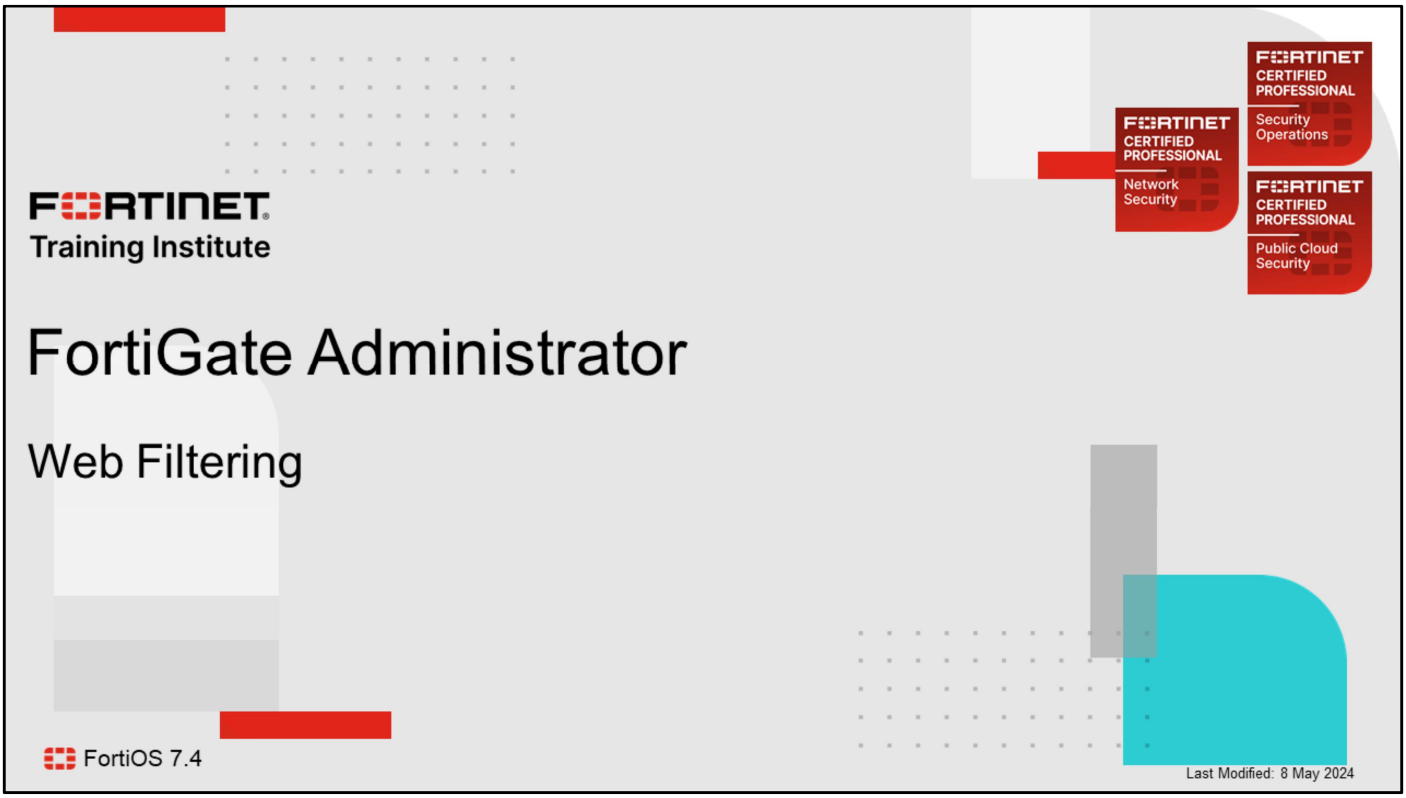


In this lesson, you will learn how to configure web filtering on FortiGate to control web traffic in your network.

