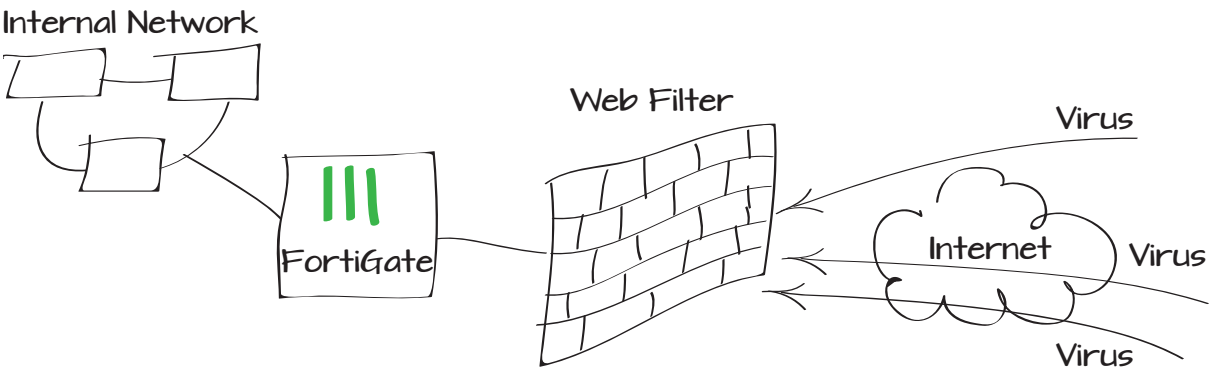
Inspecting traffic content using flow-based inspection

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

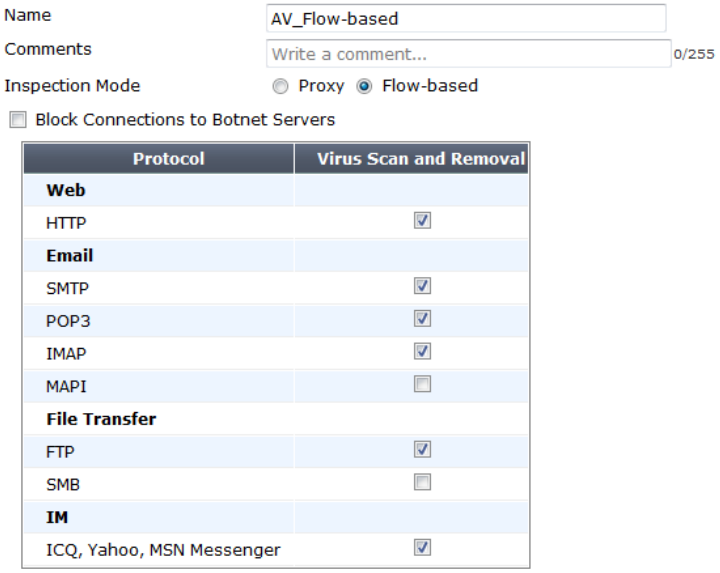


Enabling flow-based inspection in an antivirus profile

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.

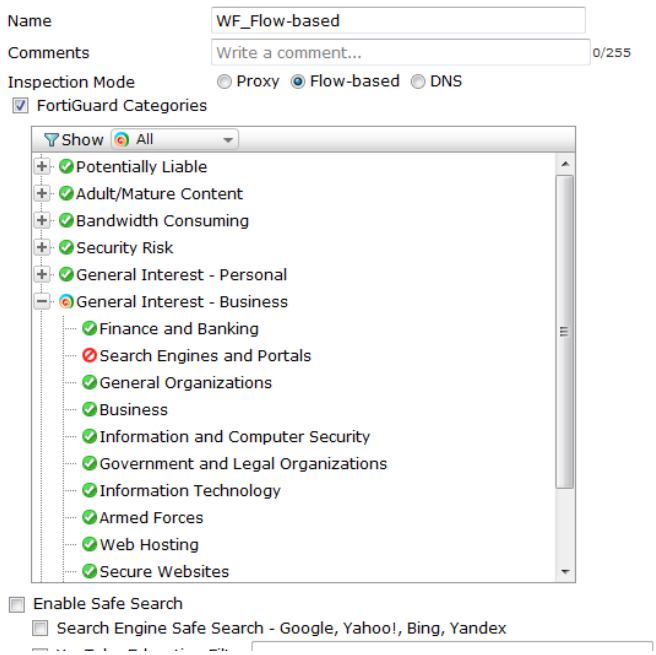


Enabling flow-based inspection in a web filtering profile

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**.

