DEPL Project

Name: Mohamed Gomaa Mohamed

Track: Fortinet cyber security

Student ID: 21050760

Group ID: CAI1_ISS8_S1e

Project: Web Filtering

Web Filtering

In this lab, you will configure one of the most used security profiles on FortiGate: web filter. This includes configuring a FortiGuard category-based filter, applying the web filter profile on a firewall policy, testing the configuration, and basic troubleshooting.

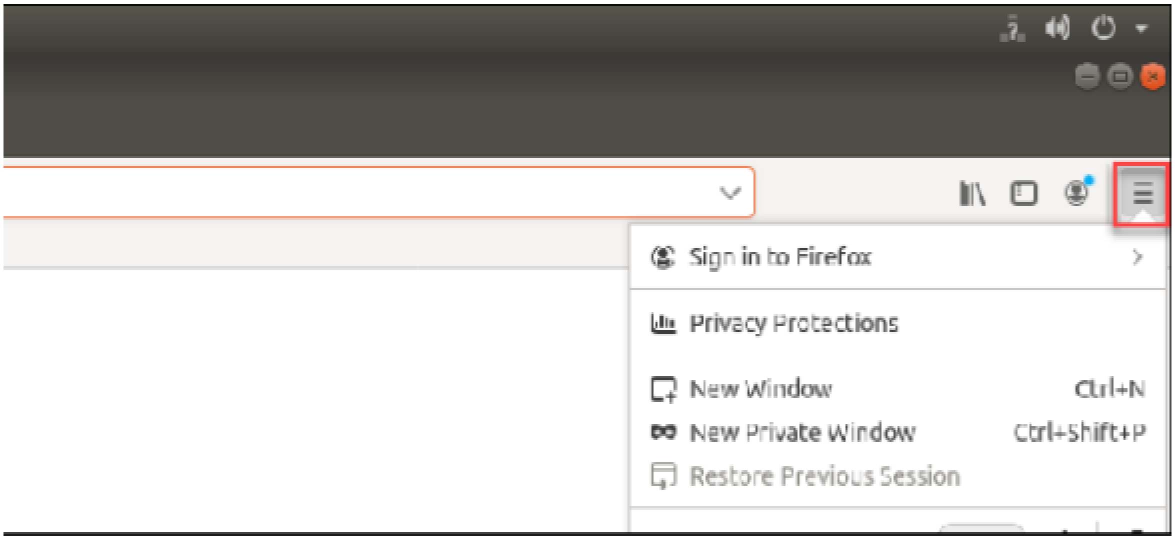
Objectives

- Configure web filtering on FortiGate
- Apply the FortiGuard category-based option for web filtering
- Troubleshoot the web filter
- Read and interpret web filter log entries

Before beginning this lab, you must clear the browser history, and then restore a configuration file to Local FortiGate.

To clear the browser history

1. On the Local-Client VM, open the browser, and then click the menu icon in the upper-right corner.



2. Click Settings > Privacy & Security.

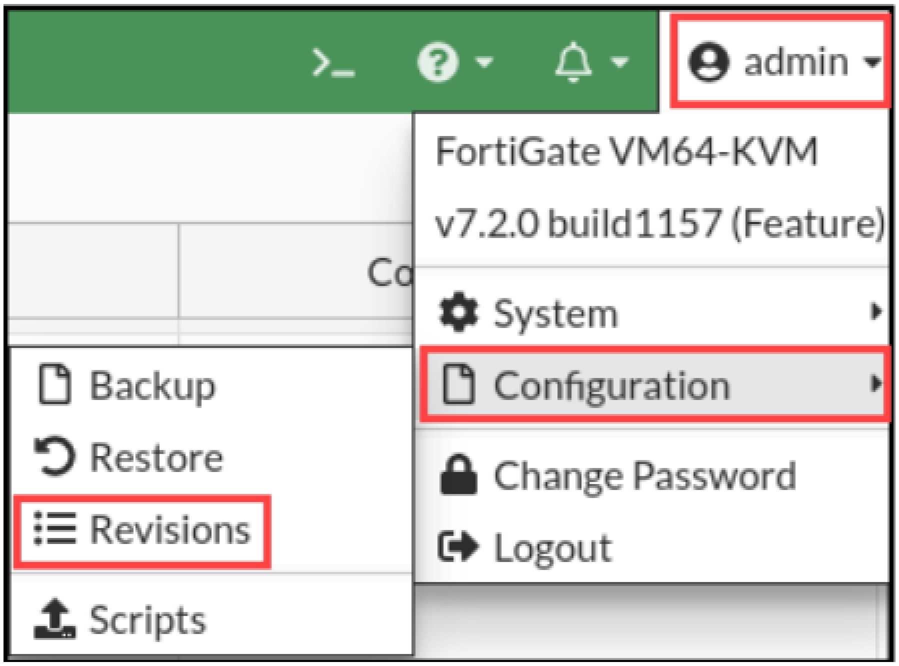
3. Scroll to History, click Clear History, and then ensure the time range to clear is set to Everything.

4. Click OK.

To restore the FortiGate configuration file

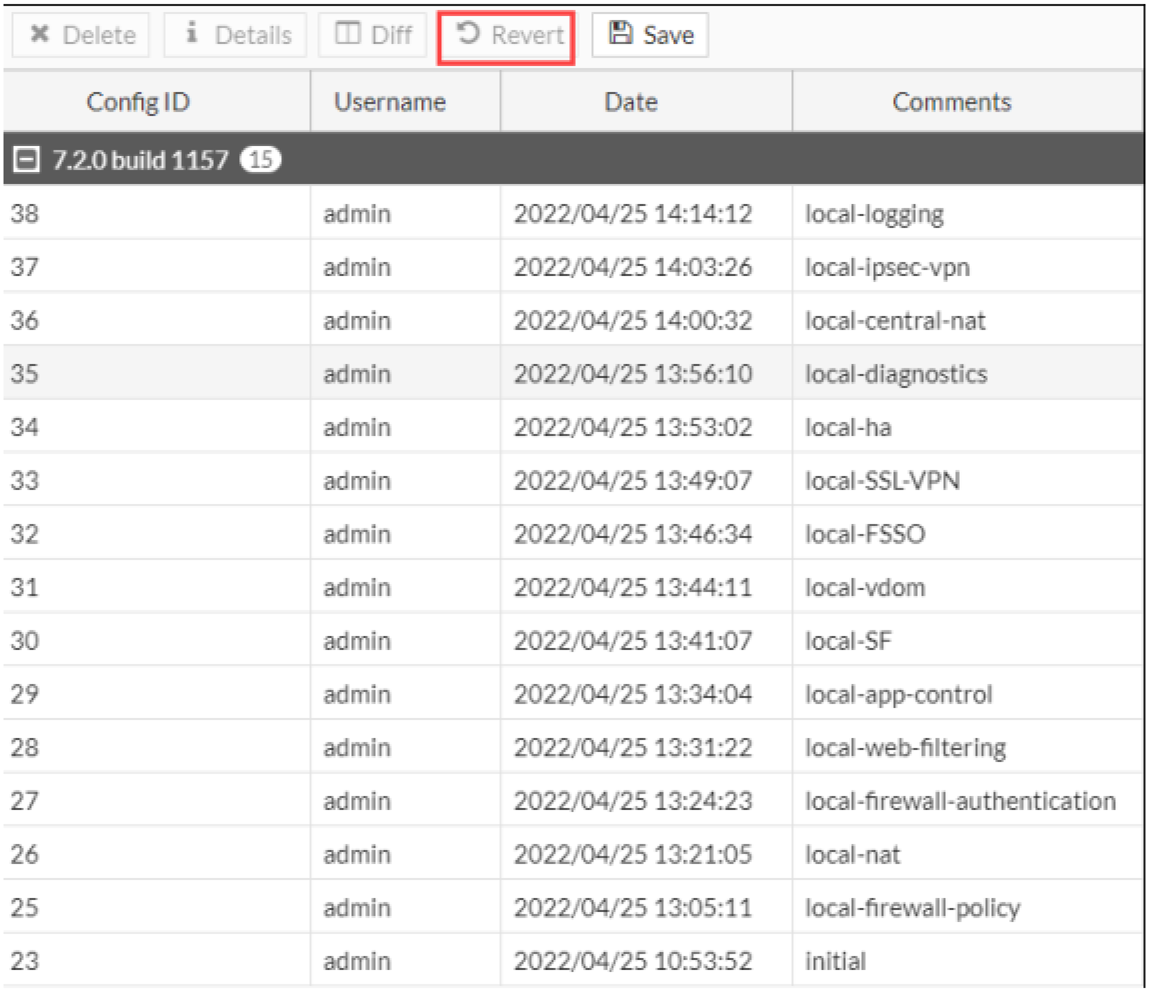
1. Connect to the Local-FortiGate GUI, and then log in with the username admin and password password .

