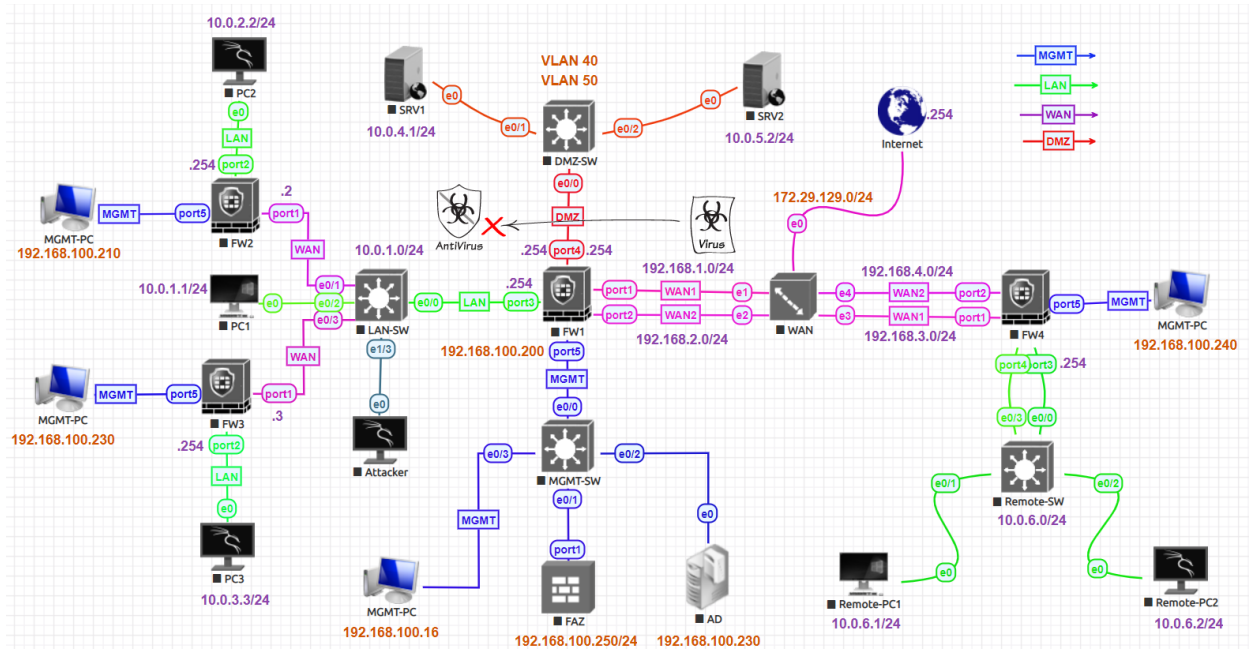


AntiVirus Profile Lab:



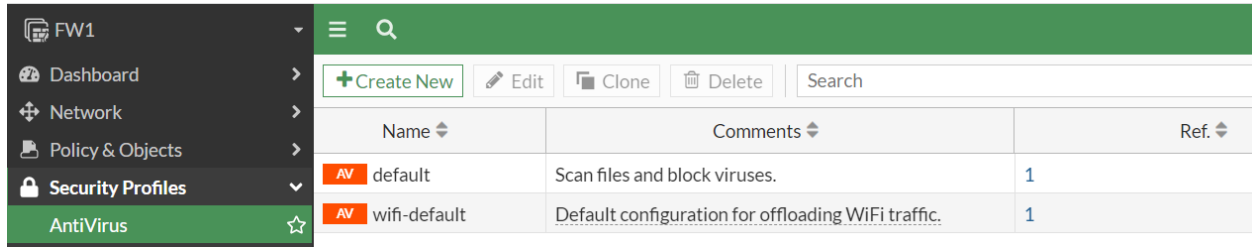
First check you have active AntiVirus License navigate to **Dashboard>Status**.

Licenses (173.243.141.6)	Virtual Machine	System Information
<ul style="list-style-type: none"> FortiCare Support Firmware & General Updates IPS AntiVirus Web Filtering 	<ul style="list-style-type: none"> FGVM04 License Allocated vCPUs: 1 / 4 (25%) Allocated RAM: 1 GB Auto Scaling: ✖ 	<ul style="list-style-type: none"> Hostname: FW1 Serial Number: FGVM04TM22003418 Firmware: v7.0.5 build0304 (GA) Mode: NAT System Time: 2022/05/24 17:00:51 Uptime: 00:00:03:03 WAN IP: 2.91.22.27

