Virtual Lab Setup Guide

for FortiGate 7.0

FORTINET NSE Training Institute

Fortinet Training

https://training.fortinet.com

Fortinet Document Library

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 Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Network Security Expert Program (NSE)

https://training.fortinet.com/local/staticpage/view.php?page=certifications

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Feedback

Email: courseware@fortinet.com

FORTINET

9/7/2021

TABLE OF CONTENTS

Disclaimer

Fortinet only supports lab environments that are built to the specifications outlined in this guide. Any modifications to, or deviations from, the environment described in this guide can impact the outcome of the student lab exercises. Lab exercises are used as a way to reenforce learning, and knowledge obtained from successfully performing these labs is essential for NSE certification preparation.

Introduction

This guide explains how to configure the lab for the following Fortinet training courses:

- FortiGate Security 7.0 (NSE 4 preparation)
- FortiGate Infrastructure 7.0 (NSE 4 preparation)

In this environment, FortiManager is acting as a local FortiGuard server. It validates the FortiGate licenses and replies to FortiGuard Web Filtering rating requests from FortiGate VMs. FortiManager is configured in *closed network mode*, providing FortiGuard services to local FortiGate VMs, without requiring Internet access.

To administer this lab as designed, you will:

1. Load, configure, and test the VM images required for this lab.
2. Save a VMware snapshot of the VM images.
3. Deploy a copy of all VMs for each student every time there is a class.

Upgrading from 6.4.0 to 7.0.0

If you have already built the environment for the *FortiGate Security* and *FortiGate Infrastructure* courses, based on the 6.4.0 firmware version, you can follow the instructions below to update the environment to the 7.0.0 firmware version.

If you have not already built the environment for the *FortiGate Security* and *FortiGate Infrastructure* courses, based on the 6.4.0 firmware version, follow the instructions that start at Materials on page 10.

The minimum resources used by each VM have slightly changed, refer to table on System Requirements on page 10

Update the VMs in your lab based on the system requirements table.

Resources folder

The Resources folder on the Local-Client VM includes the initial configurations for each lab, for both courses. You need to replace the current Resources folder on the Local-Client VM with the Resources folder that contains the updated configurations.

To replace Resources folder on Local-Client VM

1. Log in to the Local-Client VM.
2. Delete the **Resources** folder located on the desktop.
3. Delete the **Resources** folder from **Trash**.
4. From the `Virtual-Lab-Setup-Files-FGT-7.0` folder on the NSE Institute, copy the **Resources** folder to the desktop.

Upgrading FortiGate Devices to FortiOS 7.0.0

You will now upgrade Local-FortiGate, ISFW, and Remote-FortiGate to FortiOS version 7.0.0.

Upgrade Path

To upgrade the FortiGate device to 7.0.0, you will need to upgrade to firmware version 6.4.2 first, and then upgrade to firmware version 6.4.4, and then to firmware version 7.0.0.

To download the FortiGate VM firmware images

1. From the Local-Client VM, open a new browser tab and log in to the Fortinet Support site (`www.support.fortinet.com`).
2. Download the VM firmware image files for versions 6.4.2, 6.4.4, and 7.0.0.

To upgrade FortiGate VMs to FortiOS 7.0.0

Use the following steps to upgrade Remote-FortiGate, ISFW, and Local-FortiGate.

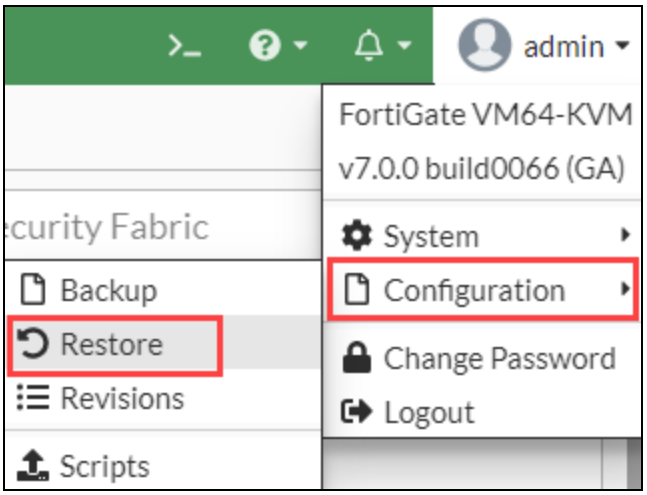
1. Continuing on the Local-Client VM, open a new browser tab and log in to the FortiGate GUI.
2. Click **System** > **Firmware**.
3. In the **Upload Firmware** section, click **Browse**.
4. Click **Downloads** and select the VM firmware image file for FortiGate 6.4.2.
5. Click **Open**.
6. Click **Backup config and upgrade**.
7. Click **Continue**.
8. Click **Cancel**.
9. Repeat steps 2 to 8, but on step 4, select the VM firmware image file for FortiGate 6.4.4
10. Repeat steps 2 to 8, but on step 4, select the VM firmware image file for FortiGate 7.0.0
11. After you have upgraded the firmware, delete the VM firmware image files for FortiGate 7.0.0 from the **Downloads** folder and the **Trash**.

Restoring the FortiGates' Initial Configuration

At this stage, you are ready to restore the initial configuration of the Local-FortiGate, Remote-FortiGate, and ISFW.

