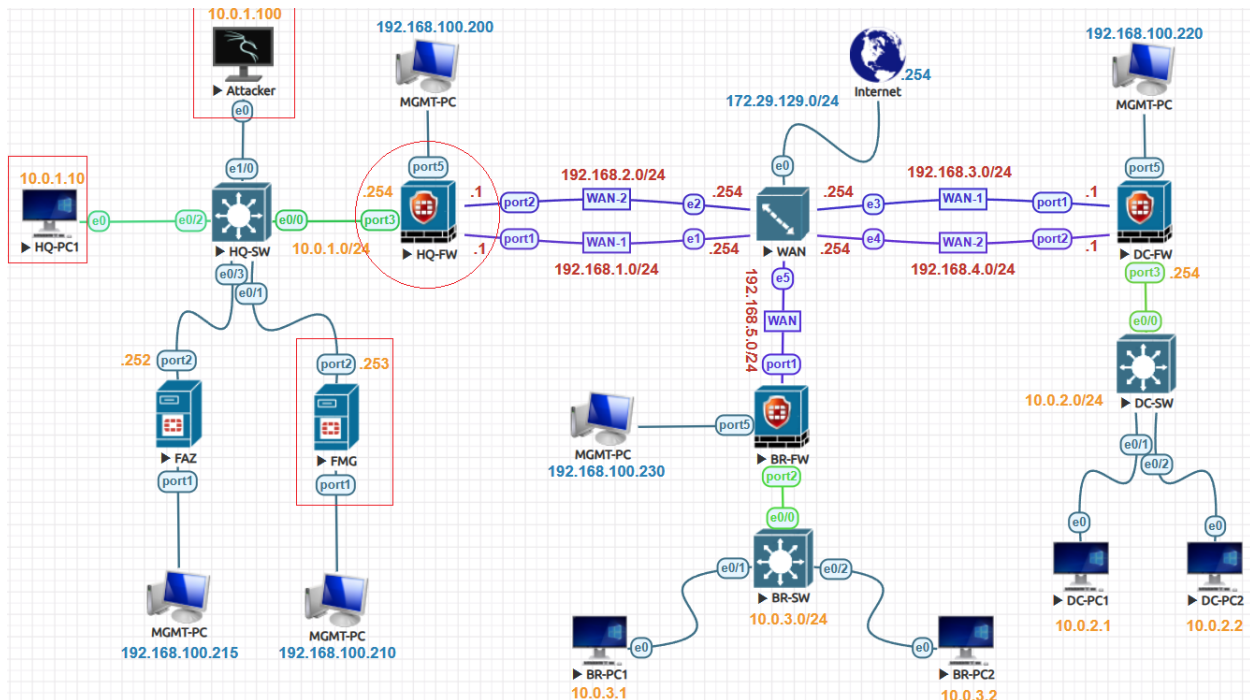


## AntiVirus Profile Lab:



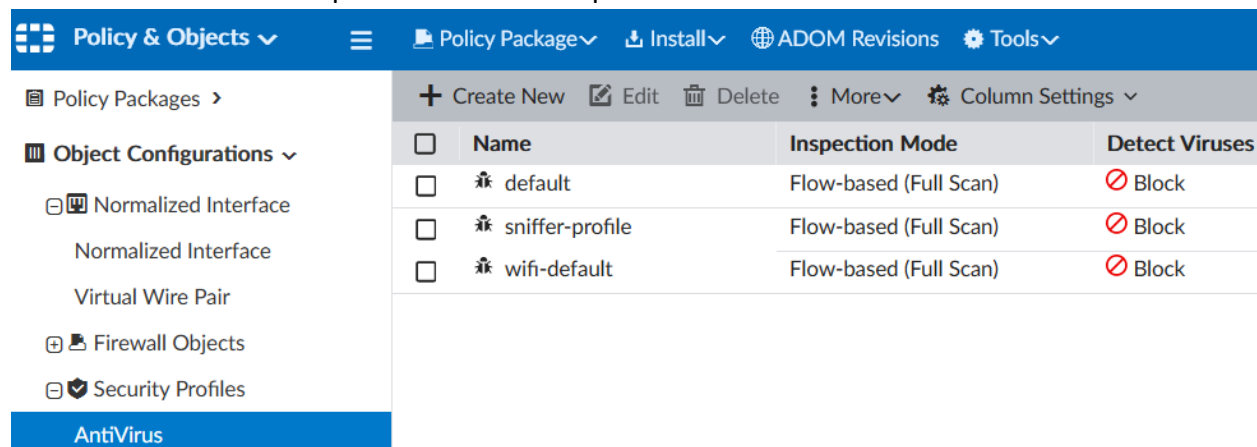
First check you have active AntiVirus License navigate to **Dashboard>Status**.