2. In the upper-right corner of the screen, click admin, and then click Configuration > Revisions.



3. Click the + sign to expand the list.

4. Select the configuration with the comment local-web-filtering, and then click Revert.



Config ID	Username	Date	Comments
7.2.0 build 1157 15			
38	admin	2022/04/25 14:14:12	local-logging
37	admin	2022/04/25 14:03:26	local-ipsec-vpn
36	admin	2022/04/25 14:00:32	local-central-nat
35	admin	2022/04/25 13:56:10	local-diagnostics
34	admin	2022/04/25 13:53:02	local-ha
33	admin	2022/04/25 13:49:07	local-SSL-VPN
32	admin	2022/04/25 13:46:34	local-FSSO
31	admin	2022/04/25 13:44:11	local-vdom
30	admin	2022/04/25 13:41:07	local-SF
29	admin	2022/04/25 13:34:04	local-app-control
28	admin	2022/04/25 13:31:22	local-web-filtering
27	admin	2022/04/25 13:24:23	local-firewall-authentication
26	admin	2022/04/25 13:21:05	local-nat
25	admin	2022/04/25 13:05:11	local-firewall-policy
23	admin	2022/04/25 10:53:52	initial

5. Click OK to reboot.

Exercise 1: Configuring FortiGuard Web Filtering

To configure FortiGate for web filtering based on FortiGuard categories, you must make sure that FortiGate has a valid FortiGuard security subscription license. The license provides the web filtering capabilities necessary to protect against inappropriate websites

Then, you must configure a category-based web filter security profile on FortiGate, and apply the security profile on a firewall policy to inspect the HTTP traffic.

Finally, you can test different actions taken by FortiGate according to the website rating.

Review the FortiGate Settings

You will review the inspection mode and license status according to the uploaded settings. You will also list the FortiGuard Distribution Servers (FDS) that your FortiGate uses to send the web filtering requests.

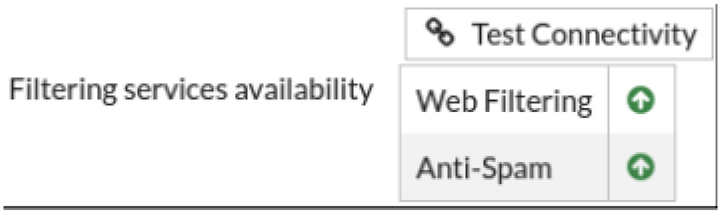
To review the restored settings on FortiGate

1. Connect to the Local-FortiGate GUI, and then log in with the username admin and password password.

2. On the Dashboard, locate the Licenses widget, and then confirm that the Web Filtering service is licensed and active.

A green check mark should appear beside Web Filtering.

Because of the reboot following the restoration of the configuration file, the web filter license status may be Unavailable. In this case, navigate to System > FortiGuard, in the Filtering section, click Test Connectivity to force an update, and then click OK to confirm.



Filtering services availability		
	Web Filtering	✓
	Anti-Spam	✓

3. Click Policy & Objects > Firewall Policy.

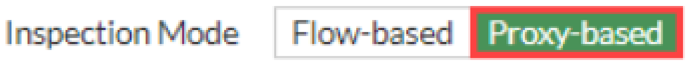
4. Double-click the Full_Access policy to edit it.

5. Verify the Inspection Mode setting.

Notice that the default inspection mode is set to Flow-based.

6. In the Inspection Mode field, select Proxy-based.

7. Click OK.



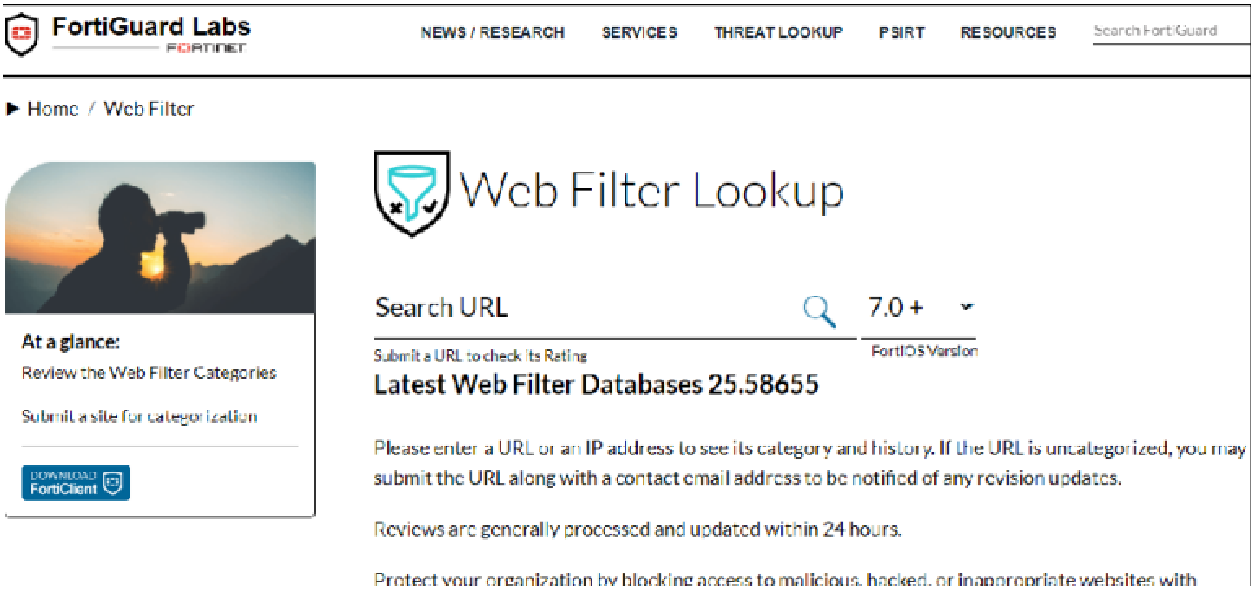
Inspection Mode Flow-based [✓ Proxy-based]

Determine Web Filter Categories To configure web filter categories

you must first identify how FortiGuard Web Filtering categorizes specific websites.

To determine web filter categories

1. On the Local-Client VM, open a new browser tab, and then go to https://www.fortiguard.com/webfilter.



FortiGuard Labs FORTINET

NEWS / RESEARCH SERVICES THREAT LOOKUP PSIRT RESOURCES Search FortiGuard

▶ Home / Web Filter

At a glance:

Review the Web Filter Categories

Submit a site for categorization

DOWNLOAD FortiClient

Web Filter Lookup

Search URL 7.0 +

Submit a URL to check its Rating FortiOS Version

Latest Web Filter Databases 25.58655

Please enter a URL or an IP address to see its category and history. If the URL is uncategorized, you may submit the URL along with a contact email address to be notified of any revision updates.

Reviews are generally processed and updated within 24 hours.

