Value
Access Range	Automatically assign addresses

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



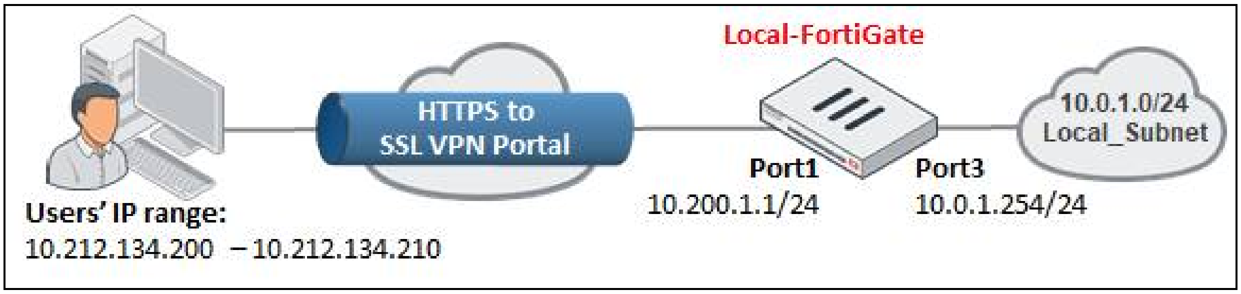
Users/Groups	Portal
All Other Users/Groups	⚠ Not Set

5. In the **Portal** drop-down list, select **web-access**, and then click **OK**.
6. Click **Apply** to save the changes.
7. Click **OK** to confirm the use of the built-in certificate.

   Notice the warning message displayed on the top of this page. It indicates that you need to create a firewall policy for SSL-VPN connections.

Create a Firewall Policy for SSL-VPN

Now, 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 portal.



To create a firewall policy for SSL-VPN

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 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
NAT	Disabled

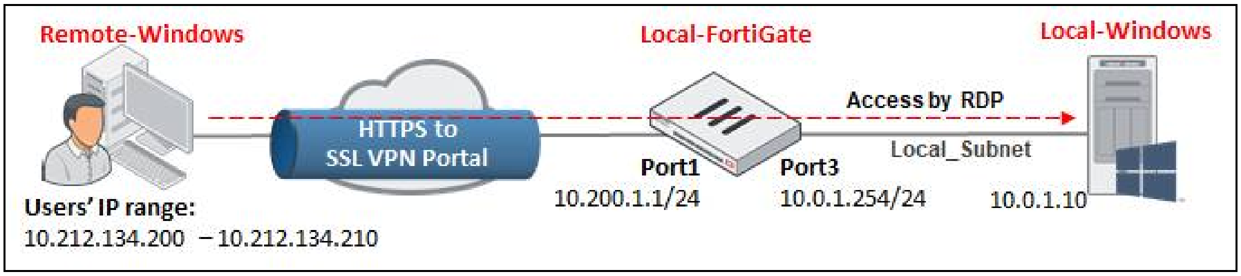
3. Click **OK**.
4. Click **OK** to confirm the use of the built-in certificate.

The SSL-VPN firewall policy will only allow traffic from users within the group **SSL_VPN_Users**.

Test the SSL-VPN Access

Now, you will test the SSL-VPN by accessing resources remotely within the local subnet (`10.0.1.0/24`).

For this, you will connect to the SSL-VPN portal using the Remote-Windows VM, and then you'll perform an RDP connection to the Local-Windows VM.



To access the SSL-VPN portal

1. In your lab environment, connect to the Remote-Windows VM.
2. Open Firefox and connect to:

   `https://10.200.1.1:10443/`

   A security warning appears.

Stop and think!

Why do you receive a security warning?

For SSL connections, FortiGate is using a built-in certificate, which is signed by a certificate authority that the browser does not trust.

3. Click **Advanced**, click **Add Exception**, and then click **Confirm Security Exception**.

   The remote login page opens.
4. Log in as `student` with the password `fortinet`.

   The SSL-VPN web portal opens. The portal is using default settings.

To test the SSL-VPN portal

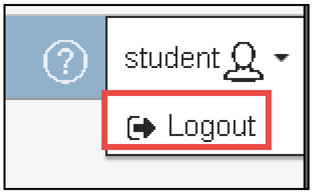
1. Continuing on the SSL-VPN portal where you are logged in as `student`, click **Quick Connection**.

   Notice all the available options the SSL-VPN portal allows for connections.
2. Click **RDP**, and configure the following setting:

Field	Value
Host	10.0.1.10

3. Keep the default values for the remaining settings, and then click **Launch**.
4. Wait five seconds, and then click **TRAININGAD\Administrator** when it appears.
5. Enter the password `password`.

   You are now remotetly connected to the Local-Windows VM.
6. Close the web browser that is running the RDP session.
7. In the upper-right corner, click **student** > **Logout** to log out of the SSL VPN portal.



Add an Admin-Based Bookmark to the SSL-VPN Portal

In this exercise, you will customize the SSL-VPN portal with a new color and a predefined bookmark.

To customize the SSL-VPN Portal

1. Return to the Local-Windows VM.
2. In the left of the browser window, click **Virtual Keyboard** > **Send Ctrl-Alt-Del**.
3. Click the**TRAININGAD\Administrator** user account.
4. Enter the password `password`.
5. Open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
6. Click **VPN** > **SSL-VPN Portals**.
7. Select **web-access**, and then click **Edit**.
8. Configure the following settings:

Field	Value
Portal Message	My Portal
Theme	Red
Show Connection Launcher	<disable>
User Bookmarks	<disable>

9. In the **Predefined Bookmarks** section, click **Create New**, and then configure the following settings:

Field	Value
Name	Local-Windows VM
Type	HTTP/HTTPS
URL	http://10.0.1.10
Single Sign-On	Disabled

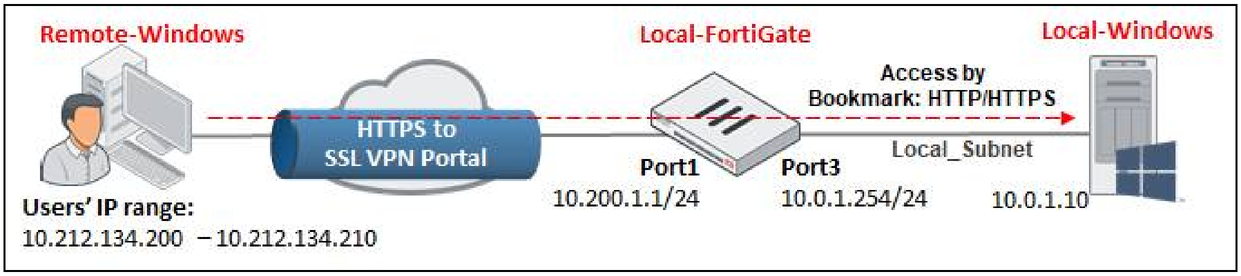
10. Click **OK**.
11. Click **OK** again to save the portal's settings.

Test SSL-VPN Access Using the Predefined Bookmark

Now, you will connect again to the SSL-VPN portal on the Remote-Windows VM to access the resources in the local subnet (`10.0.1.0/24`).

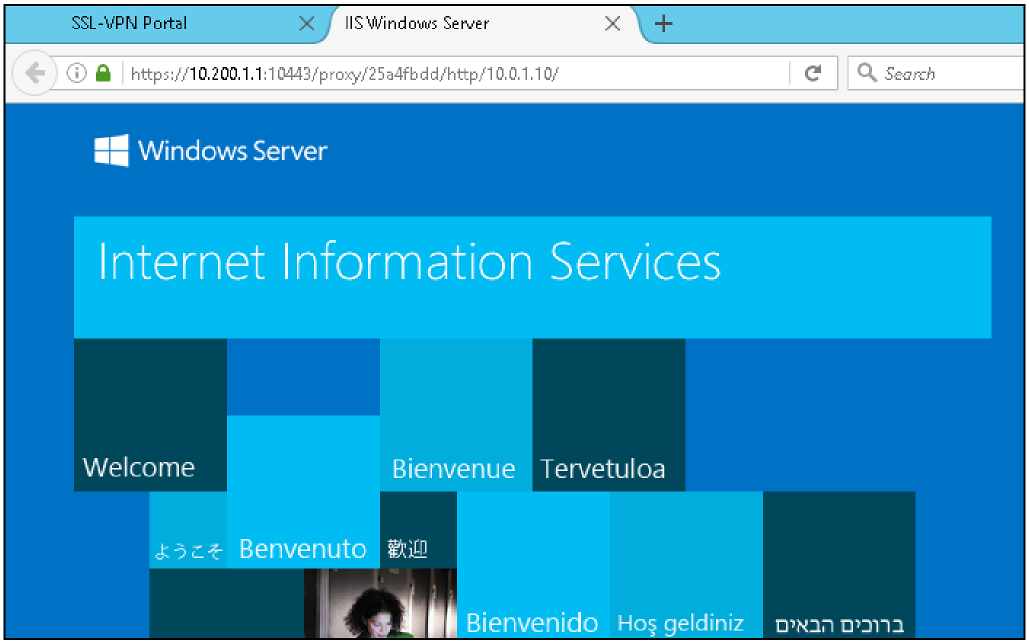
For this, you will access the Local-Windows VM using the predefined bookmark on the SSL-VPN Portal.

Notice that the SSL-VPN Portal looks different and provides fewer settings.



To test the bookmark

1. Return to the Remote-Windows VM.
2. Open Firefox, and then reconnect to the SSL VPN portal at:
   `https://10.200.1.1:10443/`
3. Log in using the username `student` with the password `fortinet`.
   Notice the SSL VPN portal no longer allows quick connections or to add bookmarks.
4. Click the **Local-Windows VM** bookmark.
   You will connect to the web server running on the Local-Windows VM at `10.0.1.10`.

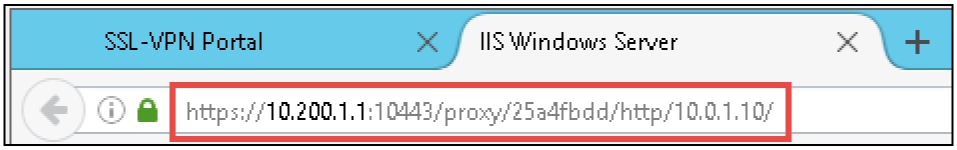


Examine the Web Mode Mechanism (Reverse HTTP Proxy)

Now, you will examine the reverse HTTP proxy mechanism, to learn how SSL-VPN connections in web mode work..

To examine the reverse HTTP proxy mechanism

1. Continuing on the Remote-Windows VM where you are connected to the web server running on the **Local-Windows** VM at `10.0.1.10`, examine the URL in the address bar.



https://10.200.1.1:10443/proxy/25a4fbdd/http/10.0.1.10/

If you were on the local network while accessing the website, the address would be `http://10.0.1.10`. But, because you are accessing it remotely through FortiGate's HTTP proxy, the URL is different.

Notice the URL structure in the browser's address bar:

```
https://10.200.1.1:10443/proxy/..../http/10.0.1.10/
```

What does it mean?

Part of the URL	Description
https://10.200.1.1:10443	Indicates that the connection is SSL/TLS-encrypted, and that the portal is on FortiGate's port1 SSL-VPN gateway.
/proxy/..../http/	Indicates that the connection is being handled by FortiGate's HTTP reverse proxy.
10.0.1.10/	Indicates the destination IP address of the website inside your private network, which you are accessing through the VPN.

FortiGate encrypts the connection to the browser, but the destination server's IP address in the URL is displayed in clear text, *not* hidden from users. The secondary connection, from FortiGate's HTTP proxy to the bookmarked website, is not encrypted.

Monitor an SSL-VPN User

Now, you will monitor and disconnect an SSL-VPN user from the FortiGate GUI.

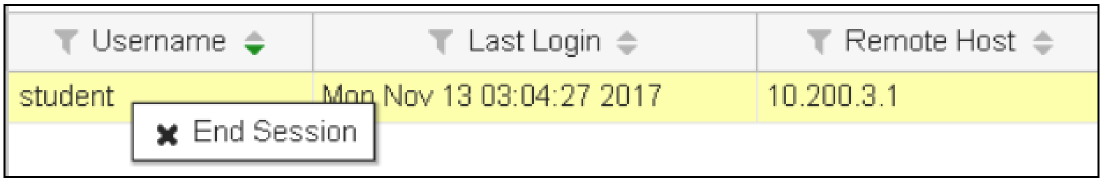
To monitor and disconnect an SSL-VPN user

1. Return to the Local-Windows VM where you are logged in to the Local-FortiGate GUI.
2. Click **Monitor** > **SSL-VPN Monitor**.

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

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

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



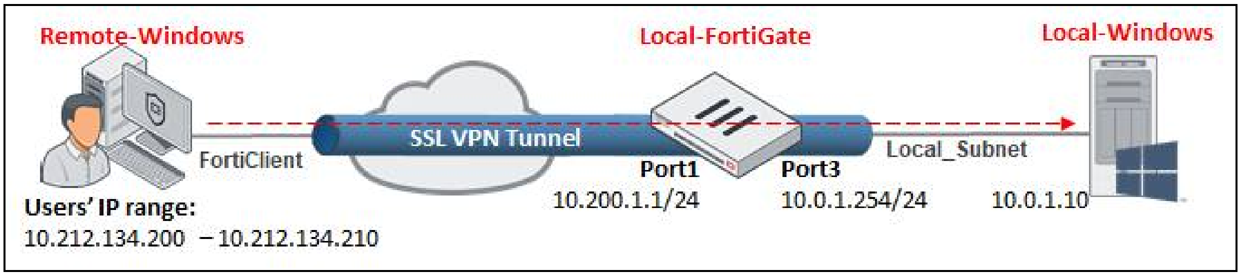
Username	Last Login	Remote Host
student	Mon Nov 13 03:04:27 2017	10.200.3.1

Exercise 2: Configuring SSL-VPN Tunnel Mode

In this exercise, you will 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-Windows VM.

You will use the remote access module of FortiClient 5.6.0, which supports Fortinet's SSL-VPN client.

FortiClient 5.6.0 is already installed on the Remote-Windows VM.