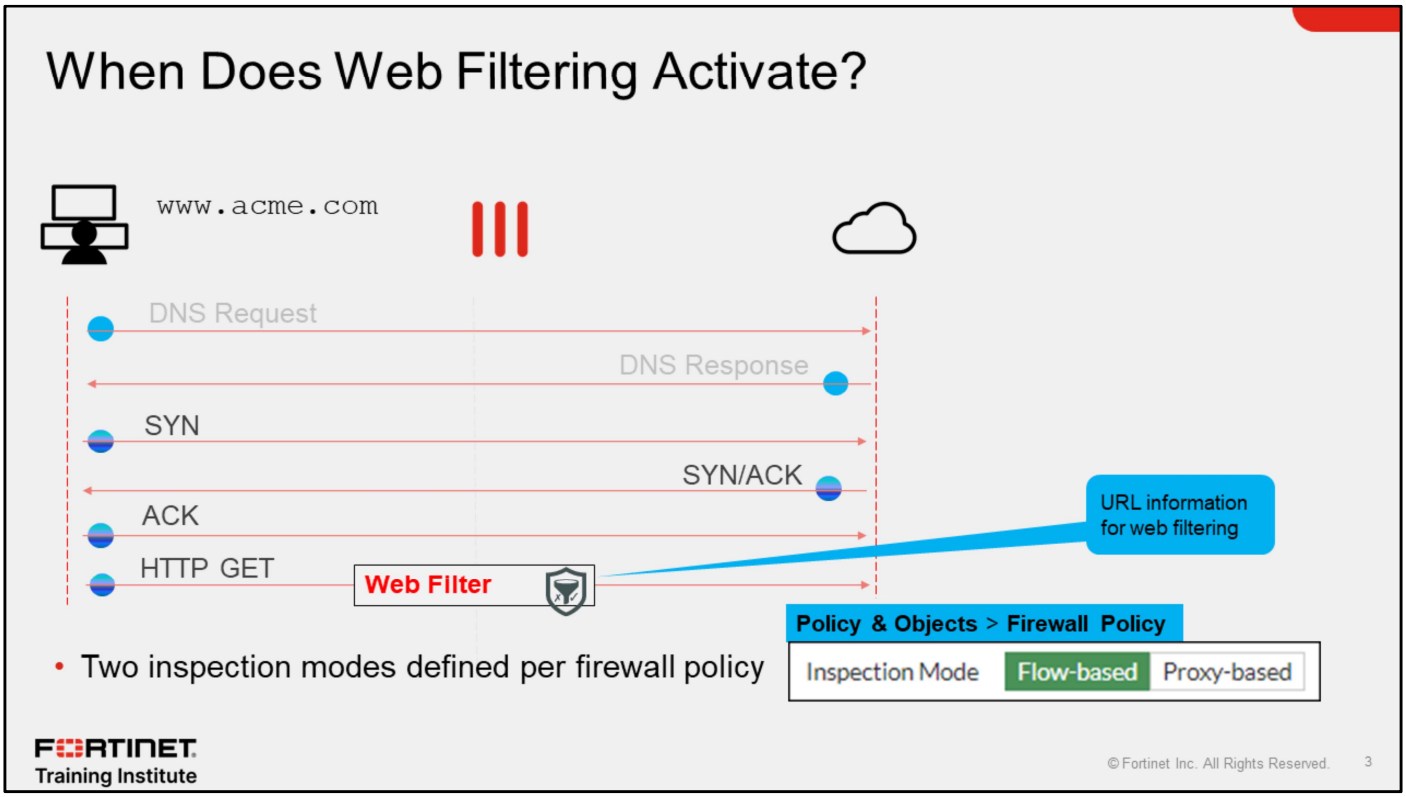
Objectives

- Select the correct inspection mode (flow or proxy) based on security needs
- Configure certificate inspection for web filtering
- Configure a web filter profile in flow-based inspection mode
- Configure a web filter profile in proxy-based inspection mode
- Configure FortiGuard categories
- Configure a URL filter
- Troubleshoot web filtering issues

FORTINET Training Institute

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in web filtering configuration, you will be able to implement the web filter profile in an effective manner.

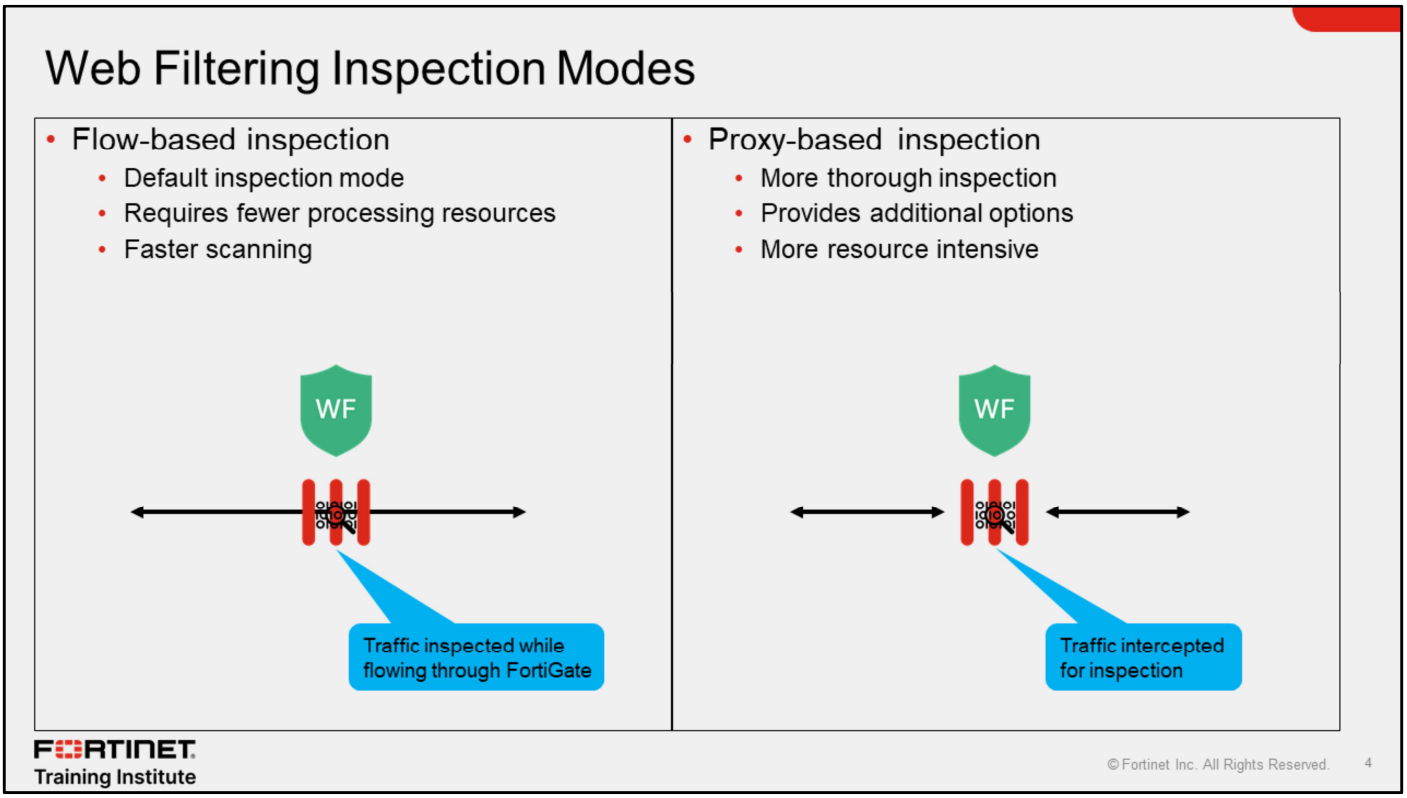


As shown in this HTTP filter process flow example, FortiGate looks for the `HTTP GET` request to collect URL information and perform web filtering.

In HTTP, the domain name and URL are separate parts. The domain name might look like the following in the header: `Host: www.acme.com`, and the URL might look like the following in the header: `/index.php?login=true`.

If you filter by domain, sometimes it blocks too much. For example, the blogs on `tumblr.com` are considered different content, because of all the different authors. In that case, you can be more specific, and block by the URL part, `tumblr.com/hacking`, for example.

In the default profile-based mode, FortiGate provides two inspection modes (flow-based and proxy-based) to perform web filtering.



You can configure web filtering in flow-based or proxy-based inspection mode.

Flow-based inspection mode examines the file as it passes through FortiGate. Packets are analyzed and forwarded as they are received. Original traffic is not altered. Therefore, advanced features that modify content, such as safe search enforcement, are not supported.

The advantages of flow-based inspection mode are:
- The user sees a faster response time for HTTP requests compared to proxy-based inspection mode.
- There is less chance of a time-out error caused by the server at the other end responding slowly.

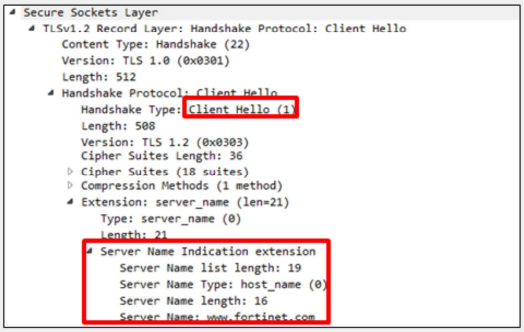
The disadvantages of flow-based inspection mode are:
- A number of security features that are available in proxy-based inspection mode are not available in flow-based inspection mode.
- Fewer actions are available based on the categorization of the website by FortiGuard services.

