

DO NOT REPRINT
© FORTINET



NSE 4 Immersion Lab Guide

for FortiOS 7.2

FORTINET®
Training Institute

DO NOT REPRINT

© FORTINET

Fortinet Training Institute - Library

<https://training.fortinet.com>

Fortinet Product Documentation

<https://docs.fortinet.com>

Fortinet Knowledge Base

<https://kb.fortinet.com>

Fortinet Fuse User Community

<https://fusecommunity.fortinet.com/home>

Fortinet Forums

<https://forum.fortinet.com>

Fortinet Product Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguard.com>

Fortinet Training Program Information

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

Fortinet | Pearson VUE

<https://home.pearsonvue.com/fortinet>

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

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



9/6/2022

TABLE OF CONTENTS

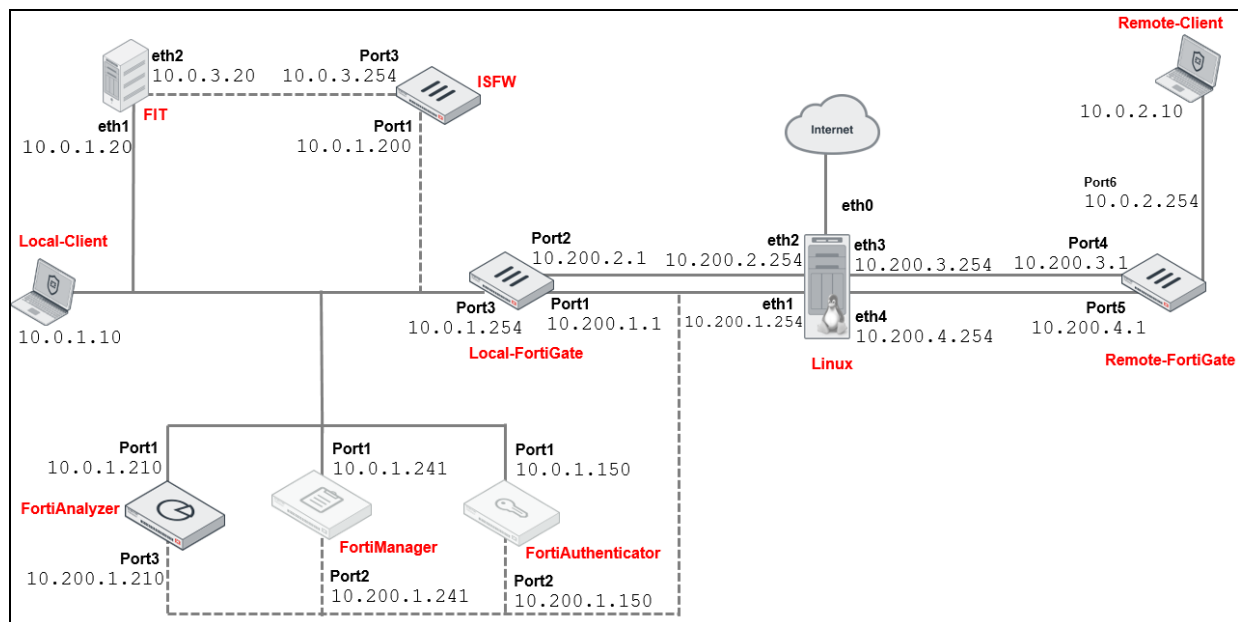
Network Topology	5
Lab Prerequisite: Fortinet CA SSL Certificate	6
Lab 1: Firewall Policy, DNAT, and Authentication	11
Exercise 1: Configuring Firewall Policies	13
Network Topology	13
Requirements	13
Solution	15
Exercise 2: Configuring Authentication	16
Requirements	16
Solution	17
Lab 2: SSL and Content Inspection	18
Exercise 1: Configuring Security Profiles	20
Network Topology	20
Configure Security Profiles	20
Solution	23
Exercise 2: Configuring Antivirus Scanning	24
Network Topology	24
Configure Antivirus Scanning	24
Solution	26
Lab 3: IPS and DoS	27
Exercise 1: Blocking Known Exploits	29
Network Topology	29
Block Known Exploits	29
Solution	31
Exercise 2: Mitigating a DoS Attack	32
Network Topology	32
Mitigate a DoS Attack	32
Solution	34
Lab 4: SSL VPN and IPsec VPN	35
Exercise 1: Configuring SSL VPN	37
Network Topology	37
Requirements	37
Solution	39

DO NOT REPRINT

© FORTINET

Exercise 2: Configuring IPsec	40
Network Topology	40
Requirements	40
Solution	42
Lab 5: ECMP Routing	43
Exercise 1: Configuring Static Routing	45
Network Topology	45
Requirements	45
Solution	47
Exercise 2: Configuring ECMP Load Balancing	48
Requirements	48
Solution	49
Lab 6: Fortinet Security Fabric	50
Exercise 1: Configuring the Security Fabric on the Root and Downstream FortiGate Devices	52
Network Topology	52
Requirements	52
Solution	54
Exercise 2: Authorizing Devices and Running the Security Rating	55
Requirements	55
Solution	56
Lab 7: HA	57
Exercise 1: Configuring HA	59
Network Topology	59
Requirements	59
Test the Configuration	60
Solution	61
Exercise 2: Configuring the HA Management Interface	62
Requirements	62
Solution	63

Network Topology



Lab Prerequisite: Fortinet CA SSL Certificate

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

In this lab, you will install the preloaded Fortinet_CA_SSL certificate.

Objectives

- Install the preloaded Fortinet_CA_SSL certificate in Firefox

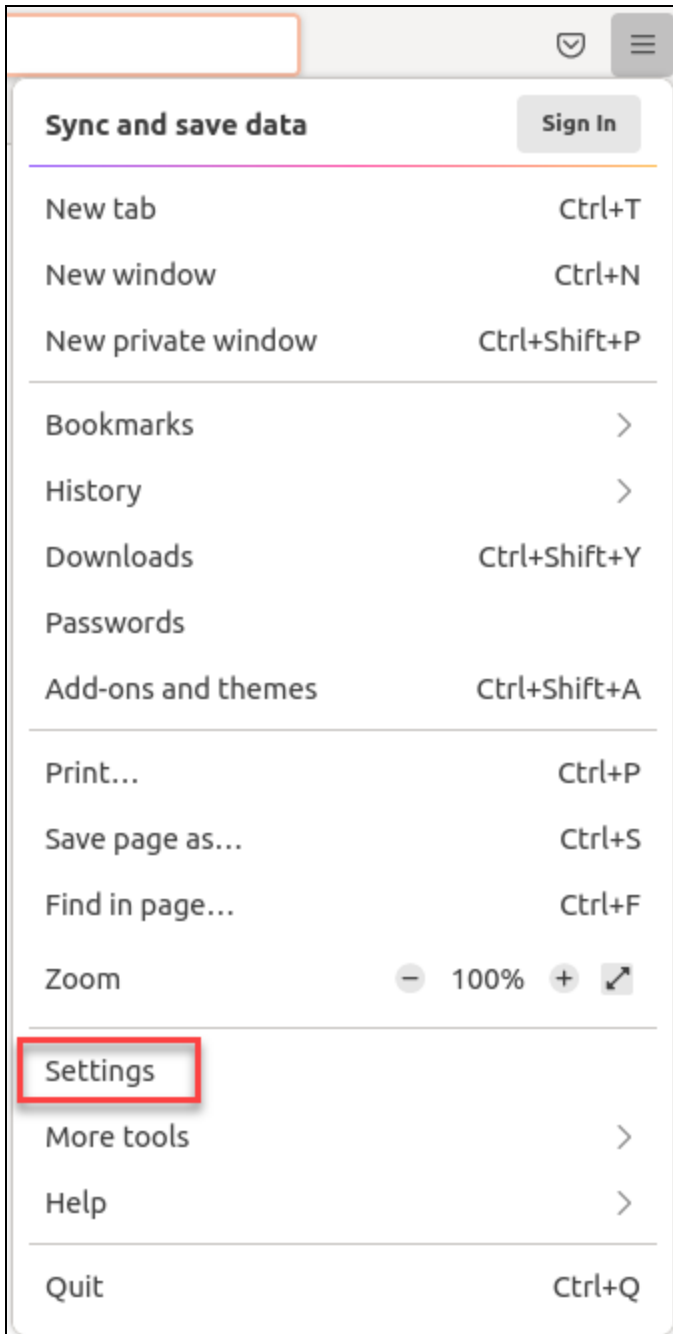
Time to Complete

Estimated: 5 minutes

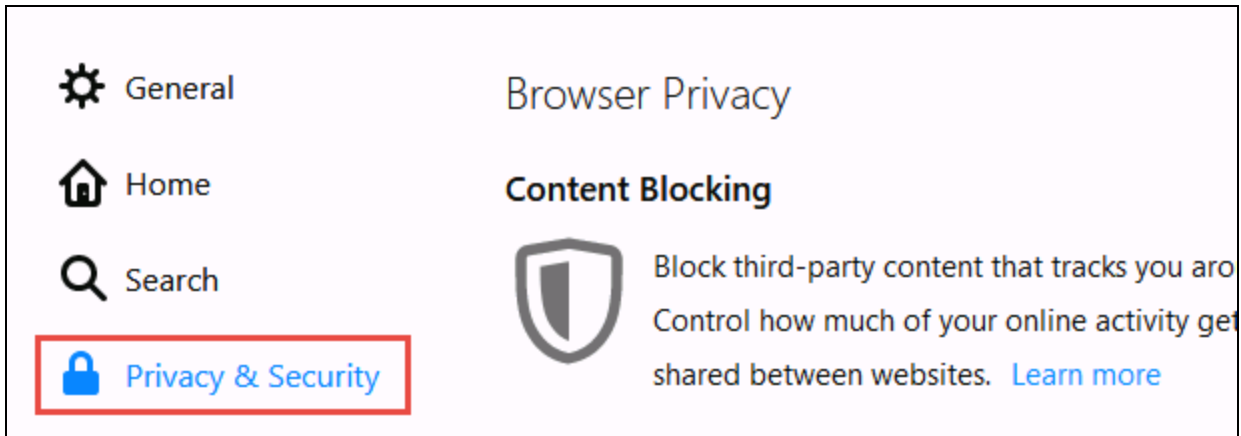
Install the Fortinet_CA_SSL Certificate

To install the Fortinet_CA_SSL certificate in the browser

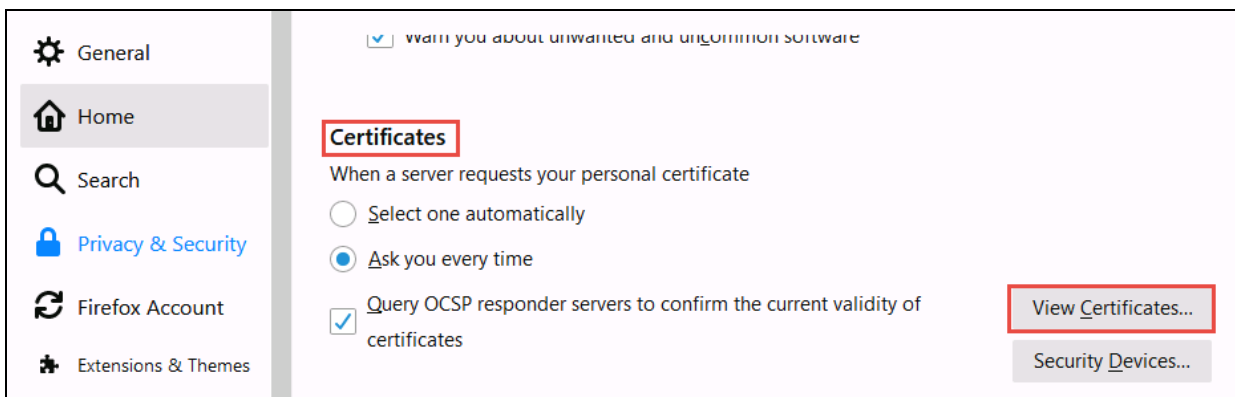
1. On the Local-Client VM, open Firefox, in the upper-right corner, click the **Open menu** icon, and then click **Settings**.