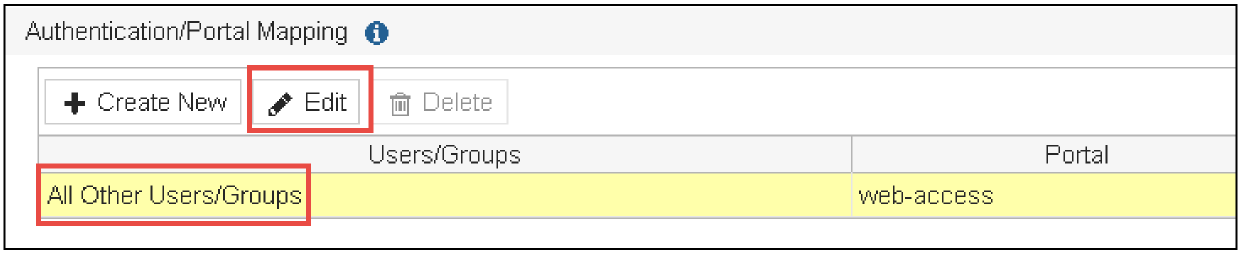
Add Tunnel Mode

Now, you will change the SSL-VPN portal mapping settings to use **tunnel-access**, in order to allow connections in tunnel mode only.

The **full-access** setting available on FortiGate supports both web and tunnel mode.

To add tunnel mode

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **VPN** > **SSL-VPN Settings**.
3. In the **Authentication/Portal Mapping** section, select **All Other Users/Groups**, and then click **Edit**.



Users/Groups	Portal
All Other Users/Groups	web-access

4. In the **Portal** drop-down list, select **tunnel-access**, and click **OK**.
5. Click **Apply**.
6. Click **OK** to confirm the use of the built-in certificate.

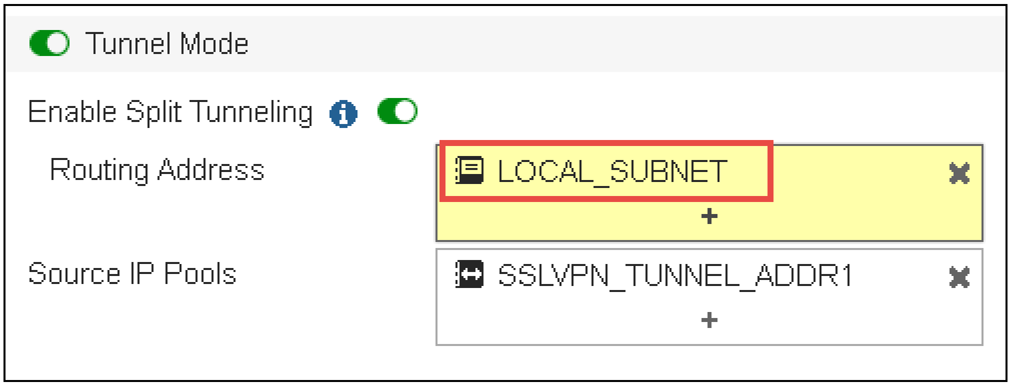
Configure the Routing for Tunnel Mode

Now, you will establish the routing address to use in tunnel mode.

Notice that in tunnel mode, the 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, set the **Routing Address** to **LOCAL_SUBNET**.



Tunnel Mode
Enable Split Tunneling
Routing Address: LOCAL_SUBNET
Source IP Pools: SSLVPN_TUNNEL_ADDR1

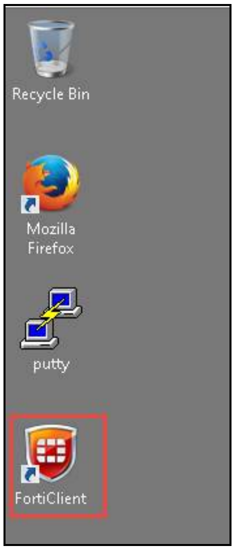
4. Click **OK**.

Configure FortiClient for SSL-VPN connections

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

To configure FortiClient for SSL-VPN

1. Connect to the Remote-Windows VM.
2. Start the **FortiClient** application located on the desktop.



3. Click **Remote Access**, and then click **Configure VPN**.
4. Select the **SSL-VPN** tab, and then configure the following settings:

Field	Value
Connection Name	Local-FortiGate
Remote Gateway	10.200.1.1
Customize port	<enable> | 10443

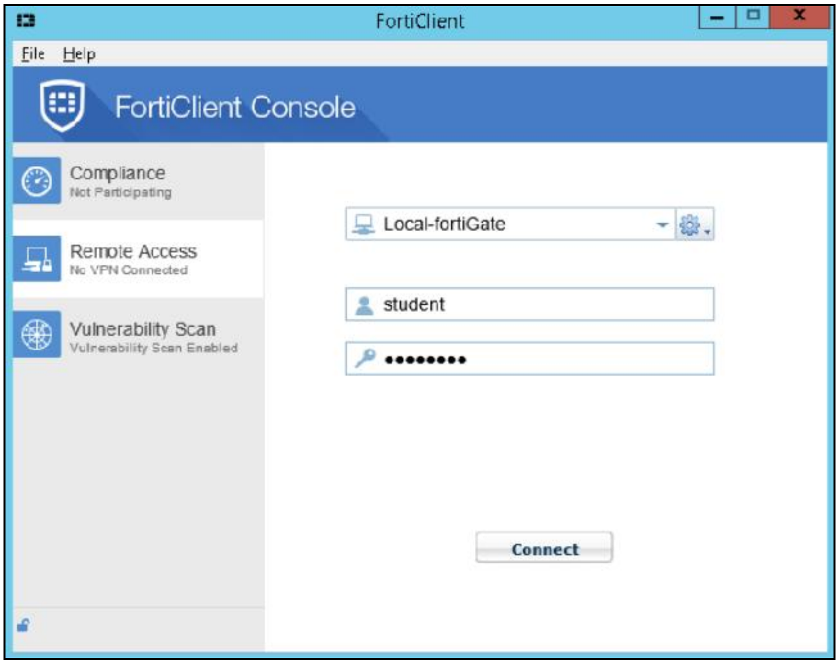
5. Click **Apply**.
6. Click **Close**.

Test SSL-VPN in Tunnel Mode

Now, you will connect using the student account to test tunnel mode.

To connect in tunnel mode

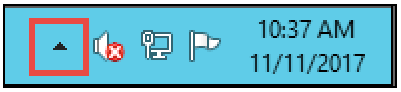
1. Open **FortiClient**, and then click **Remote Access**.
2. Enter the username `student` with the password `fortinet`.



3. Click **Connect**.
4. Click **Yes** to accept the certificate.

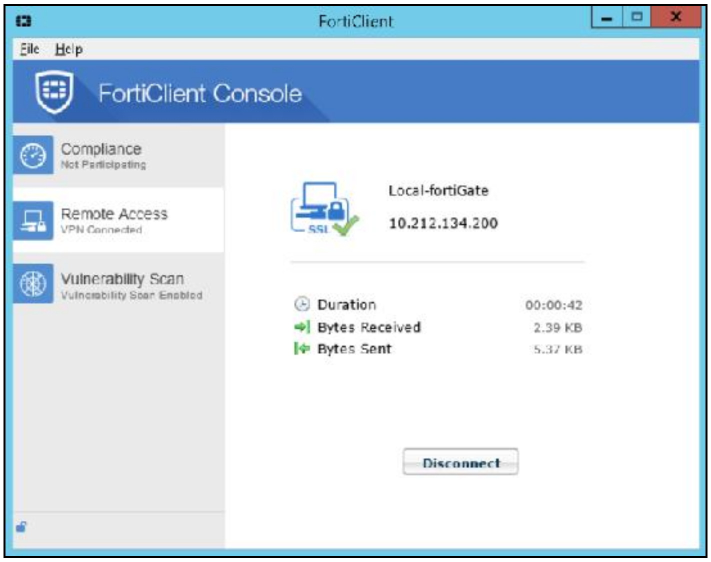
   The tunnel is connected.

5. To verify the tunnel connection, do one of the following:
   - In the Remote-Windows toolbar, click the black up arrow, and hover the cursor over the FortiClient icon.

     You should see a lock overlay on the icon and the message should show it is connected, as well as the bytes sent and received.

   - Open the **FortiClient** that is minimized in the toolbar.