On the other hand, proxy-based scanning refers to transparent proxy. It's called transparent because, at the IP layer, FortiGate is not the destination address, but FortiGate *does* intercept the traffic. When proxy-based inspection is enabled, FortiGate buffers traffic and examines it *as a whole*, before determining an action. Because FortiGate examines the data as a whole, it can examine more points of data than it does when using flow-based inspection.

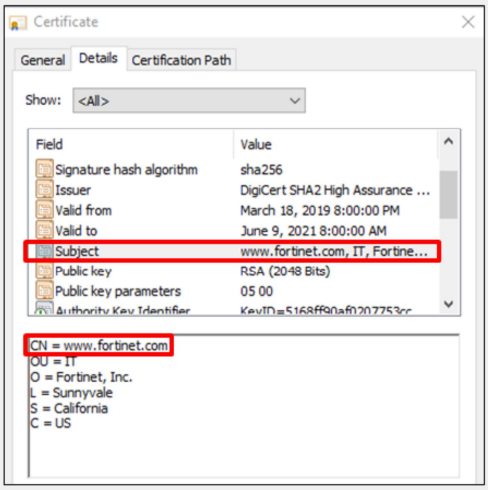
The proxy analyzes the headers and may change the headers, such as HTTP host and URL, for web filtering. If a security profile decides to block the connection, the proxy can send a replacement message to the client. This adds latency to the overall transmission speed.

SSL Certificate Inspection

- Uses the SNI extension from the Client Hello of the SSL handshake to obtain the FQDN



- If server name identification (SNI) is not present, FortiGate uses the CN field in the server certificate to obtain the FQDN

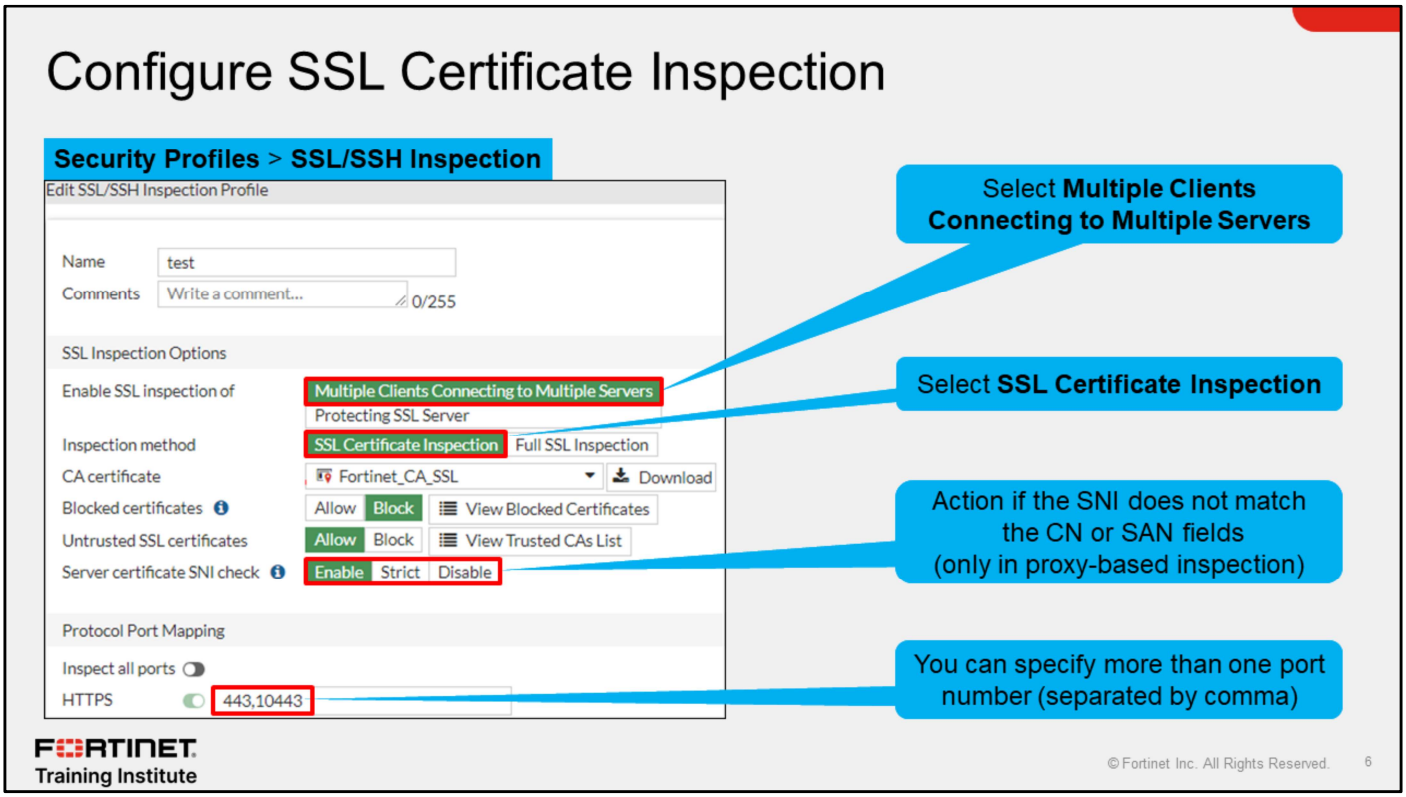


FORTINET Training Institute

For encrypted protocols, FortiGate requires additional inspection. When using SSL certificate inspection, FortiGate doesn't decrypt or inspect any encrypted traffic. Using this method, FortiGate inspects only the initial unencrypted SSL handshake. If the SNI field exists, FortiGate uses it to obtain the FQDN to rate the site. If the SNI isn't present, FortiGate retrieves the FQDN from the CN field of the server certificate.

In some cases, the CN server name might not match the requested FQDN. For example, the value of the CN field in the digital certificate of youtube.com is google.com. So, if you connect to youtube.com from a browser that doesn't support SNI, and FortiGate uses the SSL certificate inspection method, FortiGate assumes, incorrectly, that you are connecting to google.com, and uses the google.com category instead of the category for youtube.com.

SSL certificate inspection works correctly with web filtering, because the full payload does not need to be inspected.