Licenses (173.243.141.6)	Virtual Machine	System Information
<ul style="list-style-type: none"> <li>FortiCare Support</li> <li>Firmware &amp; General Updates</li> <li>IPS</li> <li>AntiVirus</li> <li>Web Filtering</li> </ul>	<ul style="list-style-type: none"> <li>FGVM04 License</li> <li>Allocated vCPUs: 1 / 4</li> <li>Allocated RAM: 1 GB</li> <li>Auto Scaling: <span style="color: red;">✖</span></li> </ul>	<ul style="list-style-type: none"> <li>Hostname: FW1</li> <li>Serial Number: FGVM04TM22003418</li> <li>Firmware: v7.0.5 build0304 (GA)</li> <li>Mode: NAT</li> <li>System Time: 2022/05/24 17:00:51</li> <li>Uptime: 00:00:03:03</li> <li>WAN IP: 2.91.22.27</li> </ul>

Also, verify updated AntiVirus signatures and database navigate to **System>FortiGuard**.

<div> <div>+</div> Virtual Machine </div> <div> <div>+</div> Firmware &amp; General Updates </div> <div> <div>+</div> Intrusion Prevention </div> <div> <div>-</div> AntiVirus </div>	<div> <div>✓</div> Valid (Expiration Date: 2022/07/24) </div> <div> <div>✓</div> Licensed (Expiration Date: 2022/07/25) </div> <div> <div>✓</div> Licensed (Expiration Date: 2022/07/25) </div> <div> <div>✓</div> Licensed (Expiration Date: 2022/07/25) </div>	<div> <div>🔗</div> FortiGate VM License </div>
<div>AI Malware Detection Model</div> <div>AV Definitions</div> <div>AV Engine</div>	<div> <div>🕒</div> Version 0.00000 </div> <div> <div>🕒</div> Version 1.00000 </div> <div> <div>🕒</div> Version 6.00270 </div>	<div> <div>+</div> Upgrade Database </div>

Go to **Policy & Objects > Object Configurations > Security Profiles > AntiVirus**. You can create New and also there are three preloaded antivirus profiles to use.



To edit the default antivirus profile, go to **Policy & Objects > Object Configurations > Security Profiles > AntiVirus** click on default to **edit**.

Edit AntiVirus Profile

Name

default

Comments

Scan files and block viruses.

29/255

Detect Viruses

Block
Monitor

Feature Set

Flow-based
Proxy-based

Inspected Protocols

HTTP

SMTP

POP3

IMAP

FTP

CIFS

<b>Name</b>	Name of the Antivirus Profile
<b>Comments</b>	Provide any comments
<b>Detect Viruses</b>	Choose option to take action Block or Monitor.
<b>Block</b>	Prevents all traffic from reaching the application and logs all occurrences.
<b>Monitor</b>	Allows the targeted traffic to continue on through the FortiGate unit but logs the traffic for analysis.
<b>Inspected Protocols</b>	Choose the type of protocols to be inspected by Antivirus engine.

Go to **Policy & Objects > Object Configurations > Security Profiles > AntiVirus** click on **Create New** to create new AntiVirus Profile. Enter the name in this case Custom-AV.

### Create New AntiVirus Profile

Name	<input type="text" value="Custom-AV"/>
Comments	<div><div></div><div>0/255</div></div>
Detect Viruses ⓘ	<span>Block</span> <span>Monitor</span>
Feature Set	<span>Flow-based</span> <span>Proxy-based</span>
<b>Inspected Protocols</b>	
HTTP	<input type="checkbox"/>
SMTP	<input type="checkbox"/>
POP3	<input type="checkbox"/>
IMAP	<input type="checkbox"/>
FTP	<input type="checkbox"/>
CIFS	<input type="checkbox"/>

Continue on the FortiManager GUI, click **Policy Packages**, Click **HQ-FW>Firewall Policy**. Select the first policy at the top of the list, and then click **Edit**.

Policy & Objects

Policy Packages

Search...

HQ-FW\_root

**Firewall Policy**

Installation Targets

default

Object Configurations

Create New Edit Delete Section Policy Lookup Collapse All

#	Name	From	To	Source
<input checked="" type="checkbox"/> 1	LAN-to-WAN	LAN-Port	WAN1-Port WAN2-Port	all
▼ Implicit (2-2 / Total: 1)				
<input type="checkbox"/> 2	Implicit Deny	any	any	all

Click the Security Profiles check box. Configure **AntiVirus Profile** and SSL/SSH Inspection and click **OK**.