Protect your organization by blocking access to malicious, hacked, or inappropriate websites with

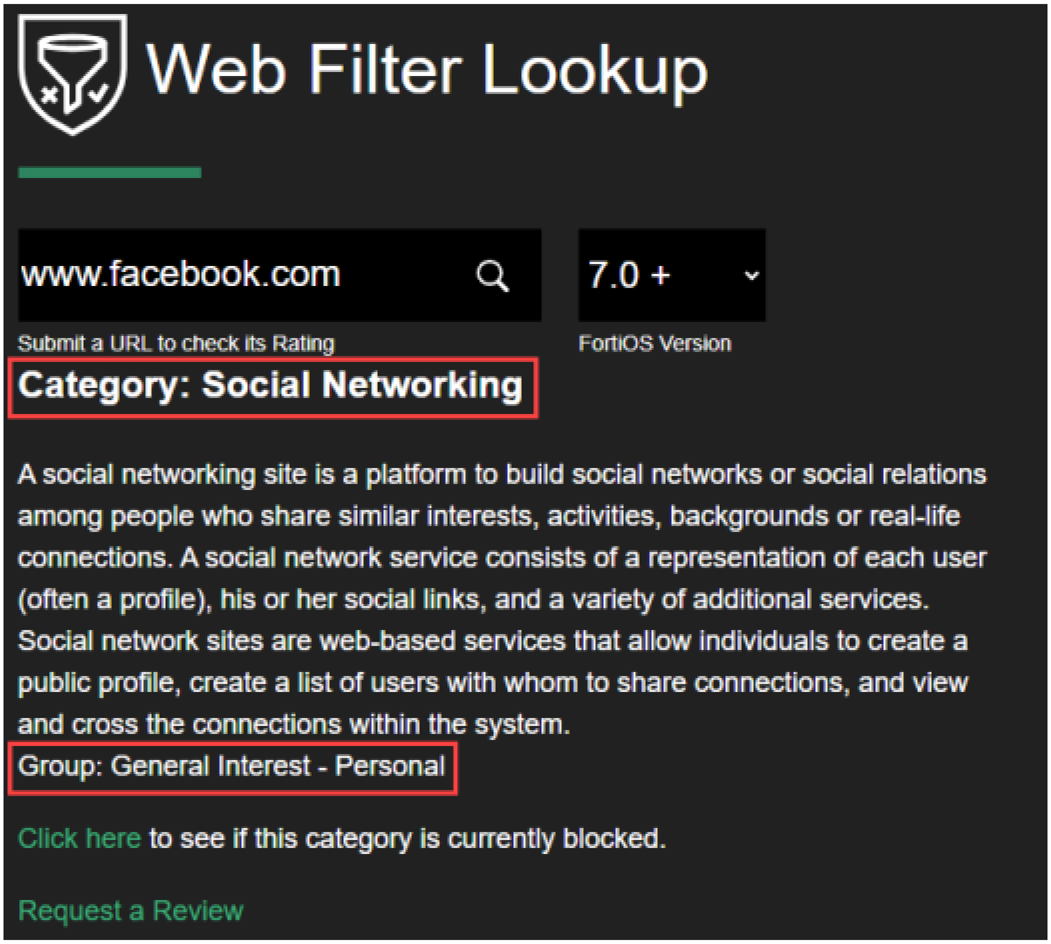
2. Use the Web Filter Lookup tool to search for the following URL: www.facebook.com

This is one of the websites you will use later to test your web filter.

3. Use the Web Filter Lookup tool again to find the web filter category for the following websites:
    - www.skype.com
    - www.ask.com
    - www.bing.com

You will test your web filter using these websites also.

The following table shows the category assigned to each URL, as well as the action you will configure FortiGate to take based on your web filter security profile:



Web Filter Lookup

www.facebook.com

Submit a URL to check its Rating

7.0 +

FortiOS Version

Category: Social Networking

A social networking site is a platform to build social networks or social relations among people who share similar interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), his or her social links, and a variety of additional services. Social network sites are web-based services that allow individuals to create a public profile, create a list of users with whom to share connections, and view and cross the connections within the system.

Group: General Interest - Personal

Click here to see if this category is currently blocked.

Request a Review

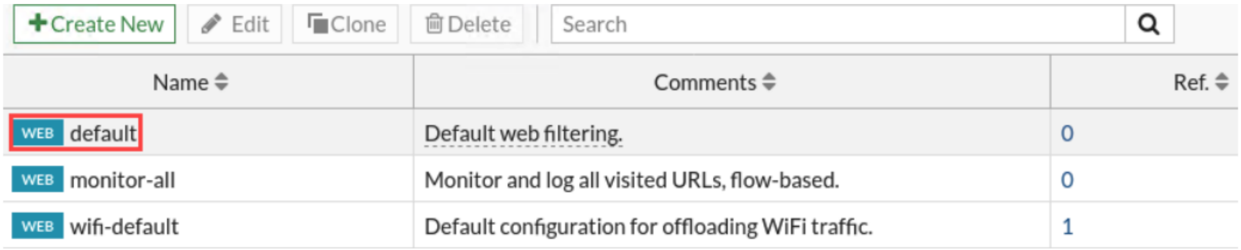
Website	Category	Action
www.skype.com	Internet Telephony	Warning
www.bing.com	Search Engines and Portals	Allow
www.ask.com	Search Engines and Portals	Allow

Configure a FortiGuard Category-Based Web Filter

You will review the default web filtering profile, and then configure the FortiGuard category-based filter.

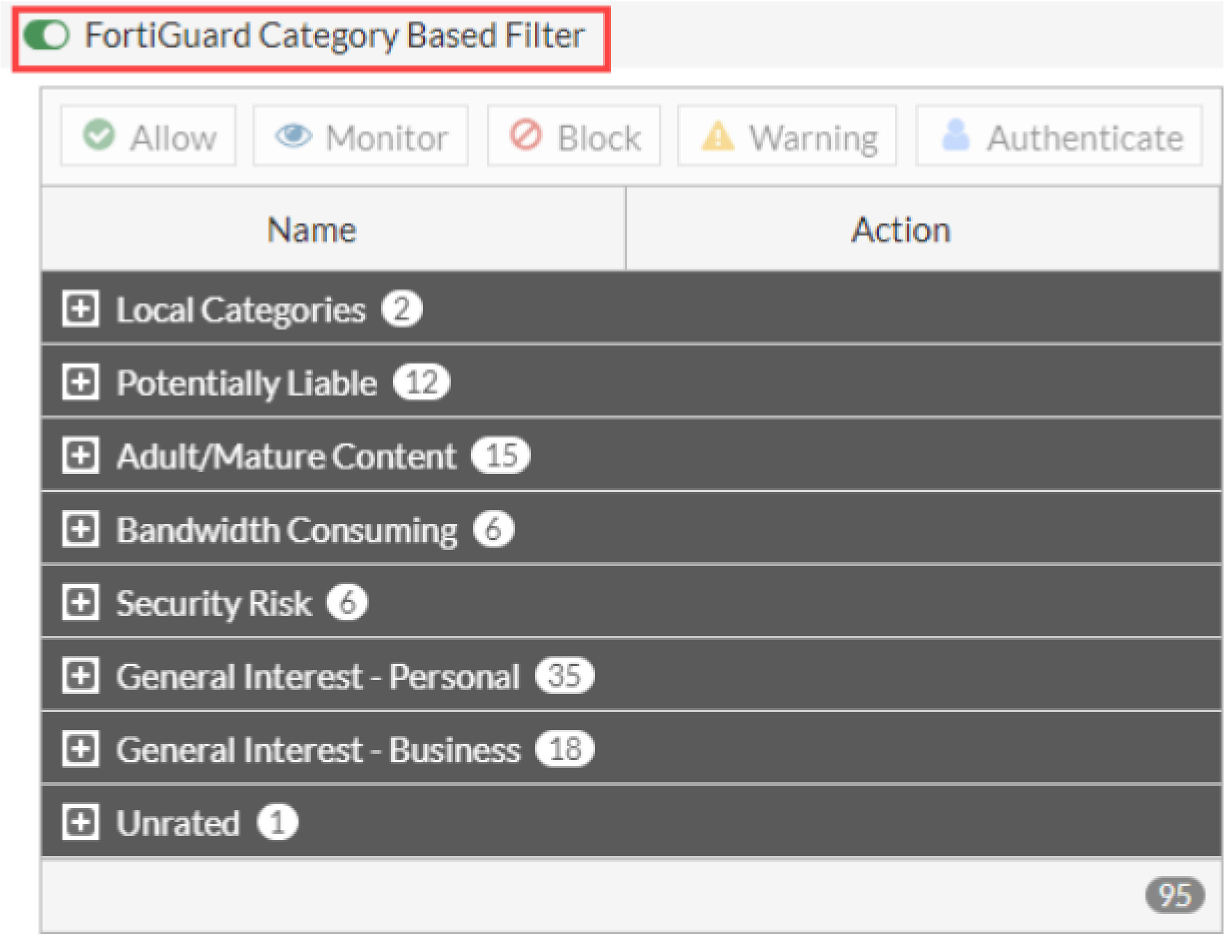
To configure the web filter security profile

1. Return to the Local-FortiGate GUI, and then click Security Profiles > Web Filter.
2. Double-click the default web filter profile to edit it.