To test the tunnel

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

   ```
   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`).

   This time, you are not using the reverse HTTP proxy as in the case of web-access mode. The IP traffic is directly encapsulated over HTTPS and sent through the tunnel.

3. Return to FortiClient, and then click **Disconnect**.

To attempt SSL-VPN access by web mode

1. Continuing on the Remote-Windows VM, open a web browser and log in to the SSL-VPN portal at `https://10.200.1.1:10443/`using the username `student` and the password `fortinet`.

2. View the warning message.

   The web access for SSL-VPN is not available because you set up the SSL-VPN settings for **tunnel-access**.

   The **full-access** setting supports both web and tunnel modes.

3. Close the web browser.

Review VPN Events

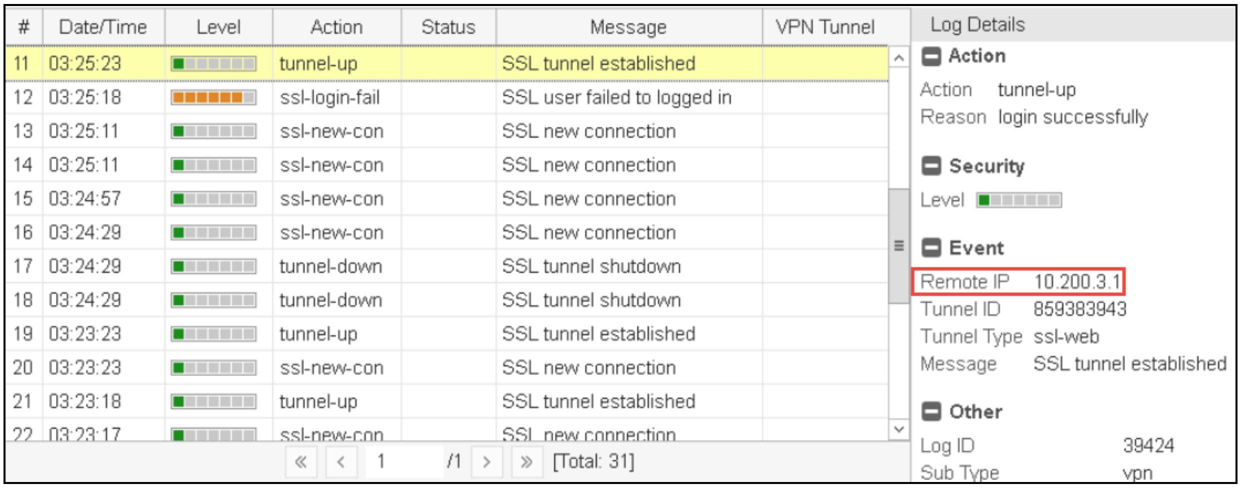
Now, you'll review the VPN events for both of the SSL-VPN connections you performed in this lab (web and tunnel modes).

To review VPN events for SSL-VPN connections

1. Return to the Local-Windows VM.
2. Open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
3. Click **Log & Report** > **VPN Events**.
4. Compare the log details of the **tunnel-up** logs you see.

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

   The most recent **tunnel-up** log shows one IP address under **Remote IP**. This log shows the recent connection to the SSL-VPN portal. Even though the SSL-VPN portal presented a warning message and it did not allow remote access to the local resources, FortiGate shows that an SSL-VPN connection was established and the tunnel was up.



#	Date/Time	Level	Action	Status	Message	VPN Tunnel
11	03:25:23	🟩	tunnel-up		SSL tunnel established	
12	03:25:18	🟧	ssl-login-fail		SSL user failed to logged in	
13	03:25:11	🟩	ssl-new-con		SSL new connection	
14	03:25:11	🟩	ssl-new-con		SSL new connection	
15	03:24:57	🟩	ssl-new-con		SSL new connection	
16	03:24:29	🟩	ssl-new-con		SSL new connection	
17	03:24:29	🟩	tunnel-down		SSL tunnel shutdown	
18	03:24:29	🟩	tunnel-down		SSL tunnel shutdown	
19	03:23:23	🟩	tunnel-up		SSL tunnel established	
20	03:23:23	🟩	ssl-new-con		SSL new connection	
21	03:23:18	🟩	tunnel-up		SSL tunnel established	
22	03:23:17	🟩	ssl-new-con		SSL new connection	

« ‹ 1 /1 › » [Total: 31]

Log Details

Action

Action	tunnel-up
Reason	login successfully

Security

Level	🟩

Event

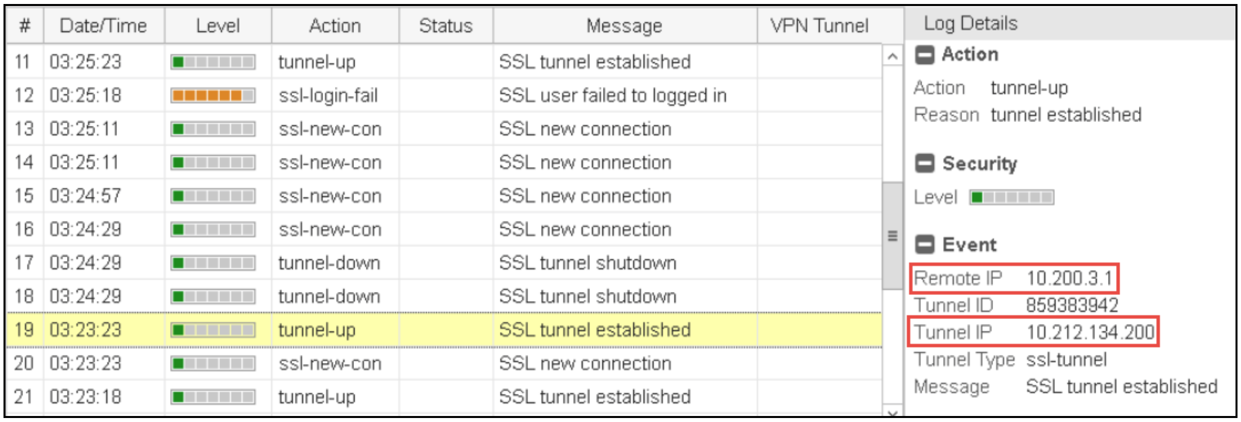
Remote IP	10.200.3.1
Tunnel ID	859383943
Tunnel Type	ssl-web
Message	SSL tunnel established

Other

Log ID	39424
Sub Type	vpn

The second most recent **tunnel-up** log in the VPN event list, shows the SSL-VPN connection in tunnel mode through FortiClient. Notice this log presents 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`.



#	Date/Time	Level	Action	Status	Message	VPN Tunnel
11	03:25:23	🟩	tunnel-up		SSL tunnel established	
12	03:25:18	🟧	ssl-login-fail		SSL user failed to logged in	
13	03:25:11	🟩	ssl-new-con		SSL new connection	
14	03:25:11	🟩	ssl-new-con		SSL new connection	
15	03:24:57	🟩	ssl-new-con		SSL new connection	
16	03:24:29	🟩	ssl-new-con		SSL new connection	
17	03:24:29	🟩	tunnel-down		SSL tunnel shutdown	
18	03:24:29	🟩	tunnel-down		SSL tunnel shutdown	
19	03:23:23	🟩	tunnel-up		SSL tunnel established	
20	03:23:23	🟩	ssl-new-con		SSL new connection	
21	03:23:18	🟩	tunnel-up		SSL tunnel established	

Log Details

Action

Action	tunnel-up
Reason	tunnel established

Security

Level	🟩

Event

Remote IP	10.200.3.1
Tunnel ID	859383942
Tunnel IP	10.212.134.200
Tunnel Type	ssl-tunnel
Message	SSL tunnel established

Stop and think!

Aside from SSL-VPN connections in web mode showing one IP address and tunnel mode showing two IP addresses, what other indicator shows how SSL-VPN users are connected?

Notice the **Tunnel Type** indicator in the log details shown in the previous step.

- **ssl-web** for web mode.
- **ssl-tunnel** for tunnel mode.

Lab 12: Dialup IPsec VPN

In this lab, you will configure a dialup VPN between two FortiGate devices. You will also create a dialup VPN between a FortiGate and FortiClient.

Objectives

- Deploy a dialup VPN between two FortiGate devices.
- Deploy a dialup VPN between FortiGate and FortiClient.

Time to Complete

Estimated: 45 minutes

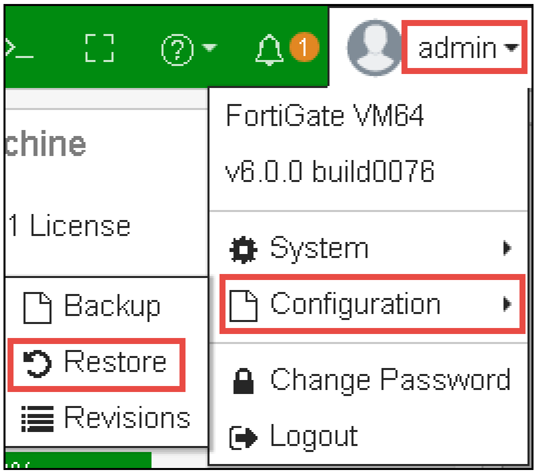
Prerequisites

Before beginning this lab, you must restore a configuration file on Remote-FortiGate and Local-FortiGate .

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

To restore the Remote-FortiGate configuration file

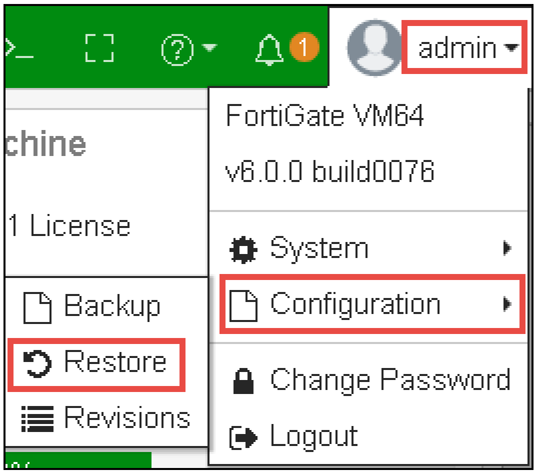
1. On the Local-Windows VM, open a browser and log in to the Remote-FortiGate GUI at `10.200.3.1` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**,and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **Dialup-IPsec** > **Dialup-IPsec-Two-FortiGates** > `remote-dialup-IPsec-TwoFGT.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**,and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **Dialup-IPsec** > **Dialup-IPsec-Two-FortiGates** > `local-dialup-IPsec-TwoFGT.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring a Dialup IPsec VPN Between Two FortiGate Devices

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

Create Phases 1 and 2 on Local-FortiGate (Dialup Server)

Now, you will configure the IPsec VPN by creating phases 1 and 2.

To create phases 1 and 2

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **VPN** > **IPsec Tunnels**, and then click **Create New**.
3. Complete the following:

Field	Value
Name	To Remote
Template Type	Custom

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

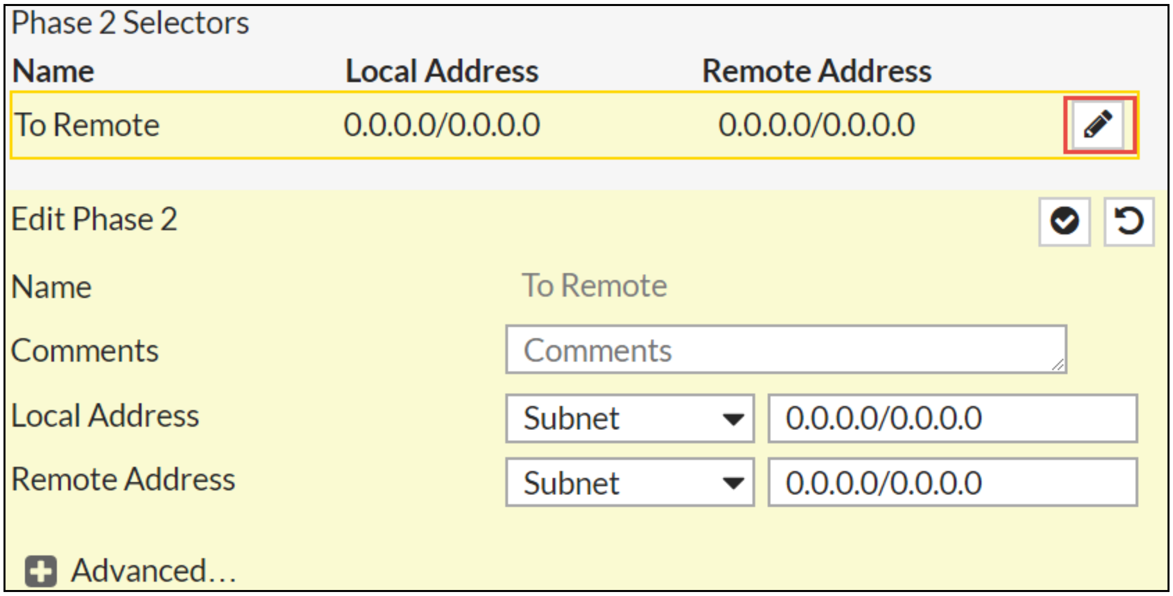
Field	Value
Remote Gateway	Dialup user
Interface	port1

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

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

The peer ID shown in the configuration above was selected, which you need if you have more than one dialup client.

7. Keep the default values for the remaining settings.
8. In the **Phase 2 Selectors** section, click the edit icon to edit the settings.



Phase 2 Selectors