To restore the Remote-FortiGate configuration file

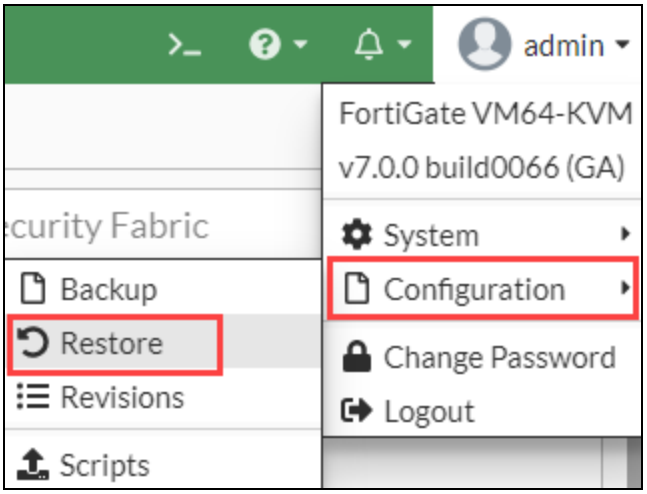
1. On the Local-Client VM, open a browser and log in to the Remote-FortiGate GUI at `10.200.3.1` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Initial-Configuration** > `remote-intial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

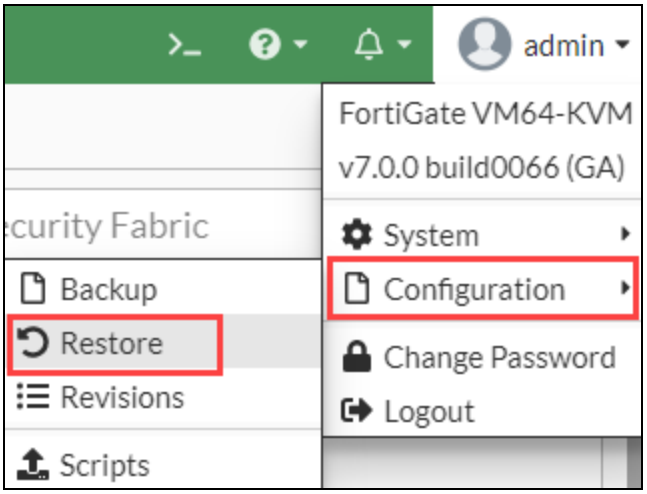
1. On the Local-Client VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



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

To restore the ISFW-FortiGate configuration file

1. On the Local-Client VM, open a browser and log in to the Local-FortiGate GUI at `10.0.1.200` 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** > **Initial-Configuration** > `ISFW-initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

FortiGate Revisions

The initial configuration restore procedure for each lab has been updated. Now, the initial configurations for all labs have been saved on each FortiGate device in the flash.

To save the configuration in FortiGate Revisions, follow the steps in Saving Configuration in FortiGate Revisions on page 27

Installing FortiManager and FortiAnalyzer 6.4.1

You need to delete the existing FortiManager and FortiAnalyzer and re-deploy the FortiManager and FortiAnalyzer based on version 6.4.1.

To install FortiManager and FortiAnalyzer 6.4.1

1. Delete the existing FortiManager and FortiAnalyzer.
2. To load the FortiManager and FortiAnalyzer follow the steps in To create the VMs on VMware Workstation 12 on page 12
3. To map network adapters for the FortiManager and FortiAnalyzer follow the steps in To configure VMware virtual networking on page 13
4. To confirm and fulfill the license and system requirement for FortiManager and FortiAnalyzer use the information and steps in Materials on page 10 and System Requirements on page 10.
5. To configure FortiManager, follow the steps in FortiManager on page 18
6. Follow the steps to configure FortiAnalyzer on FortiAnalyzer on page 21

Creating Snapshots

After you have completed and tested your configuration, save a snapshot of each VM. These snapshots are what you will deploy for each student in the class.

You can also redeploy these snapshots to revert a student's VM, if their configuration is not working and they need to quickly restore it to a functional state.

Materials

To build the virtual lab required for this class, you must purchase or download the following resources:

Resource	Information
1 VMware Workstation installation per student	For hardware system requirements, see System Requirements on page 10
3 FortiGate VM licenses	For Local-FortiGate, Remote-FortiGate, ISFW
1 FortiAnalyzer VM license	Must be registered with the IP address `10.0.1.210`
1 FortiManager VM license	Must be registered with the IP address `10.0.1.241`
3 FortiGuard Web Filtering, antivirus, and IPS contract	For Local-FortiGate, Remote-FortiGate, ISFW
3 Security Rating contracts	For Local-FortiGate, Remote-FortiGate, and ISFW
1 FortiAuthenticator VM license	Must be registered with the IP address `10.0.1.150`
1 Local-Client 1 Remote-Client 1 Ubuntu Linux VM image 1 FIT VM image	Prebuilt image is provided by Fortinet Training. The image is provided in the `Virtual-Lab-Setup-Files-FGT-7.0` folder on the NSE Institute. Note: Local-Client have `Resources` folder saved on the desktop
VM firmware image files for: • FortiGate 7.0.0 • FortiAnalyzer 6.4.1 • FortiManager 6.4.1 • FortiAuthenticator 6.0.3	After purchase, you can download the files from Fortinet Support (www.support.fortinet.com) by logging in with supplied credentials.