Name	Comments	Ref.
WEB default	Default web filtering.	0
WEB monitor-all	Monitor and log all visited URLs, flow-based.	0
WEB wifi-default	Default configuration for offloading WiFi traffic.	1

3. Verify that FortiGuard Category Based Filter is enabled.



● FortiGuard Category Based Filter

Name	Action
⊞ Local Categories 2	
⊞ Potentially Liable 12	
⊞ Adult/Mature Content 15	
⊞ Bandwidth Consuming 6	
⊞ Security Risk 6	
⊞ General Interest - Personal 35	
⊞ General Interest - Business 18	
⊞ Unrated 1	

95

4. Review the default actions for each category.

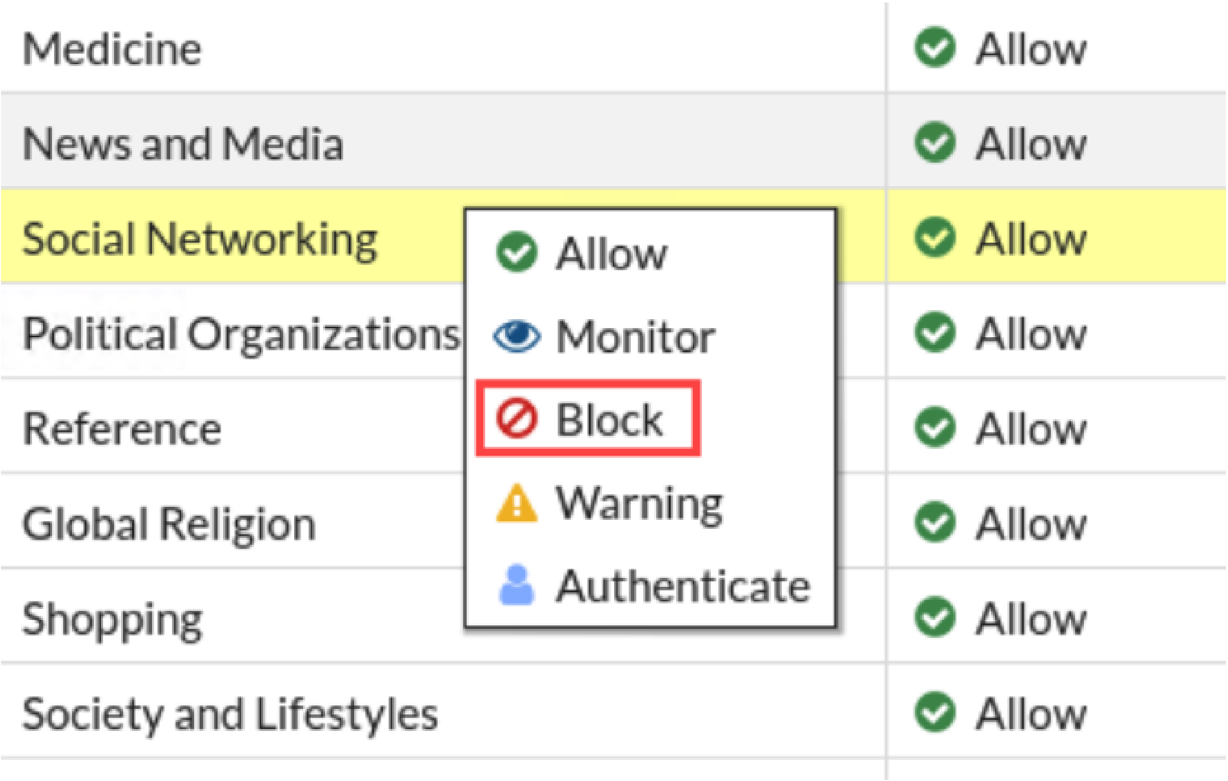
Category	Action
Local Categories	Disable
Potentially Liable	Block: Extremist Group Allow: all other subcategories

Tip: Expand Potentially Liable to view the subcategories

Adult/Mature Content	Block
Bandwidth Consuming	Allow
Security Risk	Block
General Interest - Personal	Allow
General Interest – Business	Allow
Unrated	Block

5. Expand General Interest - Personal to view the subcategories.

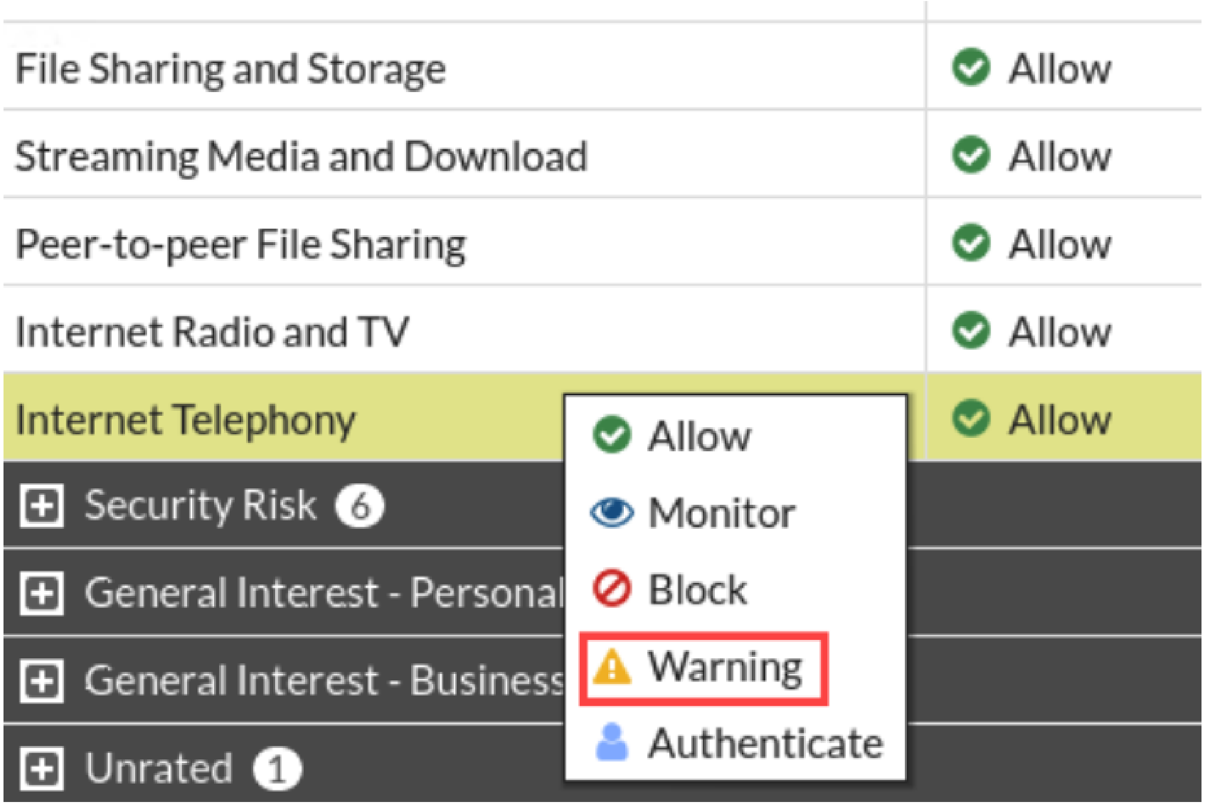
6. Right-click Social Networking, and then select Block.



