**Objective of the Lab**

The objective of this lab is to configure web filtering on a Fortigate firewall to block access to specific websites and content categories, ensuring a secure browsing environment for users.

**Topology**

1. **Fortigate Firewall**: The main device for implementing web filtering.
2. **Internal Network**: A switch connected to the Fortigate’s internal interface.
3. **External Network**: A router connected to the Fortigate’s external interface.
4. **Internet**: Simulated internet connection for testing web access.
5. **PCs or VMs**: For simulating internal network users.

**Components Used**

* **Fortigate Firewall**: Virtual or physical device.
* **Switch**: For internal network connections.
* **Router**: For external network connections.
* **PCs or VMs**: For simulating internal network users.
* **EVE-NG or GNS3**: Network simulation tools for creating the lab environment.

**Configuring FortiGuard Web Filtering**

To set up FortiGate for web filtering using FortiGuard categories, ensure that FortiGate has an active FortiGuard security subscription license. This license is essential for enabling the web filtering features to block access to inappropriate websites.

Next, create a category-based web filter security profile on FortiGate and apply this profile to a firewall policy to inspect HTTP traffic.

Finally, test the FortiGate's responses based on the website ratings to ensure the configurations are working as intended.

**Steps of Configuration:**

**Review the FortiGate Settings:**

1. Connect to the Local-FortiGate GUI, and then log in with the username and password.
2. On the Dashboard, locate the Licenses widget, and then hover over Web Filter to confirm that the service is licensed and active.
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.

1. In the Inspection Mode field, select Proxy-based.
2. Click OK

**Determine Web Filter Categories**

Identify Web Filter Categories Before configuring web filter categories, you need to determine how FortiGuard Web Filtering classifies 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](http://www.fortiguard.com/webfilter).
2. Use the **Web Filter Lookup** tool to search for the following URL for example :

[www.twitter.com](http://www.twitter.com)

As you can see, Twitter is listed in the **Social Networking** category.

1. 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:

| **Website** | **Category** | **Action** |
| --- | --- | --- |
| www.facebook.com | Social Networking | Block |
| 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.
3. Verify that **FortiGuard Category Based Filter** is enabled.
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 |

1. Expand **General Interest - Personal** to view the subcategories.
2. Right-click **Social Networking**, and then select **Block**.
3. Expand **Bandwidth Consuming** to view the subcategories.
4. Right-click **Internet Telephony**, and then select **Warning**.

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

1. Keep the default setting of 5 minutes, and then click **OK**.
2. Click **OK**.
   * **Apply the Web Filter Profile to a Firewall Policy**

With the web filter profile configured, the next step is to apply this security profile to a firewall policy to begin inspecting web traffic.

Additionally, enable logging to record and analyze the security events generated by the web traffic.

**To apply a security profile in a firewall policy**

1. Continuing 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**.
4. Hover over the warning sign that appears beside the **SSL Inspection** field.
5. In the **SSL Inspection** field, select **certification-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 Lab**

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  and 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.

1. On the Local-Client VM, open a new browser tab, and then go to [www.twitter.com](http://www.twitter.com).

Results:

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

ACCESS BLOCKED

Category: Social Networking

URL: http://[www.twitter.com](http://www.twitter.com)/

1. Open a new browser tab, and then go to [www.skype.com](http://www.skype.com).

Result:

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

ACCESS BLOCKED

Category: Internet Telephony

URL: [h](http://www.twitter.com)ttp://www.skype.com/

1. Click **Proceed** to accept the warning and access the website.
2. 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**.

1. Close the Local-Client VM browser tabs.

Configuration Done on the Devices

* Fortigate Configuration: Interface settings, web filter profile, firewall policy, logging, and monitoring configurations.