#### Disclaimer Options

Display Disclaimer



#### Security Profiles




Profile Type

Use Standard Security Profiles

Use Security Profile Group

AntiVirus Profile

 default 

Web Filter Profile



Application Control



IPS Profile



DNS Filter

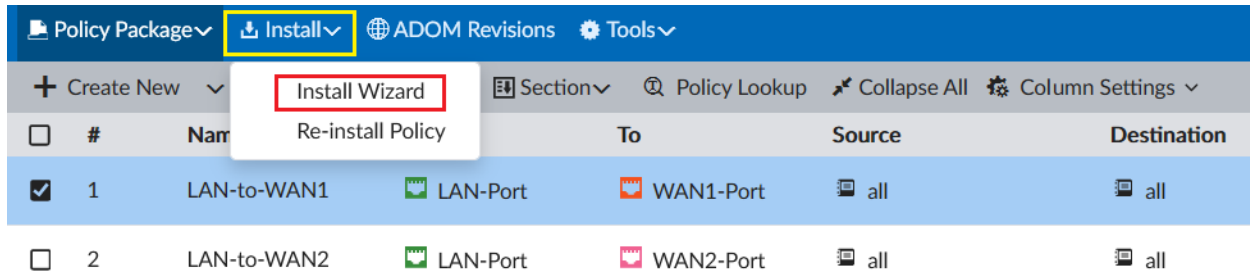


SSL/SSH Inspection

 deep-inspection 

## Install the Policy:

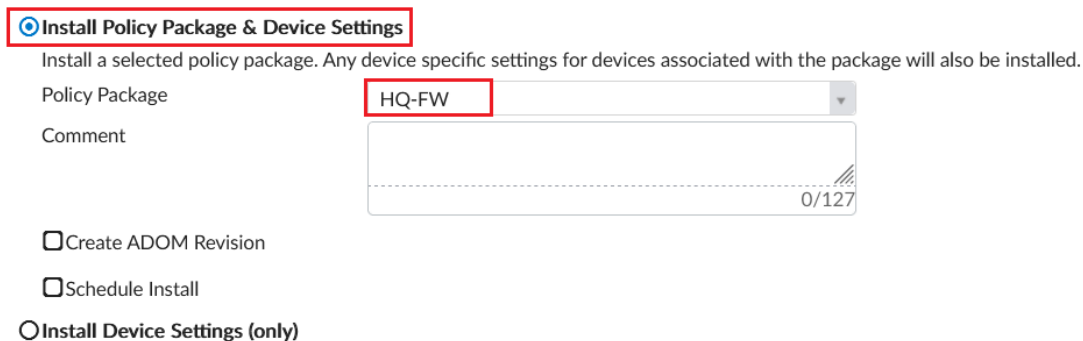
Continue on the FortiManager GUI, click **Install>Install Wizard**.



#	Name	To	Source	Destination
1	LAN-to-WAN1	LAN-Port	WAN1-Port	all
2	LAN-to-WAN2	LAN-Port	WAN2-Port	all

Select Install Policy Package & Device Settings. Conform that the HQ-FW policy package is selected. And then click **Next**.

### Install Wizard



☒ **Install Policy Package & Device Settings**

Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Policy Package: **HQ-FW**

Comment:

☐ Create ADOM Revision

☐ Schedule Install


☐ Install Device Settings (only)

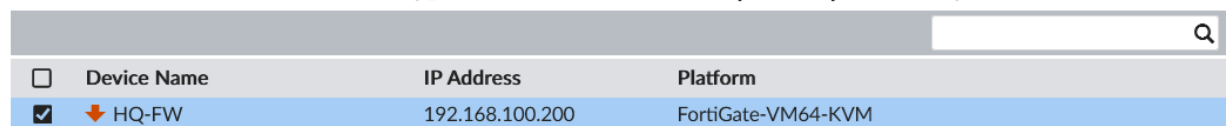
Next >

Cancel

Confirm that the **HQ-FW** device is selected, and then click **Next**.

### Install Wizard - Policy Package and Device Setting (HQ-FW)

Please select one or more devices to install (  Use checkbox or Ctrl or Shift key for multiple selections)



Device Name	IP Address	Platform
<input checked="" type="checkbox"/> HQ-FW	192.168.100.200	FortiGate-VM64-KVM

< Back




Next >




Cancel

Click Install Preview to see changes that will be applied to FortiGate. Click Close on the Install Preview page. Click **Install**.

## Install Wizard - Policy Package (HQ-FW)

Installation Preparation Total: 3/3,  Success: 3,  Warning: 0,  Error: 0 

-  Interface Validation
-  Policy and Object Validation
-  Ready to Install.