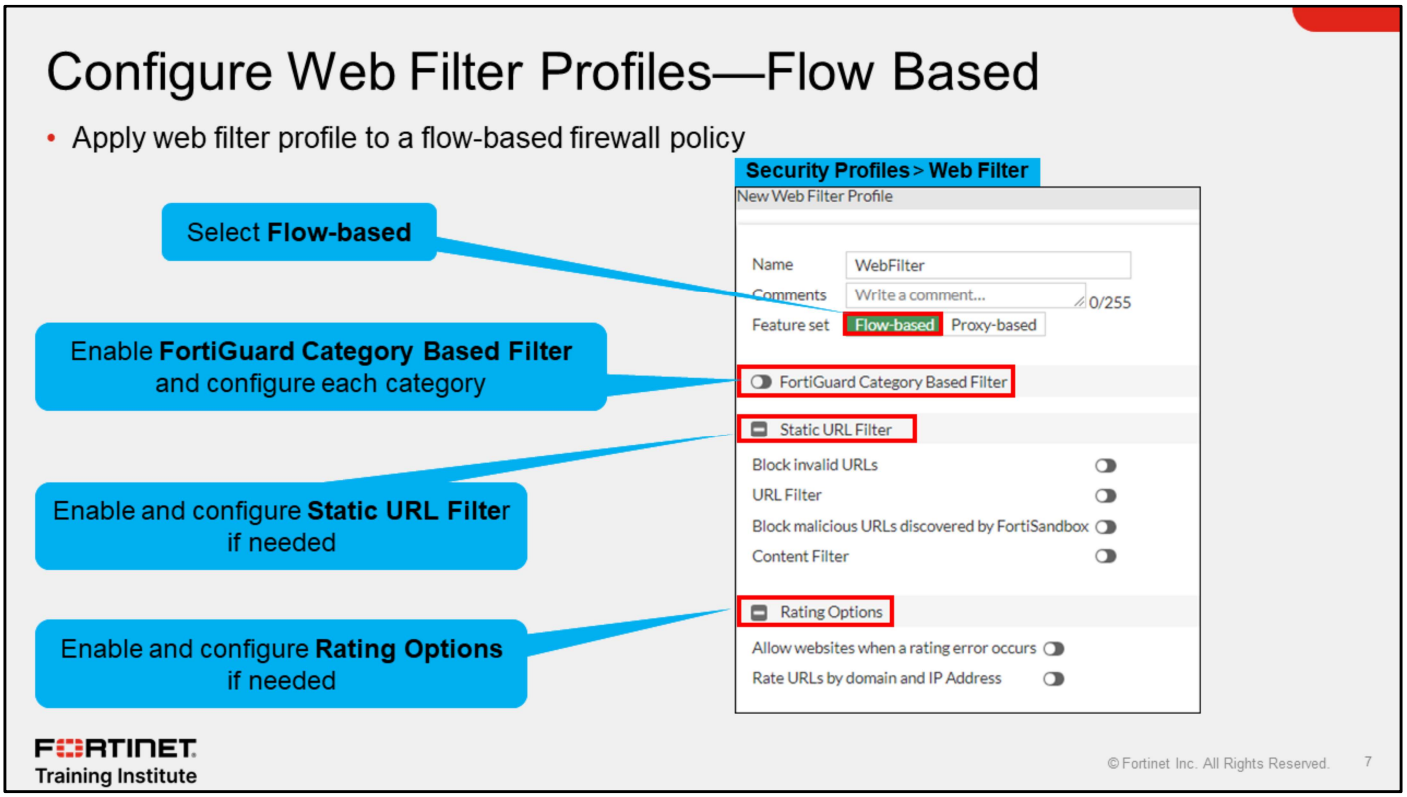


FortiGate has a read-only preconfigured profile for SSL certificate inspection named **certificate-inspection**. If you want to enable SSL certificate inspection, select this profile when configuring a firewall policy.

Alternatively, you can create your own profile for SSL certificate inspection by following these steps:

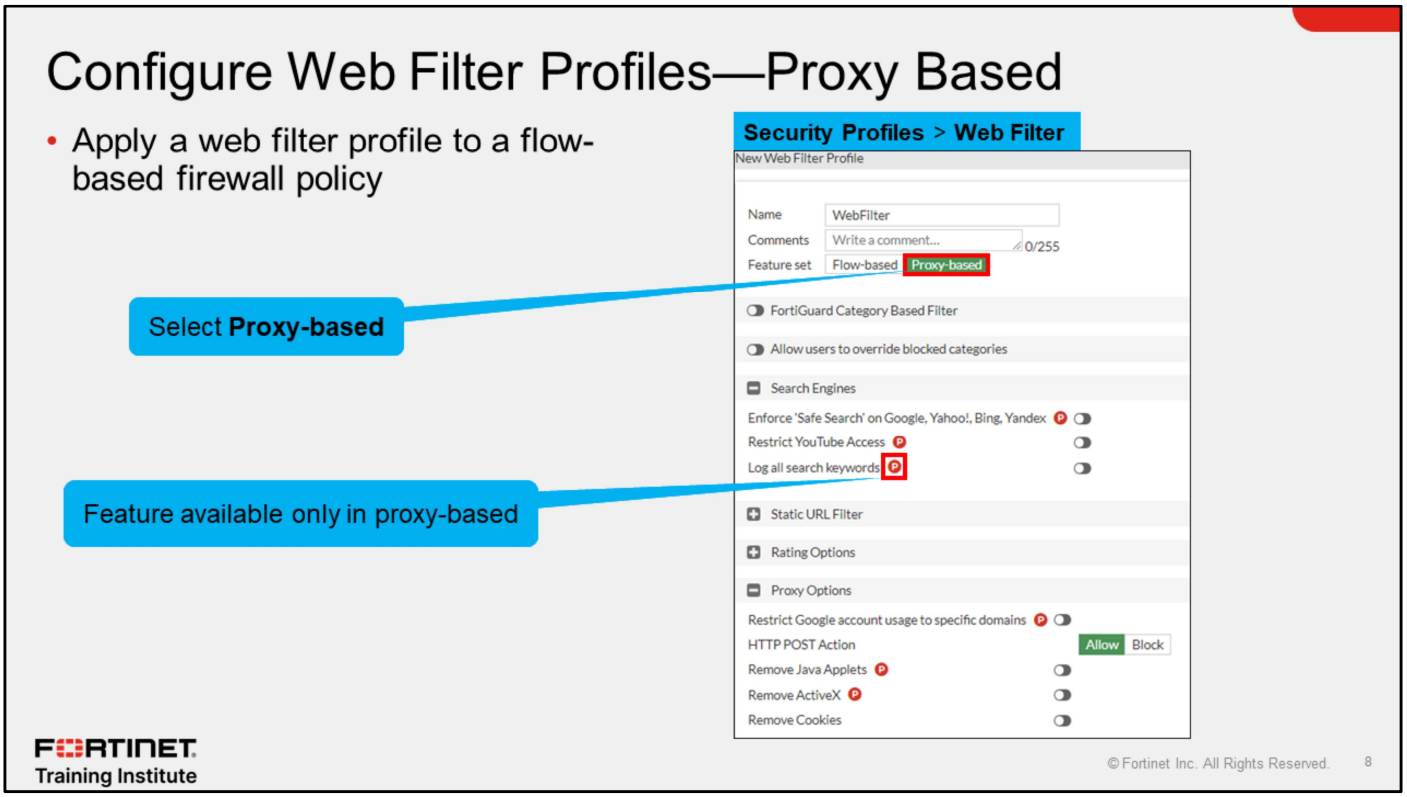
1. On the FortiGate GUI, click **Security Profiles**, and then click **SSL/SSH Inspection**.
2. Click **Create New** to create a new SSL/SSH inspection profile.
3. Select **Multiple Clients Connecting to Multiple Servers**, and then click **SSL Certificate Inspection**.
4. Select the action for **Server certificate SNI check**.