System Requirements

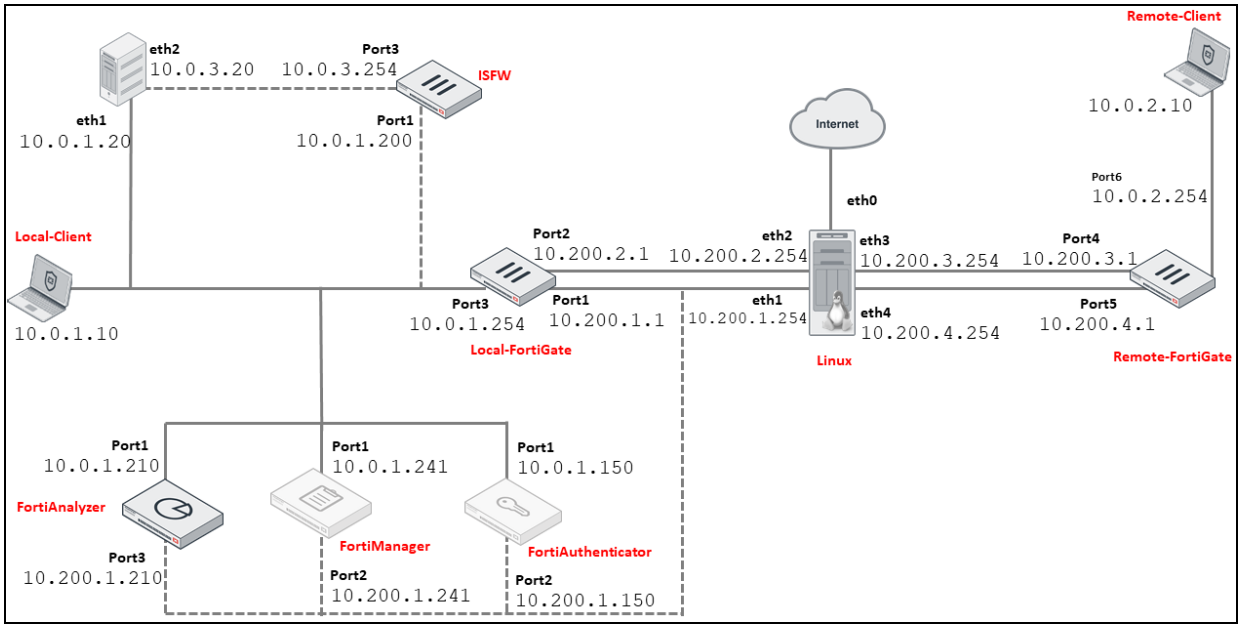
Each VM running in VMware Workstation requires the following resources:

Device	Number of CPUs	RAM (GB)	Disk Size (GB)
Local-FortiGate	1	2	32

Device	Number of CPUs	RAM (GB)	Disk Size (GB)
Remote-FortiGate	1	2	32
ISFW	1	2	32
Linux	1	1	20
FIT	1	1	20
Local-Client	2	2	16
Remote-Client	2	2	16
FortiAnalyzer	2	4	82
FortiManager	2	4	82
FortiAuthenticator	2	2	61
Total Resources	15	22	393

These are the minimum recommended resources for each VM. If you experience slowness or lag in any VMs, you can increase the resources for that VM.

Network Topology



Loading the VMs in VMware Workstation

This section outlines how to load the VMs in VMware Workstation, including the Linux VMs and the Fortinet VMs (FortiGate, FortiManager, FortiAuthenticator, and FortiAnalyzer).

The `Virtual-Lab-Setup-Files-FGT-7.0` folder on the NSE Institute provides prebuilt images of the Linux VMs and FIT VM, which do not require additional configuration. You only need to load them and deploy them.

Loading the VMs on VMware Workstation 12

There are 10 VMs in total in the network topology. The following procedure outlines how to load the VMs on VMware Workstation 12:

- Local-FortiGate
- Remote-FortiGate
- ISFW
- FortiManager
- FortiAnalyzer
- FortiAuthenticator
- Local-Client
- Remote-Client
- FIT
- Linux

To create the VMs on VMware Workstation 12

1. Click **File** > **Open**.
2. Select the **Open Virtualization Format** file format.
3. Select the file name **FortiGate-VM.ovf**.
4. Name the VM `Local-FortiGate`.
5. Repeat for each VM, naming the VMs according to the network topology diagram.
   - Remote-FortiGate
   - ISFW
   - FortiManager
   - FortiAnalyzer
   - FortiAuthenticator
   - Local-Client
   - Remote-Client
   - FIT
   - Linux

Configuring VMware Virtual Networking

After you've loaded the VMs, you must configure their virtual network adapters to make the lab's required virtual network topology.

The following VMs should be inside each student's virtual lab environment:

- Local-FortiGate
- Remote-FortiGate
- ISFW
- FortiManager
- FortiAnalyzer
- FortiAuthenticator
- Local-Client
- Remote-Client
- FIT
- Linux

The topology supports both HA and non-HA topology, which the students will switch between during the labs by reconfiguring their VMs; no VMware reconfiguration is required.