Name	Local Address	Remote Address
To Remote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name: To Remote

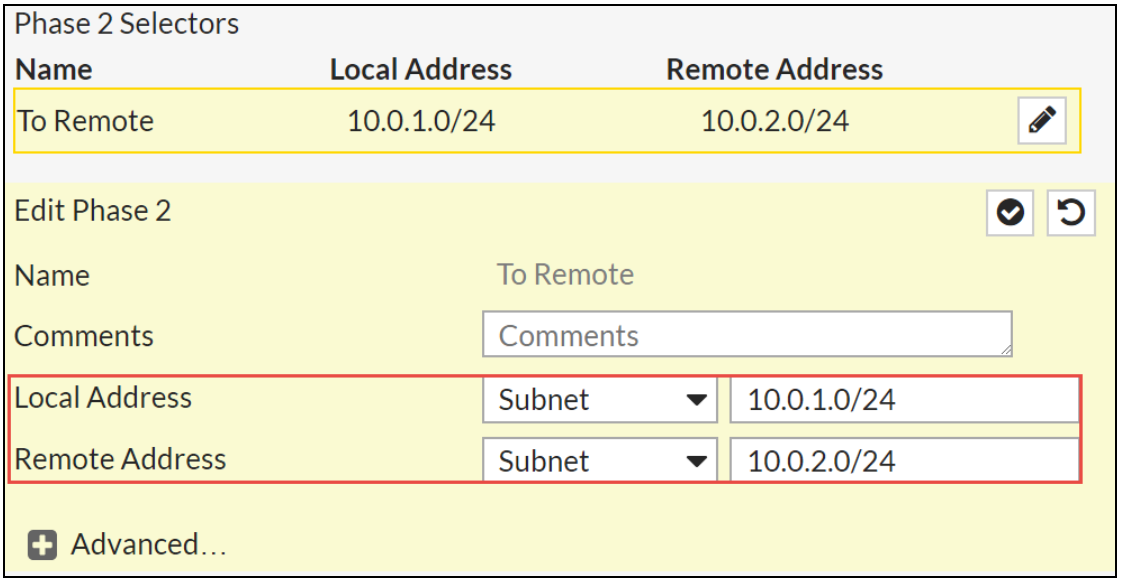
Comments: Comments

Local Address: Subnet 0.0.0.0/0.0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0.0

9. Complete the following:

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



Phase 2 Selectors

Name	Local Address	Remote Address
To Remote	10.0.1.0/24	10.0.2.0/24

Edit Phase 2

Name	To Remote	
Comments	Comments	
Local Address	Subnet	10.0.1.0/24
Remote Address	Subnet	10.0.2.0/24

Advanced...

10. Click **OK**.

Although you have created a route-based IPsec tunnel, you do not need to add a static route because it is a dialup VPN. FortiGate will dynamically add or remove appropriate routes to each dialup peer, each time the peer's VPN is trying to connect.

Create Firewall Policies for VPN Traffic on Local-FortiGate (Dialup server)

Now, you will create two firewall policies between **port3** and **To Remote**: one for each traffic direction.

To create the firewall policies for VPN traffic

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	Remote_out
Incoming Interface	port3
Outgoing Interface	To Remote
Source	LOCAL_SUBNET
Destination	REMOTE_SUBNET

Field	Value
Schedule	always
Service	ALL
Action	ACCEPT

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

Field	Value
Name	Remote_in
Incoming Interface	To Remote
Outgoing Interface	port3
Source	REMOTE_SUBNET
Destination	LOCAL_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

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

Create Phases 1 and 2 on Remote-FortiGate (Dialup Client)

Now, you will add phases 1 and 2 on Remote-FortiGate.

To create phases 1 and 2

1. Continuing on the Local-Windows VM, open a browser and log in to the Remote-FortiGate GUI at `10.200.3.1` with the user name `admin` and password `password`.
2. Click **VPN** > **IPsec Tunnels**.
3. Click **Create New**.
4. Complete the following:

Field	Value
Name	To local
Template Type	Custom

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

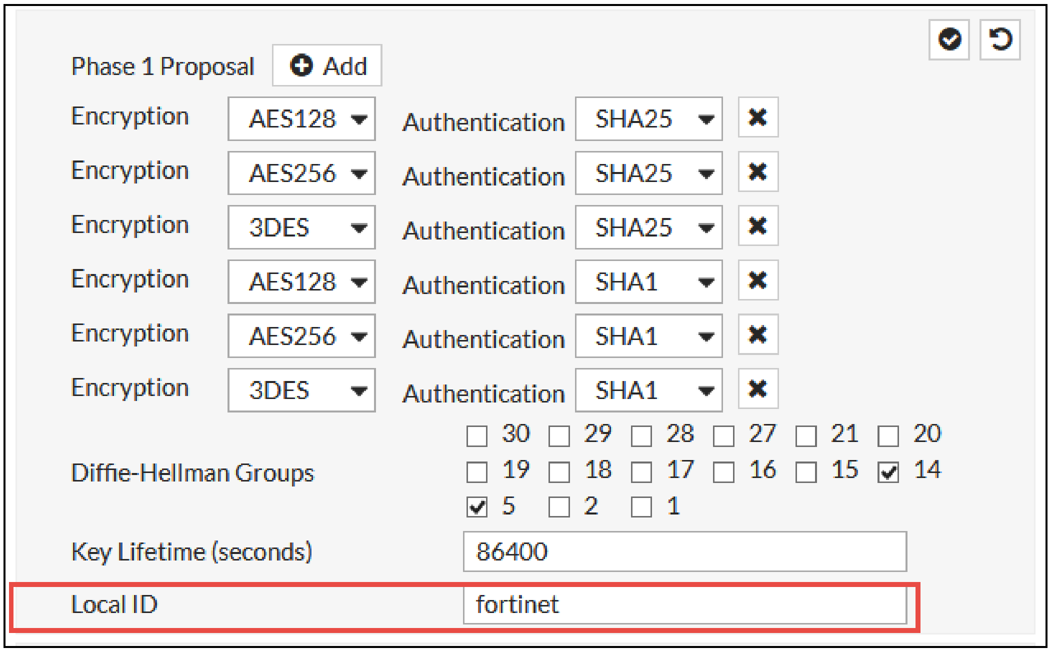
Field	Value
Remote Gateway	Static IP Address
IP Address	10.200.1.1
Interface	port4

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

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

8. In the **Phase 1 Proposal** section, configure the following settings:

Field	Value
Local ID	fortinet



Encryption	AES128	Authentication	SHA25	✖
Encryption	AES256	Authentication	SHA25	✖
Encryption	3DES	Authentication	SHA25	✖
Encryption	AES128	Authentication	SHA1	✖
Encryption	AES256	Authentication	SHA1	✖
Encryption	3DES	Authentication	SHA1	✖

Diffie-Hellman Groups

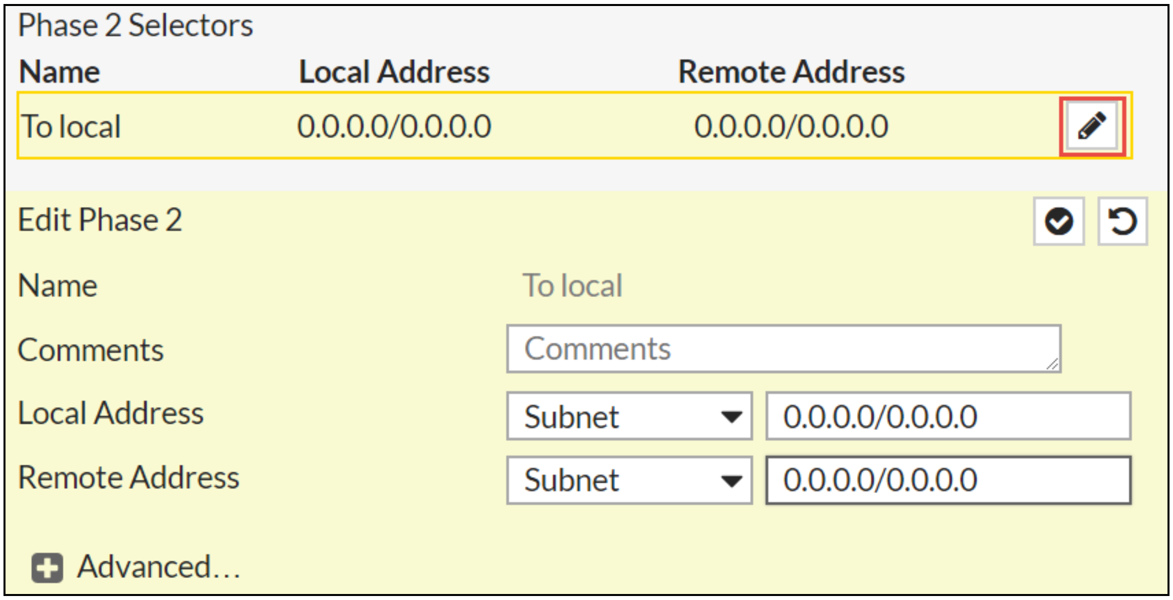
□ 30 □ 29 □ 28 □ 27 □ 21 □ 20
□ 19 □ 18 □ 17 □ 16 □ 15 ☑ 14
☑ 5 □ 2 □ 1

Key Lifetime (seconds): 86400

Local ID: fortinet

The local ID should be same as the peer ID that you configured on the Local-FortiGate that is acting as the dialup server.

9. Keep the default values for the remaining settings.
10. In the **Phase 2 Selectors** section, click the edit icon to edit the settings.


Phase 2 Selectors

Name	Local Address	Remote Address
To local	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name: To local

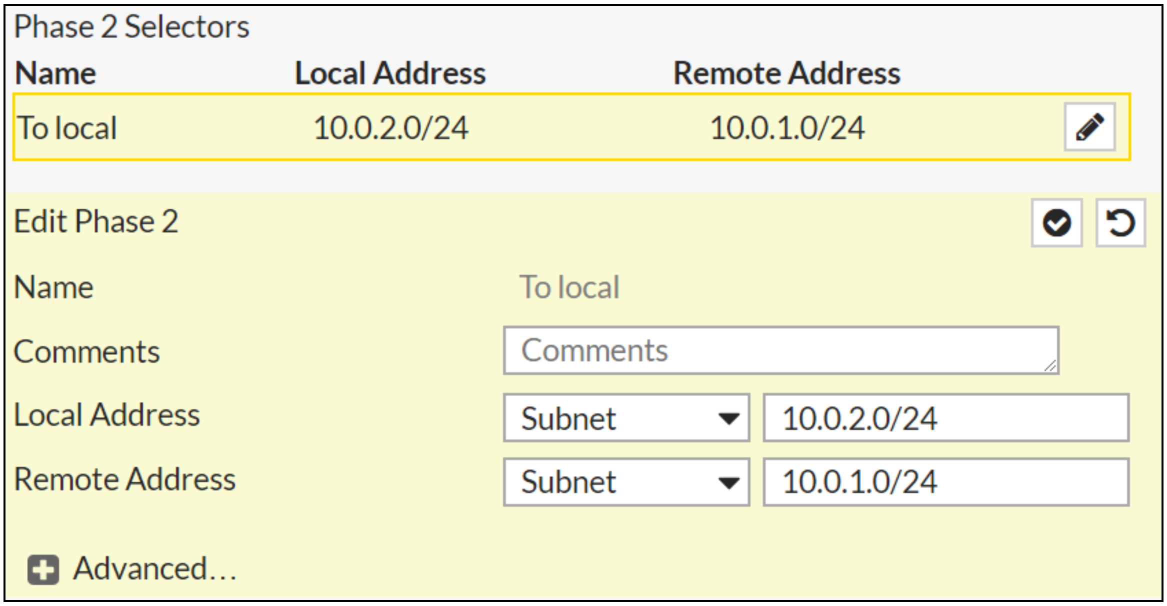
Comments: Comments

Local Address: Subnet 0.0.0.0/0.0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0.0

11. Complete the following:

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



Phase 2 Selectors

Name	Local Address	Remote Address
To local	10.0.2.0/24	10.0.1.0/24

Edit Phase 2

Name: To local

Comments: Comments

Local Address: Subnet 10.0.2.0/24

Remote Address: Subnet 10.0.1.0/24

12. Click **OK**.

Now the quick mode selectors in both sides mirror each other. If that is not the case, the tunnel will not come up.

Create a Static Route for Route-Based VPN on Remote-FortiGate (Dialup Client)

Now, you will create one static route, because the current VPN is route based.

To create a static route for a route-based VPN

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

Feild	Value
Destination	Subnet 10.0.1.0/24
Interface	To local

4. Click **OK**.

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

Now, you will create two firewall policies between **port6** and **To Local**: one for each traffic direction.

To create the firewall policies for VPN traffic

1. Continuing on the Remote-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	Local_out
Incoming Interface	port6
Outgoing Interface	To local
Source	REMOTE_SUBNET
Destination	LOCAL_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
Incoming Interface	To local

Field	Value
Outgoing Interface	port6
Source	LOCAL_SUBNET
Destination	REMOTE_SUBNET
Schedule	always
Service	ALL
Action	ACCEPT

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

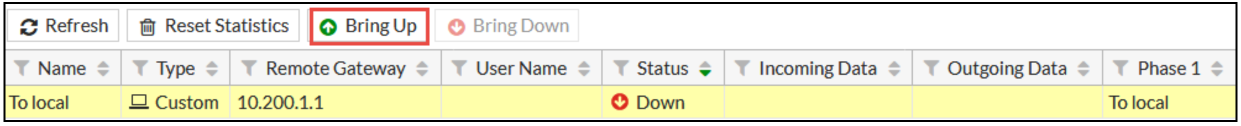
Exercise 2: Testing and Monitoring the VPN

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

To test the VPN

1. On the Local-Windows VM, open a browser and log in to the Remote-FortiGate GUI at `10.200.3.1` with the user name `admin` and password `password`.
2. Click **Monitor** > **IPsec Monitor**.

   Notice that the VPN is currently down.
3. Click the VPN and click **Bring Up**.



Name	Type	Remote Gateway	User Name	Status	Incoming Data	Outgoing Data	Phase 1
To local	Custom	10.200.1.1		Down			To local

The **Status** column of the VPN now contains a green up arrow, indicating that the tunnel is up.

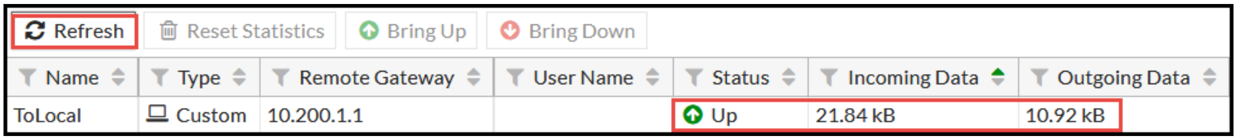
> **Stop and think!**
>
> Do I always have to bring up the tunnel manually after creating it?
>
> No. With the current configuration, the tunnel will stay down until you manually bring it up or there is traffic that should be routed through the tunnel. Because you are not generating traffic between `10.0.2.0/24` 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 only initiate a tunnel from Remote-FortiGate because it is a dialup client .

4. Switch to the Remote-Windows VM.
5. Open a command prompt window, and then run the following command to ping the Local-Windows VM:

```
ping 10.0.1.10
```

   The ping should work.
6. Return to the Local-Windows VM.
7. On the Remote-FortiGate GUI, click **Monitor** > **IPsec Monitor**.
8. Click **Refresh** to refresh the screen.

   You will notice that counters for **Incoming Data** and **Outgoing Data** have increased. This indicates that the traffic between `10.0.1.10` is `10.0.2.10` is being encrypted successfully and routed through the tunnel.



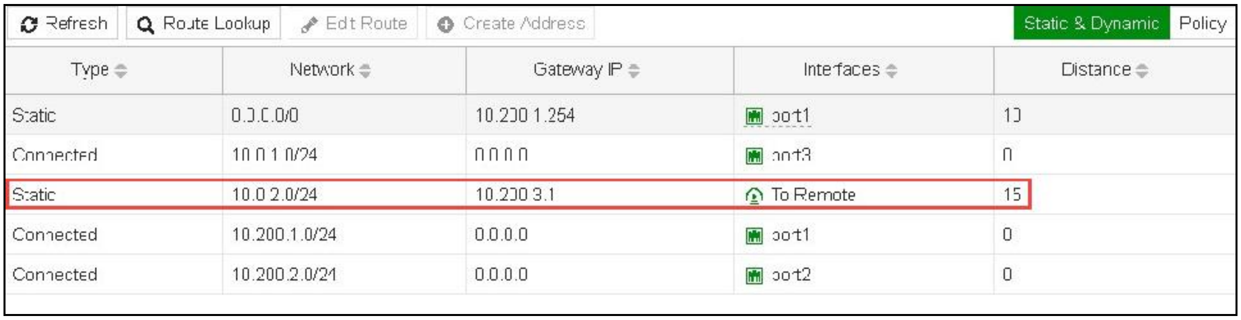
Name	Type	Remote Gateway	User Name	Status	Incoming Data	Outgoing Data
ToLocal	Custom	10.200.1.1		Up	21.84 kB	10.92 kB

9. Open a new browser tab and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
10. Click **Monitor** > **Routing Monitor**.

Find the static route that was dynamically added to the FortiGate.

11. View the details of the **To Remote** VPN connection.

    Notice the **Remote Gateway** IP address.



Type	Network	Gateway IP	Interfaces	Distance
Static	0.0.0.0/0	10.200.1.254	port1	10
Connected	10.0.1.0/24	0.0.0.0	port3	0
Static	10.0.2.0/24	10.200.3.1	To Remote	15
Connected	10.200.1.0/24	0.0.0.0	port1	0
Connected	10.200.2.0/24	0.0.0.0	port2	0

Exercise 3: Creating an IPsec VPN Between FortiGate and FortiClient

Now, you will now create a dialup VPN between FortiGate and FortiClient.

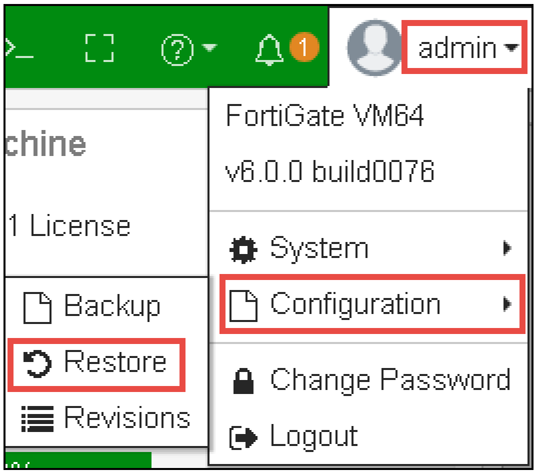
Prerequisites

Before beginning this lab, you must restore a configuration file on Remote-FortiGate and Local-FortiGate.

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

To restore the Remote-FortiGate configuration file

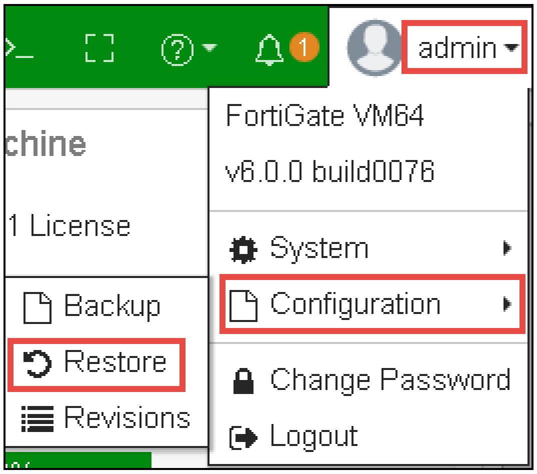
1. On the Local-Windows VM, open a browser and log in to the Remote-FortiGate GUI at `10.200.3.1` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **Dialup-IPsec** > **Dialup-IPsec-Forticlient** > `remote-dialup-IPsec-VPN.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** >**Dialup-IPsec** > **Dialup-IPsec-Forticlient** > `local-dialup-IPsec-VPN.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

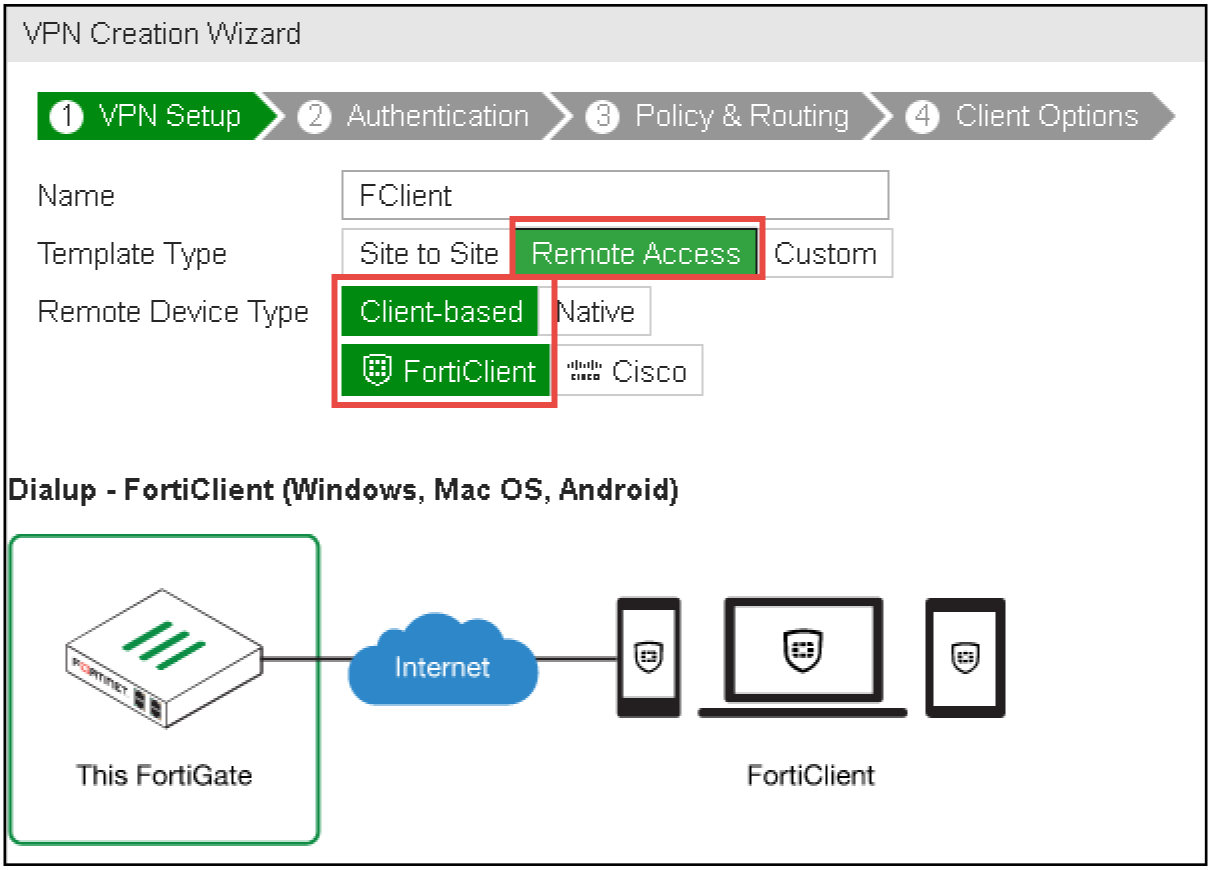
Configure a Dialup VPN

Now, you will create the dialup VPN on Local-FortiGate.

To create the dialup VPN

1. Continuing on the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **VPN** > **IPsec Tunnels**, and then click **Create New**.
3. Complete the following:

Field	Value
Name	FClient
Template Type	Remote Access
Remote Device Type	Client-based FortiClient



VPN Creation Wizard

Name: FClient

Template Type: Site to Site [✓ Remote Access] Custom

Remote Device Type: [✓ Client-based] Native

[✓ FortiClient] Cisco

Dialup - FortiClient (Windows, Mac OS, Android)

4. Click **Next**.
5. Configure the following settings:

Field	Value
Incoming Interface	port1
Authenticated Method	Pre-shared Key
Pre-Shared Key	fortinet
User Group	training

For the purpose of this exercise, the User Group **training** is preconfigured for you.

6. Click **Next**.
7. Configure the following settings:

Field	Value
Local Interface	port3
Local Address	LOCAL_SUBNET
Client Address Range	172.20.1.1-172.20.1.5
Subnet	255.255.255.0
DNS Server	Use System DNS
Enable IPv4 Split Tunnel	<enable>
Allow Endpoint Registration	<disable>

8. Click **Next**.
9. Verify that **Save Password** is enabled.
10. Click **Create**.

    The VPN wizard creates IPsec phases 1 and 2, as well as client address range firewall address, and one firewall policy that allows incoming traffic from the VPN to the internal subnet.

11. Click **Show Tunnel List** to view the tunnel.

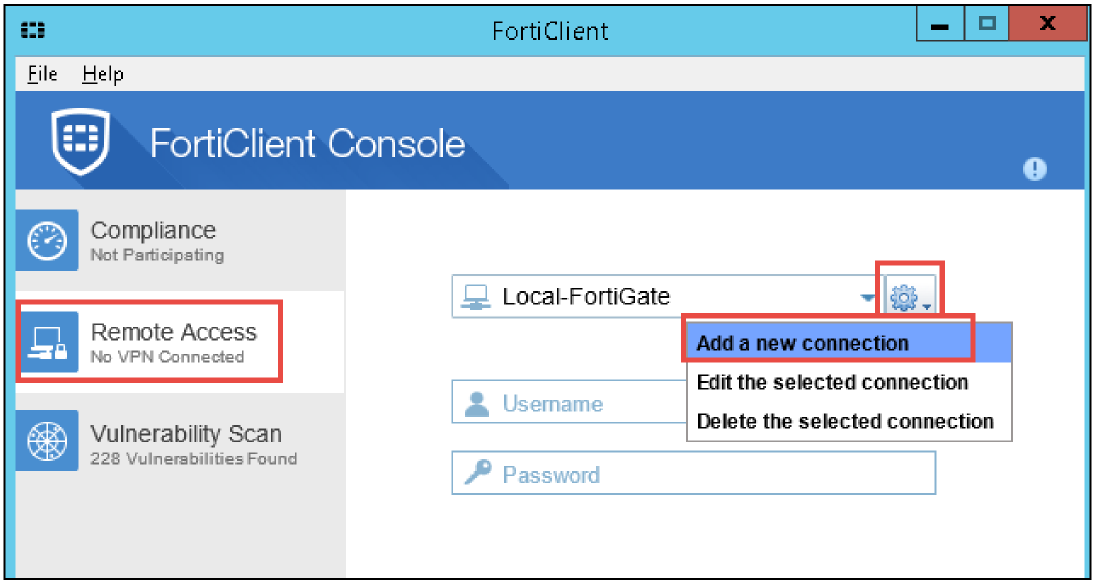
Although you have created a route-based IPsec tunnel, you do not need to add a static route because it is a dialup VPN. FortiGate will dynamically add or remove appropriate routes to each dialup peer, each time a peer's VPN is established or disconnected.

Configure FortiClient for Dialup VPN

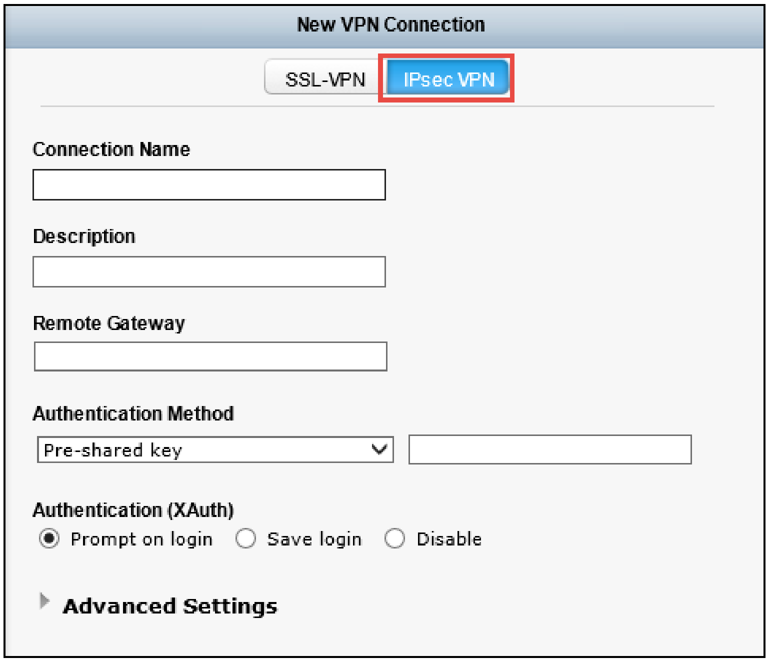
Now, you will configure the FortiClient IPsec client to connect to Local-FortiGate. You will use the FortiClient installed on the Remote-Windows VM.

To configure FortiClient for dialup VPN

1. On the Remote-Windows VM, launch the **FortiClient** application from the desktop.
2. Click **Remote Access**.
3. Click the **Settings** icon, and then click **Add a new connection**.



4. Select **IPsec VPN**.



5. Configure the following settings:

Field	Value
Connection Name	FC_VPN
Remote Gateway	10.200.1.1
Authentication Method	Pre-shared key fortinet

Field	Value
Authentication (XAuth)	Save Login
Username	student

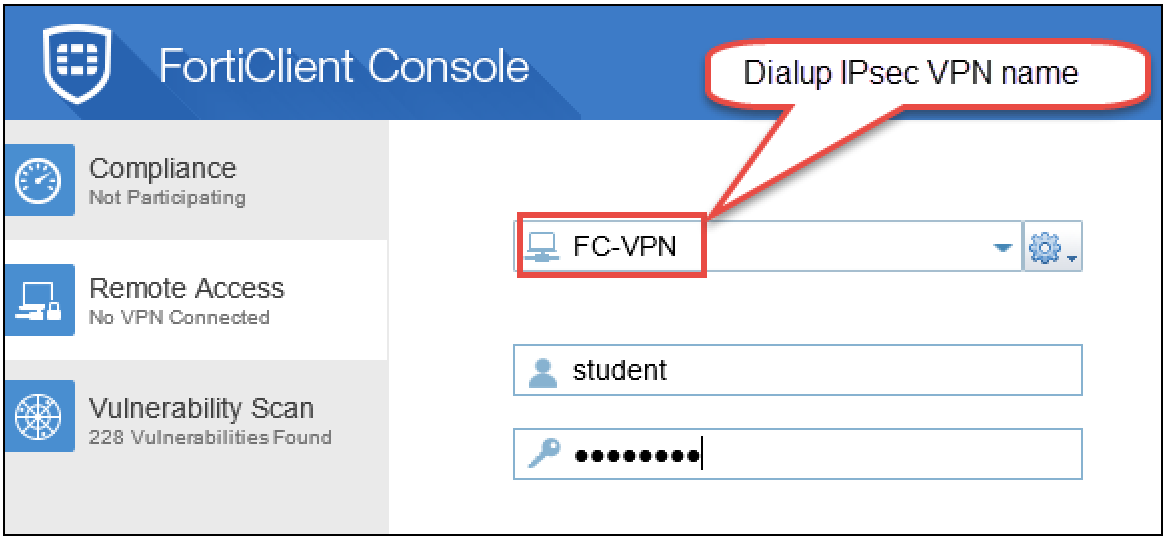
6. Click **Apply**.
7. Click **Close**.

Connect to the Dialup VPN

Now, you will use FortiClient to connect to the dialup VPN you created on Local-FortiGate.

To connect to the dialup VPN

1. Continuing on the Remote-Windows VM in the FortiClient application, enter the password `fortinet`.



FC-VPN

student

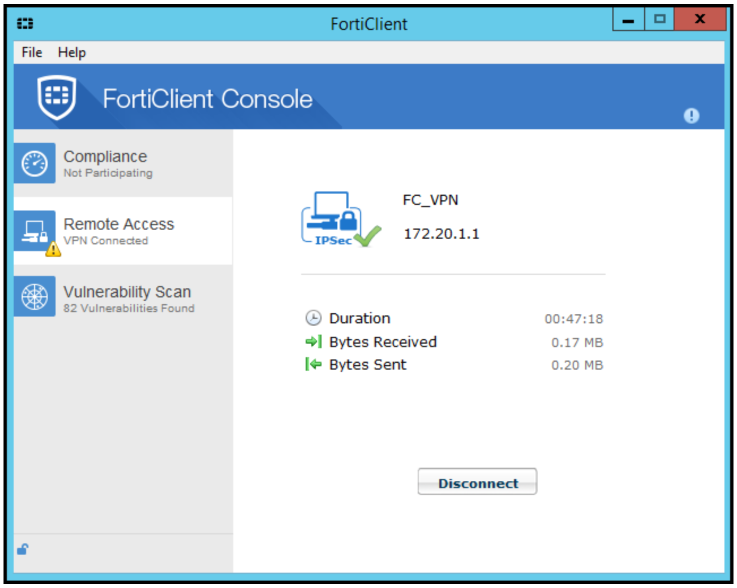
●●●●●●●●

2. Click **Connect**.

   Wait for few seconds.

3. Open the FortiClient application that has minimized to the toolbar.

   A green checkmark confirms that the tunnel is up:



FC_VPN

172.20.1.1

Duration 00:47:18
Bytes Received 0.17 MB
Bytes Sent 0.20 MB

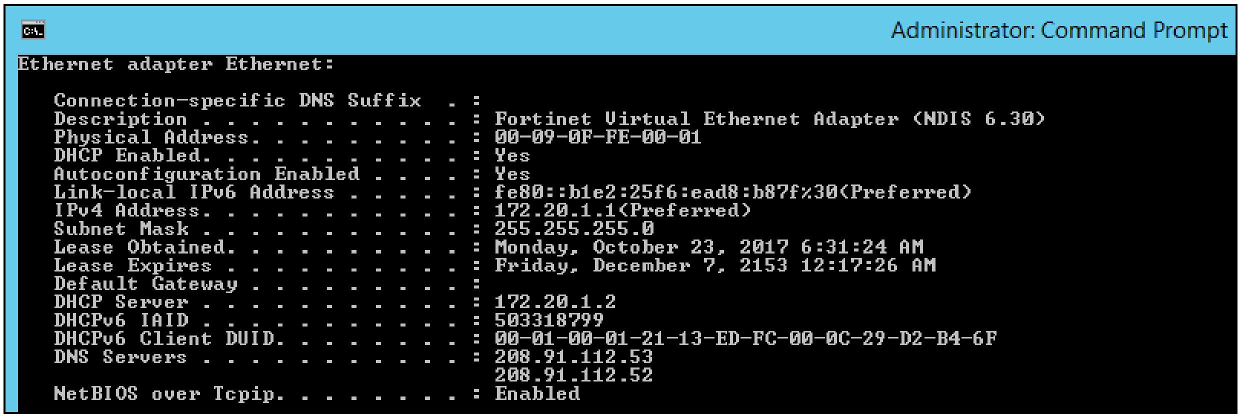
Check the IP Address and Route Added to the Remote-Windows VM

While the dialup VPN is up, the Remote-Windows VM receives an IP address in the `172.20.1.1 - 172.20.1.5` range. FortiGate also installs a route to the subnet `10.0.1.0/24`.

To check the IP address and route added to the Remote-Windows VM

1. Continuing on the Remote-Windows VM, open a command prompt window and enter the following command:

```
ipconfig /all
```



```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Fortinet Virtual Ethernet Adapter (NDIS 6.30)
   Physical Address. . . . . . . . . : 00-09-0F-FE-00-01
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::b1e2:25f6:ead8:b87f%30(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.20.1.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, October 23, 2017 6:31:24 AM
   Lease Expires . . . . . . . . . . : Friday, December 7, 2153 12:17:26 AM
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 172.20.1.2
   DHCPv6 IAID . . . . . . . . . . . : 503318799
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-13-ED-FC-00-0C-29-D2-B4-6F
   DNS Servers . . . . . . . . . . . : 208.91.112.53
                                       208.91.112.52
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

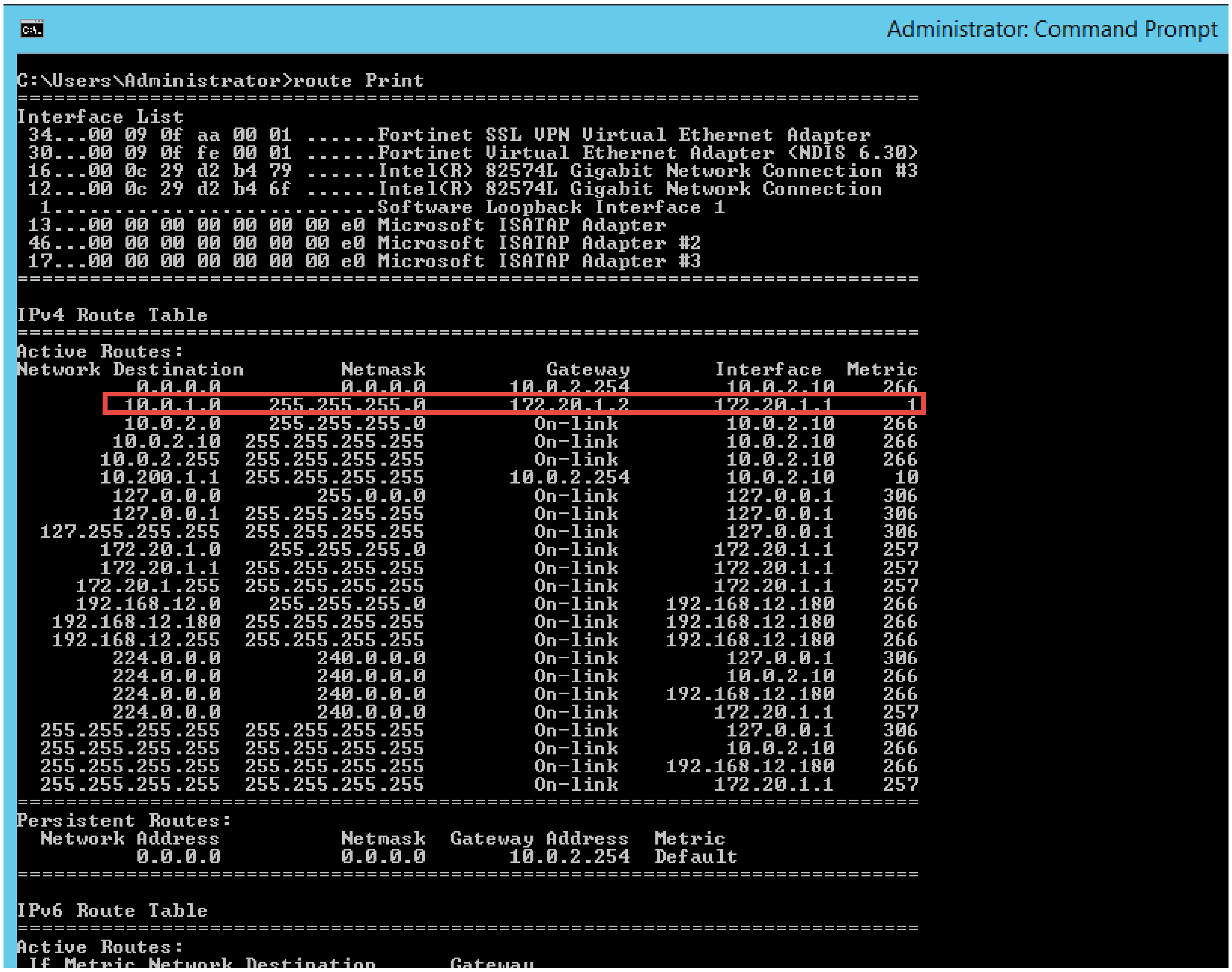
2. Analyze the output.

   You should observe a virtual ethernet adapter with an IP address in the `172.20.1.1` to `172.20.1.5` range.

3. Enter the following command to display the routing table information:

```
route print
```

4. Locate the `10.0.1.0/24` network entry in the output.



```
C:\Users\Administrator>route Print
===========================================================================
Interface List
 34...00 09 0f aa 00 01 ......Fortinet SSL VPN Virtual Ethernet Adapter
 30...00 09 0f fe 00 01 ......Fortinet Virtual Ethernet Adapter (NDIS 6.30)
 16...00 0c 29 d2 b4 79 ......Intel(R) 82574L Gigabit Network Connection #3
 12...00 0c 29 d2 b4 6f ......Intel(R) 82574L Gigabit Network Connection
  1...........................Software Loopback Interface 1
 13...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
 46...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
 17...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #3
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.0.2.254       10.0.2.10    266
         10.0.1.0    255.255.255.0       172.20.1.2      172.20.1.1      1
         10.0.2.0    255.255.255.0         On-link        10.0.2.10    266
        10.0.2.10  255.255.255.255         On-link        10.0.2.10    266
       10.0.2.255  255.255.255.255         On-link        10.0.2.10    266
       10.200.1.1  255.255.255.255       10.0.2.254       10.0.2.10     10
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    306
       172.20.1.0    255.255.255.0         On-link       172.20.1.1    257
       172.20.1.1  255.255.255.255         On-link       172.20.1.1    257
     172.20.1.255  255.255.255.255         On-link       172.20.1.1    257
     192.168.12.0    255.255.255.0         On-link    192.168.12.180    266
   192.168.12.180  255.255.255.255         On-link    192.168.12.180    266
   192.168.12.255  255.255.255.255         On-link    192.168.12.180    266
        224.0.0.0        240.0.0.0         On-link        127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link        10.0.2.10    266
        224.0.0.0        240.0.0.0         On-link    192.168.12.180    266
        224.0.0.0        240.0.0.0         On-link       172.20.1.1    257
  255.255.255.255  255.255.255.255         On-link        127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link        10.0.2.10    266
  255.255.255.255  255.255.255.255         On-link    192.168.12.180    266
  255.255.255.255  255.255.255.255         On-link       172.20.1.1    257
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0       10.0.2.254  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
```

5. Close the command prompt.

Test the Dialup VPN

Now, you will test the dialup VPN by sending traffic from the Remote-Windows VM to the Local-Windows VM.

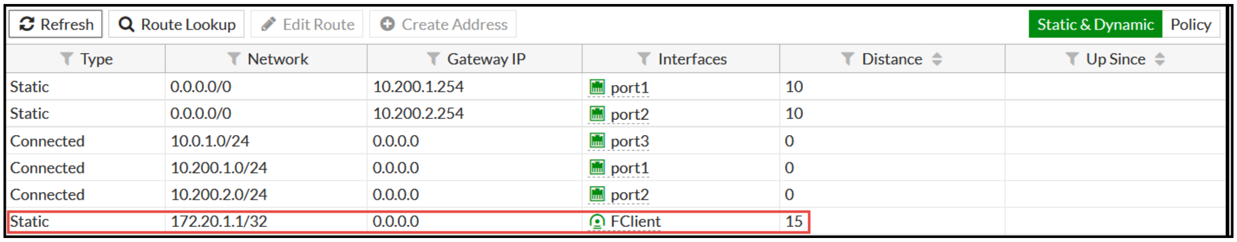
To test the dialup VPN

1. Continuing on the Remote-Windows VM in the command prompt window try to ping the Local-Windows VM:

   ```
   ping 10.0.1.10
   ```

   The ping succeeds, confirming that the tunnel is working.

2. Return to the Local-Windows VM.
3. In the browser tab where you are logged in to the Local-FortiGate GUI, click **Monitor** > **Routing Monitor**.
4. Find the static route that was dynamically added to the FortiGate.



Type	Network	Gateway IP	Interfaces	Distance	Up Since
Static	0.0.0.0/0	10.200.1.254	port1	10	
Static	0.0.0.0/0	10.200.2.254	port2	10	
Connected	10.0.1.0/24	0.0.0.0	port3	0	
Connected	10.200.1.0/24	0.0.0.0	port1	0	
Connected	10.200.2.0/24	0.0.0.0	port2	0	
Static	172.20.1.1/32	0.0.0.0	FClient	15	

5. Click **Monitor** > **IPsec Monitor**.
6. View the details of the **FClient_0** VPN connection.

   Notice the **Remote Gateway** IP address.

Disconnect the Dialup VPN

Now, you will disconnect the Remote-Windows VM from the dialup VPN.

To disconnect the dialup VPN

1. On the Remote-Windows VM, open FortiClient.
2. Click **Disconnect**.

Lab 13: Data Leak Prevention (DLP)

In this lab, you will use data leak prevention (DLP) rules and sensors to block sensitive data from leaving the private network.

Objectives

- Configure DLP to block ZIP files.
- Read and interpret DLP log entries.
- Set up DLP banning and quarantining.
- Configure DLP fingerprinting.

Time to Complete

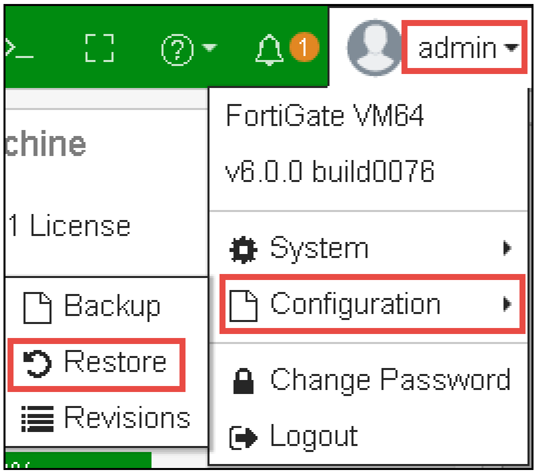
Estimated: 30 minutes

Prerequisites

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

To restore the Local-FortiGate configuration file

1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiGate-Security** > **DLP** > `local-dlp.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Blocking Files by File Type

There are multiple ways to configure DLP to prevent sensitive information from leaving your network.

In this exercise, you will configure DLP to block files by file type, and apply DLP to a firewall policy. Then, you will test the configuration and view the logs.The DLP feature is only available in the proxy mode.

Enable DLP

By default, DLP is not enabled in the GUI. You will enable DLP to be visible in the GUI.

To enable DLP

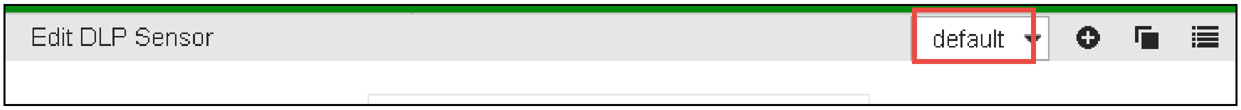
1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **System** > **Feature Visibility**.
3. In the **Security Features** section, enable **DLP**.
4. Click **Apply**.

Configure the DLP Sensor and DLP Filter

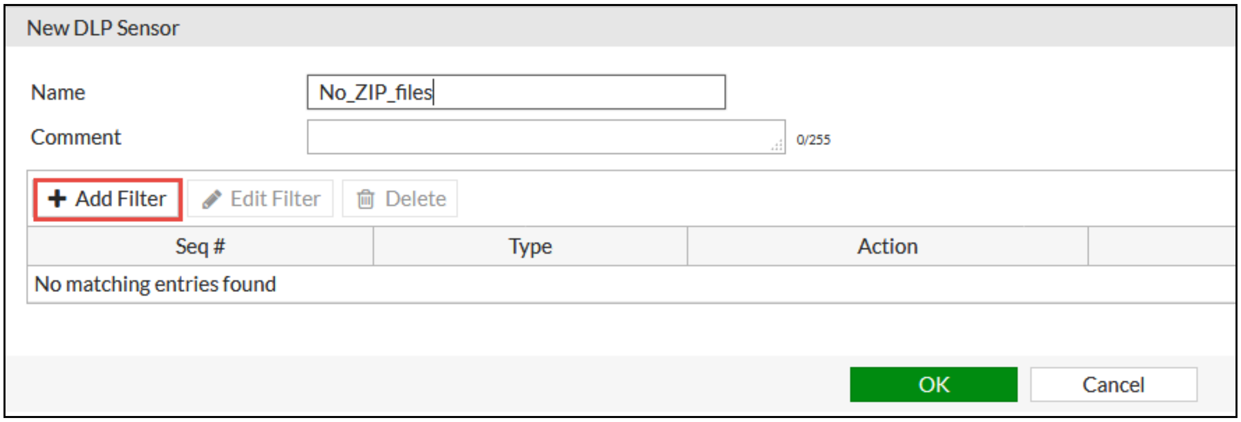
You will configure a new DLP sensor, and create a DLP filter to block ZIP files.

To configure the DLP sensor and DLP filter

1. Continuing on the Local-FortiGate GUI, click **Security Profiles** > **Data Leak Prevention**.
2. In the top right corner of the GUI, click the **+** icon to create a new sensor.



3. In the **Name** field, enter **No_ZIP_files**.
4. Click **Add Filter** to create a new filter.



Name: No_ZIP_files

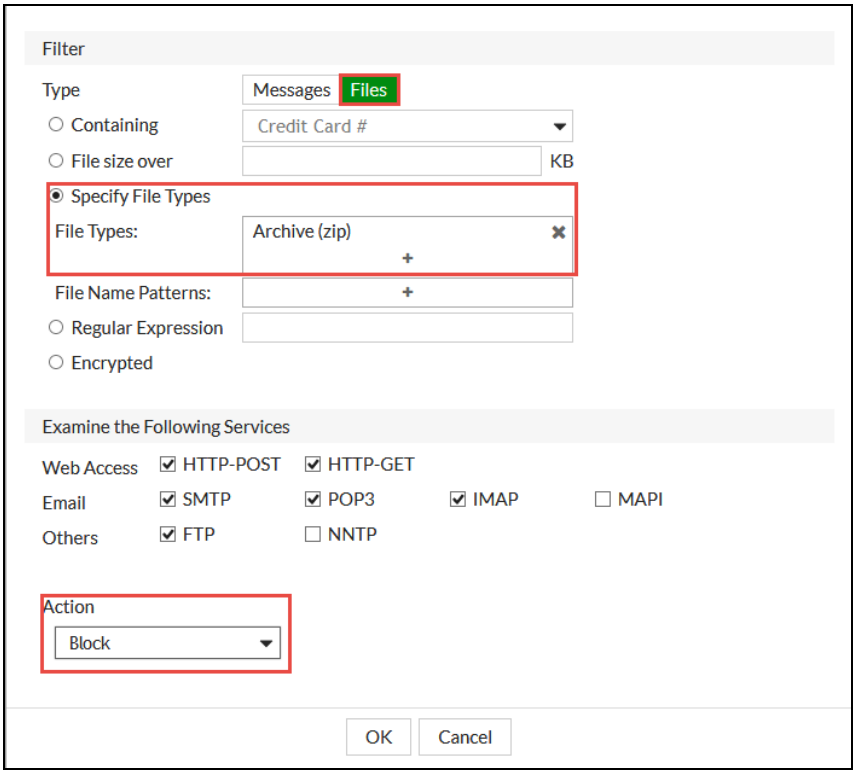
Comment: 0/255

No matching entries found

5. Configure the following settings:

Field	Value
Type	Files
Specify File Types	<select>
File Types	Archive (zip) **Tip**: On right side of the screen, type the name in the search box, and then click file types to add.
Action	Block

Your configuration should look like the following example:



Type: Files

○ Containing: Credit Card #

○ File size over: KB

● Specify File Types

File Types: Archive (zip)

File Name Patterns:

○ Regular Expression

○ Encrypted

Web Access ☑ HTTP-POST ☑ HTTP-GET

Email ☑ SMTP ☑ POP3 ☑ IMAP □ MAPI

Others ☑ FTP □ NNTP

Action: Block

6. Click **OK**.
7. Click **Apply**.

You can also block traffic based on a file name of *.zip, but it is not recommended. A person could circumvent that type of DLP by changing the filename to, for example, `*.zp1`, or `*.txt`.