When the **Server certificate SNI check** configuration is **Enable**, FortiGate uses the domain in the `CN` field instead of the domain in the `SNI` field if the domain in the `SNI` field does not match any of the domains listed in the `CN` and `SAN` fields. With **Strict**, FortiGate closes the client connection if there is a mismatch. When **SNI check** is **Disable**, FortiGate always rates URLs based on the FQDN.



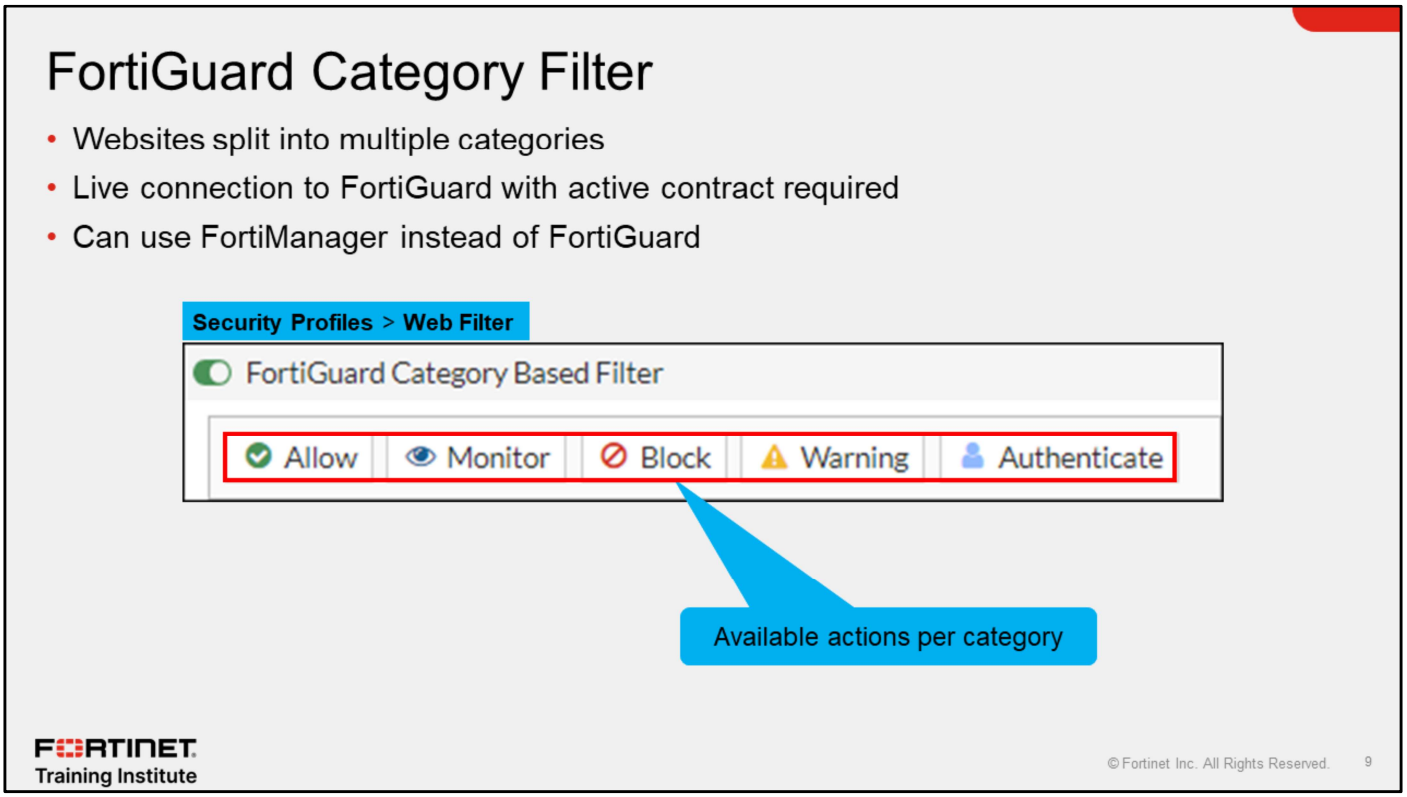
Now, you will look at the web filter profile.

You can configure this security profile to use a feature set for proxy-based or flow-based inspection modes. However, depending on the mode you select, the available settings are different. Flow-based inspection has fewer available options.



In the example shown on this slide, the security profile is configured to use a proxy-based feature set. It provides features specific to proxy-based configuration.

After you configure your web filter profile, you can apply this profile to the firewall policy configured to use proxy-based inspection mode, so the filtering is applied to your web traffic.



In the web filter profile, Fortiguard category filtering enhances the web filter features. Rather than block or allow websites individually, it looks at the category that a website has been rated with. Then, FortiGate takes action based on that category, not based on the URL.

FortiGuard category filtering is a live service that requires an active contract. The contract validates connections to the FortiGuard network. If the contract expires, there is a two-day grace period during which you can renew the contract before the service ends. If you do not renew, after the two-day grace period, FortiGate reports a rating error for every rating request made. In addition, by default, FortiGate blocks web pages that return a rating error. You can change this behavior by enabling the **Allow websites when a rating error occurs** setting.