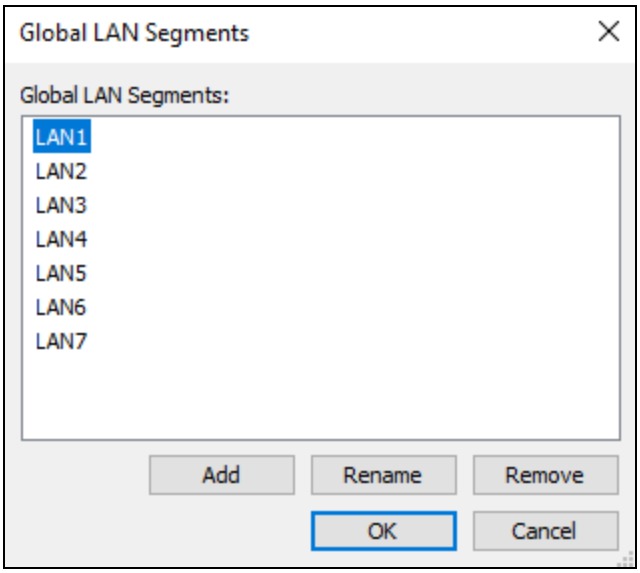
The key to this flexible networking is the seven LAN segments used in the current setup, plus the predefined interfaces: `vmnet0` and `vmnet1`.

- `vmnet0` bridges the physical NIC which provides the default route to the Internet.
- `vmnet1` is a host-only private network shared between the host and the guest systems.

By mapping the guest VMs' virtual NICs to virtual LAN segments, you create the topology.

To configure VMware virtual networking

1. Ensure that the prebuilt Linux VM has five NICs. If not, add the as many as needed to have five.
2. Create the LAN segments:
   a. Right-click the **Local-Client** VM and select **Settings**.
   b. Select any of the two **Network Adapters**.
   c. Click **LAN Segments**.
   d. Click **Add** as many times as needed to create the seven LAN segments:



e. Click **OK** twice to close the windows.

4. Map the LAN segments to each vNIC:
   - For the **Local-Client** VM, map this network adapter:

Network Adapter	LAN Segment
1	LAN3

   - For the **Remote-Client** VM, map this network adapter:

Network Adapter	LAN Segment
1	LAN6

   - For both FortiGate VMs (**Local-FortiGate** and **Remote-FortiGate**), map the first seven network adapters:

Network Adapter	LAN Segment
1	LAN1
2	LAN2
3	LAN3
4	LAN4
5	LAN5
6	LAN6
7	LAN3

   - For the **ISFW** VM, map these network adapters:

Network Adapter	LAN Segment
1	LAN3
3	LAN7

- For the **FortiManager** VM, map these network adapters:

Network Adapter	LAN Segment
1	LAN3
2	LAN1

- For the **FortiAnalyzer** VM, map these network adapters:

Network Adapter	LAN Segment
1	LAN3
3	LAN1

- For the **FortiAuthenticator** VM, map these network adapters:

Network Adapter	LAN Segment
1	LAN3
2	LAN1

- For the **Linux** VM, map these network adapters:

Network Adapter	LAN Segment
1	VMnet0
2	LAN1
3	LAN2
4	LAN4
5	LAN5

- For the **FIT** VM, map these network adapters:

Network Adapter	LAN Segment
1	LAN3
2	LAN7

Configuring the VMs

All the VMs required for the lab have been prebuilt. After loading the VM images in VMware Workstation, you must configure some initial settings on the VMs so that they have network connectivity, and for some VMs, you also need to load their license.

The prebuilt Linux VM provided with the `Virtual-Lab-Setup-Files-FGT-7.0` folder on the NSE Institute is already configured. The root password for the prebuilt VM is: `password`.

The prebuild FIT VM provided in the `Virtual-Lab-Setup-Files-FGT-7.0` folder on the NSE Institute is already configured.

Local-FortiGate

The following procedure outlines how to configure the network interfaces on Local-FortiGate.

To configure network interfaces on Local-FortiGate

1. Start the Local-FortiGate VM and open the VM console.
2. Log in as `admin`, and leave the password field empty.
3. Enter the following command:
   ```
   exec formatlogdisk
   ```
   This formats the virtual disk, which is required to store data such as local reports or logs. The device reboots after the format is complete.
4. Enter this configuration to configure the network interfaces:
   ```
   config system interface
      edit port1
         set ip 10.200.1.1 255.255.255.0
         set allowaccess http
      next
      edit port2
         set ip 10.200.2.1 255.255.255.0
         set allowaccess http
      next
      edit port3
         set ip 10.0.1.254 255.255.255.0
         set allowaccess http
      next
   end
   config router static
      edit 1
         set gateway 10.200.1.254
   ```

```
      set device port1
   next
end
config firewall policy
   edit 1
      set srcintf port3
      set dstintf port1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
      set nat enable
   next
end
```

FortiManager

Even though FortiManager is not the focus of the FortiAnalyzer and FortiGate courses, it is required for the lab setup due to the use of *closed network mode*. More information about the FortiManager closed network mode can be found in this document:

https://docs.fortinet.com/

Requesting Closed Network Entitlement File

After you have purchased VM licenses and registered them on https://support.fortinet.com, you must request closed network entitlement file. This file is required for manually uploading FortiGate license validation information to FortiManager in close network mode.