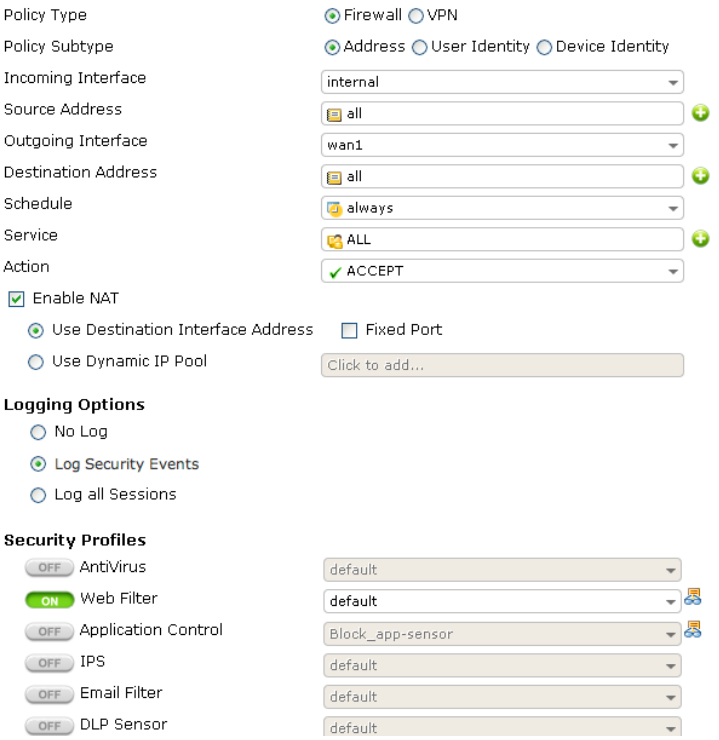
Configure the profile to block traffic based on your network needs.



Adding the new profiles to a security policy

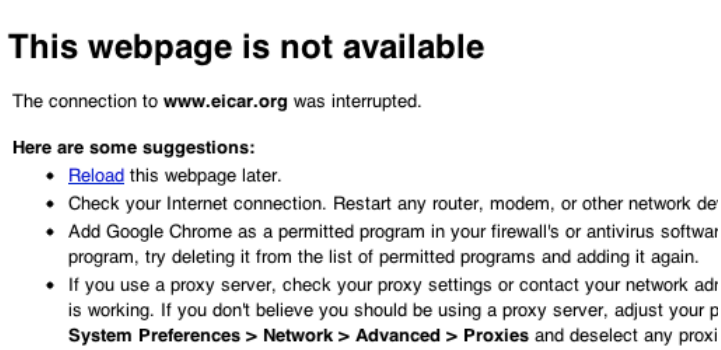
Go to **Policy > Policy > Policy**.

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.

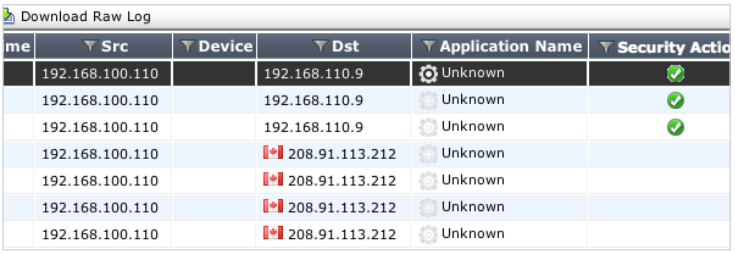


Results

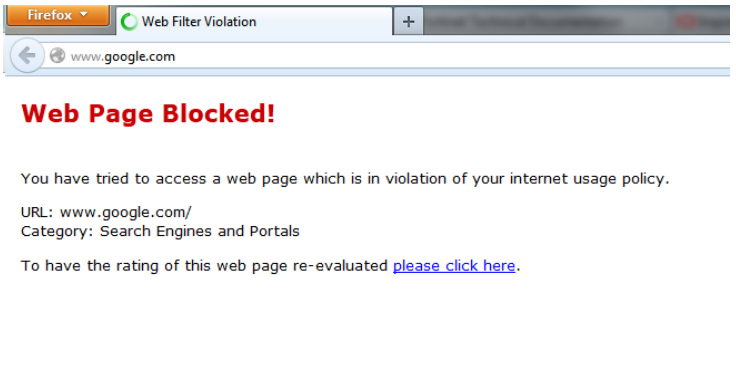
To test the AV scanning, go to www.eicar.org and try to download a test file. The browser will time out and display a message similar to what is shown here from Google Chrome.



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



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



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