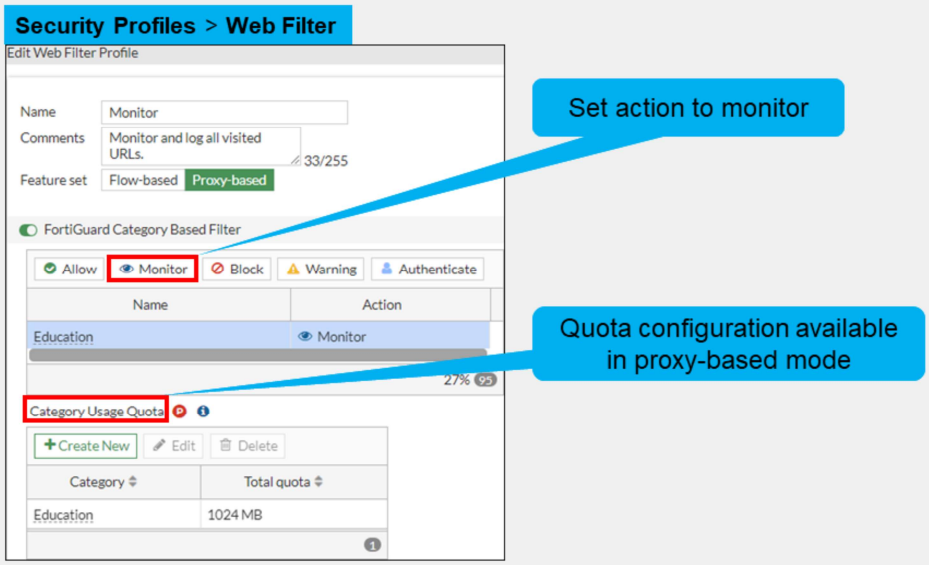
You can configure FortiManager to act as a local FortiGuard server. To do this, you must download the databases to FortiManager, and configure FortiGate to validate the categories against FortiManager, instead of FortiGuard.

You can enable the FortiGuard category filtering on the web filter profile. Categories are listed, and you can customize the actions to perform individually. In the default profile-based mode, the actions available are **Allow**, **Monitor**, **Block**, **Warning**, and **Authenticate**.

To review the complete list of categories, visit the FortiGuard web filter website.

Web Filter FortiGuard Category Action—Monitor

- Monitor action allows and logs web sites accesses

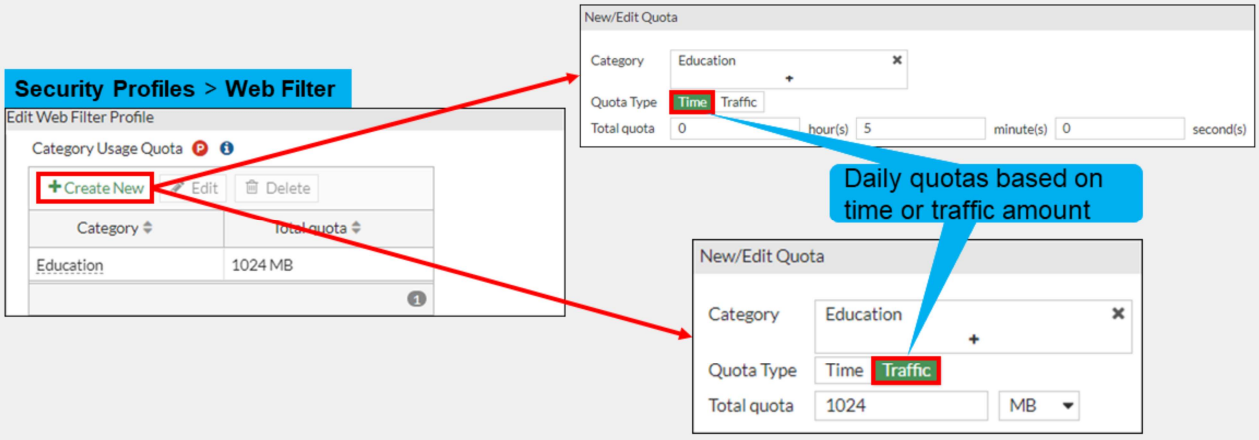


FORTINET Training Institute

Besides the **Allow** and **Block** actions, which respectively permit and block access to the sites, the **Monitor** action allows access to the sites in the category and logs it at the same time. In proxy-based mode, you can also configure a usage quota.

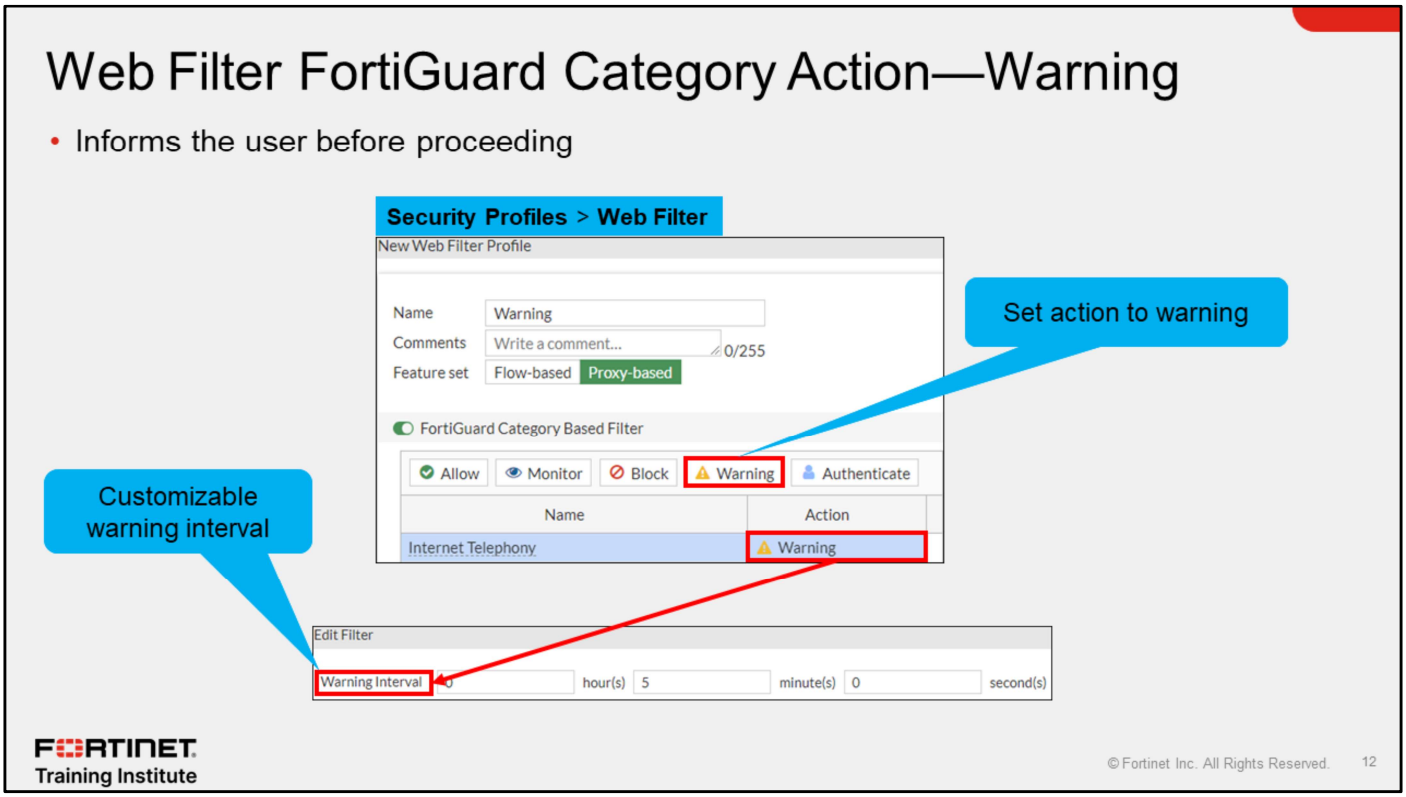
Web Filter FortiGuard Category Action—Quotas