To request closed network entitlement file

1. On the Fortinet Technical Support website (https://support.fortinet.com/), create a ticket with Fortinet Technical Support by clicking **Assistance** > **Create Ticket** > **Customer Service** > **Submit Ticket**.
2. Enter the **Serial Number**.

   Tip: You can enter the serial number of FortiManager.
3. Under **Category**, select **CS Contact/License**.
4. In the **Comment** field, ask for an entitlement file for your FortiGate VMs and provide the serial numbers and license numbers.

   If you don't remember them, you can find them in **Asset** > **Manage View Products** > <Select product>.

   Example:

   Serial Number: FGVM010000000000

   License Number: FGVM0000000

Alternatively, as with registration, you can attach a spreadsheet that contains serial and license numbers if you want to ask for entitlement files for two or more FortiGate VMs at the same time. Fortinet Technical Support will provide one entitlement file that contains validation information for all of your FortiGate VMs. All FortiGate VMs must be registered with the same account; devices registered under different accounts cannot be combined into the same entitlement file.

Within a day or two, you should receive an entitlement file from customer service.

To configure the FortiManager initial settings

1. Start the FortiManager and open the VM console.
2. From the console make the following changes:

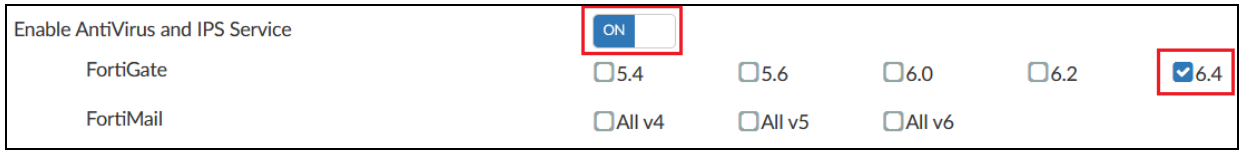
```
config system interface
   edit port1
      set ip 10.0.1.241 255.255.255.0
      set allowaccess http https ssh ping telnet
   next
```

```
end
```

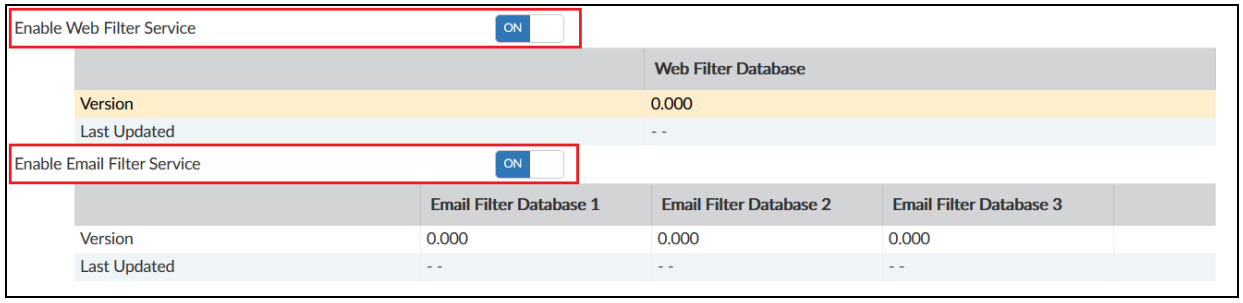
3. Connect to the GUI from the Local-Client VM and restore `FMG-initial.dat` file from the folder `Resources/Initial-Configuration`.
4. Upload a valid FortiManager VM license.

To configure FortiManager as a local FDN server

1. Log into the FortiManager GUI and click **FortiGuard**.
2. From the left menu, click **Settings**.
3. Enable **Enable Communication with FortiGuard Server** and click **Apply**.
4. Enable **Enable AntiVirus and IPS Service**and enable **FortiGate 6.4**.



5. Enable the following services:
   - **Enable Web Filter Service**
   - **Enable Email Filter Service**



6. Click **Apply**.
7. Wait until FortiManager has downloaded and synchronized all the service packages and updates. This could take several hours.
8. Check the status of the updates using the following CLI commands:

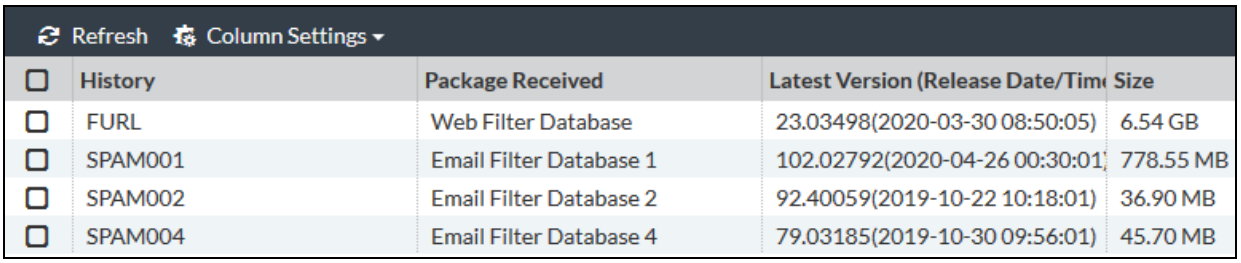
```
# diagnose fmupdate update-status fds
# diagnose fmupdate update-status fgd
```

Once complete, the `upullStat` should say `Synced`. Note that it will sync after every package FortiManager downloads, so you can run these commands multiple times to verify the status. It should take several hours to complete.