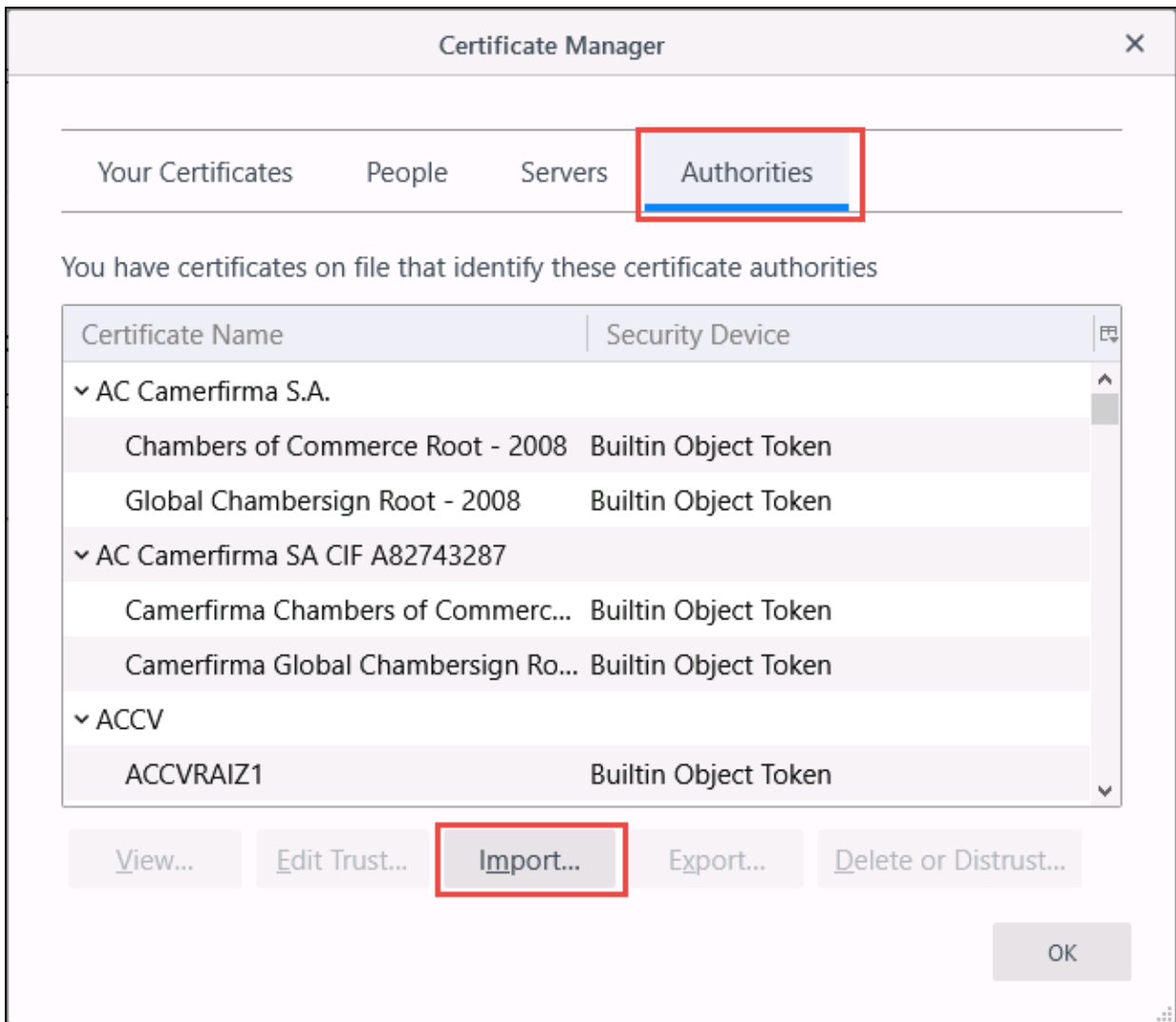
2. Click **Privacy & Security**.



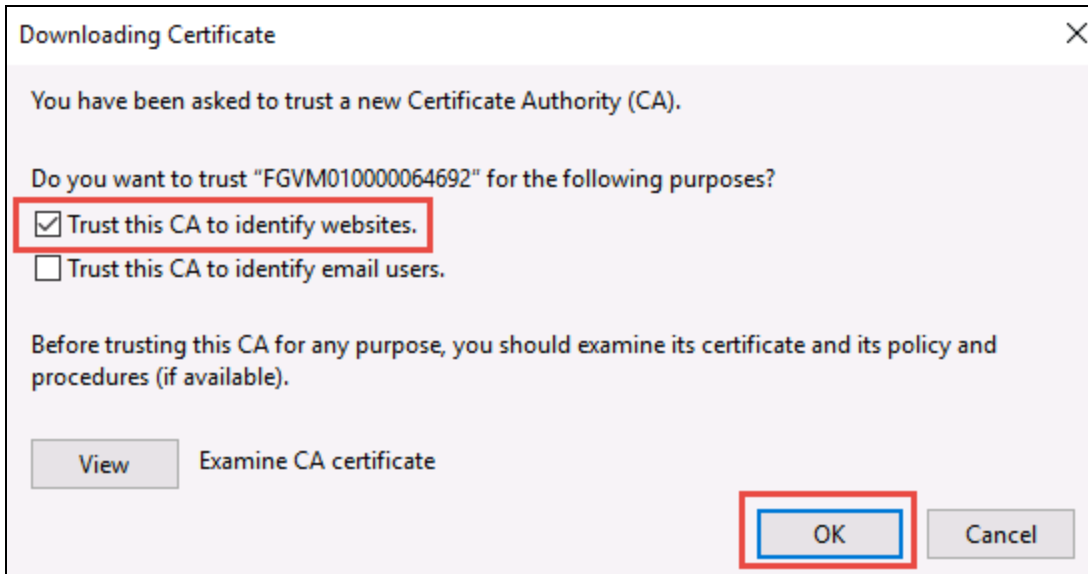
3. In the **Certificates** section, click **View Certificates**.



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



5. Click **Desktop > Resources > NSE4-Immersion > Fortinet_CA_SSL.cer**, and then click **Open**.
6. In the **Downloading Certificate** window, select **Trust this CA to identify websites**, and then click **OK**.



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

7. Click **OK**.
8. Restart Firefox.

Lab 1: Firewall Policy, DNAT, and Authentication

In this lab, you will examine how to configure firewall objects and policies, NAT, and firewall authentication. You will verify each objective and test access control on FortiGate devices.

Objectives

- Configure a firewall address object and a firewall policy to allow traffic from the local subnet
- Configure a firewall policy, and reorder the sequence of firewall policies to block outbound ICMP traffic
- Configure a VIP and DNAT firewall policy to allow inbound traffic from the remote subnet
- Configure server-based authentication using LDAP to authenticate users
- Configure captive portal to force authentication for users accessing the internet

Time to Complete

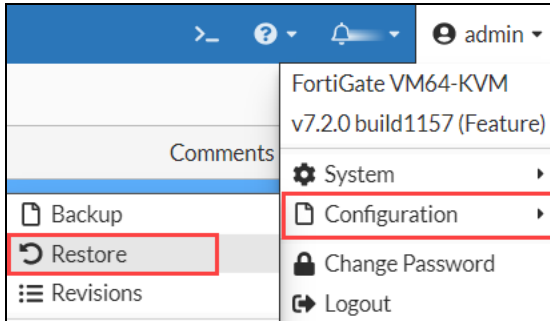
Estimated: 40 minutes

Prerequisites

Before beginning this lab, you must restore configuration files on Remote-FortiGate and Local-FortiGate. The ISFW configuration is preloaded.

To restore the Remote-FortiGate configuration file

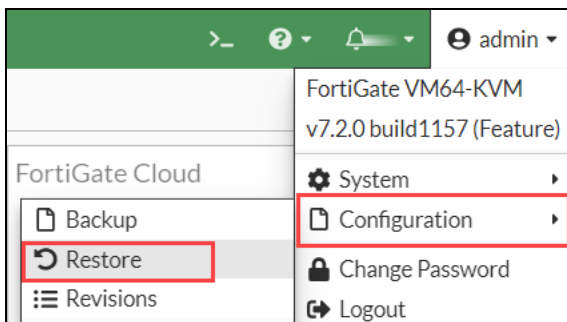
1. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration > Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > NSE4-Immersion > Policy-NAT-Auth > remote-initial.conf**, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

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



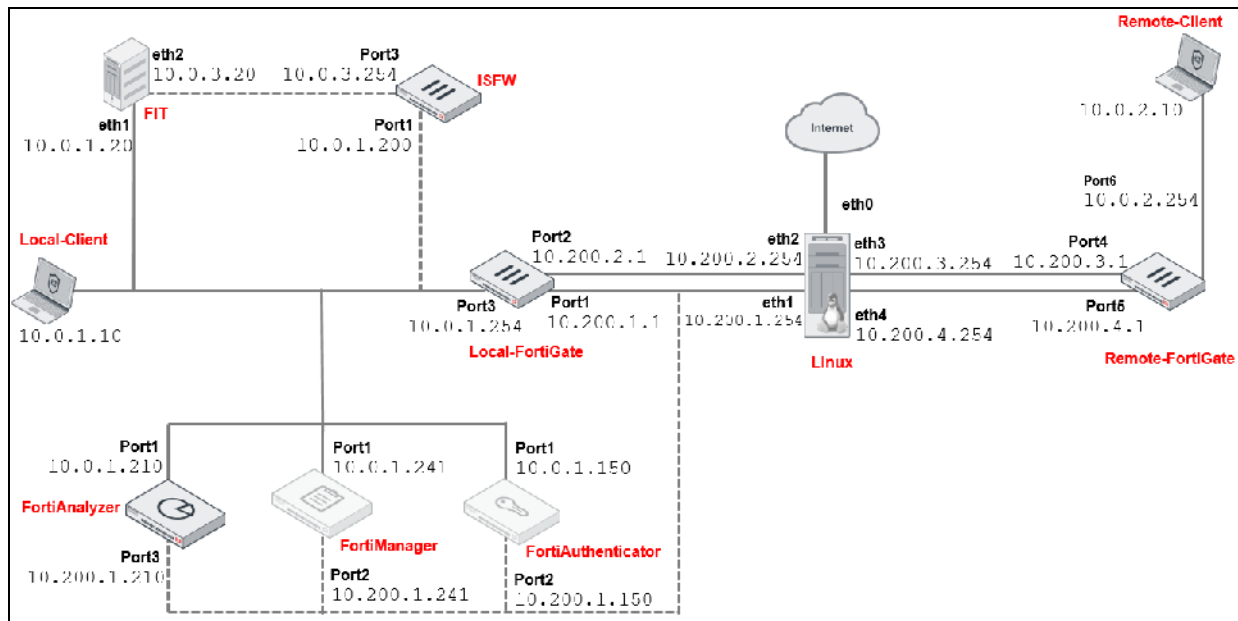
3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > NSE4-Immersion > Policy-NAT-Auth > local-firewall-policy.conf**, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring Firewall Policies

In this exercise, you will examine how to configure firewall address objects, firewall policies, and VIP based on the following requirements:

- Configure a firewall address object and a firewall policy on Local-FortiGate
- Configure a new firewall policy to block ICMP traffic and reorder accordingly
- Configure an inbound VIP and a firewall policy to allow inbound traffic

Network Topology



Review the current configuration before proceeding to the next step. You will have basic connectivity from Fortinet devices to FortiManager so that you can perform license verification. Do not make changes to the policies that allow this traffic.

Requirements

To configure a firewall address object and a firewall policy on Local-FortiGate

1. Create a new firewall address object using the following settings:

Field	Value
Name	LOCAL_SUBNET
IP	10.0.1.0/24

2. Create a new firewall policy to allow access to the internet, and name it `Internet_Access`.
3. Configure the **Internet_Access** firewall policy to use the address object you created.
4. Select only services that allow typical web and troubleshooting traffic to pass through.
5. Enable SNAT and logging, and then set **Logging Options** to **All Sessions**.

To generate traffic and view logs on Local-FortiGate

1. Attempt to access several websites using the client machine behind FortiGate.
2. Display traffic logs that match the **Internet_Access** firewall policy.
3. Identify and review the log entries linked to the websites you accessed.

To configure a new firewall policy and reorder the sequence to block ICMP traffic on Local-FortiGate

1. Create a new firewall policy to block a specific type of traffic, and name it `Block_Ping`.
2. Configure the **Block_Ping** firewall policy to block ICMP traffic for the local subnet to the internet, and enable logging.
3. Reorder the **Block_Ping** firewall policy, as required, to control ICMP traffic.
4. Confirm the new firewall policy is working using the client machine behind FortiGate.

To configure a VIP firewall object and an inbound firewall policy on Local-FortiGate

1. Create a new VIP to allow access to the local server (Local-Client), and use the external interface where inbound traffic is coming in.
2. Configure the VIP using the following settings:

Field	Value
Name	VIP-INTERNAL-HOST
External IP	10.200.1.200
Mapped IP	10.0.1.10

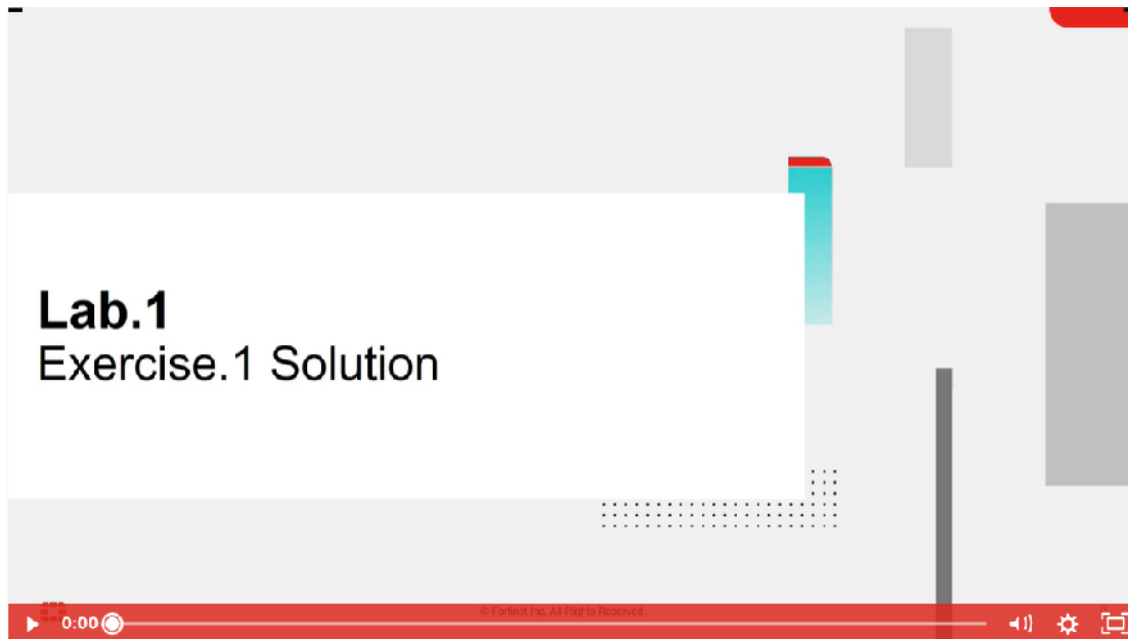
3. Create a new firewall policy to allow inbound web traffic, and name it `Web-Server-Access`.
4. Configure the **Web-Server-Access** firewall policy to use the VIP object you created and to log all sessions.
5. Attempt to access the VIP you created using an external client host machine to generate web traffic.