- Applies to **Monitor**, and also **Warning** and **Authenticate** actions
- Quotas available only in proxy-based mode



FORTINET Training Institute

Quotas allow daily access for a specific length of time or bandwidth. At midnight, quotas reset. Once the daily quota is reached for a category, FortiGate blocks the traffic and displays a replacement message page. Besides the **Monitor** action, you can also apply quotas to the **Warning** and **Authenticate** actions.

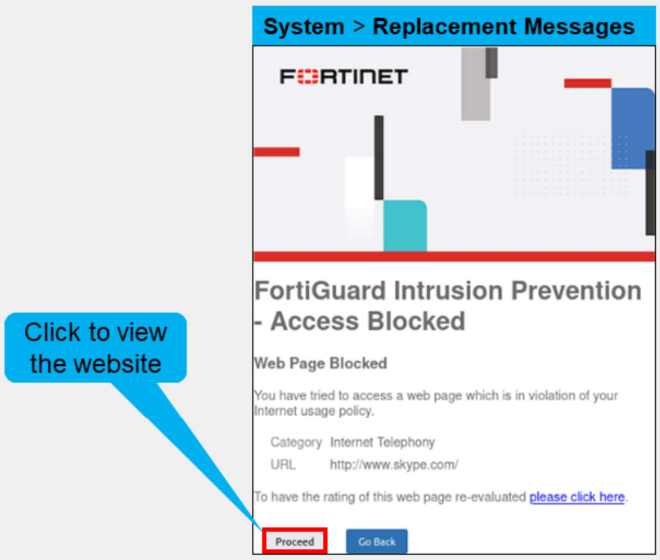


The **Warning** action informs users that the requested website is not allowed by the internet policies. However, the action gives the user the option to proceed to the requested website, or return to the previous website.

You can customize the warning interval. When the timer expires, FortiGate displays the warning message again if you access other websites in the same category.

Web Filter FortiGuard Category Action—Warning (Contd)

- Displays a customizable warning message



FORTINET Training Institute

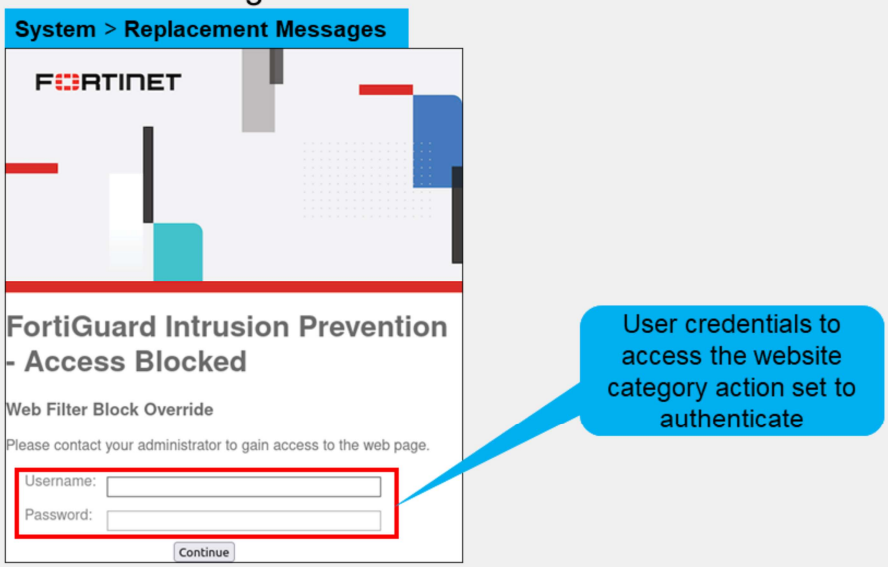
You can customize the warning replacement message. By default, it provides information of the URL and its corresponding category. With this information, the user can click **Proceed** to override the internet usage policy.

The **Authenticate** action blocks the requested websites, unless the user enters a successful username and password. FortiGate supports local and remote authentication using LDAP, RADIUS, and so on for web filtering authentication. Choosing this action prompts you to define user groups that are allowed to override the block.

You can also customize the interval of time to allow access. Users are not prompted to authenticate again if they access other websites in the same category until the timer expires.

Web Filter FortiGuard Category Action—Authenticate (Contd)