If you do not see any progress in the downloads, for example, the `UpullStat` remains in the `Connected` state, you can manually trigger the update through the following commands:

```
# diagnose fmupdate updatenow fds
# diagnose fmupdate updatenow fgd
```

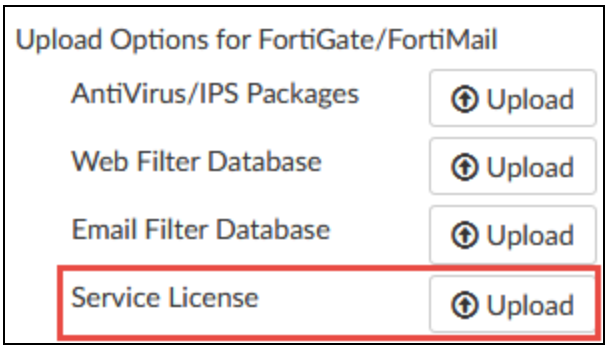
9. Once complete, the file size for web filtering (FURL) and email filter (SPAM00x) under **Query Server Management** > **Receive Status** should be approximately as they appear in this screenshot:



10. After the FortiGuard packages and updates are synchronized, click **Settings** and disable **Enable Communication with FortiGuard Server**.
11. Click **Apply**.

To upload the entitlement files to FortiManager

1. Log in to the FortiManager GUI and click **FortiGuard**.
2. From the left menu, click **Settings**.
3. In the **Upload Options for FortiGate/FortiMail** section,beside **Service Licesnse**,click **Upload** for **Service License**.



4. Upload the FortiGate entitlement file.
5. Click **Apply**.
6. Upload the FortiAnalyzer IOC license file (only if you are teaching the FortiAnalyzer 6.4 training).
7. Click **Apply**.

FortiAnalyzer

The following procedure outlines how to configure the FortiAnalyzer system settings.

To configure the FortiAnalyzer initial settings

1. Start **FortiAnalyzer** and open the VM console.
2. From the console, make the following changes:

```
config system interface
   edit port1
      set ip 10.0.1.210 255.255.255.0
      set allowaccess http https ssh ping telnet
   next
end
```

3. Connect to the GUI from the Local-Client VM and restore the file from the folder:
   `Resources/Initial-Configuration/FAZ-initial.dat`
4. Upload the FortiAnalyzer VM license.

Restoring the Local-FortiGate Initial Configuration and License

At this stage, you are ready to restore the Local-FortiGate initial configuration and license.

To restore the Local-FortiGate initial configuration and license

1. On the Local-Client VM, open a web browser and connect to the FortiGate VM GUI.
2. Upload `local-initial.conf` from `Resources/Initial-Configuration`.
3. After that, upload the VM license.
   FortiGate should query FortiManager to validate its VM license and FortiGuard service contracts.

If the license status does not appear as Valid, run the following command:

```
# execute update-now
```

Remote-FortiGate

The following procedure outlines how to configure the network interfaces on Remote-FortiGate.

To configure network interfaces on Remote-FortiGate

1. Start the Remote-FortiGate VM and open the VM console.
2. Log in as `admin`, and leave the password field empty.
3. Enter:
   ```
   exec formatlogdisk
   ```
   This formats the virtual disk, which is required to store data such as local reports or logs. The device reboots after the format is complete.
4. Enter this configuration to configure the network interfaces:
   ```
   config system interface
      edit port4
         set ip 10.200.3.1 255.255.255.0
         set allowaccess ping https ssh http fgfm
      next
   end
   config router static
      edit 1
         set device port4
         set gateway 10.200.3.254
      next
   end
   ```
5. Connect to the GUI from the Local-Client VM and upload the `remote-initial.conf` file from the folder `Resources/Initial-Configuration`.
6. Upload the VM license for this device.
   FortiGate should validate the license and FortiGuard service contracts against FortiManager.

If the license status does not appear as valid, run the following command:

```
# execute update-now
```

ISFW

The following procedure outlines how to configure the network interfaces on ISFW.

To configure network interfaces on ISFW

1. Start the ISFW VM and open the VM console.
2. Log in as `admin`, and leave the password field empty.
3. Enter:
   ```
   exec formatlogdisk
   ```
   This formats the virtual disk, which is required to store data such as local reports or logs. The device reboots after the format is complete.
4. Enter this configuration to configure the network interfaces:
   ```
   config system interface
      edit port1
         set ip 1.0.1.200 255.255.255.0
         set allowaccess http
      next
      edit port3
         set ip 10.0.3.254 255.255.255.0
         set allowaccess http
      next
   end
   config router static
      edit 1
         set gateway 10.0.1.254
         set device port1
      next
   end
   config firewall policy
      edit 1
         set srcintf port3
         set dstintf port1
         set srcaddr all
         set dstaddr all
         set action accept
         set schedule always
         set service ALL
         set nat enable
      next
   end
   ```
5. Connect to the GUI from the Local-Client VM and upload the `ISFW-initial.conf` file from the folder `Resources/Initial-Configuration`.
6. Upload the VM license for this device.
   FortiGate should validate the license and FortiGuard service contracts against FortiManager.