Solution

Watch this short video for the solution to Lab 1, Exercise 1.



Videos are converted to static images in print-based outputs (navigate to <https://nsei.wistia.com/medias/mhd1va6rqg> to view the video).



Exercise 2: Configuring Authentication

In this exercise, you will examine how to configure LDAP remote service and captive portal based on the following requirements:

- Configure a remote user group to contain specific LDAP user groups and assign it to a firewall policy
- Configure captive portal to use a local firewall user group to force authentication

Requirements

To assign an LDAP user group to a firewall user group and assign it to the firewall policy

1. Modify the **Remote-users** user group to add the **AD_users** Active Directory user group, located in the **External_Server** remote server.
2. Configure the **Internet_Access** firewall policy to include the **Remote-users** group and change policy **Inspection Mode** to **Proxy-based** to match the web filter profile inspection mode.
3. Enable the web filter, and then select the **Category_Monitor** profile.
4. Set logging on the firewall policy to allow all sessions.
5. Attempt to access websites that belong to blocked categories defined in the web filter profile, such as elite-hackers.com.
6. Log in with the username `aduser1` and password `Training!`.
7. In the dashboard, review the current authenticated firewall users, and then deauthenticate **aduser1**.

To configure captive portal and assign a user group

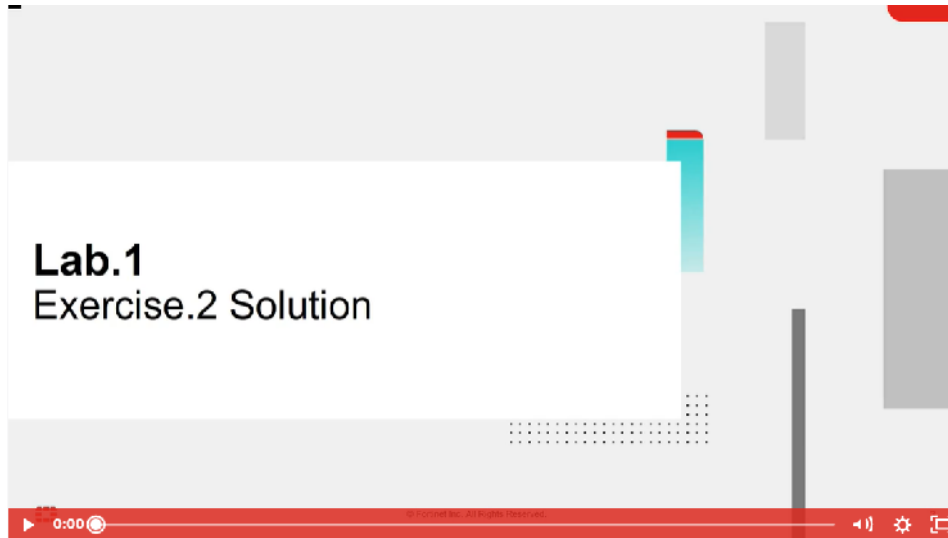
1. Configure the **Internet_Access** firewall policy to allow traffic without user groups.
2. Create a new firewall user group, and name it `CP-group`.
3. Configure the **CP-group** user group to contain the **student** local user.
4. Enable captive portal on port3 to use the local authentication, and then select the user group you just created.
5. Using the CLI, enable the disclaimer replacement message on the **Internet_Access** firewall policy.
6. Attempt to access several websites, such as `www.eicar.org`, using the client machine behind FortiGate to force authentication.
7. Log in with the username `student` and password `fortinet`.
8. Accept the terms and disclaimer agreement.

Solution

Watch this short video for the solution to Lab 1, Exercise 2.



Videos are converted to static images in print-based outputs (navigate to <https://nsei.wistia.com/medias/9bo14zpi8z> to view the video).



Lab 2: SSL and Content Inspection

In this lab, you will examine how to configure full SSL and content inspection for encrypted internet-bound traffic, and apply the configured security actions.

Objectives

- Configure a full SSL inspection profile and enable security inspection on the firewall policy
- Configure a web filter profile based on a FortiGuard category-based filter
- Configure an application profile to override applications based on filter type
- Configure an antivirus profile to block access to infected files

Time to Complete

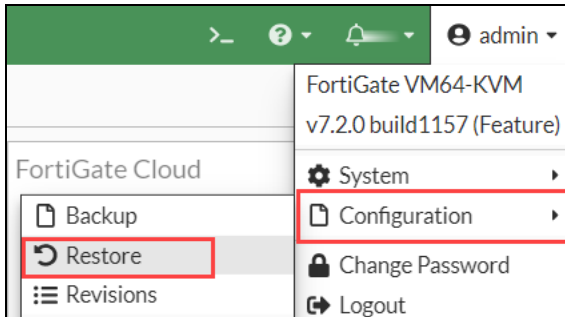
Estimated: 50 minutes

Prerequisites

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

To restore the Local-FortiGate configuration file

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



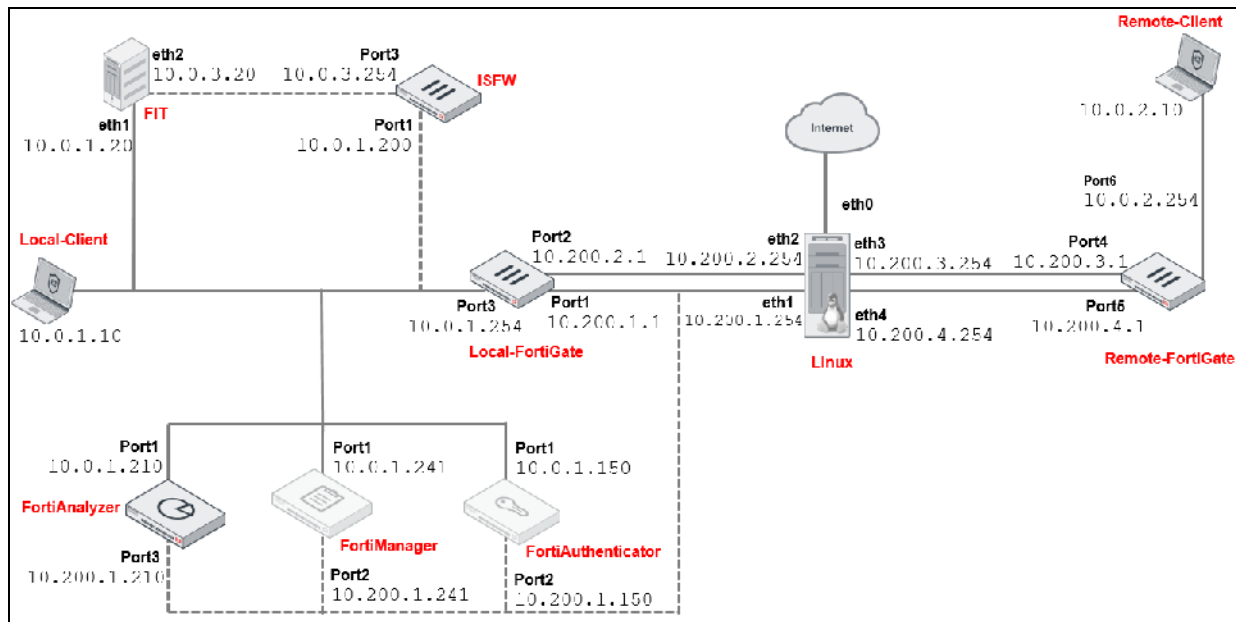
3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > NSE4-Immersion > Initial-Configuration > local-initial.conf**, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring Security Profiles

In this exercise, you will examine how to configure an SSL/SSH inspection profile, a web filter profile, and an application filter profile based on the following requirements:

- Configure an SSL/SSH inspection profile on Local-FortiGate
- Review the FortiGate settings
- Determine web filter categories
- Configure a FortiGuard category-based web filter
- Configure an application filter override
- Configure an application signature override

Network Topology



Review the current configuration before proceeding to the next step. You will have basic connectivity from Fortinet devices to FortiManager so that you can perform license verification. Do not make changes to the policies that allow this traffic.

Configure Security Profiles

To configure a full SSL inspection profile and a firewall policy on Local-FortiGate

1. Create a new SSL/SSH inspection profile, and name it `Custom_Full_Inspection`.
2. Configure the **Custom_Full_Inspection** profile to perform full inspection, and to allow invalid SSL certificates.

3. Configure the **Full_Access** firewall policy to enable a web filter, and then select the SSL inspection profile you created.
4. Set logging on the firewall policy to log all sessions.
5. Try to access secured websites.

To review the FortiGate settings

1. Connect to the Local-FortiGate GUI, and then on the dashboard, confirm that the web filtering service is licensed and active.
2. In the **Full_Access** policy, set the **Inspection Mode** setting to **Flow-Based**.

To determine web filter categories

1. On the FortiGuard website, access the web filter lookup tool.
2. Use the web filter lookup tool to search for the following URLs:
 - www.twitter.com
 - www.skype.com
 - www.bing.com
 - www.dailymotion.com

Later, you will test web filtering using the same websites.

To configure the web filter security profile

1. In the default web filter profile, set the **Inspection Mode** to **Flow-Based**.
2. In the default web filter profile, verify that the FortiGuard category-based filter is enabled, and then review the default actions for each category.
3. Based on the category assigned to the URLs that you searched for in the previous procedure, apply the following actions:

Website	Action
www.twitter.com	Block
www.skype.com	Warning
www.bing.com	Allow
www.ask.com	Allow
www.dailymotion.com	Block

4. In the firewall policy, enable the web filter profile.
5. Try to access the websites listed in the table above.
What results do you get?
6. Modify the web filter profile to allow access to `www.twitter.com` and `www.dailymotion.com`.

To configure an application filter override to block excessive bandwidth

1. Modify the default application control profile to add a new category and application filter override.
2. Configure the category to block access to `www.twitter.com`.

3. Configure the new override to block the excessive bandwidth type of traffic.
4. Enable the option to display a replacement message when blocking HTTP-based applications.
5. In the **Full_Access** firewall policy, set **Inspection Mode** to **Flow-based**.
6. Enable the application profile on the firewall policy.

To configure an application signature override to allow Dailymotion on Local-FortiGate

1. Modify the default application control profile to add a new application signature override.
2. Configure the new override to allow **Dailymotion** application traffic, and then reorder override rules accordingly.
3. Try to access a website, such as <http://dailymotion.com>.

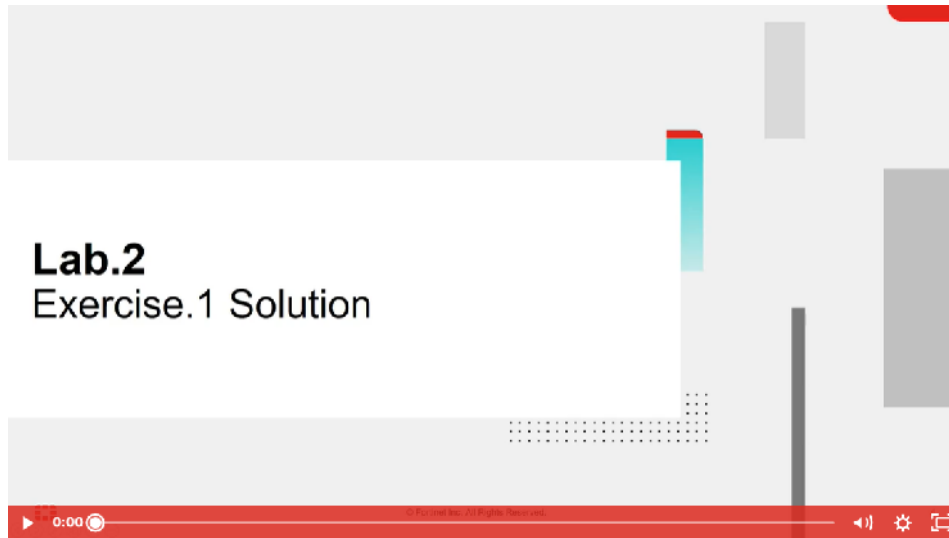
You may need to close the browser, and then open a new browser window to access the website.

Solution

Watch this short video for the solution to Lab 2, Exercise 1.



Videos are converted to static images in print-based outputs (navigate to <https://nse.wistia.com/medias/f3a1a59zli> to view the video).