Medicine	✓ Allow
News and Media	✓ Allow
Social Networking	✓ Allow
Political Organizations	✓ Allow
Reference	✓ Allow
Global Religion	✓ Allow
Shopping	✓ Allow
Society and Lifestyles	✓ Allow

7. Expand Bandwidth Consuming to view the subcategories.

8. Right-click Internet Telephony, and then select Warning.



File Sharing and Storage	✓ Allow
Streaming Media and Download	✓ Allow
Peer-to-peer File Sharing	✓ Allow
Internet Radio and TV	✓ Allow
Internet Telephony	✓ Allow
⊞ Security Risk 6	
⊞ General Interest - Personal	
⊞ General Interest - Business	
⊞ Unrated 1	

The Edit Filter window opens, which allows you to modify the warning interval.

9. Keep the default setting of 5 minutes, and then click OK.

10. Click OK.

Apply the Web Filter Profile to a Firewall Policy

Now that you have configured the web filter profile, you must apply this security profile to a firewall policy in order to start inspecting web traffic.

You will also enable the logs to store and analyze the security events that the web traffic generates.

Take the Expert Challenge!

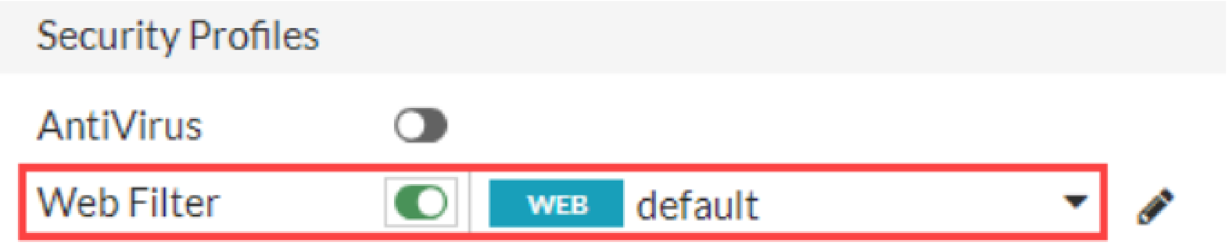
On the Local-FortiGate GUI, apply the web filter profile to the existing Full_Access firewall policy. Make sure that logging is also enabled and set to Security Events.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Test the Web Filter on page 1.

To apply a security profile in a firewall policy

1. 1Continuing on the Local-FortiGate GUI, click Policy & Objects > Firewall Policy.
2. Double-click the Full_Access policy to edit it.
3. In the Security Profiles section, enable Web Filter, and then select default.



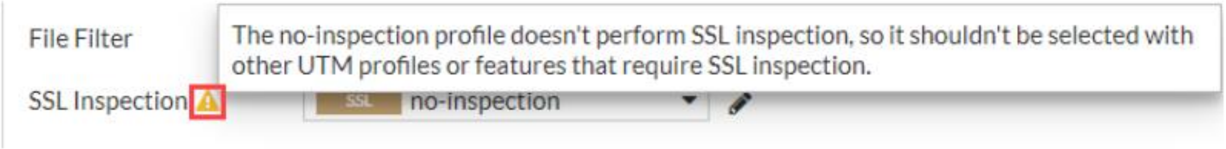
Security Profiles

AntiVirus ○

Web Filter ● WEB default

4. Hover over the warning sign that appears beside the SSL Inspection field.

The message should be similar to the following example:



File Filter

The no-inspection profile doesn't perform SSL inspection, so it shouldn't be selected with other UTM profiles or features that require SSL inspection.

SSL Inspection ⚠ SSL no-inspection

5. In the SSL Inspection field, select certification-inspection.

Because web filtering requires URL information and does not inspect the full payload, you can select **certification-inspection** instead of **deep-inspection**.

6. Under Log Allowed Traffic, make sure that Security Events is selected.

7. Keep all other default settings, and then click OK.

Test the Web Filter

You will test the web filter security profile you configured for each category.

To test the web filter

1. On the Local-FortiGate CLI, log in with the username admin and password password.

2. Enter the following command to verify the web filter status:

get webfilter status The get webfilter status and diagnose debug rating commands show the list of FDS that FortiGate uses to send web filtering requests. In normal operations, FortiGate sends the rating requests only to the server at the top of the list. Each server is probed for round-trip time (RTT) every 2 minutes.

Stop and think!

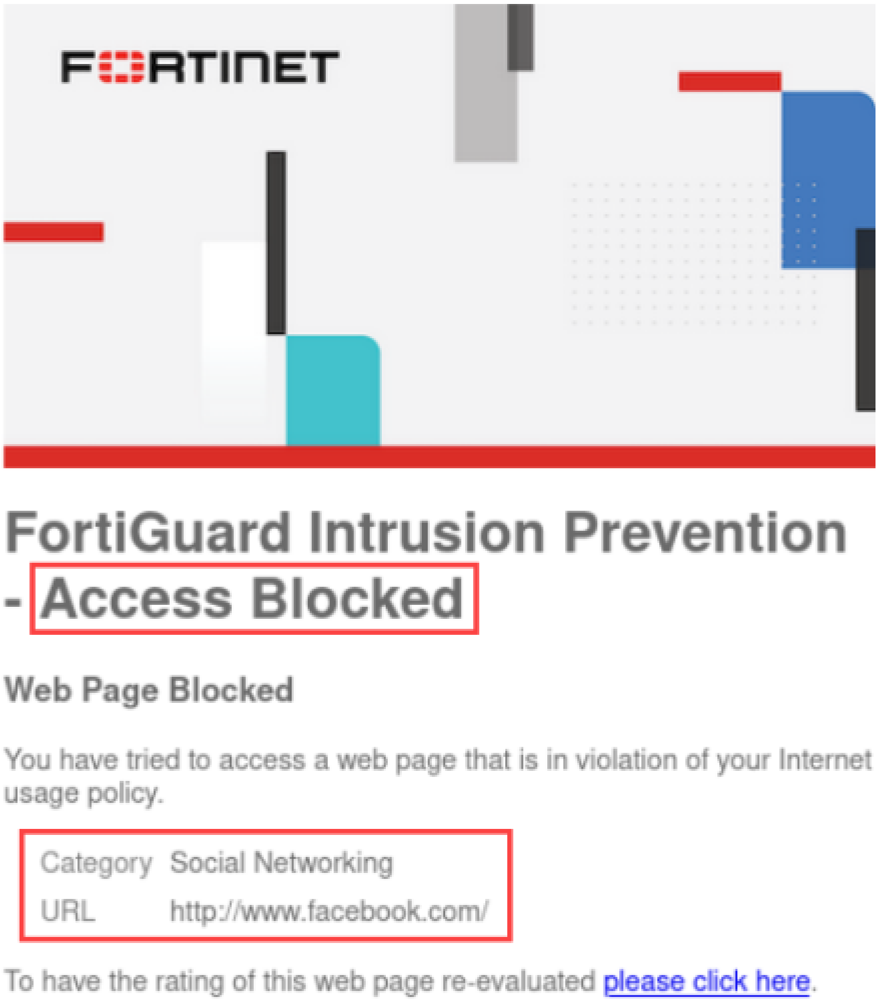
Why does only one IP address from your network appear in the server list?

Your lab environment uses a FortiManager at 10.0.1.241, which is configured as a local FDS. It contains a local copy of the FDS web rating database.

FortiGate sends the rating requests to FortiManager instead of to the public FDS. For this reason, the output of the command lists the FortiManager IP address only.

3-On the Local-Client VM, open a new browser tab, and then go to www.facebook.com.

A warning appears, according to the predefined action for this website category.