If the license status does not appear as valid, run the following command:

```
# execute update-now
```

FortiAuthenticator

To configure FortiAuthenticator, you must set the FortiAuthenticator IP and default gateway, upload the license, and restore the FortiAuthenticator initial configuration file.

To set the FortiAuthenticator IP and default gateway

1. Power on the FortiAuthenticator VM from the VM library.
2. Log in to the FortiAuthenticator VM console.
   - **FortiAuthenticator login**: admin
   - **Password**: <blank>
3. Type the following commands:

```
config system interface
   edit port1
      set ip 10.0.1.150/24
      set allowaccess gui https ssh
   end
```

   Your default gateway is the FortiGate. Refer to the network topology for more information.

To upload the FortiAuthenticator license

1. Log in to the Local-Client VM.
2. Open a browser and go to the FortiAuthenticator Web-based manager (`https://10.0.1.150`).
   Confirm the security exception if prompted.
3. Log in as `admin` and leave the password empty.
4. Click **System** > **Administration** > **Licensing**.
5. Browse to the location of your license file and click **OK**.
6. Click **OK** to reboot.
   The FortiAuthenticator reboots and your license is added.

To restore the FortiAuthenticator initial configuration file

1. Log back in to the FortiAuthenticator Web-based manager (https://`10.0.1.150`) as `admin`.
2. Click **System** > **Dashboard** > **Status**.
3. In the **System Information** widget, under **System Configuration**, click **Backup/Restore**. **System Configuration**
4. Browse to **Desktop** > **Resources** > **Initial-Configuration** and upload `FortiAuthenticator_initial.conf`.
5. Click **Restore**.
6. Click **OK**.

In FortiAuthenticator, the configuration file is tied to the license. As such, after uploading the configuration file, check the license number in the **System Information** widget of the dashboard. If it is not the same license number you uploaded earlier, re-upload the license again and then backup your configuration. This way, the initial configuration file will be saved with your own license. This applies to all configuration files (that is, for the labs).

Saving Configuration in FortiGate Revisions

All the initial configurations for all labs have been saved on each FortiGate device in the flash.

There are many lab configurations that use the same initial configuration from *FortiGate Security Lab1* (`Initial-Configuration` folder).

The mapping of old configuration path to new configuration is shown in the table below:

- FortiGate Security

Lesson	Old Configuration Path (in `Resources` folder)	New Configuration Mapping (in FortiGate revisions)
1: Introduction and Initial Configuration	**Introduction** > `local-initial`	`initial`
2: Security Fabric	**Security-Fabric** > `local-SF`	`local-SF`
	Security-Fabric > `remote-SF`	`remote-SF`
3: Firewall Policies	**Firewall-Policies** > `local-firewall-policy`	`local-firewall-policy`
	Firewall-Policies > `remote-initial`	`initial`
	Firewall-Policies > `ISFW-initial`	`initial`
4: Network Address Translation (NAT)	**NAT** > `local-nat`	`local-nat`
	NAT > `local-central-nat`	`local-central-nat`
	NAT > `remote-initial`	`initial`
5: Firewall Authentication	**Firewall-Authentication** > `local-firewall-authentication`	`local-firewall-authentication`
6: Logging and Monitoring	**Logging** > `local-logging.conf`	`local-logging`
7: Certificate Operations	**Certificate-Operations** > `local-certificate-operations`	`initial`
	Certificate-Operations > `remote-certificate-operations`	`initial`

Lesson	Old Configuration Path (in `Resources` folder)	New Configuration Mapping (in FortiGate revisions)
8: Web Filtering	**Web-Filtering** > `local-web-filtering.conf`	`local-web-filtering`
9: Application Control	**Application Control** > `local-app-control`	`local-app-control`
10: Antivirus	**Antivirus** > `local-AV-flow-based`	`initial`
11: Intrusion Prevention and Denial of Service	**Intrusion-Prevention-System** > `local-intrusion-prevention-system`	`initial`
12: SSL-VPN	**SSL-VPN** > `local-SSL-VPN`	`local-SSL-VPN`

- FortiGate Infrastructure

Lesson	Old Configuration Path (in `Resources` folder)	New Configuration Mapping (in FortiGate revisions)
1: Routing	**Routing** > `local-routing`	`initial`
2: Software-Defined WAN	**SDWAN** > `local-sdwan`	`initial`
3: Virtual Domains (VDOMs)	**VDOM** > `local-vdom`	`local-vdom`
4: Layer 2 Switching	**Layer2** > `local-layer-2`	`local-layer-2`
5: IPsec VPN	**IPsec-VPN** > `local-ipsec-vpn`	`local-ipsec-vpn`
	IPsec-VPN > `remote-ipsec-vpn`	`initial`
	IPsec-VPN > `remote-redundant-ipsec-vpn`	`remote-redundant-ipsec-vpn`
6: Fortinet Single Sign-On (FSSO)	**FSSO** > `local-FSSO`	`local-FSSO`
7: High Availability (HA)	**HA** > `local-ha`	`local-ha`
	HA > `remote-ha`	`initial`
	HA > `remote-initial`	`initial`
8: Diagnostics	**Diagnostics** > `local-diagnostics`	`local-diagnostics`