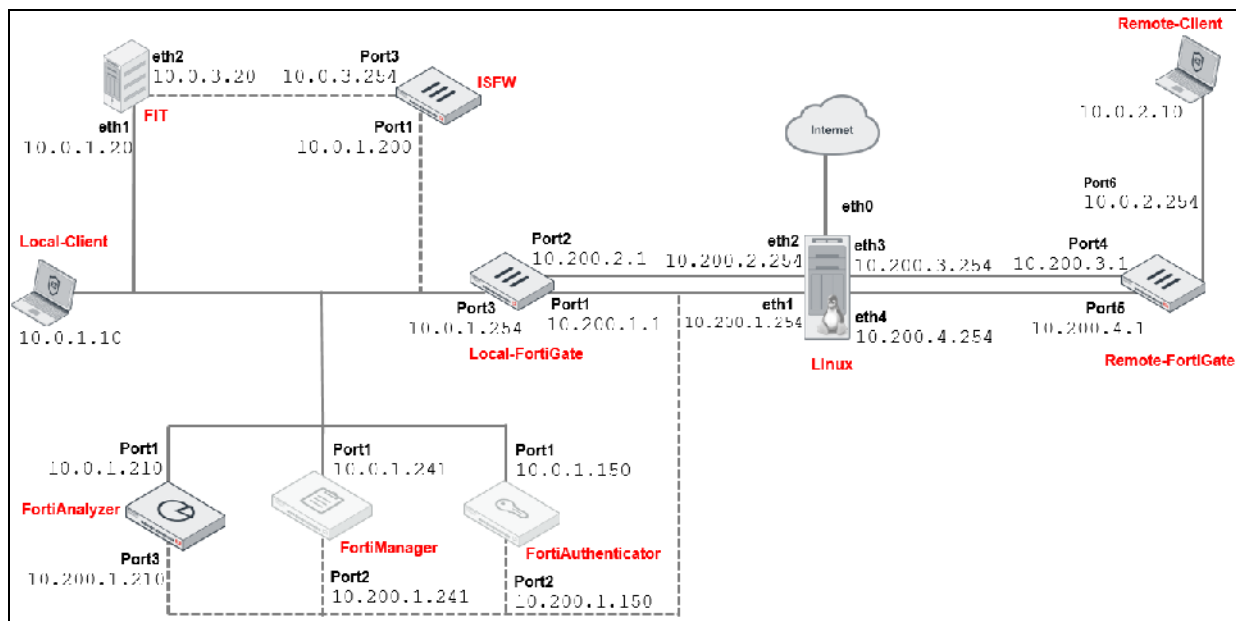


Exercise 2: Configuring Antivirus Scanning

In this exercise, you will examine how to configure and monitor antivirus scanning in a flow-based profile based on the following requirements:

- Configure antivirus scanning in flow-based inspection mode
- Test the antivirus profile using HTTP and FTP
- Review antivirus logs

Network Topology



Review the current configuration before proceeding to the next step. You will have basic connectivity from Fortinet devices to FortiManager so that you can perform license verification. Do not make changes to the policies that allow this traffic.

Configure Antivirus Scanning

To verify the antivirus profile settings

1. In the default antivirus profile, verify that **AntiVirus Scan** is set to block and that the feature set is set to **Flow-Based**.
2. In the profile, in the **Inspected Protocols** section, ensure that **HTTP** and **FTP** are enabled.

To change the firewall policy to apply an antivirus profile

1. Modify the **Full_Access** firewall policy to disable the web filter and application control.
2. In the firewall policy, disable the **Web Filter** and **Application Control** security profiles.
3. In the firewall policy, enable the antivirus profile.

To test the antivirus configuration

1. Access the website `http://10.200.1.254/test_av.html`.
2. In the **Download area** section, left click on any EICAR sample file. What is the result?
3. Right click the `eicar.com.txt` file, select **Save Link As**, and then save the file on the desktop.
What is the result when you download the file using the **Save Link As** method?



FortiGate allows the file to download. However, after FortiOS finishes its inspection, the payload is either released to the destination (if the traffic is clean) or dropped and replaced with a message (if the traffic contains violations). FortiGate injects the block message into the partially downloaded file. You can use Notepad to open and view the file.

4. Open the file in Notepad. What do you notice in the contents of the file?
5. Delete the downloaded file.

To test the antivirus configuration for FTP download

1. Use FileZilla FTP client software to connect to the FTP server.
2. On the **Site Manager** icon, select **Linux**.
3. On the remote site, attempt to download the file `eicar.com`.
What connection errors do you see?



If FortiGate detects a violation in the traffic, it issues a reset packet to the receiver, which terminates the connection and prevents the payload from being sent successfully.

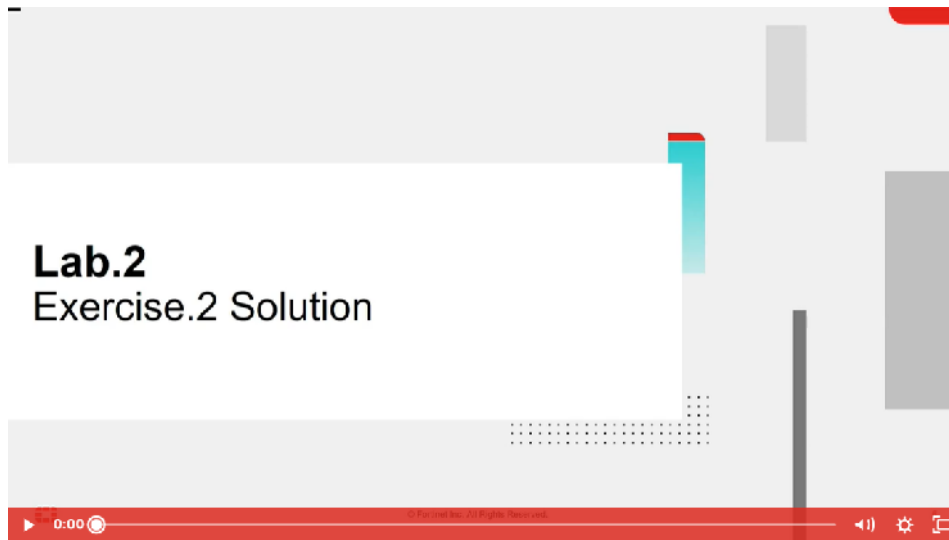
4. Close the FTP client.
5. Review the log entries for the traffic and for the security profile.

Solution

Watch this short video for the solution to Lab 2, Exercise 2.



Videos are converted to static images in print-based outputs (navigate to <https://nsei.wistia.com/medias/r27ua70et9> to view the video).



Lab 3: IPS and DoS

In this lab, you will examine how to set up intrusion prevention system (IPS) profiles and denial of service (DoS) policies. You will also use a vulnerability scanner and a custom script to generate attacks on Local-FortiGate.

Objectives

- Protect your network against known attacks using IPS signatures
- Mitigate and block DoS attacks

Time to Complete

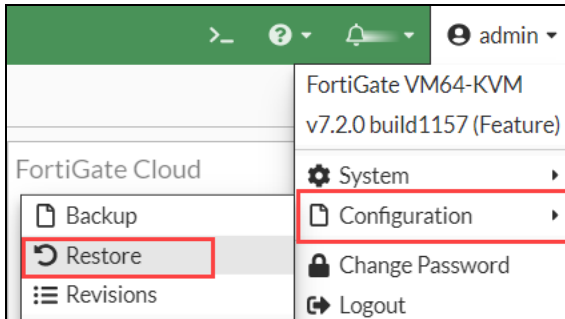
Estimated: 25 minutes

Prerequisites

Before beginning this lab, you must restore configuration files on Local-FortiGate.

To restore the Local-FortiGate configuration file

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



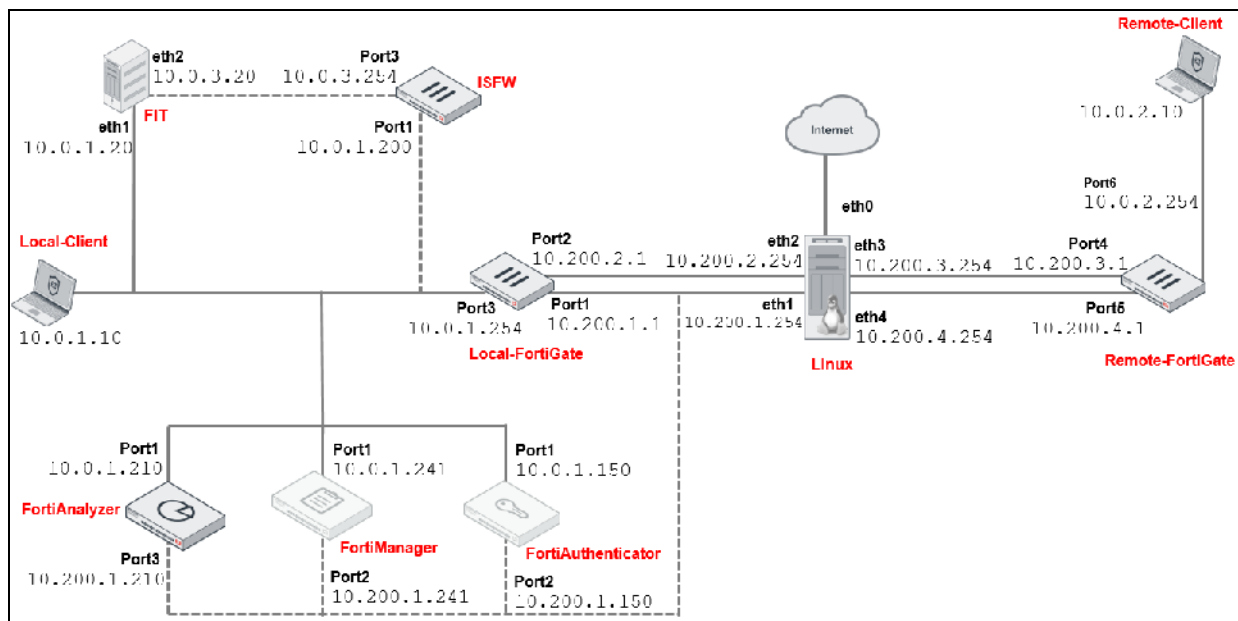
3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > NSE4-Immersion > IPS > local-IPS.conf**, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Blocking Known Exploits

In this exercise, you will examine how to configure an IPS inspection profile, a virtual IP address, and a firewall policy. You will also generate an attack and monitor IPS logs based on the following requirements:

- Configure an IPS inspection security profile
- Configure a new virtual IP address and a firewall policy, and then apply the IPS security profile
- Generate an attack from the Linux server
- Monitor IPS logs on FortiGate

Network Topology



Review the current configuration before proceeding to the next step. You will have basic connectivity from Fortinet devices to FortiManager so that you can perform license verification. Do not make changes to the policies that allow this traffic.

Block Known Exploits

To configure IPS sensor

1. Configure a new IPS inspection profile and name it **WEBSERVER**.
2. In the new IPS profile, create an IPS filter to add a severity of **medium**, **high**, or **critical**.

To create a virtual IP object

1. Create a new VIP object to allow access to the local server (Local-Client), and use the external interface that receives inbound traffic.
2. Configure the VIP using the following settings:

Field	Value
Name	VIP-WEB-SERVER
Interface	port1
External IP address/range	10.200.1.200
Map to IPv4 address/range	10.0.1.10

To configure a new firewall policy and apply the IPS security profile

1. Create a new firewall policy to allow inbound web traffic, and name it `Web_Server_Access_IPS`.
2. Configure the **Web_Server_Access_IPS** firewall policy to use the VIP object you created and to log all sessions.
3. Apply the **WEBSERVER** IPS profile in the security profile section.

To generate attacks and view IPS logs

1. Use PuTTY on Local-Client VM to connect over SSH to the saved Linux session.
2. Log in with the username `student` and password `password`.
3. Run the following script to start the attacks on the *VIP-WEB-SERVER* public IP address:

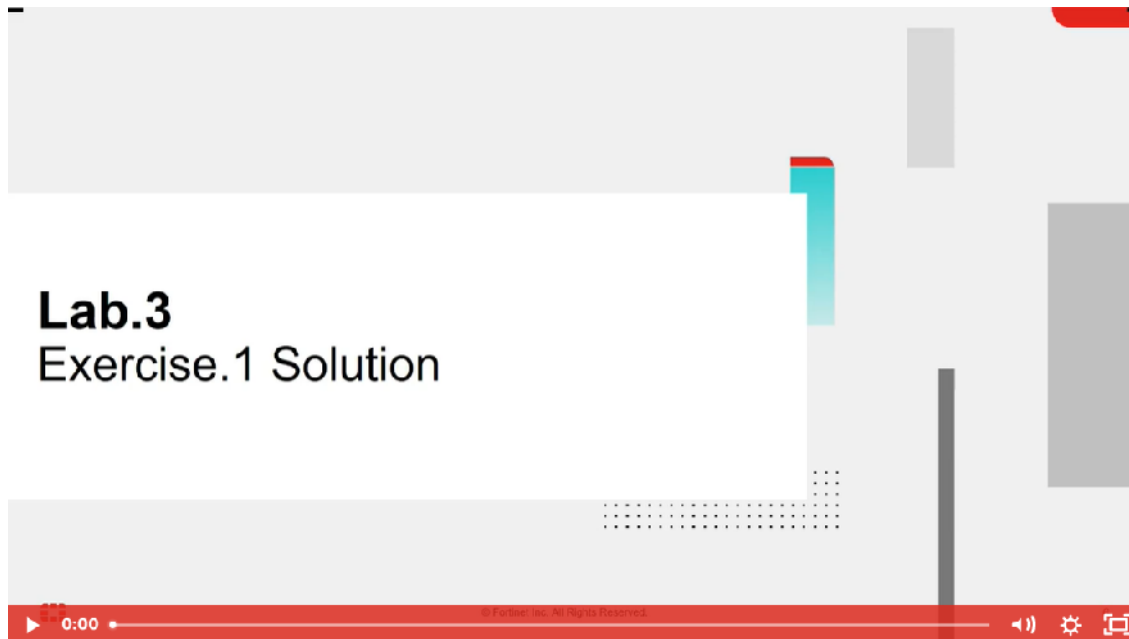
```
nikto.pl -host <Server external IP>
```
4. Leave the PuTTY session open (you can minimize it) so that the Linux server continues to generate traffic.
5. On FortiGate, review the log entries for the detected and dropped attacks.

Solution

Watch this short video for the solution to Lab 3, Exercise 1.



Videos are converted to static images in print-based outputs (navigate to <https://nsei.wistia.com/medias/h8ran992gn> to view the video).