By comparison, file type identification works by analyzing the binary layout of the file.

Apply a DLP Sensor to a Firewall Policy

Now that you have created a DLP sensor, you will edit the existing firewall policy to apply the DLP sensor to it.

Take the Expert Challenge!

On the Local-FortiGate GUI (`10.0.1.254`), apply the previously created DLP sensor to the existing firewall policy named **DLP**.

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

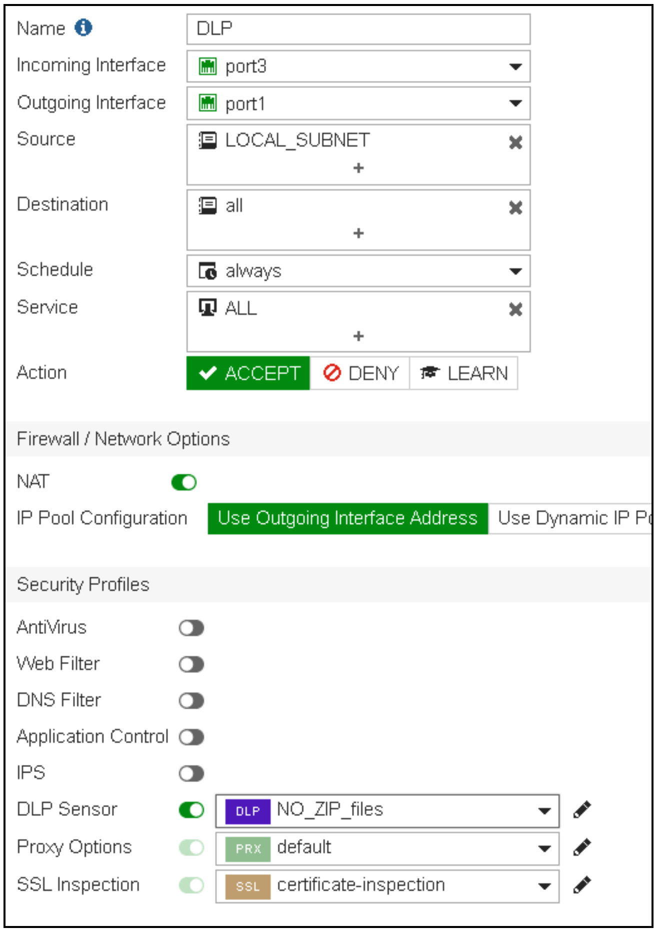
After you complete the challenge, see Test the DLP Sensor on page 217 .

To apply a DLP sensor to firewall policy

1. Continuing on the Local-FortiGate GUI, click **Policy & Objects** > **IPv4 Policy**.
2. Right-click the **ID** column for the **DLP** firewall policy and click **Edit**.
3. In the **Security Profiles** section, enable **DLP Sensor**, and from the drop-down menu, select **No_ZIP_files**.

When selecting a DLP sensor, **Proxy Options** and **SSL/SSH Inspection** is automatically enabled. You cannot disable **Proxy Options** and **SSL/SSH Inspection**, but you can select any preconfigured profile in the associated drop-down menu.

Your configuration should look like the following example:



Name	DLP
Incoming Interface	port3
Outgoing Interface	port1
Source	LOCAL_SUBNET
Destination	all
Schedule	always
Service	ALL
Action	[✓ ACCEPT] DENY LEARN

Firewall / Network Options

NAT	●
IP Pool Configuration	[✓ Use Outgoing Interface Address] Use Dynamic IP P

Security Profiles

AntiVirus	○	
Web Filter	○	
DNS Filter	○	
Application Control	○	
IPS	○	
DLP Sensor	●	DLP NO_ZIP_files
Proxy Options	●	PRX default
SSL Inspection	●	SSL certificate-inspection

4. Click **OK**.
5. Optionally, if you would like to see the **default** proxy options profile that is selected in the firewall policy, click **Security Profiles** > **Proxy Options**.

   This profile determines how FortiGate’s proxies pick up protocols. For example, the HTTP listening port is set to port 80.

Test the DLP Sensor

Now, you will test the DLP sensor by trying to transmit a ZIP file by uploading the file to a web URL.

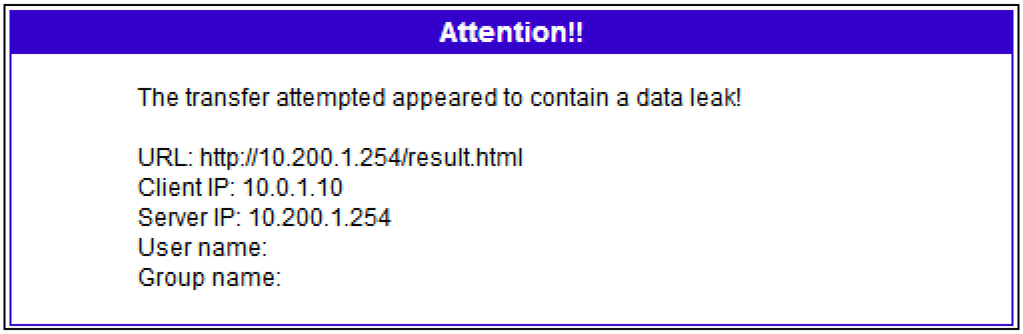
To test the DLP sensor

1. Continuing on the Local-Windows VM, open a new web browser tab and go to the following URL:

   `http://10.200.1.254/fileupload.html`

2. On the web page, click **Browse**.
3. Browse to **Desktop** > **Resources** > **FortiGate-Security** > **DLP** > `DLP_Lab.zip`, and then click **Open**.
4. Click **Submit the file**.

   The DLP block message will appear.



Attention!!

The transfer attempted appeared to contain a data leak!

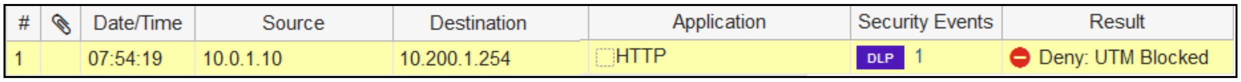
URL: http://10.200.1.254/result.html
Client IP: 10.0.1.10
Server IP: 10.200.1.254
User name:
Group name:

Check the DLP Logs

Now, you will check the logs related to DLP for the test you performed previously.

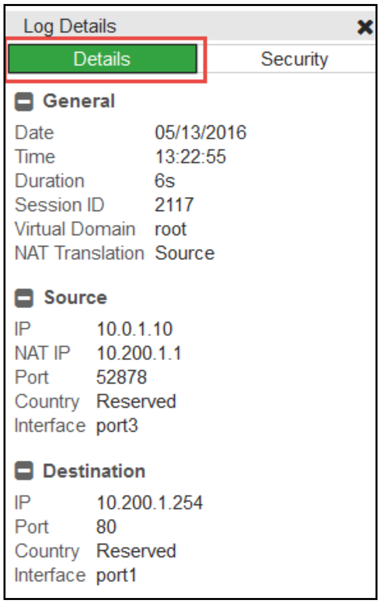
To check the DLP logs

1. On the Local-FortiGate GUI, click **Log & Report** > **Forward Traffic**.
2. Locate the log entry that has **DLP** in the **Security Events** column and a **Deny: UTM Blocked** in the **Result** column for this attempted data leak.
3. Double-click that log entry to view more details.



#		Date/Time	Source	Destination	Application	Security Events	Result
1		07:54:19	10.0.1.10	10.200.1.254	HTTP	DLP 1	⛔ Deny: UTM Blocked

4. On the right side of the screen, the **Details** tab shows the forward traffic log information, such as NAT translation, NAT IP, policy ID, and security action.



General

Date	05/13/2016
Time	13:22:55
Duration	6s
Session ID	2117
Virtual Domain	root
NAT Translation	Source

Source

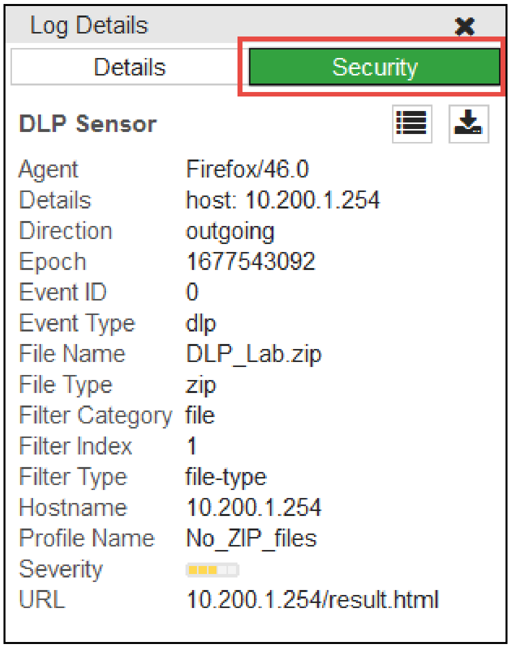
IP	10.0.1.10
NAT IP	10.200.1.1
Port	52878
Country	Reserved
Interface	port3

Destination

IP	10.200.1.254
Port	80
Country	Reserved
Interface	port1

5. Click the **Security** tab to view security log information.

   This tab provides information that is more specific to the security profile, such as event type, file name, file type, filter type, filter category, and security profile name.



DLP Sensor

Agent	Firefox/46.0
Details	host: 10.200.1.254
Direction	outgoing
Epoch	1677543092
Event ID	0
Event Type	dlp
File Name	DLP_Lab.zip
File Type	zip
Filter Category	file
Filter Index	1
Filter Type	file-type
Hostname	10.200.1.254
Profile Name	No_ZIP_files
Severity	▮▮▮▯▯
URL	10.200.1.254/result.html

You can also view DLP logs under **Log & Report** > **Data Leak Prevention**.

The **DLP** logs section will not display if there are no DLP logs. FortiGate will show it after creating logs. If the DLP menu item does not display in the GUI, refresh your browser or log out of the Local-FortiGate GUI and log back in again.

Exercise 2: Quarantining IP Addresses

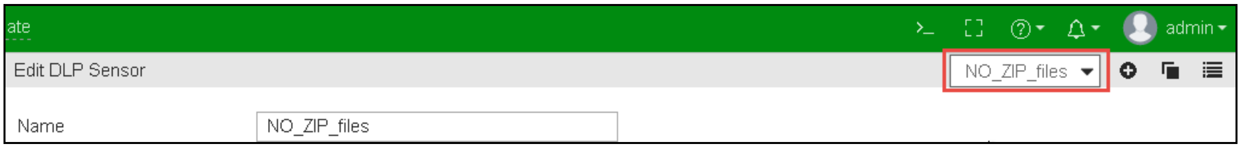
You can configure the DLP filter to quarantine IP addresses that are trying to leak sensitive information. The quarantined IP address will be blocked from accessing the network so that you have time to investigate the issue.

Quarantine an IP Address

Now, you will modify the action of the previously configured DLP filter to quarantine the IP address.

To quarantine an IP address

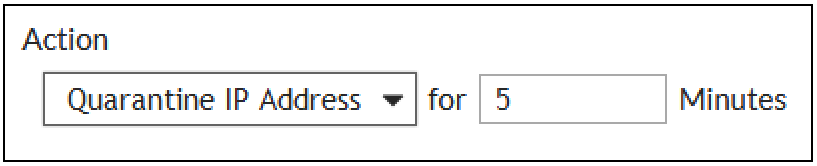
1. On the Local-Windows VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. Click **Security Profiles** > **Data Leak Prevention**.
3. In the upper-right corner of the screen, from the drop-down menu, select **No_ZIP_files**.



Edit DLP Sensor

Name: NO_ZIP_files

4. Select **Seq# 1**, and then click **Edit Filter**.
5. In the Action drop-down list, select **Quarantine IP Address**, and enter an interval of **5** minutes.



Action

Quarantine IP Address for 5 Minutes

6. Click **OK**.
7. Click **Apply**.

Test the Quarantined IP Address

Now, you will test the quarantine action by trying to upload a ZIP file.

To test the quarantined IP address

1. Continuing on the Local-Windows VM, open a web browser and go to the following URL:

   `http://10.200.1.254/fileupload.html`

2. On the web page, click **Browse**.
3. Browse to **Desktop** > **Resources** > **FortiGate-Security** > **DLP** > `DLP_Lab.zip`, and then click **Open**.
4. Click **Submit the file**.

The DLP block message will appear.

5. On the Local-Windows VM, open a few new web browser tabs and go to the following websites:
   - http://10.200.1.254
   - http://10.200.3.254

   A replacement message appears instead of the website. This occurs because the IP address that is sending the request has been quarantined and is not allowed through the firewall policy on FortiGate.

Remove a Quarantined IP Address From the Banned Entry List

Now, you will remove the quarantined IP address from the banned entry list so that you can access the network.

To remove a quarantined IP address from the banned entry list

1. Return to your browser tab where you are logged in to the Local-FortiGate GUI, and click **Monitor** > **Quarantine Monitor**.
2. Select the entry with the banned IP **10.0.1.10**.
3. Click **Delete** to remove it from the banned entry list.
4. Click **OK**.
5. On the Local-Windows VM, open additional web browser tabs and go to a few websites, such as:
   - http://www.bbc.com
   - http://dailymotion.com

   You should be able to access the Internet, even if the five minutes time interval you set has not yet elapsed.
6. Close all browser tabs except for the Local-FortiGate GUI.

Exercise 3: DLP Fingerprinting

DLP fingerprinting is a technique that uses content-based filtering and identifies specific files using one or more cyclic redundancy checks (CRC) for the files in the configured network share.

Configure a DLP Filter for the Network Share

A network share is preconfigured on the Local-Windows VM with a user account of `Administrator` and share name of `DLPshare`.

In the configuration that you uploaded at the beginning of this exercise, FortiGate is preconfigured to access the network share.