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

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

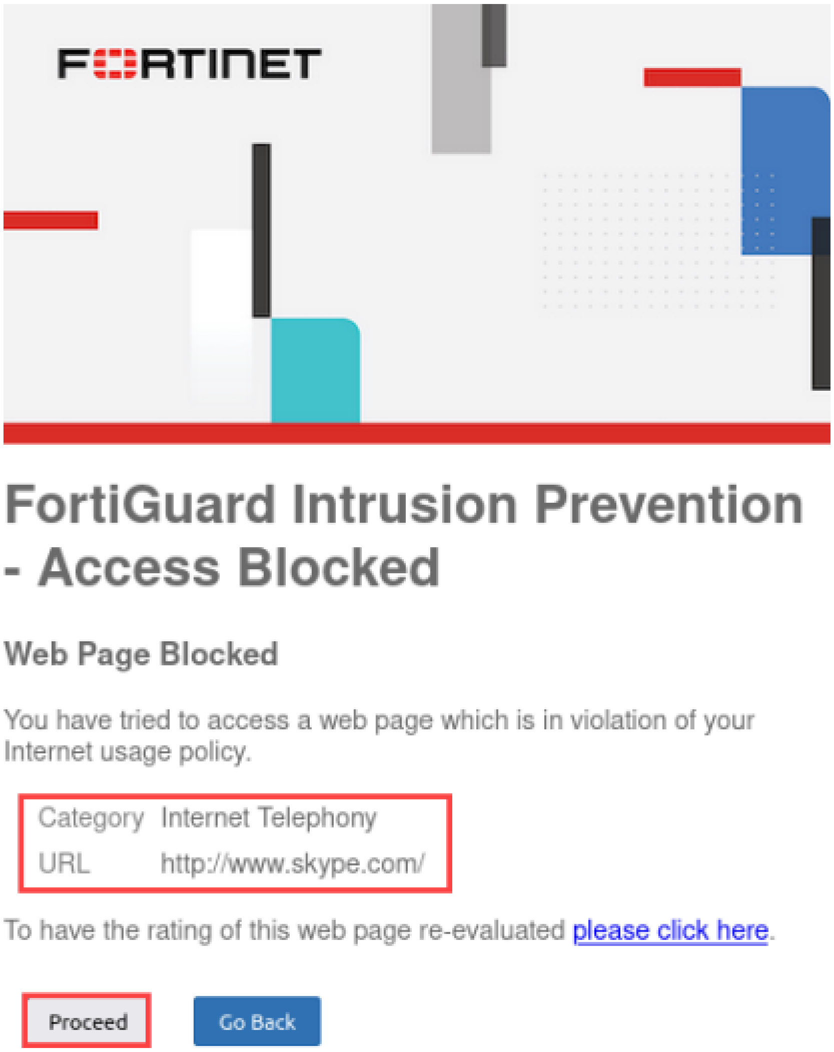
Category Social Networking

URL http://www.facebook.com/

To have the rating of this web page re-evaluated please click here.

4-Open a new browser tab, and then go to www.skype.com .

A warning appears, according to the predefined action for this website category.



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

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

Category Internet Telephony
URL http://www.skype.com/

To have the rating of this web page re-evaluated please click here.

5. Click Proceed to accept the warning and access the website.

6. Open a new browser tab, and then go to www.bing.com.

This website appears because it belongs to the Search Engines and Portals category, which is set to Allow.

6. Close the Local-Client VM browser tabs.

Create a Web Rating Override

You will override the category for www.bing.com .

To create a web rating override

1. Return to the Local-FortiGate GUI, and then click Security Profiles > Web Rating Overrides.

2. Click Create New, and then configure the following settings:

Field	Value
URL	www.bing.com
Category	Security Risk

Field	Value
Sub-Category	Malicious Websites

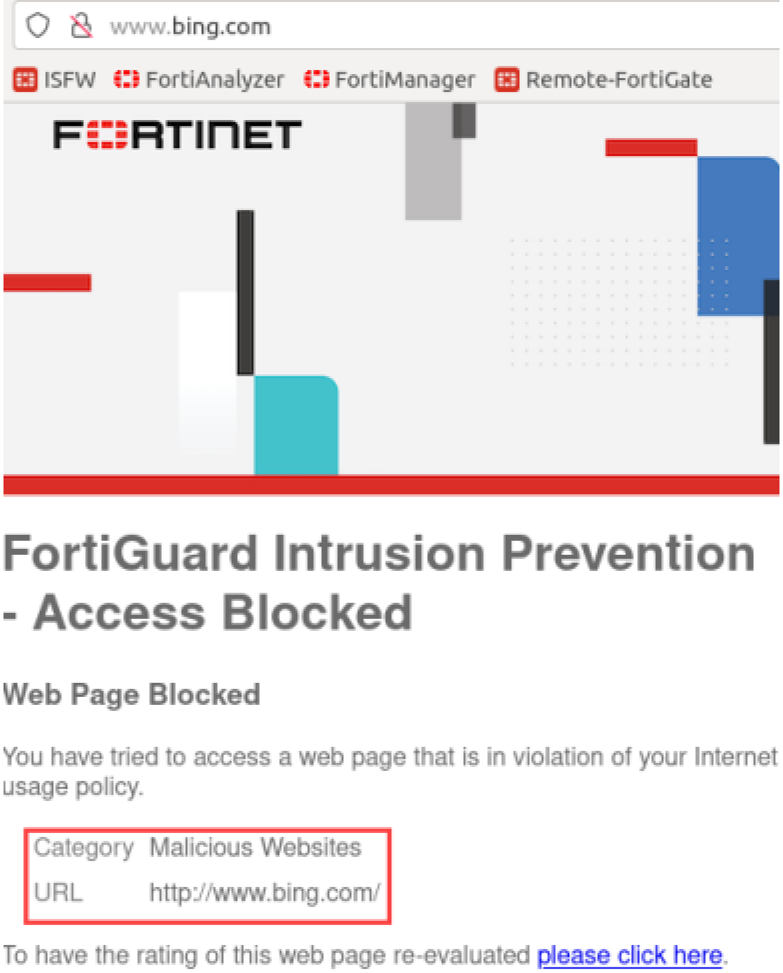
2. Click OK.

Test the Web Rating Override

You will test the web rating override you created in the previous procedure.

To test the web rating override

1. On the Local-Client VM, open a new browser tab, and then try to access the www.bing.com website again.
   The website is blocked, and it matches a local rating instead of a FortiGuard rating.



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

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

Category	Malicious Websites
URL	http://www.bing.com/

To have the rating of this web page re-evaluated please click here.

Stop and think!

Why is the website www.bing.com blocked?

The web rating override changes the category. In the default web profile applied in the firewall policy, the Malicious Websites category is set to Block. As a consequence, the website www.bing.com is now blocked

Configure an Authenticate Action

You will set the action for the Malicious Websites FortiGuard category to Authenticate.
You will then define a user in order to test the authenticate action.

To set up the authenticate action

1. Continuing on the Local-FortiGate GUI, click Security Profiles > Web Filter.
2. Double-click the default web filter profile to edit it.
3. Under FortiGuard Category Based Filter, expand Security Risk, right-click Malicious Websites, and then select Authenticate.

The Edit Filter window opens, which allows you to modify the warning interval and select the user groups.

4. Configure the following settings:

Field	Value
Warning Interval	5 minutes
Selected User Groups	Override_Permissions

5. Click OK.
6. Click OK.

To create a user

1. Continuing on the Local-FortiGate GUI, click User & Authentication > User Definition.
2. Click Create New.
3. In the User Type field, select Local User.
4. Click Next, and then configure the following settings:

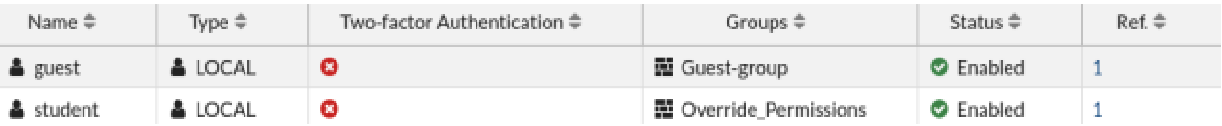
Field	Value
Username	student
Password	Fortinet

5. Click Next. 6. Click Next.

7. Enable User Group, and then select Override_Permissions

8. Click Submit.

The student user is created.