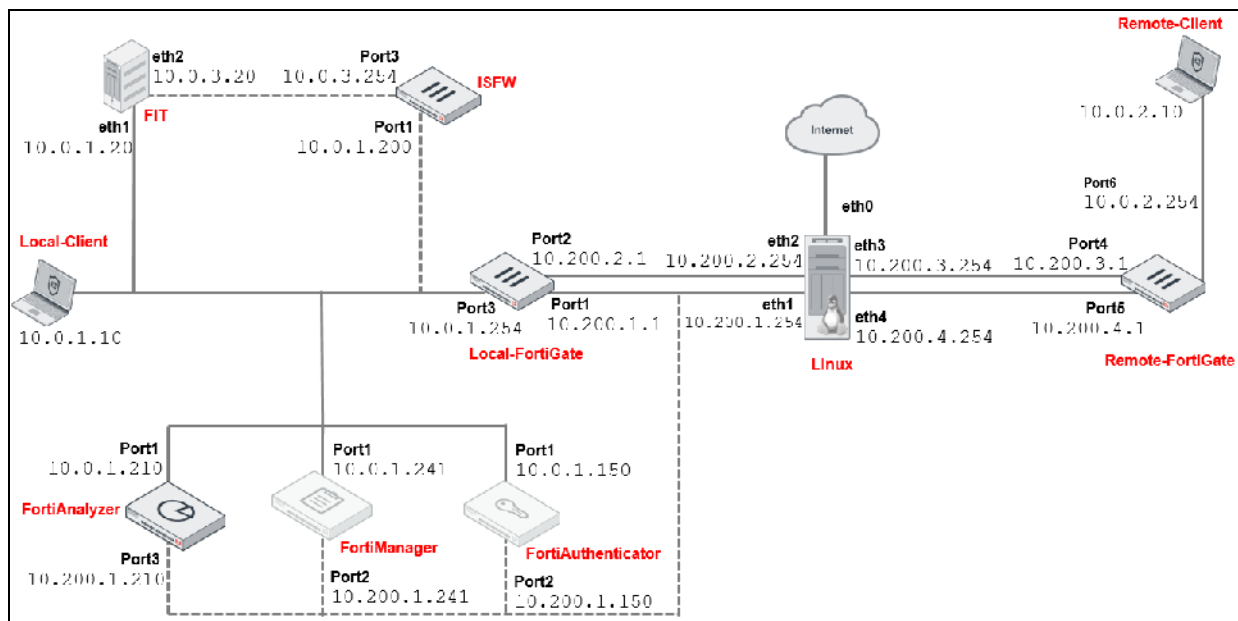


Exercise 2: Mitigating a DoS Attack

In this exercise, you will examine how to configure an IPv4 DoS policy, set the ICMP floods threshold, generate an ICMP flood, and view anomaly logs based on the following requirements:

- Create a new IPv4 DoS policy for port
- Configure the policy to block ICMP floods with a threshold of 200
- Generate an ICMP flood
- View anomaly logs on FortiGate

Network Topology



Review the current configuration before proceeding to the next step. You will have basic connectivity from Fortinet devices to FortiManager so that you can perform license verification. Do not make changes to the policies that allow this traffic.

Mitigate a DoS Attack

To create a DoS policy

1. Create a IPv4 DoS policy and name it `ICMP_Floods`.
2. Configure the DoS policy to block ICMP attacks on port1 from all source addresses, destination addresses, and services.

3. Under **L4 Anomalies**, enable logging for **icmp_flood**.
4. Set the action to **Block**, with a threshold value of **200**.

To test DoS policy and view anomaly logs

1. Use the PuTTY on the Local-Client VM to connect over SSH to the saved Linux session.
2. Log in with the username `student` and password `password`.
3. Enter the following command to generate an ICMP flood to the Local-FortiGate:

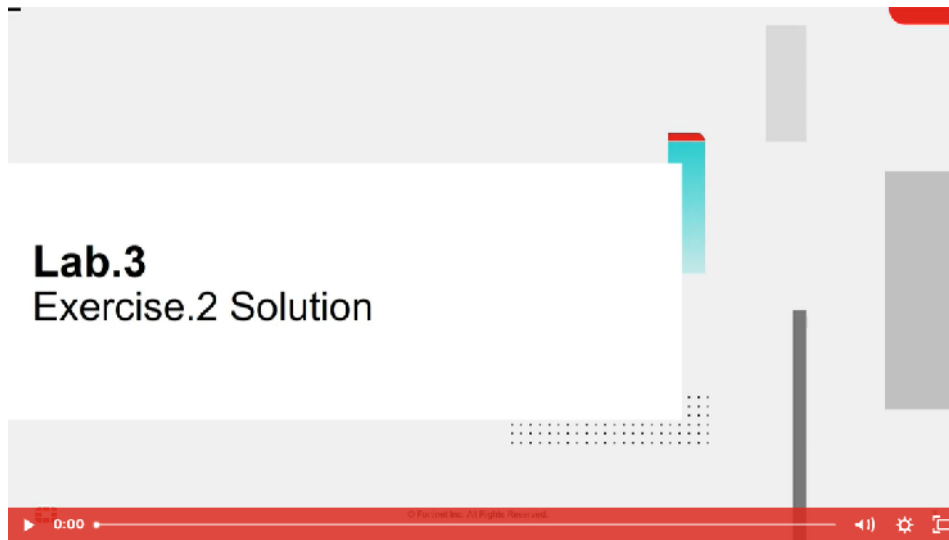
```
sudo ping -f 10.200.1.1
```
4. At the password prompt, enter `password`.
The SSH session displays a period for every ping sent.
5. Leave the SSH connection open with the ping running (you can minimize the window).
6. On the Local-FortiGate, examine the anomaly log entries.
Note that the ICMP flood was blocked, indicated by the **clear_session** entry in the **Action** field.
7. In the PuTTY window, press `Ctrl+C` to stop the ping.
8. Close the PuTTY session.

Solution

Watch this short video for the solution to Lab 3, Exercise 2.



Videos are converted to static images in print-based outputs (navigate to <https://nsei.wistia.com/medias/v9fqesbdfc> to view the video).



Lab 4: SSL VPN and IPsec VPN

In this lab, you will configure SSL VPN web mode to connect from a remote location to access local resources. You will also configure a site-to-site IPsec VPN between two FortiGate devices to encrypt packets that are sent between the two sites.

Objectives

- Configure SSL VPN web mode, and test the connection from a remote device
- Configure an IPsec site-to-site VPN tunnel between two FortiGate devices
- Configure IPsec firewall policies and static routes, and generate traffic between the two sites

Time to Complete

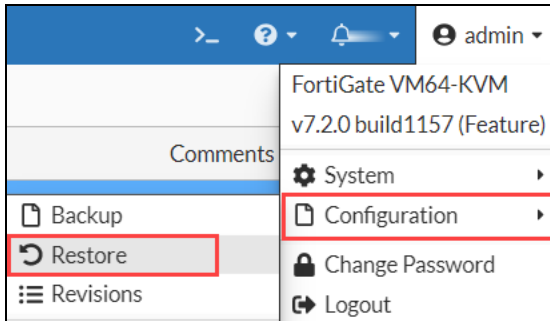
Estimated: 40 minutes

Prerequisites

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

To restore the Remote-FortiGate configuration file

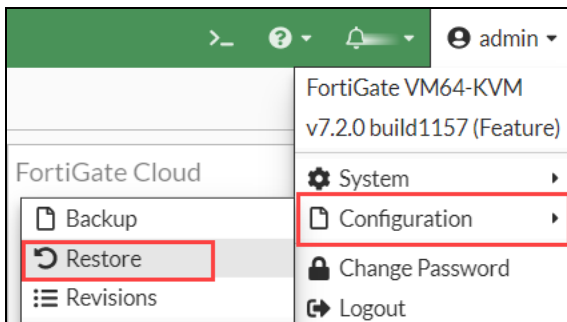
1. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration > Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > NSE4-Immersion > SSLVPN-IPsec > remote-initial.conf**, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

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



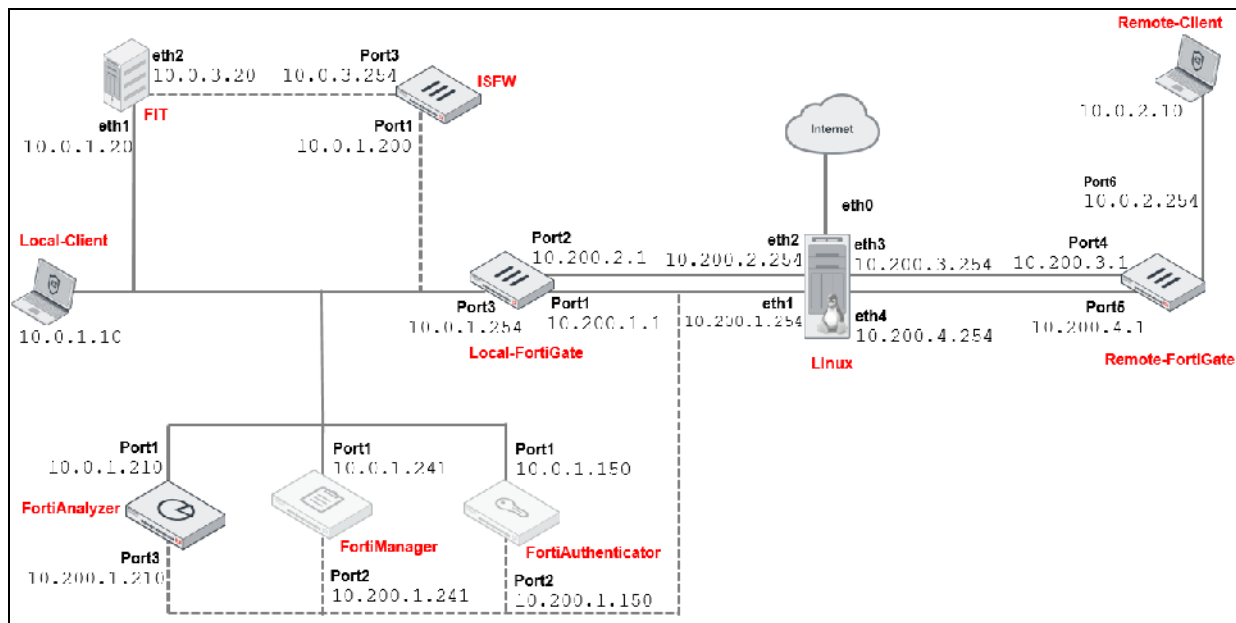
3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > NSE4-Immersion > SSLVPN-IPsec > local-SSL-VPN.conf**, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring SSL VPN

In this exercise, you will configure SSL VPN settings, an SSL VPN firewall policy, and a firewall policy based on the following requirements:

- Configure SSL VPN web mode access and a firewall policy on Local-FortiGate.

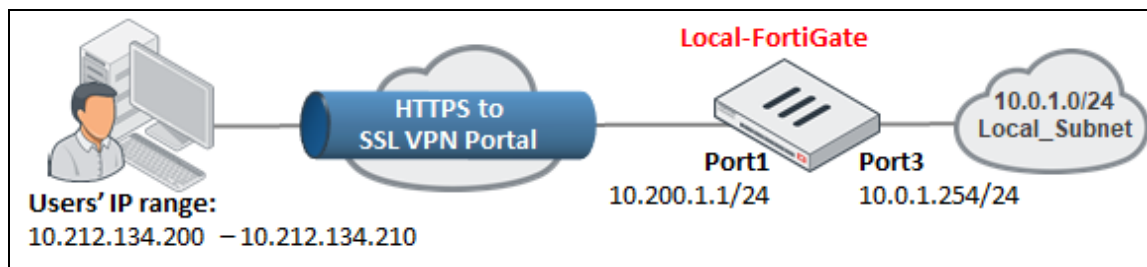
Network Topology



Review the current configuration before proceeding to the next section. You will have basic connectivity from Fortinet devices to FortiManager so that you can perform license verification. Do not make changes to the policies that allow this traffic.

Requirements

To configure SSL VPN web mode settings on Local-FortiGate

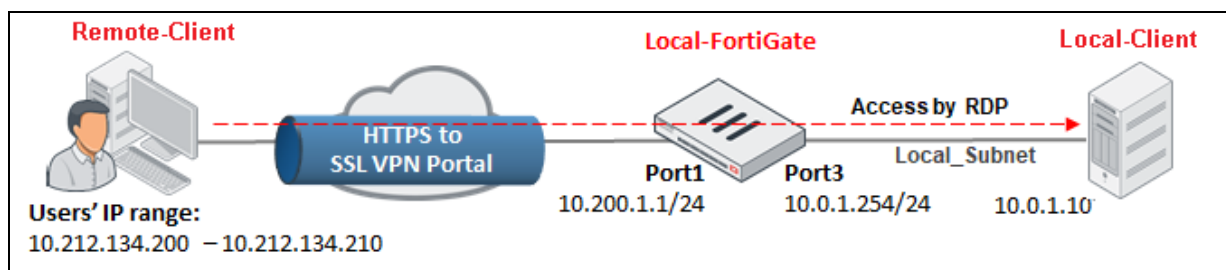


1. Create a local user with the following settings:

Field	Value
Username	student
Password	fortinet

2. Add the user to the **SSL_VPN_USERS** user group.
3. Configure the SSL VPN settings to listen on the external interface and on port 10443.
4. Increase the idle logout to disconnect SSL VPN to 3000.
5. Use the **Fortinet_Factory** server certificate, and then set the default authentication portal to **web-access**.

To configure an SSL VPN firewall policy on Local-FortiGate and access the SSL VPN portal



1. Create a new firewall policy to allow inbound SSL VPN traffic, and name it **SSL-VPN-Access**.
2. Configure the **SSL-VPN-Access** firewall policy to use the SSL VPN interface as the incoming interface to access the local subnet.
3. Select the **SSLVPN_TUNNEL_ADDR1** address object and the **SSL_VPN_USERS** user group.
4. Select the address object that represents the local resources network.
5. Attempt to connect from the remote client host machine by establishing the SSL VPN web access.
6. Access the local machine through RDP using the following settings:



You must log out of the Local-Client VM before and after you access the local machine remotely.