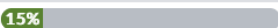
 Install Preview	 Policy Package Diff	
<input type="checkbox"/> Device Name	Status	Action
<input checked="" type="checkbox"/> HQ-FW[root]	 Connection Up	

Install

Cancel

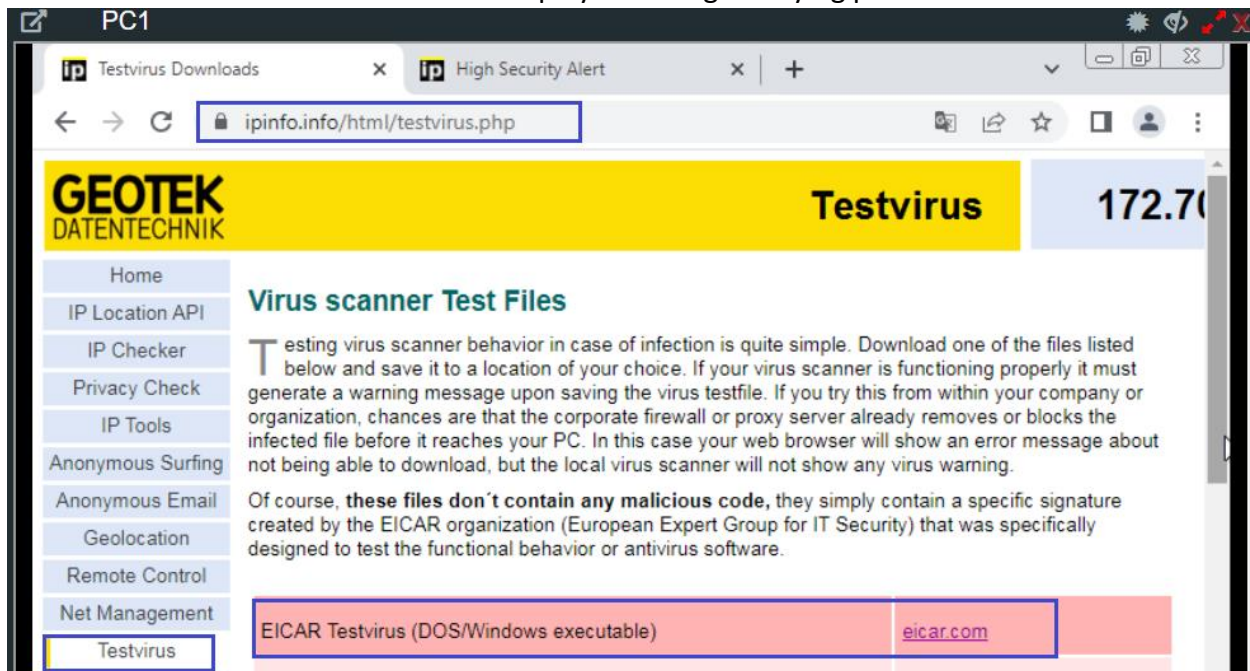
Once done click **Finish**.

## Install Wizard - Policy Package (HQ-FW)

22%			
Total: 0/1,  Pending: 0,  In Progress: 1,  Completed: 0 			
 View Installation Log	 View Progress Report	 Column Settings ▾	Search... 
#	Name	Time Used	Status
1	HQ-FW	N/A	 15%

## Verification & Testing:

To test the antivirus scanning, go to [www.ipinfo.info/html/testvirus.php](http://www.ipinfo.info/html/testvirus.php) and attempt to download a test file. The browser will display a message denying permission to download file.



## High Security Alert

You are not permitted to download the file "eicar.com" because it is infected with the virus "EICAR\_TEST\_FILE".

URL <https://meineipadresse.de/testvirus/eicar.com>

Quarantined File Name

Reference URL [http://www.fortinet.com/ve?vn=EICAR\\_TEST\\_FILE](http://www.fortinet.com/ve?vn=EICAR_TEST_FILE)

