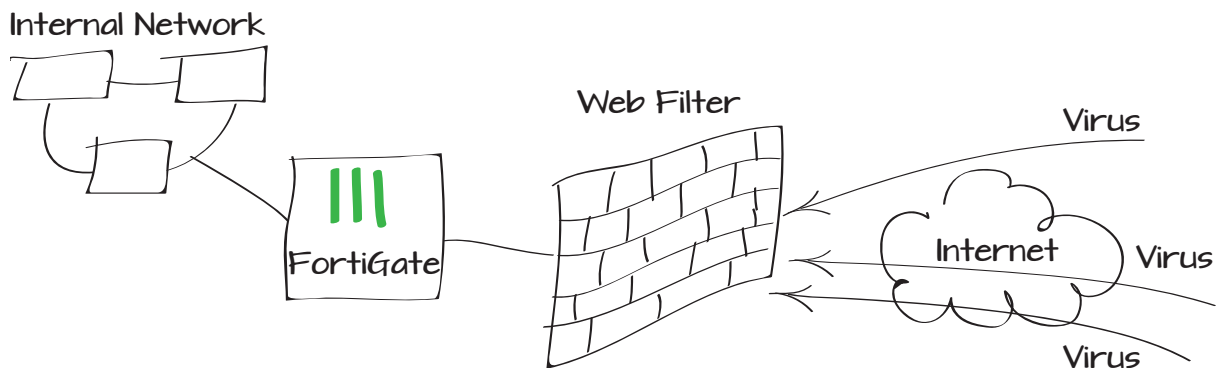


Inspecting traffic content using flow-based inspection

Flow-based inspection offers an alternative to proxy-based inspection, which imposes some limitations on performance and also changes some aspects of packets as they pass through your FortiGate unit. This example enables flow-based inspection for antivirus and web filtering.

1. Enabling flow-based inspection in an antivirus profile
2. Enabling flow-based inspection in a web filtering profile
3. Adding the new profiles to a security policy
4. Results



Enabling flow-based inspection in an antivirus profile

Go to **Security Profiles > Antivirus > Profile**. Select the plus icon in the upper right corner of the window to create a new profile.

Select **Flow-based** as the **Inspection Mode**.

Configure the profile to inspect traffic based on your network needs.

Name

Comments 0/255

Inspection Mode Proxy Flow-based

Block Connections to Botnet Servers

Protocol	Virus Scan and Removal
Web	
HTTP	<input checked="" type="checkbox"/>
Email	
SMTP	<input checked="" type="checkbox"/>
POP3	<input checked="" type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>
MAPI	<input type="checkbox"/>
File Transfer	
FTP	<input checked="" type="checkbox"/>
SMB	<input type="checkbox"/>
IM	
ICQ, Yahoo, MSN Messenger	<input checked="" type="checkbox"/>

Enabling flow-based inspection in a web filtering profile

Go to **Security Profiles > Web Filter > Profile**. Select the plus icon in the upper right corner of the window to create a new profile.

Select **Flow-based** as the **Inspection Mode**.

Configure the profile to block traffic based on your network needs.

Name

Comments 0/255

Inspection Mode Proxy Flow-based DNS

FortiGuard Categories

Show All

- Potentially Liable
- Adult/Mature Content
- Bandwidth Consuming
- Security Risk
- General Interest - Personal
- General Interest - Business
 - Finance and Banking
 - Search Engines and Portals
 - General Organizations
 - Business
 - Information and Computer Security
 - Government and Legal Organizations
 - Information Technology
 - Armed Forces
 - Web Hosting
 - Secure Websites

Enable Safe Search

Search Engine Safe Search - Google, Yahoo!, Bing, Yandex

Adding the new profiles to a security policy

Go to **Policy > Policy > Policy**.

Edit the policy controlling the traffic you wish to inspect. Under **Security Features**, enable **Antivirus** and **Web Filter** and set them to use the new profiles.

Results

To test the AV scanning, go to www.eicar.org and try to download a test file. The browser will time out and display a message similar to what is shown here from Google Chrome.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	internal
Source Address	all
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	Click to add...
Logging Options	
<input type="radio"/> No Log	
<input checked="" type="radio"/> Log Security Events	
<input type="radio"/> Log all Sessions	
Security Profiles	
<input type="checkbox"/> AntiVirus	default
<input checked="" type="checkbox"/> Web Filter	default
<input type="checkbox"/> Application Control	Block_app-sensor
<input type="checkbox"/> IPS	default
<input type="checkbox"/> Email Filter	default
<input type="checkbox"/> DLP Sensor	default

This webpage is not available

The connection to www.eicar.org was interrupted.

Here are some suggestions:

- [Reload](#) this webpage later.
- Check your Internet connection. Restart any router, modem, or other network device.
- Add Google Chrome as a permitted program in your firewall's or antivirus software program, try deleting it from the list of permitted programs and adding it again.
- If you use a proxy server, check your proxy settings or contact your network administrator. If you don't believe you should be using a proxy server, adjust your proxy settings in **System Preferences > Network > Advanced > Proxies** and deselect any proxy servers.

Go to **Log & Report > Traffic Log > Forward Traffic** to see the blocked traffic.

Download Raw Log

me	Src	Device	Dst	Application Name	Security Action
	192.168.100.110		192.168.110.9	Unknown	✓
	192.168.100.110		192.168.110.9	Unknown	✓
	192.168.100.110		192.168.110.9	Unknown	✓
	192.168.100.110		208.91.113.212	Unknown	
	192.168.100.110		208.91.113.212	Unknown	
	192.168.100.110		208.91.113.212	Unknown	
	192.168.100.110		208.91.113.212	Unknown	

To test the web filtering, browse to www.google.com. The FortiGate unit will display a block message.

Firefox Web Filter Violation +

www.google.com

Web Page Blocked!

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

URL: www.google.com/
 Category: Search Engines and Portals

To have the rating of this web page re-evaluated [please click here](#).

Go to **Security Profiles > Monitor > Web Monitor** to see information about blocked Internet traffic.