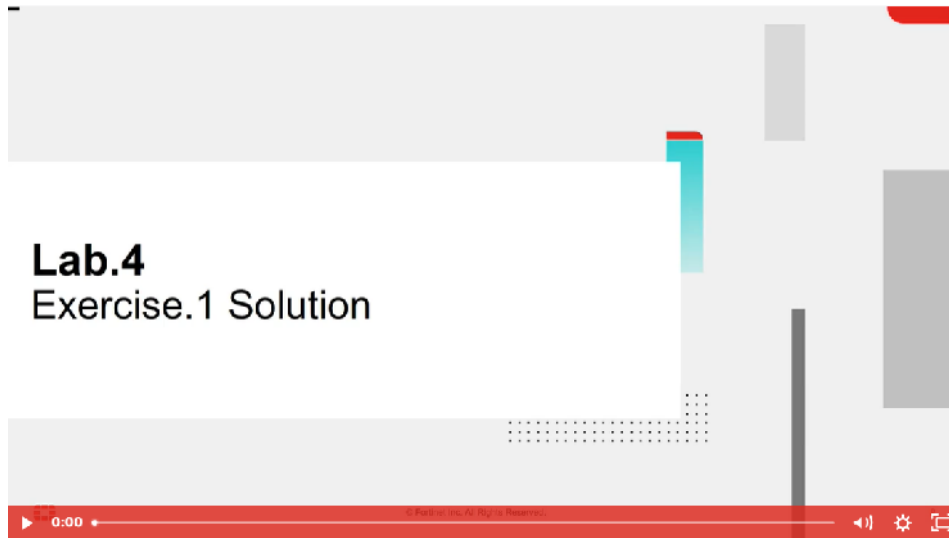
Field	Value
Connection type	RDP
Host	10.0.1.10
Username	Administrator
Password	password

Solution

Watch this short video for the solution to Lab 4, Exercise 1.



Videos are converted to static images in print-based outputs (navigate to <https://nsei.wistia.com/medias/zw564bsl52> to view the video).

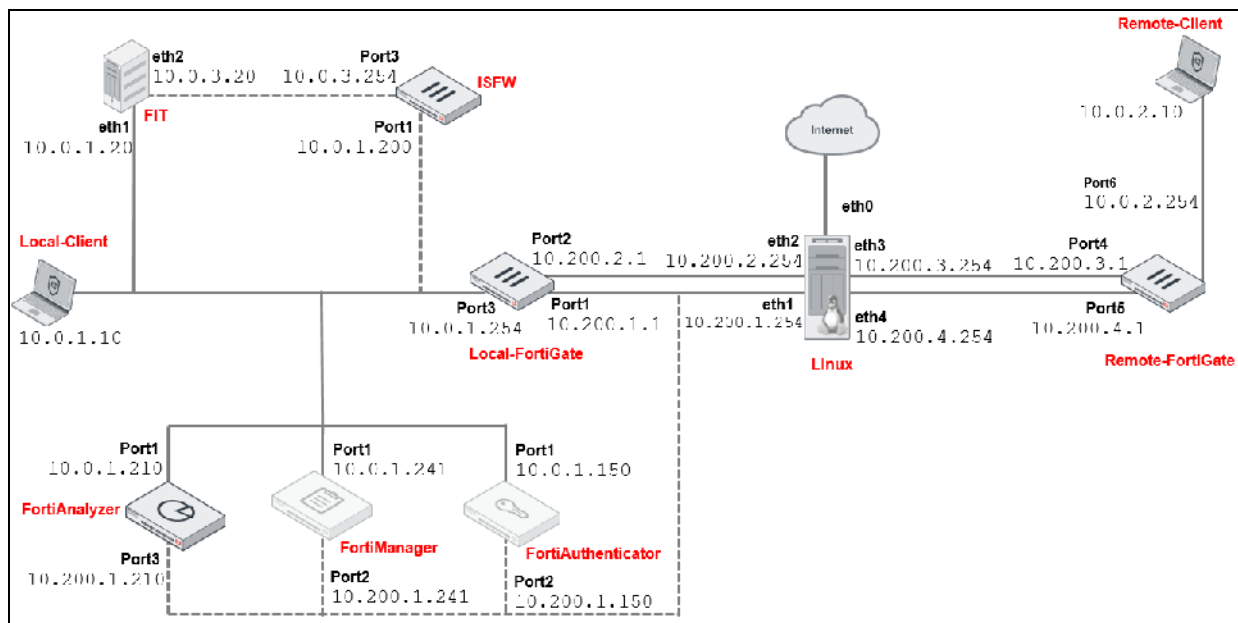


Exercise 2: Configuring IPsec

In this exercise, you will configure an IPsec phase 1 and phase 2, IPsec firewall policies, and IPsec VPN tunnel static routes, based on the following requirements:

- Configure an IPsec VPN site-to-site tunnel on Local-FortiGate and Remote-FortiGate.
- Configure VPN firewall policies on Local-FortiGate and Remote-FortiGate.
- Configure VPN tunnel static routes on Local-FortiGate and Remote-FortiGate.

Network Topology



Review the current configuration before proceeding to the next section. You will have basic connectivity from Fortinet devices to FortiManager so that you can perform license verification. Do not make changes to the policies that allow this traffic.

Requirements

Requirements for Local-FortiGate

To configure a custom site-to-site IPsec VPN tunnel and static route on Local-FortiGate

1. Create a new custom IPsec tunnel, and name it **ToRemote**.
2. Configure **ToRemote** to use the static site-to-site remote gateway IP and use the external interface.

3. Configure the IP address of the Remote-FortiGate external interface, and in Dead Peer Detection (DPD), select **On Idle**.
4. Configure the pre-shared key to `fortinet`.
5. Set the **Mode** to **Aggressive** and accept any peer.
6. Create a static route to point Local-FortiGate towards the remote subnet traffic through the VPN tunnel.

To configure firewall policies for VPN traffic on Local-FortiGate

1. Create a new firewall policy, and name it `Remote_out`.
2. Configure the **Remote_out** firewall policy to use the internal interface as the incoming interface and the VPN tunnel as the outgoing interface.
3. Select the appropriate address objects as the source and destination.
4. Create another firewall policy, and name it `Remote_in`.
5. Configure the **Remote_in** firewall policy in a similar way to the **Remote_out** firewall policy, but for the reverse traffic flow.

Requirements for Remote-FortiGate

To configure a custom site-to-site IPsec VPN tunnel and static route on Remote-FortiGate

1. Create a new custom IPsec tunnel, and name it `ToLocal`.
2. Configure **ToLocal** to use the static site-to-site remote gateway IP and use the external interface.
3. Configure the IP address of the Local-FortiGate external interface, and in DPD, select **On Idle**.
4. Configure authentication to use an aggressive pre-shared key, and then set it to `fortinet` and to accept any peer.
5. Create a static route to point Local-FortiGate towards the remote subnet traffic through the VPN tunnel.

To configure firewall policies for VPN traffic on Remote-FortiGate

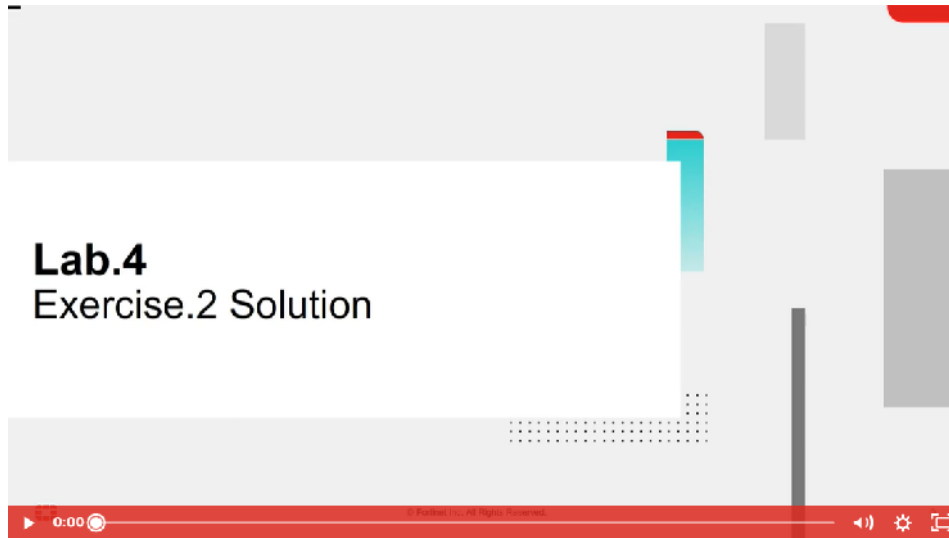
1. Create a new firewall policy, and name it `Local_out`.
2. Configure the **Local_out** firewall policy to use the internal interface as the incoming interface and the VPN tunnel as the outgoing interface.
3. Select the appropriate address objects as the source and destination.
4. Create another firewall policy, and name it `Local_in`.
5. Configure the **Local_in** firewall policy in a similar way to the **Local_out** firewall policy, but for the reverse traffic flow.
6. Attempt to generate traffic between the two sites to bring the VPN tunnel up.
You can use the different tools that are available on either host machine, such as the terminal.

Solution

Watch this short video for the solution to Lab 4, Exercise 2.



Videos are converted to static images in print-based outputs (navigate to <https://nsei.wistia.com/medias/54d365twuk> to view the video).



Lab 5: ECMP Routing

In this lab, you will configure ECMP routing by creating a new backup default route, and configuring a new firewall policy. You will then configure a link health monitor for all available external interfaces and test failover. Then, you will configure an ECMP load balancing method for ECMP to follow, and modify the required changes.

Objectives

- Configure a secondary default route and create a new firewall policy to allow outbound traffic
- Configure a link health monitor on all available external interfaces to fail over traffic
- Configure an ECMP load-balancing method to route traffic based on the source and destination IP addresses

Time to Complete

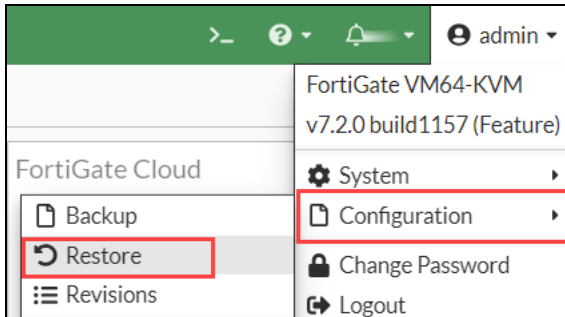
Estimated: 40 minutes

Prerequisites

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

To restore the Local-FortiGate configuration file

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



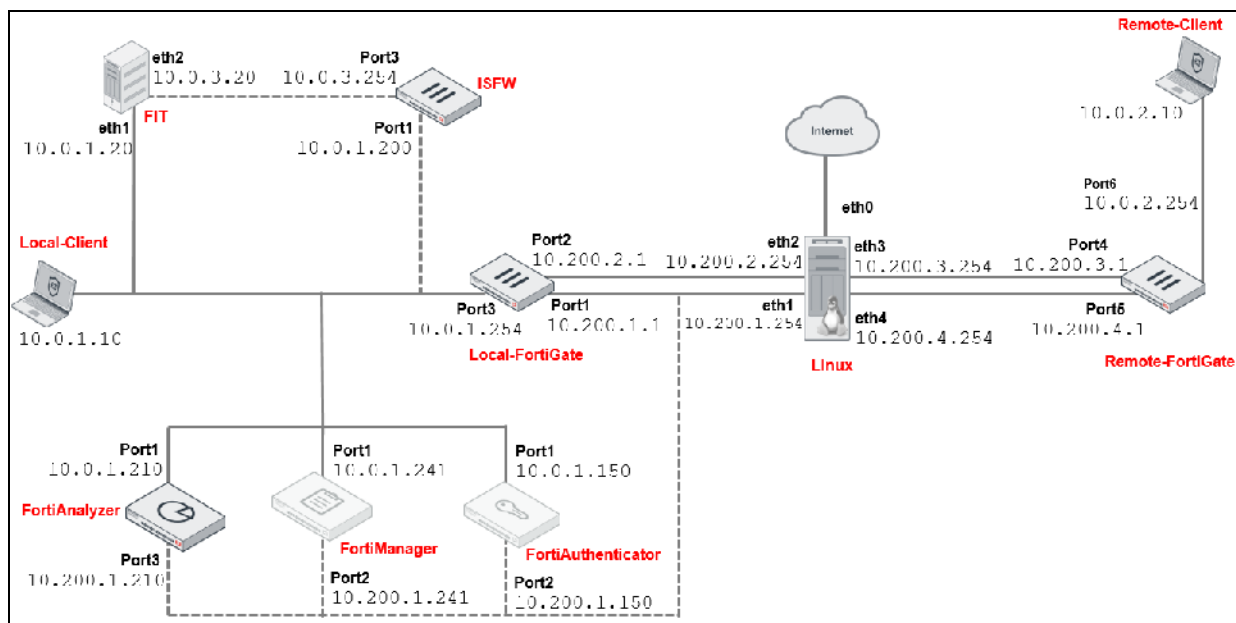
3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > NSE4-Immersion > Routing > local-initial.conf**, and then click **Select**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring Static Routing

In this exercise, you will configure a secondary default route based on the following requirements:

- Configure a secondary external interface on Local-FortiGate.
- Configure a firewall policy for the external interface on Local-FortiGate.
- Configure a link health monitor for each external interface on Local-FortiGate.

Network Topology



Review the current configuration before proceeding to the next step. You will have basic connectivity from Fortinet devices to FortiManager so that you can perform license verification. Do not make changes to the policies that allow this traffic.

Requirements

To configure a second default route on Local-FortiGate

1. Create a new static route to point Local-FortiGate to the second default gateway.
2. Configure the new default route with higher administrative distance and priority values.