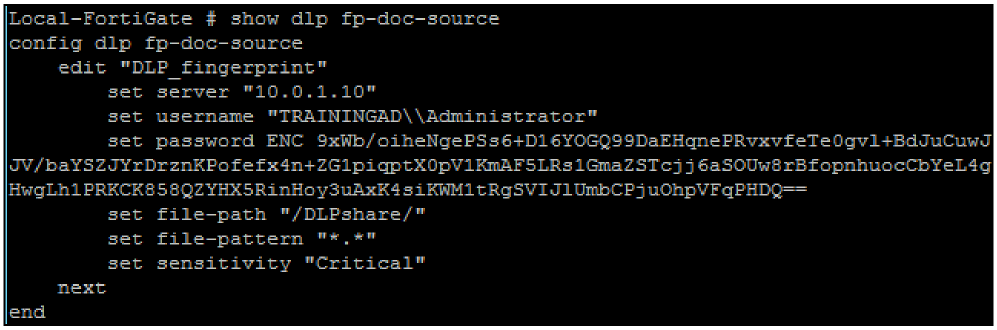
In this procedure, you will first view the DLP configuration for the network share, and then you will configure a new filter for DLP fingerprinting.

To configure a DLP filter for the network share

1. On the Local-Windows VM, open PuTTY and connect over SSH to the **LOCAL-FORTIGATE** saved session.
2. At the login prompt, enter the user name `admin` and password `password`.
3. Enter the following command to check the DLP fingerprinting configuration.

   ```
   show dlp fp-doc-source
   ```

   You will notice that the Local-FortiGate is configured to access the network share configured on Local-Windows with an IP address of `10.0.1.10`.

   ```
   Local-FortiGate # show dlp fp-doc-source
   config dlp fp-doc-source
       edit "DLP_fingerprint"
           set server "10.0.1.10"
           set username "TRAININGAD\\Administrator"
           set password ENC 9xWb/oiheNgePSs6+D16YOGQ99DaEHqnePRvxvfeTe0gvl+BdJuCuwJ
   JV/baYSZJYrDrznKPofefx4n+ZG1piqptX0pV1KmAF5LRs1GmaZSTcjj6aSOUw8rBfopnhuocCbYeL4g
   HwgLh1PRKCK858QZYHX5RinHoy3uAxK4siKWM1tRgSVIJlUmbCPjuOhpVFqPHDQ==
           set file-path "/DLPshare/"
           set file-pattern "*.*"
           set sensitivity "Critical"
       next
   end
   ```

4. Enter the following commands to configure a new filter for DLP fingerprinting in the DLP sensor named **No_ZIP_files**:

   ```
   config dlp sensor
      edit No_ZIP_files
      config filter
      edit 2
      set proto http-post
      set filter-by fingerprint
      set fp-sensitivity Critical
      set action block
   end
   end
   ```

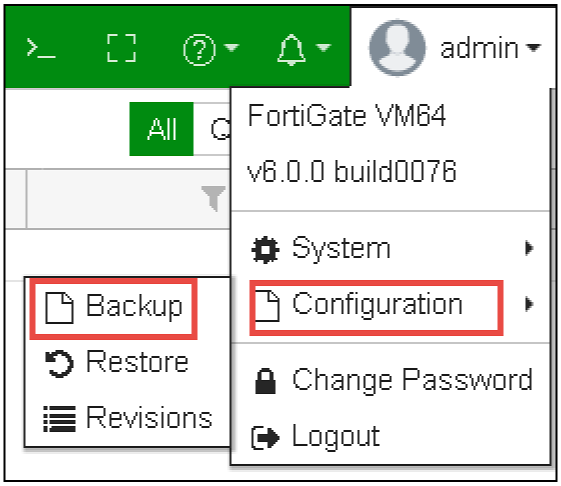
The DLP fingerprinting filter can be configured using only the CLI. After it is configured, it is visible on the GUI.

Add a File to the Network Share

Now, you will add a file to the network share.

To add file to the network share

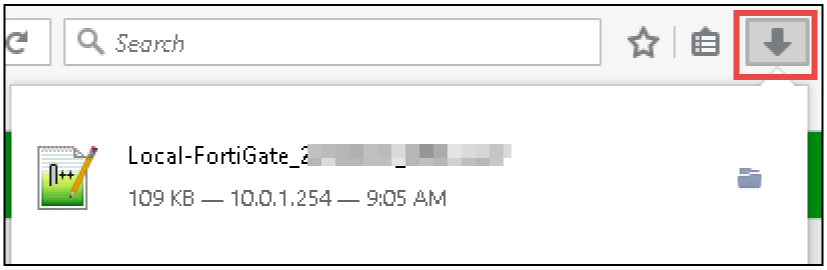
1. Continuing on the Local-Windows VM,open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Backup**.



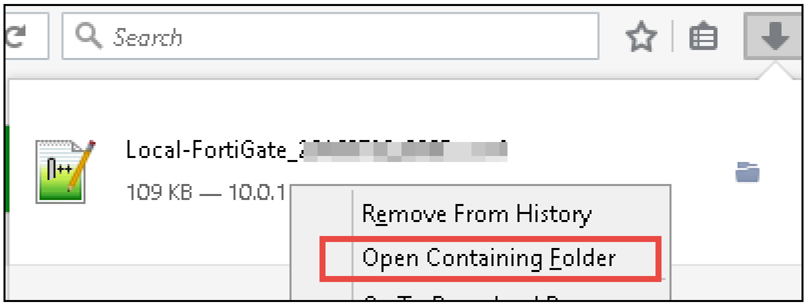
3. Click **OK**.
4. Click **Save File**.
5. Click **OK**.

The file saves to the **Downloads** folder.

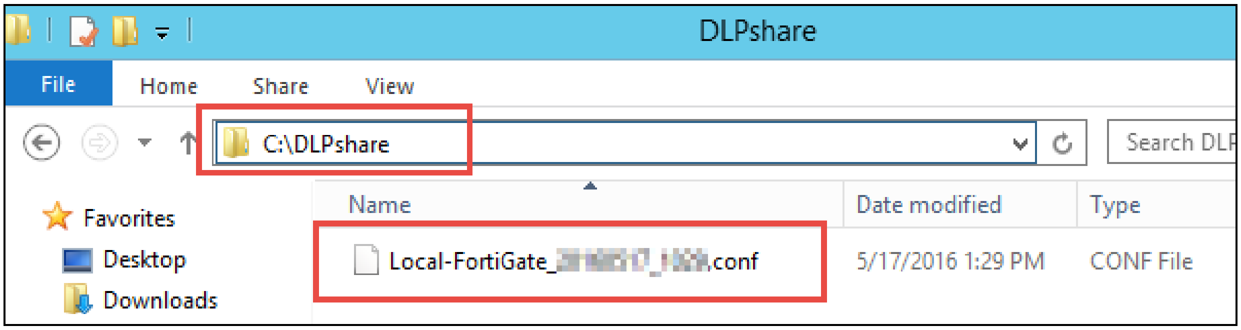
7. Click the down arrow download icon on the top right of the browser.



8. Right-click the backup file for your configuration, and then click **Open Containing Folder**.



9. Right-click the configuration file and click **Copy**.
10. Go to **C:\DLPshare**.
11. Right-click and click **Paste** to paste the configuration file in that folder.



Test DLP Fingerprinting

Now, you will test DLP fingerprinting for the file you added to the network share. DLP fingerprinting is configured based on a schedule. For the purpose of this lab, we will trigger fingerprint checksums manually, using CLI commands. This is because training is conducted at different times globally, and a configured schedule may not work correctly.

To test DLP fingerprinting

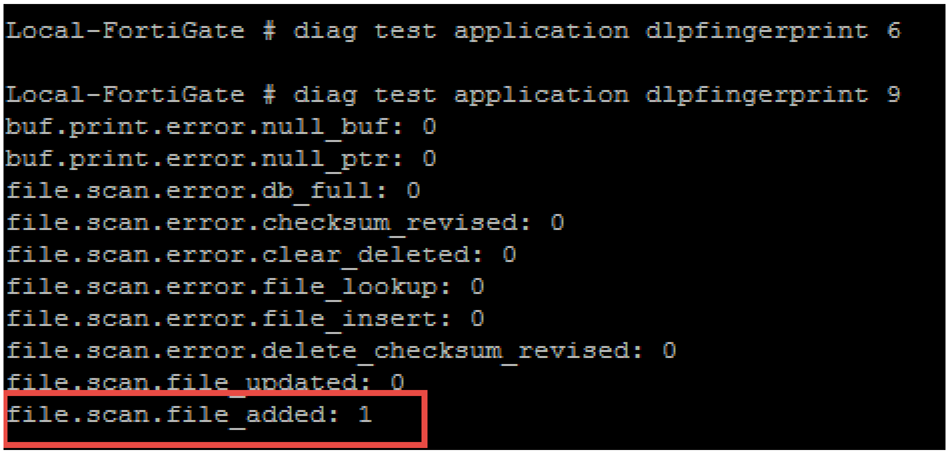
1. Continuing on the Local-Windows VM, return to the**LOCAL-FORTIGATE** PuTTY session, and run the following command to refresh the DLP fingerprint checksums:

```
diagnose test application dlpfingerprint 6
```

2. Run the following command to check the updated checksum:

```
diagnose test application dlpfingerprint 9
```

You will see that a new file has been added.



```
Local-FortiGate # diag test application dlpfingerprint 6

Local-FortiGate # diag test application dlpfingerprint 9
buf.print.error.null_buf: 0
buf.print.error.null_ptr: 0
file.scan.error.db_full: 0
file.scan.error.checksum_revised: 0
file.scan.error.clear_deleted: 0
file.scan.error.file_lookup: 0
file.scan.error.file_insert: 0
file.scan.error.delete_checksum_revised: 0
file.scan.file_updated: 0
file.scan.file_added: 1
```

3. Open a new browser tab and go to the following URL:

   `http://10.200.1.254/fileupload.html`

4. On the web page, click **Browse**, and go to **C:** > **DLPshare** > `Local-FortiGate_<yourtimestamp>.conf`.
5. Click **Open**.
6. Click **Submit the file**.

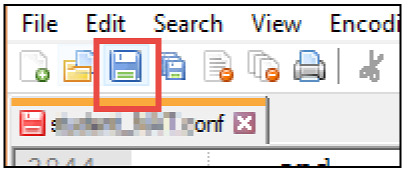
   The file upload should be blocked.

Modify a File in the Network Share

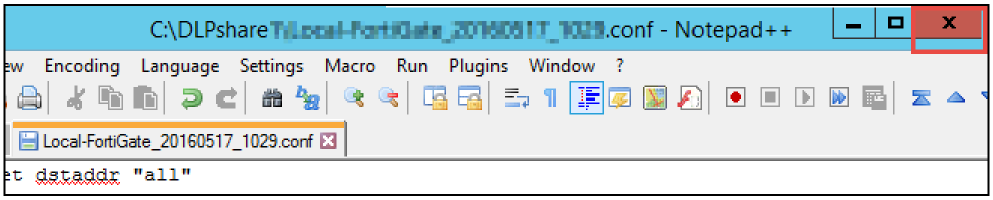
Now, you will modify a file in the network share.

To modify a file in the Network Share

1. Continuing on the Local-Windows VM, open **File Explorer**, and go to **C:** > **DLPshare**.
2. Right-click the FortiGate configuration file and click **Edit with Notepad++**.
3. Make a few small changes to different areas of the configuration.
4. Click **Save**.



5. Close **Notepad++**.


C:\DLPshare[redacted].conf - Notepad++
ew
Encoding
Language
Settings
Macro
Run
Plugins
Window
?
Local-FortiGate_20160517_1029.conf
et dstaddr "all"

Test DLP Fingerprinting With the Modified File

Now, you will test DLP fingerprinting using the modified file in the network share. DLP fingerprinting is configured based on schedule. For the purpose of this lab, you will trigger fingerprint checksums manually, using CLI commands. This is because training is conducted at different times globally and using a configured schedule might not work correctly.

To test DLP fingerprinting with the modified file

1. Continuing on Local-Windows, return to **LOCAL-FORTIGATE** PuTTY session, run the following command to refresh the DLP fingerprint checksums:

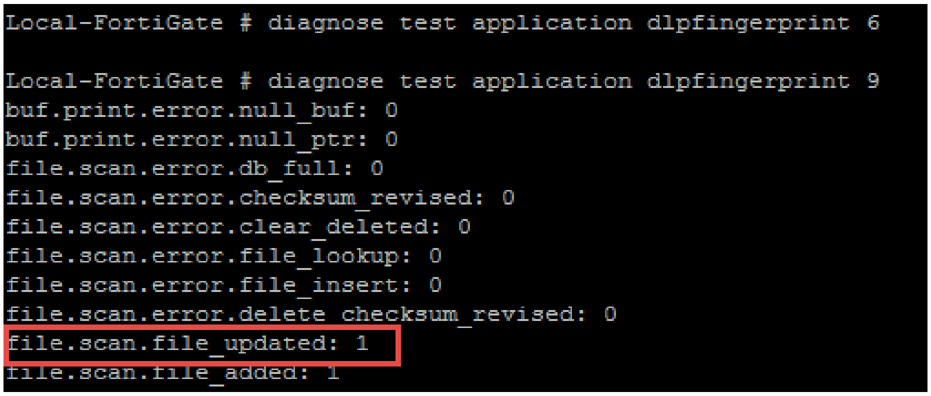
   ```
   diagnose test application dlpfingerprint 6
   ```

   Tip: You can press the up button on your keyboard twice to get that command you entered previously.

2. Run the following command to check the updated checksum:

   ```
   diagnose test application dlpfingerprint 9
   ```

   You will see that the file has been updated.



```
Local-FortiGate # diagnose test application dlpfingerprint 6

Local-FortiGate # diagnose test application dlpfingerprint 9
buf.print.error.null_buf: 0
buf.print.error.null_ptr: 0
file.scan.error.db_full: 0
file.scan.error.checksum_revised: 0
file.scan.error.clear_deleted: 0
file.scan.error.file_lookup: 0
file.scan.error.file_insert: 0
file.scan.error.delete_checksum_revised: 0
file.scan.file_updated: 1
file.scan.file_added: 1
```

3. Open a browser and go to the following URL:

   ```
   http://10.200.1.254/fileupload.html
   ```

4. On the web page, click **Browse** and go to **C:** > **DLPshare**.
5. Click the configuration file.
6. Click **Open**.
7. Click **Submit the file**.

   The file upload should be blocked (assuming that changes to file were not too large, and not made in too many areas).

Fingerprinting breaks the file into chunks and performs checksums on each part. By default, DLP will detect a match if any part's checksum from the fingerprint matches.