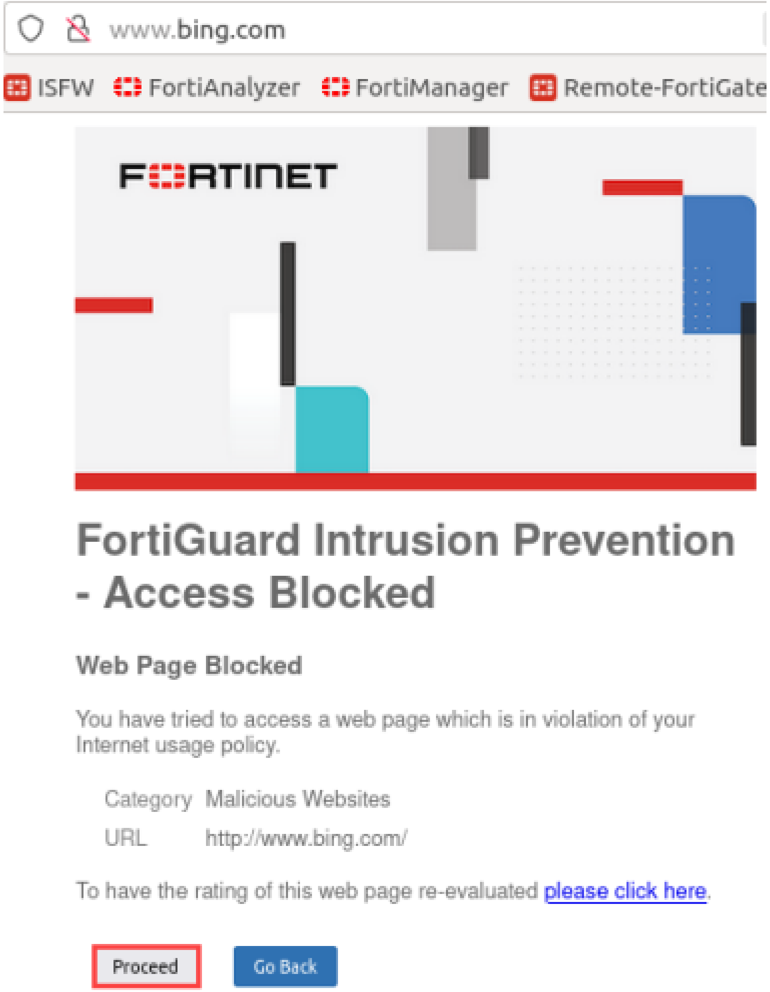


Name	Type	Two-factor Authentication	Groups	Status	Ref.
guest	LOCAL	⊗	Guest-group	✓ Enabled	1
student	LOCAL	⊗	Override_Permissions	✓ Enabled	1

To test the web rating override

1. On the Local-Client VM, open a new browser tab, and then try to access www.bing.com .

A warning appears. Notice that it is a different message from the one that appeared before.



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

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

Category	Malicious Websites
URL	http://www.bing.com/

To have the rating of this web page re-evaluated please click here.

2. Click Proceed

3. Enter the following credentials:

Field	Value
Username	student
Password	fortinet

4. Click Continue. The www.bing.com website now displays correctly.

 5. Close the Local-Client VM browser tabs. LAB-8 > Configuring FortiGuard Web Filtering

Exercise 2: Configuring Static URL Filtering

In this exercise, you will configure a static URL filter and apply the security profile to a firewall policy in flow-based inspection mode. You will then review the web filter logs.

Set Up the Static URL Filter in Flow-Based Inspection Mode

 You will create a static URL filter entry and change the inspection mode to flow-based.

To create a static URL filter

1. Connect to the Local-FortiGate GUI, and then log in with the username admin and password password.

2. Click Security Profiles > Web Filter.

3. Double-click the default web filter profile to edit it.

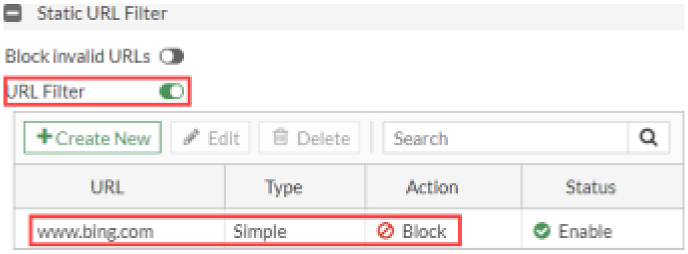
4. In the Static URL Filter section, enable URL Filter.

5. Click Create New, and then configure the following settings:

Field	Value
URL	www.bing.com
Type	Simple
Action	Block
Status	Enable

6.Click OK.

Your configuration should match the following example:



Static URL Filter

Block invalid URLs ○

URL Filter ●

URL	Type	Action	Status
www.bing.com	Simple	⊘ Block	✓ Enable

7. Click OK.

To change the inspection mode to flow-based

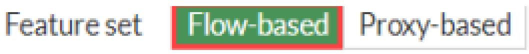
1. Continuing on the Local-FortiGate GUI, click Security Profiles > Web Filter.

2. Double-click the default web filter profile to edit it

3. In the Feature set field, select Flow-based.

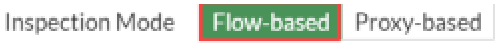
4. Click OK.

5. Click Policy & Objects > Firewall Policy.


Feature set [✓ Flow-based] Proxy-based

6. Double-click the Full_Access policy to edit it.

7. In the Inspection Mode field, select Flow-based.

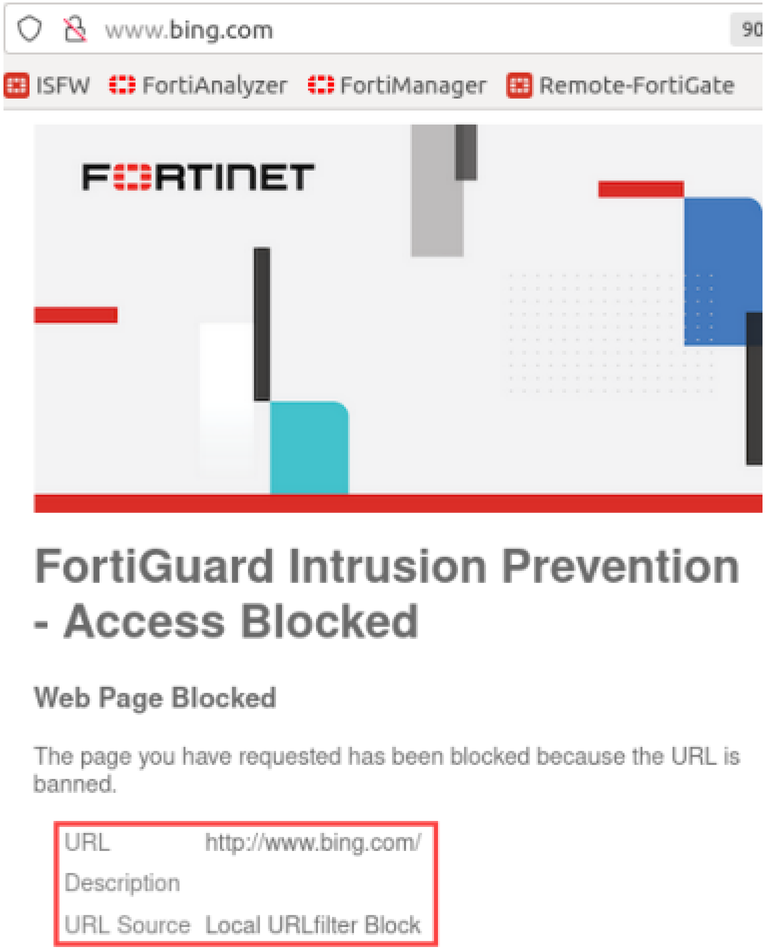

Inspection Mode [✓ Flow-based] Proxy-based

8. Click OK.

To test the static URL filter

1. On the Local-Client VM, open a new browser tab, and then try to access www.bing.com.

A warning appears. Notice that it is a different message from the one that appeared before



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

The page you have requested has been blocked because the URL is banned.

URL	http://www.bing.com/
Description	
URL Source	Local URLfilter Block

Stop and think!