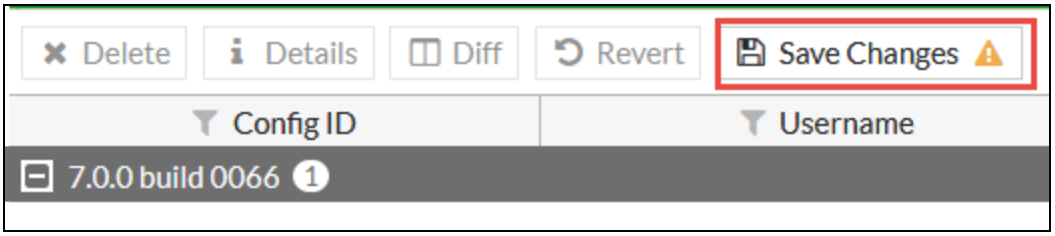
The desktop still contains the resources folder which includes the initial configurations for each lab in the same format used previously. If any student encounter issues with restoring the configuration from the FortiGate flash, instructor can help the students' to restore the configurations from the **Resources** folder.

Saving Configurations in the FortiGate Revisions

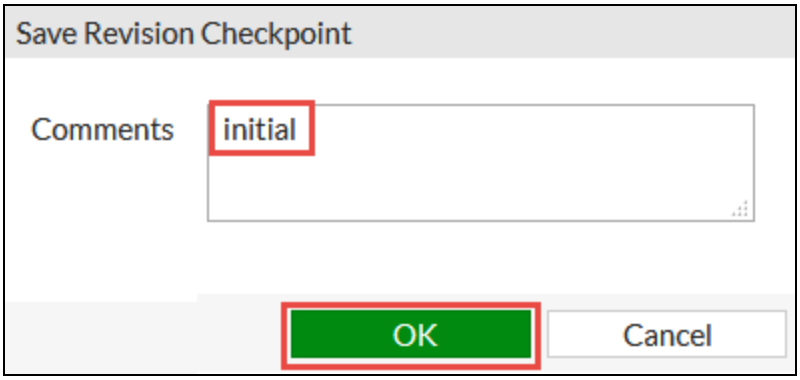
You will use the above tables to save each FortiGate configurations in Revisions.

To save configurations in the FortiGate Revisions

1. On the Local-Client 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** > **Initial-Configuration** > `local-initial.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.
7. Open a browser and log in to the Local-FortiGate GUI at `10.0.1.254` with the user name `admin` and password `password`.
8. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Revisions**.
9. Click **Save Changes**.



10. In the **Save Revision Checkpoint** pop-up window, in the **Comments** field, type `initial`.



Make sure to use the same names as per the tables above in column **New Configuration Mapping (in FortiGate revisions)** for **Save Revision Checkpoint**. If you make a mistake and correct it, FortiGate will save the changes. However, after FortiGate reboots, FortiGate will revert your comments.

To fix it, you need to delete the configuration with incorrect name and restore the configuration again and use the correct name.

11. Follow the above procedure for all configurations based on the table above for Local-FortiGate, Remote-FortiGate, and ISFW.

Testing

After you install all of the VMs, and configure all LAN segments, host IP settings, and virtual network connections, then you test connectivity.

From Local-Client server, test connectivity to:

10.0.1.254	LAN3 Local-FortiGate_port3
10.0.1.241	FortiManager
10.0.1.200	ISFW
10.0.1.210	FortiAnalyzer
10.0.1.20	FIT
10.0.1.150	FortiAuthenticator

From Local-FortiGate, test connectivity to:

10.0.1.10	LAN3 Local-Client
10.200.1.254	LAN1 LINUX_eth1
10.200.2.254	LAN2 LINUX_eth2
10.0.1.241	FortiManager
10.0.1.200	ISFW
10.0.1.210	FortiAnalyzer
4.2.2.2	To test IP forwarding and NAT on your Linux VM
10.0.1.20	LAN3 FIT
10.0.1.150	FortiAuthenticator
10.200.1.150	FortiAuthenticator

From the ISFW, test connectivity to:

10.0.1.254	LAN3 Local-FortiGate_port3
10.0.3.20	LAN7 FIT

From the Linux host, test connectivity to:

10.200.1.1	LAN1 Local-FortiGate_port1
10.200.2.1	LAN2 Local-FortiGate_port2
10.200.3.1	LAN4 Remote-FortiGate_port4
10.200.4.1	LAN5 Remote-FortiGate_port5
4.2.2.2	LAN0

From Remote-FortiGate, test connectivity to:

10.0.2.10	LAN6 Remote-Client
10.200.3.254	LAN4 LINUX_eth3
10.200.4.254	LAN5 LINUX_eth4
10.200.1.241	FortiManager
10.200.1.210	FortiAnalyzer

From Remote-Client, test connectivity to:

10.0.2.254	LAN6 Remote-FortiGate_port6

From FortiAnalyzer, test connectivity to:

10.0.1.20	FIT
10.0.1.254	LAN3 Local-FortiGate_port3
10.200.1.254	LAN1 LINUX_eth1

Creating Snapshots

After you have completed and tested your configuration, save a snapshot of each VM. These snapshots are what you will deploy for each student in the class.

You can also re-deploy these snapshots to revert a student's VM if their configuration is not working and they need to quickly restore it to a functional state.