To configure a firewall policy for the second default route on Local-FortiGate

1. Create a new firewall policy and name it `Backup_Access`.
2. Configure the **Backup_Access** firewall policy to use the internal interface as the incoming interface, and the second external interface as the outgoing interface.
3. Select the appropriate address objects as the source and destination.
4. Enable logging for all sessions.
5. Review the routing table on the CLI using the `get router info routing-table database` command.

To configure a link health monitor on Local-FortiGate

1. On the CLI, create a link health monitor for each external interface in the `system link-monitor` settings.
2. On the CLI, configure the following settings for each link health monitor:

Attribute	Value
srcintf	port1 and port2
server	4.2.2.1 and 4.2.2.2
gateway-ip	10.200.1.254 and 10.200.2.254
protocol	ping
update-static-route	enable

3. Try to visit a few websites, such as <http://www.pearsonvue.com/fortinet> and <http://www.eicar.org>.
4. Review the forward traffic event logs, and then add a column to display the **Destination Interface** for each event.

To configure a link health monitor to fail on port1 on Local-FortiGate

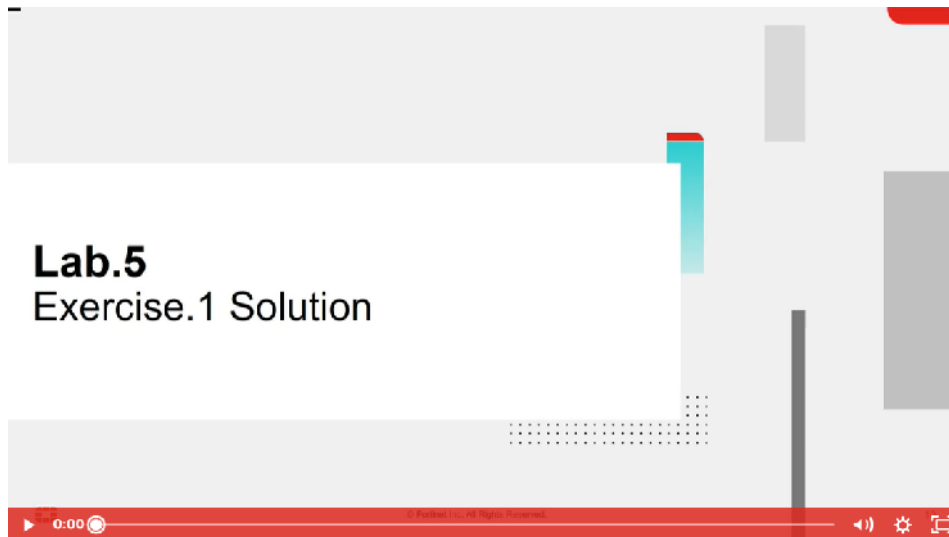
1. Modify the link health monitor you created for port1 to monitor a non-existent IP address.
2. Review the forward traffic event logs again to check if a failure has been detected.
3. Review the routing table to confirm the link health monitor has failed over the default route to the backup interface.
4. Try to visit a few websites, such as <http://www.pearsonvue.com/fortinet> and <http://www.eicar.org>.
5. Review the system and forward traffic event logs again to confirm the backup interface is being used.
6. Modify the link health monitor to point to the original server IP address (x.x.x.x) before starting the next procedure.

Solution

Watch this short video for the solution to Lab 5, Exercise 1.



Videos are converted to static images in print-based outputs (navigate to <https://nsei.wistia.com/medias/wu7g4ayhep> to view the video).



Exercise 2: Configuring ECMP Load Balancing

In this exercise, you will configure a secondary default route based on the following requirement:

- Configure an ECMP load balancing method on Local-FortiGate.

Requirements

To configure an ECMP load balancing method on Local-FortiGate

1. Modify the default routes to have an equal administrative distance value of 10.
2. On the CLI, configure the ECMP load balancing method to use `source-dest-ip-based` in the system settings.
3. Try to visit a few websites, such as <http://www.pearsonvue.com/fortinet> and <http://www.eicar.org>.
4. Review the forward traffic event logs again to confirm that the new load balancing method is functioning.



When you review the forward event logs, you should see only one outgoing interface being used. Next, you will fix this issue to confirm that the new ECMP load balancing method is functioning.

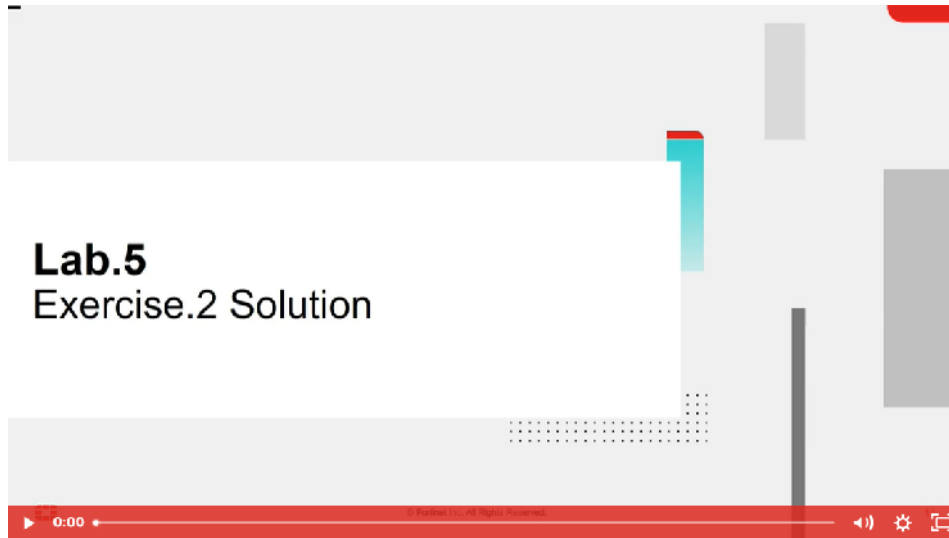
5. Modify the default routes to have an equal priority value of 1.
6. On the CLI, review the routing table using the `get router info routing-table database` command.
7. On the CLI, set up a packet sniffer to monitor traffic while the new load balancing method is taking effect.
8. Try to visit a few websites, such as <http://www.pearsonvue.com/fortinet> and <http://www.eicar.org>.

Solution

Watch this short video for the solution to Lab 5, Exercise 2.



Videos are converted to static images in print-based outputs (navigate to <https://nsei.wistia.com/medias/sl33fxmp5k> to view the video).



Lab 6: Fortinet Security Fabric

In this lab, you will configure the Fortinet Security Fabric. After you configure the Security Fabric, you will access the physical and logical topology views, and apply security ratings recommendations.

Objectives

- Configure the Security Fabric on root and downstream devices
- Configure the settings for the security ratings recommendations

Time to Complete

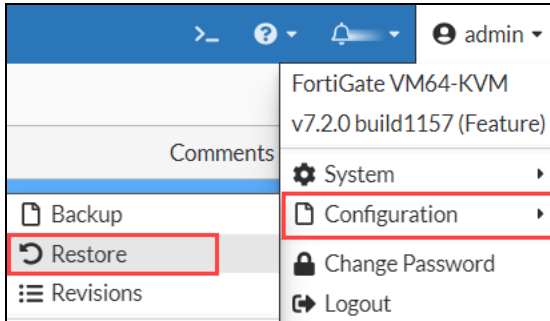
Estimated: 40 minutes

Prerequisites

Before beginning this lab, you must restore configuration files on Remote-FortiGate and Local-FortiGate. The ISFW configuration is preloaded.

To restore the Remote-FortiGate configuration file

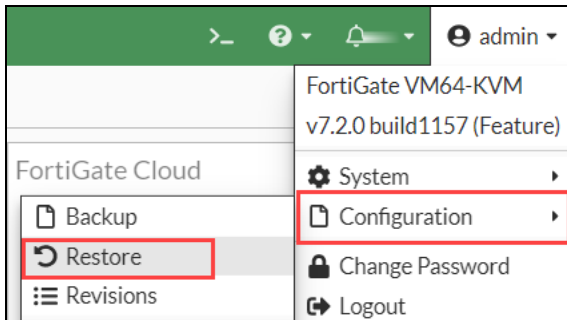
1. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration > Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > NSE4-Immersion > Security-Fabric > remote-SF.conf**, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

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



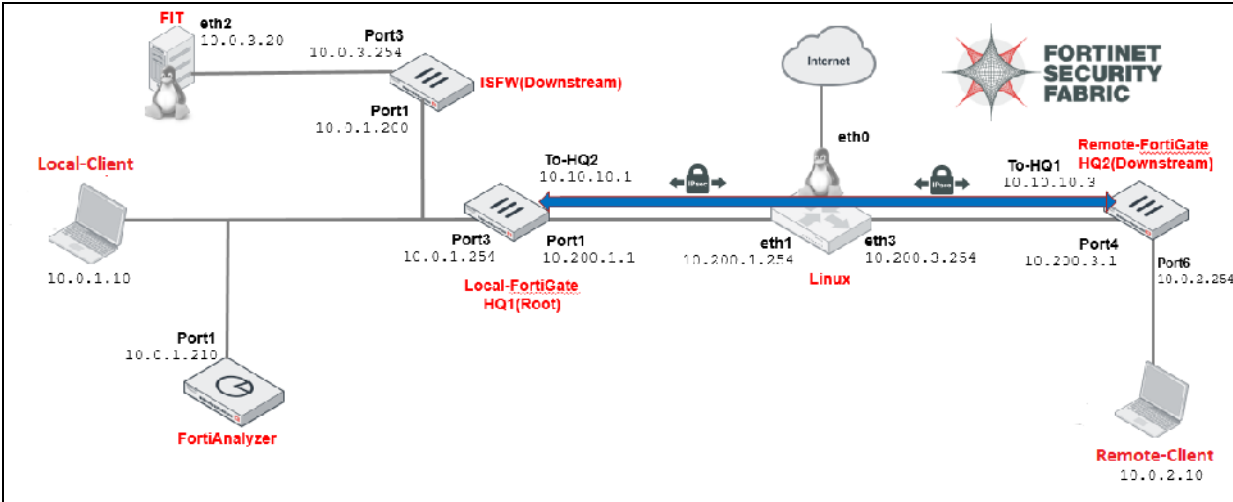
3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > NSE4-Immersion > Security-Fabric > local-SF.conf**, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring the Security Fabric on the Root and Downstream FortiGate Devices

In this exercise, you will configure the Security Fabric based on the following requirements:

- Local-FortiGate is the Security Fabric root device.
- ISFW and Remote-FortiGate are the Security Fabric downstream devices.

Network Topology



Review the current configuration before proceeding to the next step. You will have basic connectivity from Fortinet devices to FortiManager so that you can perform license verification. Do not make changes to the policies that allow this traffic.

Requirements

To configure the Security Fabric on the root device

1. Configure the following FortiAnalyzer settings:

Field	Value
IP address	10.0.1.210
Upload option	Real Time

2. Enable the Security Fabric connection settings on the **port3** and **To-Remote-HQ2** interfaces.
3. Enable the Security Fabric settings to serve as the Security Fabric root.
4. Configure the following Security Fabric settings:

Field	Value
Fabric name	fortinet
Allow other Security Fabric devices to join	enable
	Tip: Review the topology to select the required interfaces.

To configure the Security Fabric on the ISFW downstream device

1. Enable the Security Fabric connection settings on the **port1** and **port3** interfaces.
2. Enable the Security Fabric settings to join the **fortinet** Security Fabric.
3. Use the root FortiGate as the upstream FortiGate.

Field	Value
Upstream FortiGate IP	10.0.1.254
Default admin profile	super_admin
Management IP/FQDN	Specify : 10.0.1.200

4. Authorize the new downstream device on the root FortiGate.

To configure the Security Fabric on the Remote-FortiGate downstream device

1. Enable the Security Fabric connection settings on the **port6** and **To-Local-HQ1** interfaces.
2. Enable the Security Fabric settings to join the **fortinet** Security Fabric.
3. Use the root FortiGate as the upstream FortiGate.

Field	Value
Upstream FortiGate IP	10.10.10.1
Default admin profile	super_admin
Management IP/FQDN	Specify : 10.200.3.1

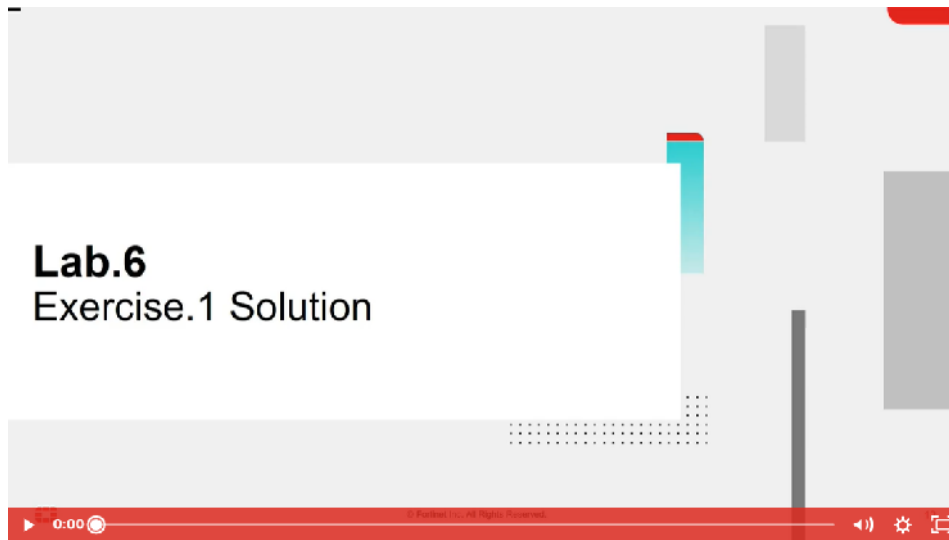
4. Authorize the new downstream device on the root FortiGate.