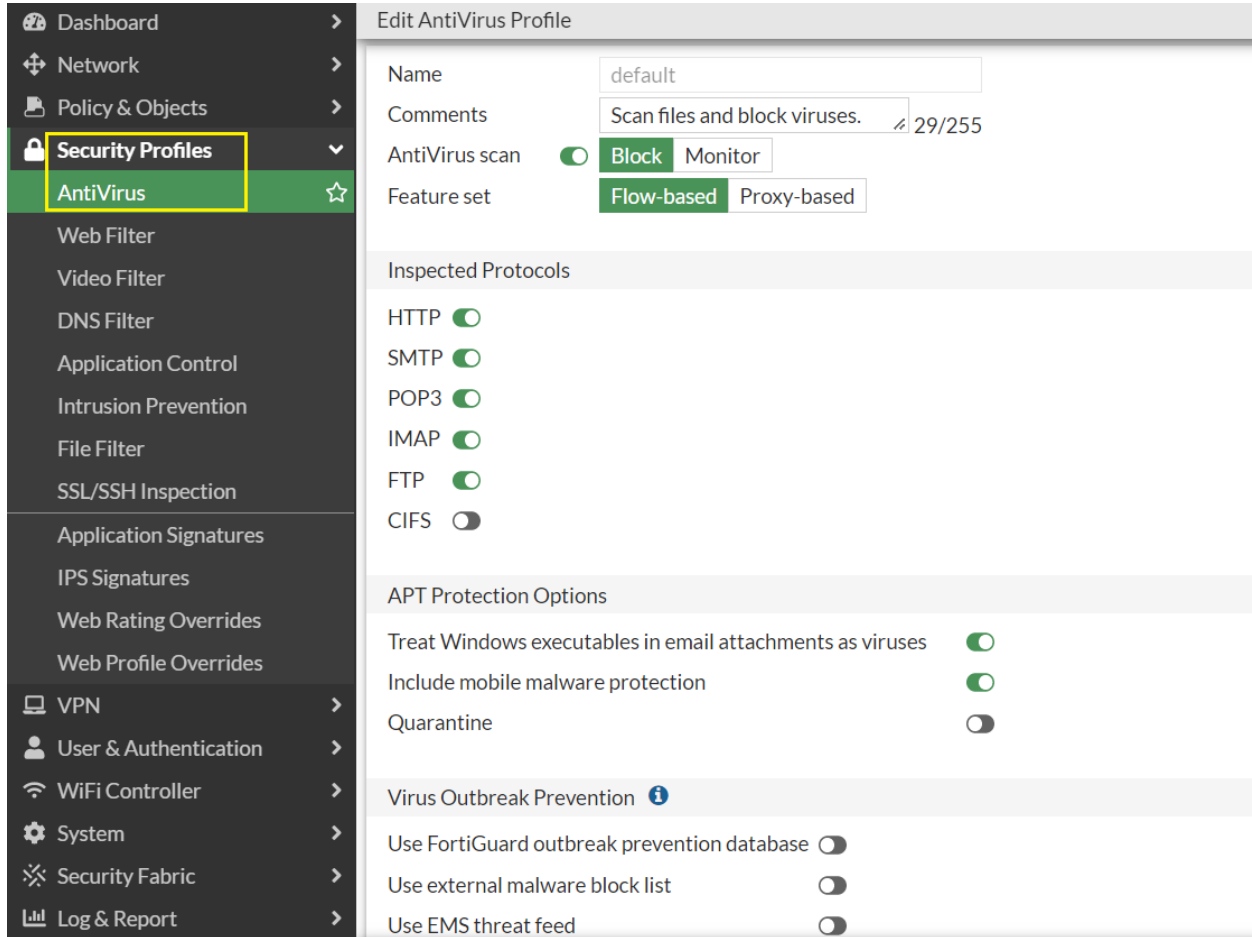
Also, verify updated AntiVirus signatures and database navigate to **System>FortiGuard**.

<ul style="list-style-type: none"> Virtual Machine Firmware & General Updates Intrusion Prevention AntiVirus 	<ul style="list-style-type: none"> Valid (Expiration Date: 2022/07/24) Licensed (Expiration Date: 2022/07/25) Licensed (Expiration Date: 2022/07/25) Licensed (Expiration Date: 2022/07/25) AI Malware Detection Model: Version 0.00000 AV Definitions: Version 1.00000 AV Engine: Version 6.00270 Mobile Malware: Version 0.00000 	<ul style="list-style-type: none"> FortiGate VM License Upgrade Database
--	--	--

Navigate to **Security Profiles > AntiVirus** there are two preloaded antivirus profiles.



To edit the default antivirus profile, go to **Security Profiles > AntiVirus** click on default to edit.



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

Go to **Security Profiles > AntiVirus** click on **Create New** to create new AntiVirus Profile.

Go to edit Internet access policy, go to **Policy & Objects > Firewall Policy**, Under **Security Profiles**, enable **AntiVirus** and select the profile which we created. **SSL Inspection** is enabled by default. Select **deep-inspection**. Click **OK** to apply the changes.

Verification & Testing:

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

GEOTEK DATENTECHNIK Testvirus 172.70

Home
IP Location API
IP Checker
Privacy Check
IP Tools
Anonymous Surfing
Anonymous Email
Geolocation
Remote Control
Net Management
Testvirus

Virus scanner Test Files

Testing virus scanner behavior in case of infection is quite simple. Download one of the files listed below and save it to a location of your choice. If your virus scanner is functioning properly it must generate a warning message upon saving the virus testfile. If you try this from within your company or organization, chances are that the corporate firewall or proxy server already removes or blocks the infected file before it reaches your PC. In this case your web browser will show an error message about not being able to download, but the local virus scanner will not show any virus warning.

Of course, **these files don't contain any malicious code**, they simply contain a specific signature created by the EICAR organization (European Expert Group for IT Security) that was specifically designed to test the functional behavior or antivirus software.

EICAR Testvirus (DOS/Windows executable)	eicar.com
--	--

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

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

Date/T...	Service	Source	File Na...	Virus/Botnet	U...
Hour ago	HTTPS	10.0.1.1	eicar.com	EICAR_TEST_FILE	U
Hour ago	HTTPS	10.0.1.1	eicar.com	EICAR_TEST_FILE	U

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

Date/Time	Source	Device	Destination	Result
2 seconds ago	10.0.1.1	USER-PC	159.69.68.106	Deny: UTM Blocked
5 seconds ago	10.0.1.1	USER-PC	159.69.68.106	Deny: UTM Blocked
6 seconds ago	10.0.1.1	USER-PC	159.69.68.106	Deny: UTM Blocked
8 seconds ago	10.0.1.1	USER-PC	208.91.114.120	152 B / 0 B
9 seconds ago	10.0.1.1	USER-PC	208.91.114.120	152 B / 0 B

Also, from **Dashboard > Status > Advanced Threat Protection Statistics** if this Widget is not available can add to click on Add Widget