To view information about the blocked file, go to **Log & Report>AntiVirus**

Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action
42 seconds ago	HTTPS	10.0.1.10	eicar3.zip	EICAR_TEST_FILE		URL: https://meineipadresse.de/testvirus/eicar3.zip	blocked
44 seconds ago	HTTPS	10.0.1.10	eicar3.zip	EICAR_TEST_FILE		URL: https://meineipadresse.de/testvirus/eicar3.zip	blocked
47 seconds ago	HTTPS	10.0.1.10	eicar2.zip	EICAR_TEST_FILE		URL: https://meineipadresse.de/testvirus/eicar2.zip	blocked
48 seconds ago	HTTPS	10.0.1.10	eicar2.zip	EICAR_TEST_FILE		URL: https://meineipadresse.de/testvirus/eicar2.zip	blocked
53 seconds ago	HTTPS	10.0.1.10	eicar.zip	EICAR_TEST_FILE		URL: https://meineipadresse.de/testvirus/eicar.zip	blocked
54 seconds ago	HTTPS	10.0.1.10	eicar.zip	EICAR_TEST_FILE		URL: https://meineipadresse.de/testvirus/eicar.zip	blocked
Minute ago	HTTPS	10.0.1.10	eicar.com	EICAR_TEST_FILE		URL: https://meineipadresse.de/testvirus/eicar.com	blocked
Minute ago	HTTPS	10.0.1.10	eicar.com	EICAR_TEST_FILE		URL: https://meineipadresse.de/testvirus/eicar.com	blocked
Hour ago	HTTPS	10.0.1.10	eicar.com	EICAR_TEST_FILE		URL: https://meineipadresse.de/testvirus/eicar.com	blocked
Hour ago	HTTPS	10.0.1.10	eicar.com	EICAR_TEST_FILE		URL: https://meineipadresse.de/testvirus/eicar.com	blocked



To view logs information about blocked files, go to **Log & Reports > Forward Traffic**

Date/Time		Source	Device	Destination	Application Name	Result
7 seconds ago		10.0.1.10	DESKTOP-W10	40.81.120.44 (win10.ipv6.microsoft.com)		✓ 16.82 kB / 25.34 kB
12 seconds ago		10.0.1.10	DESKTOP-W10	8.8.8.8 (dns.google)		✓ 972 B / 5.00 kB
39 seconds ago		10.0.1.10	DESKTOP-W10	20.198.119.143 (client.wns.windows.com)		✓ 6.37 kB / 10.75 kB
49 seconds ago		10.0.1.10	DESKTOP-W10	208.91.114.120		✓ 152 B / 0 B
51 seconds ago		10.0.1.10	DESKTOP-W10	216.58.204.138		✓ 2.69 kB / 6.48 kB
51 seconds ago		10.0.1.10	DESKTOP-W10	162.159.61.3 (chrome.cloudflare-dns.com)		✓ 2.49 kB / 2.83 kB
54 seconds ago		10.0.1.10	DESKTOP-W10	208.91.114.120		✓ 152 B / 0 B
56 seconds ago		10.0.1.253	50:00:00:08:00:01	208.91.112.63 (ntp1.fortinet.net)		✓ 76 B / 76 B
Minute ago		10.0.1.10	DESKTOP-W10	208.91.114.120		✓ 152 B / 0 B
Minute ago		10.0.1.10	DESKTOP-W10	167.235.222.242 (web02.geotek.de)		Deny: UTM Blocked
Minute ago		10.0.1.10	DESKTOP-W10	167.235.222.242 (web02.geotek.de)		Deny: UTM Blocked
Minute ago		10.0.1.10	DESKTOP-W10	167.235.222.242 (web02.geotek.de)		✓ 979 B / 4.92 kB

Also, from FortiAnalyzer navigate to **Log View>FortiGate>Security>Antivirus**

All FortiGate - Last 1 Hour - 09:33:53 To 10:33:52							
Add Filter							
#	▼ Date/Time	Device ID	Action	Source	Service	Destination IP	Virus/Botnet
1	10:31:51	FGVM01TM23005901	blocked	10.0.1.10	HTTPS	167.235.222.242	EICAR_TEST_FILE
2	10:31:49	FGVM01TM23005901	blocked	10.0.1.10	HTTPS	167.235.222.242	EICAR_TEST_FILE
3	10:31:46	FGVM01TM23005901	blocked	10.0.1.10	HTTPS	167.235.222.242	EICAR_TEST_FILE
4	10:31:45	FGVM01TM23005901	blocked	10.0.1.10	HTTPS	167.235.222.242	EICAR_TEST_FILE
5	10:31:40	FGVM01TM23005901	blocked	10.0.1.10	HTTPS	167.235.222.242	EICAR_TEST_FILE
6	10:31:39	FGVM01TM23005901	blocked	10.0.1.10	HTTPS	167.235.222.242	EICAR_TEST_FILE
7	10:31:29	FGVM01TM23005901	blocked	10.0.1.10	HTTPS	167.235.222.242	EICAR_TEST_FILE
8	10:31:27	FGVM01TM23005901	blocked	10.0.1.10	HTTPS	167.235.222.242	EICAR_TEST_FILE