Solution

Watch this short video for the solution to Lab 6, Exercise 1.



Videos are converted to static images in print-based outputs (navigate to <https://nsei.wistia.com/medias/f1sa2j732s> to view the video).



Exercise 2: Authorizing Devices and Running the Security Rating

In this exercise, you will configure the Security Fabric based on the following requirements:

- Authorize the root and downstream FortiGate devices on FortiAnalyzer.
- The security ratings recommendations for administrative access setting must be applied on Local-FortiGate.

Requirements

To authorize Security Fabric devices on FortiAnalyzer

1. Authorize the devices added to the **fortinet** Security Fabric group to send logs to FortiAnalyzer.
2. Confirm the authorization status is complete for all devices.
3. Verify the FortiAnalyzer logging status on each device in the **fortinet** Security Fabric.

To apply security ratings recommendations on the root FortiGate

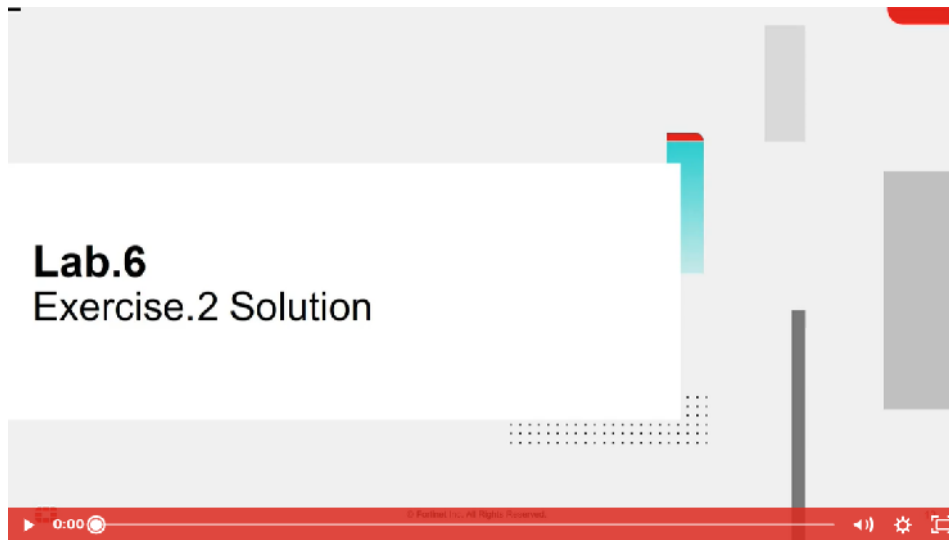
1. Review the scores provided in the Security Fabric security ratings.
2. Apply the suggested recommendation for **Administrative Access** in the security posture.
3. Run the security rating report to generate a new security posture score.

Solution

Watch this short video for the solution to Lab 6, Exercise 2.



Videos are converted to static images in print-based outputs (navigate to <https://nsei.wistia.com/medias/zoaylhg52r> to view the video).



Lab 7: HA

In this lab, you will set up a FortiGate Clustering Protocol (FGCP) high availability (HA) cluster of FortiGate devices. You will explore active-active HA mode and observe FortiGate HA behavior. You will also perform an HA failover.

Objectives

- Set up an HA cluster using FortiGate devices
- Observe HA synchronization and interpret diagnostic output
- Perform an HA failover

Time to Complete

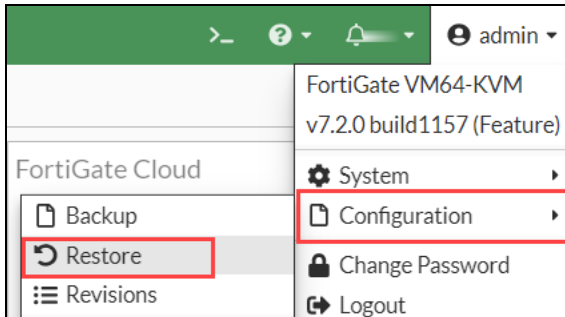
Estimated: 40 minutes

Prerequisites

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

To restore the Local-FortiGate configuration file

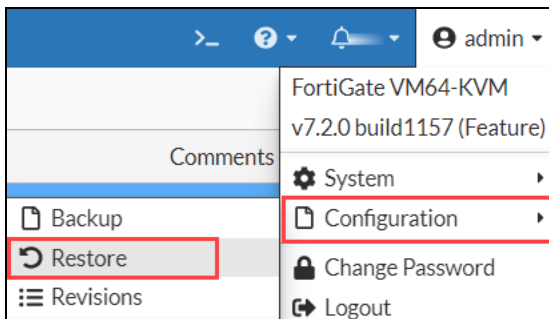
1. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration > Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > NSE4-Immersion > HA > local-ha.conf**, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Remote-FortiGate configuration file

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



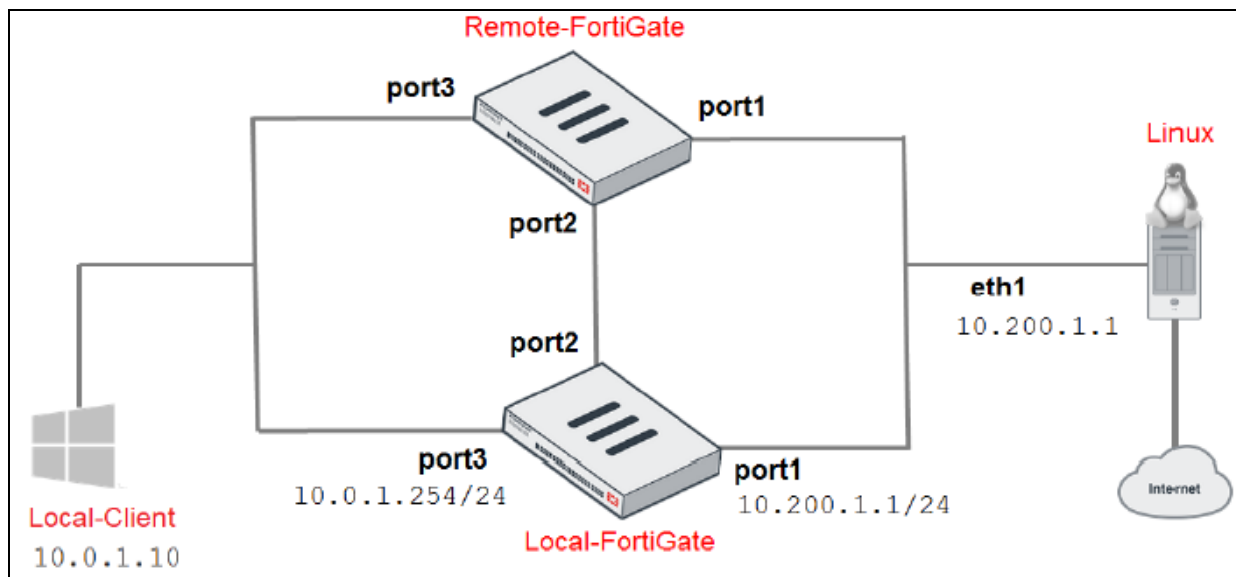
3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop > Resources > NSE4-Immersion > HA > remote-ha.conf**, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Configuring HA

In this exercise, you will configure HA for two FortiGate devices, based on the following requirements:

- Configure active-active HA between Local-FortiGate and Remote-FortiGate.
- Local-FortiGate must be the primary FortiGate, and the configuration on Local-FortiGate must sync to Remote-FortiGate.
- Trigger HA failover for testing.

Network Topology



Requirements

- Set up an active-active HA cluster between Local-FortiGate and Remote-FortiGate with the heartbeat interface set as port2 on both FortiGate devices.
- Local-FortiGate must be the primary device.
- Make sure session pickup is enabled.
- Make sure the configuration is in sync.
- Trigger an HA failover to make sure the traffic fails over to the backup FortiGate.

Test the Configuration

To test the HA setup

1. Enter the following commands to check if the devices are in sync:

```
diagnose sys ha checksum cluster  
get system ha status
```
2. Enter the following command to check the role of Local-FortiGate—it must be the primary device:

```
get system status
```

To test failover

1. On the Local-Client VM, open a terminal window, and then start a ping to 8 . 8 . 8 . 8.
2. Trigger a failover using the method of your choice, and then monitor the ping.
The ping test must succeed, with the possibility of a few ping tests failing.
3. Enter the following command to make sure Remote-FortiGate is now the primary device:

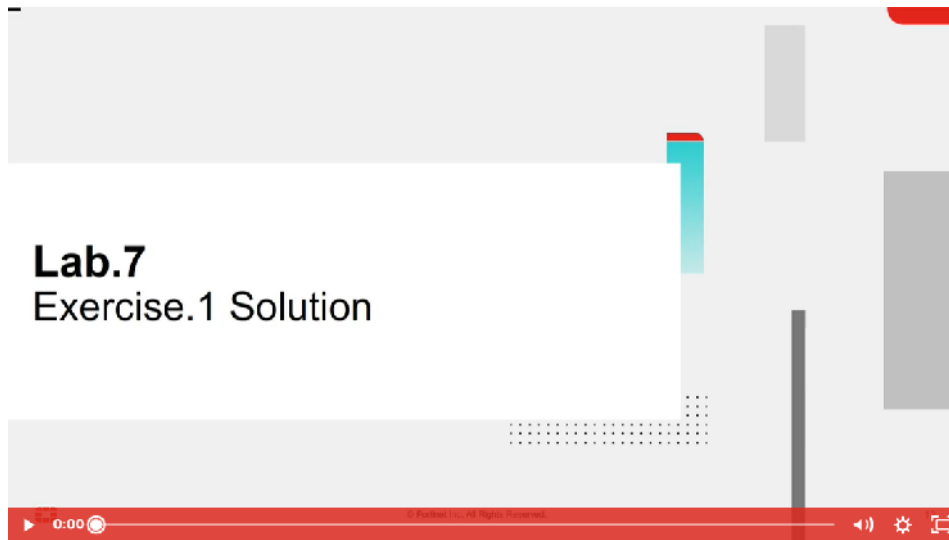
```
ping  
get system status
```

Solution

Watch this short video for the solution to Lab 7, Exercise 1.



Videos are converted to static images in print-based outputs. (Navigate to <https://nsei.wistia.com/medias/gkb74rm21h> to view the video.)



Exercise 2: Configuring the HA Management Interface

In this exercise, you will configure the HA management interface.

Requirements

To configure the HA management interface on both the primary and secondary devices

1. Enable the management interface reservation on the system HA settings, and then select **port7** as the interface.
2. Verify the current HA primary device using the non-synchronized attribute, which is the host name.
3. Use the CLI to log in to the current HA secondary device, using the command `execute ha manage`.
4. Use the CLI to verify the current HA secondary device host name, using the command `get system status`.
5. Configure the following settings to configure the port7 interface, on the CLI, for Local-FortiGate:

Field	Value
ip	10.0.1.253/24
allowaccess	http snmp ping ssh

6. Configure the following settings to configure the port7 interface, on the CLI, for Remote-FortiGate:

Field	Value
ip	10.0.1.252/24
allowaccess	http snmp ping ssh

7. After GUI access is available through port7 on each device, remove the current HA secondary device from the HA cluster.
8. Use **port3** to confirm the request, and use `10.0.1.251/24` as the IP address.
9. Log in to the removed HA secondary FortiGate GUI console using `http://10.0.1.251`.
10. Restore the configuration files you restored at the beginning of this lab for each device.



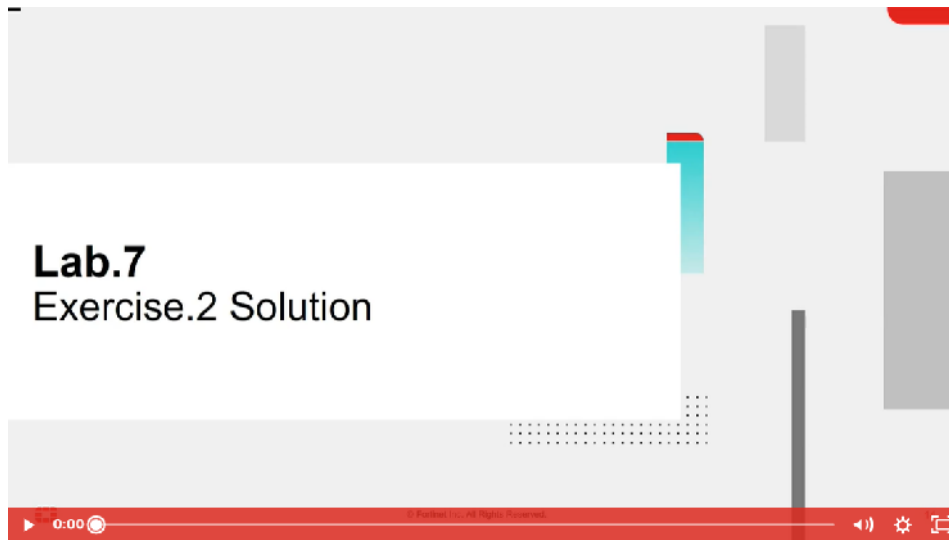
Failure to verify the host name of each FortiGate and restore the correct configuration file will prevent you from conducting other labs.

Solution

Watch this short video for the solution to Lab 7, Exercise 2.



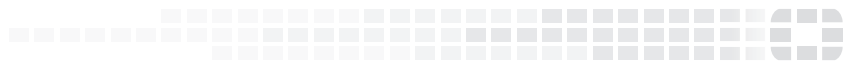
Videos are converted to static images in print-based outputs. (Navigate to <https://nsei.wistia.com/medias/2mhj08q9xj> to view the video.)



DO NOT REPRINT
© FORTINET



FORTINET®



No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.