Why is the replacement message different?

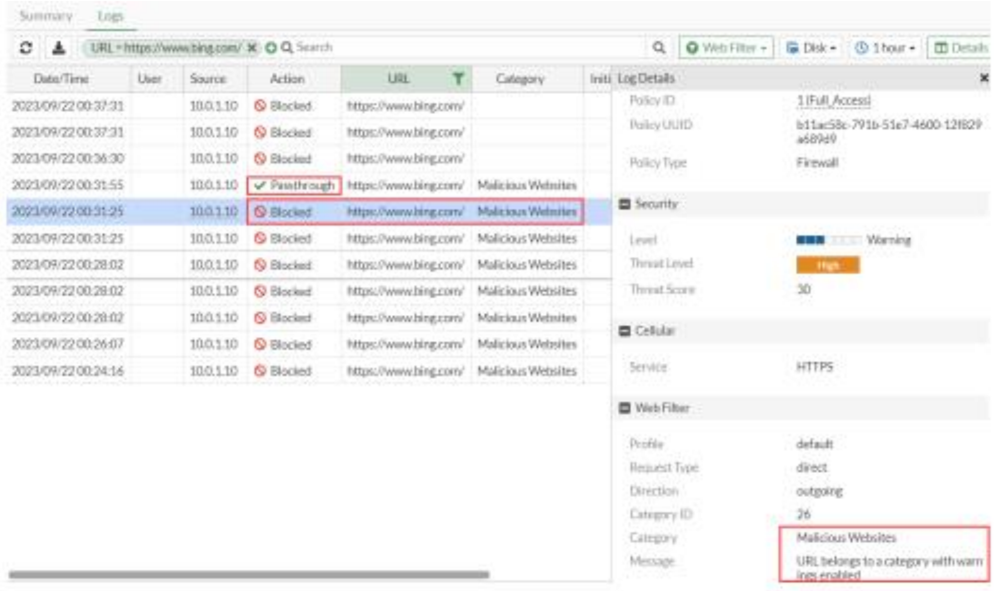
FortiGate applies the static URL filter before the FortiGuard category filter. The www.bing.com URL matches the URL filter pattern and therefore is now blocked, and FortiGate displays the corresponding URL filter message.

To review the web filter logs

1. Return to your browser tab where you are logged in to the Local-FortiGate GUI, and then click Log & Report > Security Events.

2. Under Summary, click Web Filter.

You should see information similar to the following example:



Date/Time	User	Source	Action	URL	Category	Initi
2023/09/22 00:37:31		10.0.1.10	Blocked	https://www.bing.com/		
2023/09/22 00:37:31		10.0.1.10	Blocked	https://www.bing.com/		
2023/09/22 00:36:30		10.0.1.10	Blocked	https://www.bing.com/		
2023/09/22 00:31:55		10.0.1.10	✓ Passthrough	https://www.bing.com/	Malicious Websites	
2023/09/22 00:31:25		10.0.1.10	Blocked	https://www.bing.com/	Malicious Websites	
2023/09/22 00:31:25		10.0.1.10	Blocked	https://www.bing.com/	Malicious Websites	
2023/09/22 00:28:02		10.0.1.10	Blocked	https://www.bing.com/	Malicious Websites	
2023/09/22 00:28:02		10.0.1.10	Blocked	https://www.bing.com/	Malicious Websites	
2023/09/22 00:28:02		10.0.1.10	Blocked	https://www.bing.com/	Malicious Websites	
2023/09/22 00:26:07		10.0.1.10	Blocked	https://www.bing.com/	Malicious Websites	
2023/09/22 00:24:16		10.0.1.10	Blocked	https://www.bing.com/	Malicious Websites	

Log Details

Policy ID	1 (Full_Access)
Policy UUID	b11ac58c-791b-51e7-4600-12f829a689d9
Policy Type	Firewall
Security	
Level	Warning
Threat Level	High
Threat Score	30
Cellular	
Service	HTTPS
Web Filter	
Profile	default
Request Type	direct
Direction	outgoing
Category ID	26
Category	Malicious Websites
Message	URL belongs to a category with warnings enabled

Stop and think!

Why is the first log entry for the www.bing.com website defined as blocked?

Initially, the www.bing.com website has the category Search Engines and Portals, which was set to Allow and does not generate a security log.

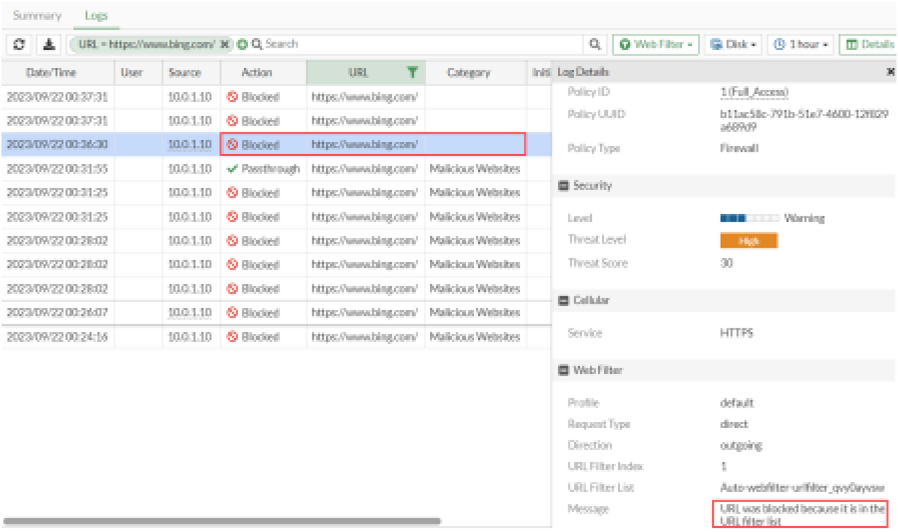
To allow a website and generate a security log at the same time, you must set the category to Monitor.

Then, according to the logs, http://www.bing .com is blocked, but after you clicked Proceed and authenticated, the logs show a different action: passthrough.

Remember that you overrode the Search Engines and Portals category to Malicious Websites, which was set to Block, and then to Authenticate

2. Double-click a log entry with an empty category.

You should see information similar to the following example:



Date/Time	User	Source	Action	URL	Category	Initi
2023/09/22 00:37:31		10.0.1.10	Blocked	https://www.bing.com/		
2023/09/22 00:37:31		10.0.1.10	Blocked	https://www.bing.com/		
2023/09/22 00:36:30		10.0.1.10	Blocked	https://www.bing.com/		
2023/09/22 00:31:55		10.0.1.10	✓ Passthrough	https://www.bing.com/	Malicious Websites	
2023/09/22 00:31:25		10.0.1.10	Blocked	https://www.bing.com/	Malicious Websites	
2023/09/22 00:31:25		10.0.1.10	Blocked	https://www.bing.com/	Malicious Websites	
2023/09/22 00:28:02		10.0.1.10	Blocked	https://www.bing.com/	Malicious Websites	
2023/09/22 00:28:02		10.0.1.10	Blocked	https://www.bing.com/	Malicious Websites	
2023/09/22 00:28:02		10.0.1.10	Blocked	https://www.bing.com/	Malicious Websites	
2023/09/22 00:26:07		10.0.1.10	Blocked	https://www.bing.com/	Malicious Websites	
2023/09/22 00:24:16		10.0.1.10	Blocked	https://www.bing.com/	Malicious Websites	

Log Details

Policy ID	1 (Full_Access)
Policy UUID	b11ac58c-791b-51e7-4600-12f029 a689d9
Policy Type	Firewall
Security	
Level	Warning
Threat Level	High
Threat Score	30
Cellular	
Service	HTTPS
Web Filter	
Profile	default
Request Type	direct
Direction	outgoing
URL Filter Index	1
URL Filter List	Auto-webfilter-urlfilter_qvy0ayvsw
Message	URL was blocked because it is in the URL filter list

Stop and think!

Why is the category field empty?

Because the website is blocked by the static URL filter, FortiGuard does not apply the FortiGuard web rating, and does not provide the category