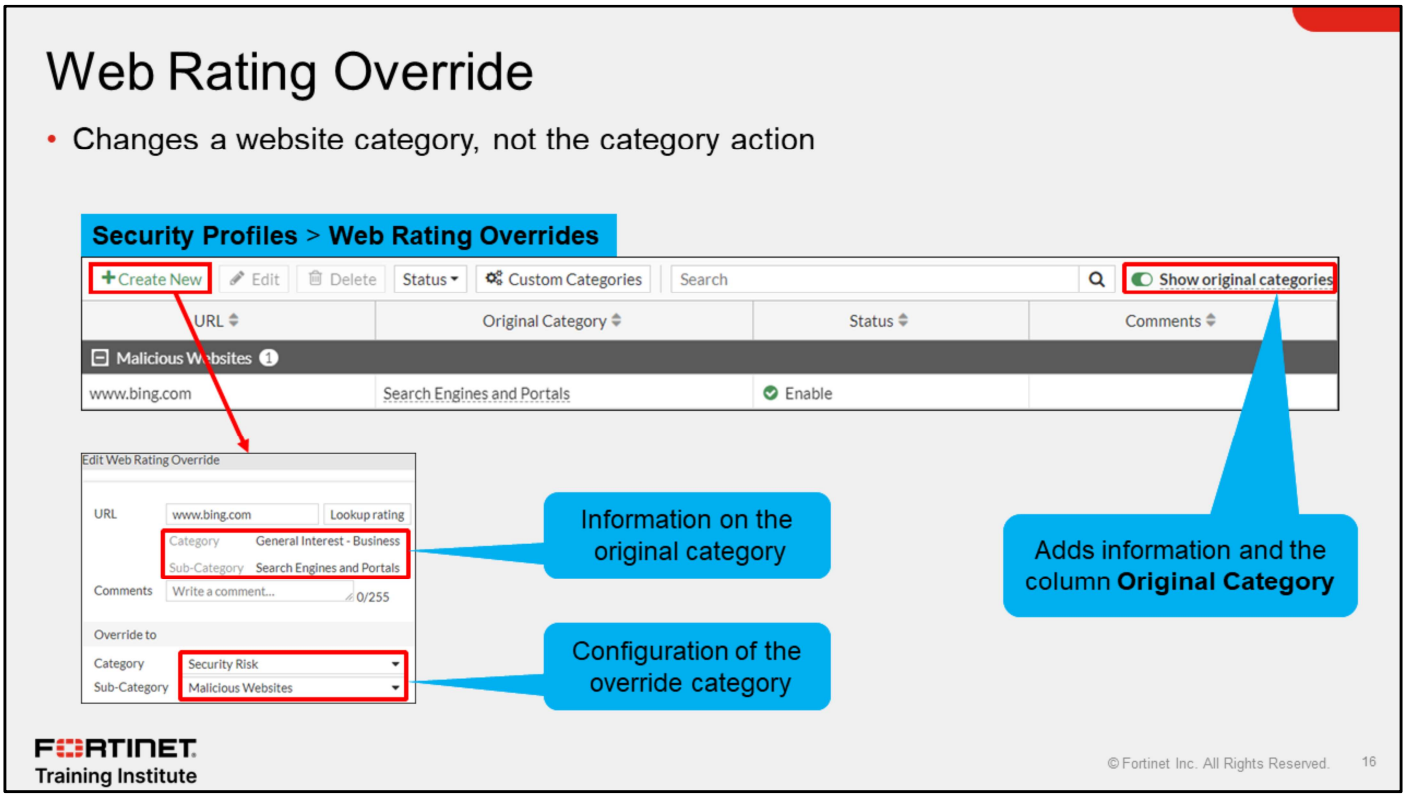
- User credentials requested in message



FORTINET Training Institute

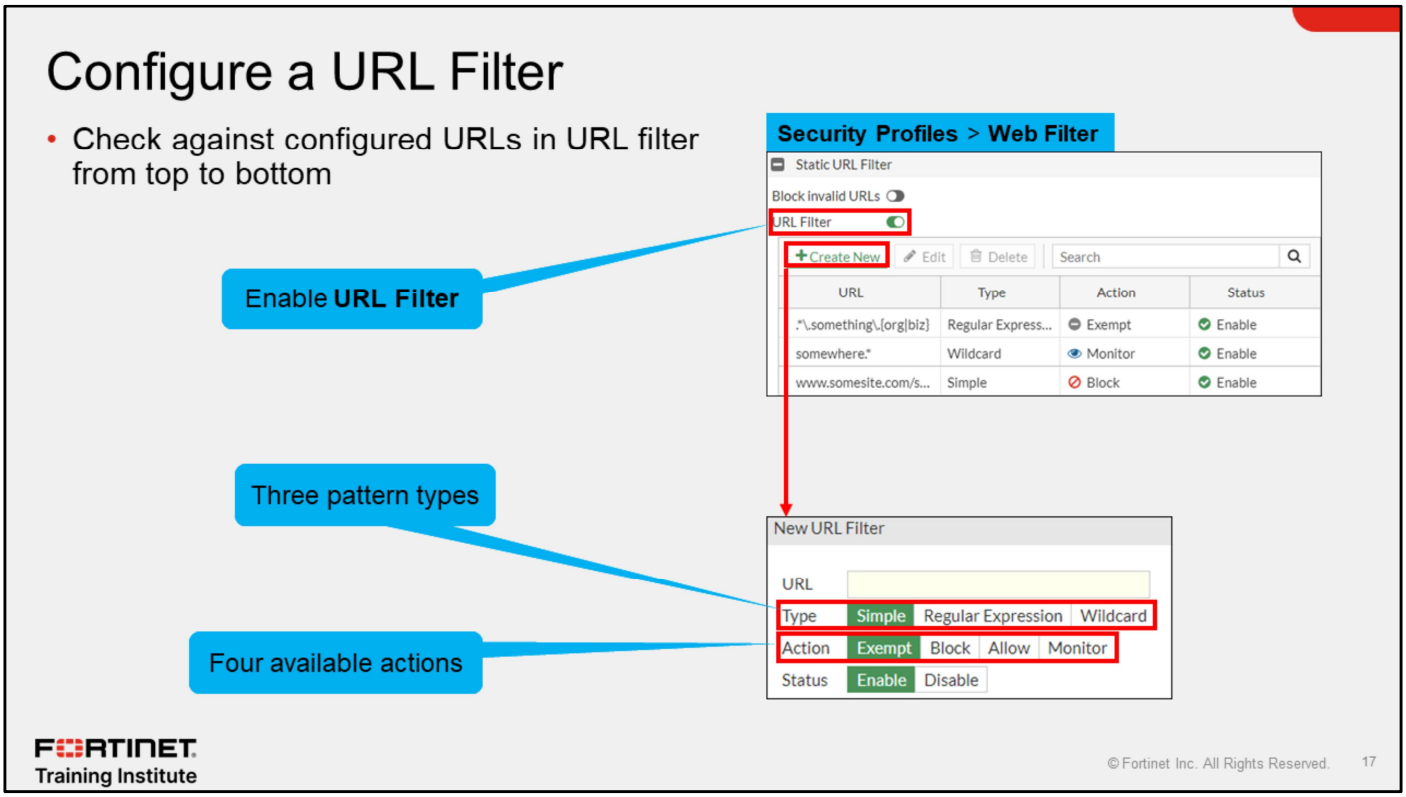
Like the **Warning** action, FortiGate displays a replacement message to proceed and a second one asks for the user credentials. You can customize these replacement messages in **System** > **Replacement Messages**.

.



If you consider that a particular URL does not have the correct category, you can ask to re-evaluate the rating in the Fortinet URL Rating Submission website. You can also override a web rating for an exceptional URL in the FortiGate configuration.

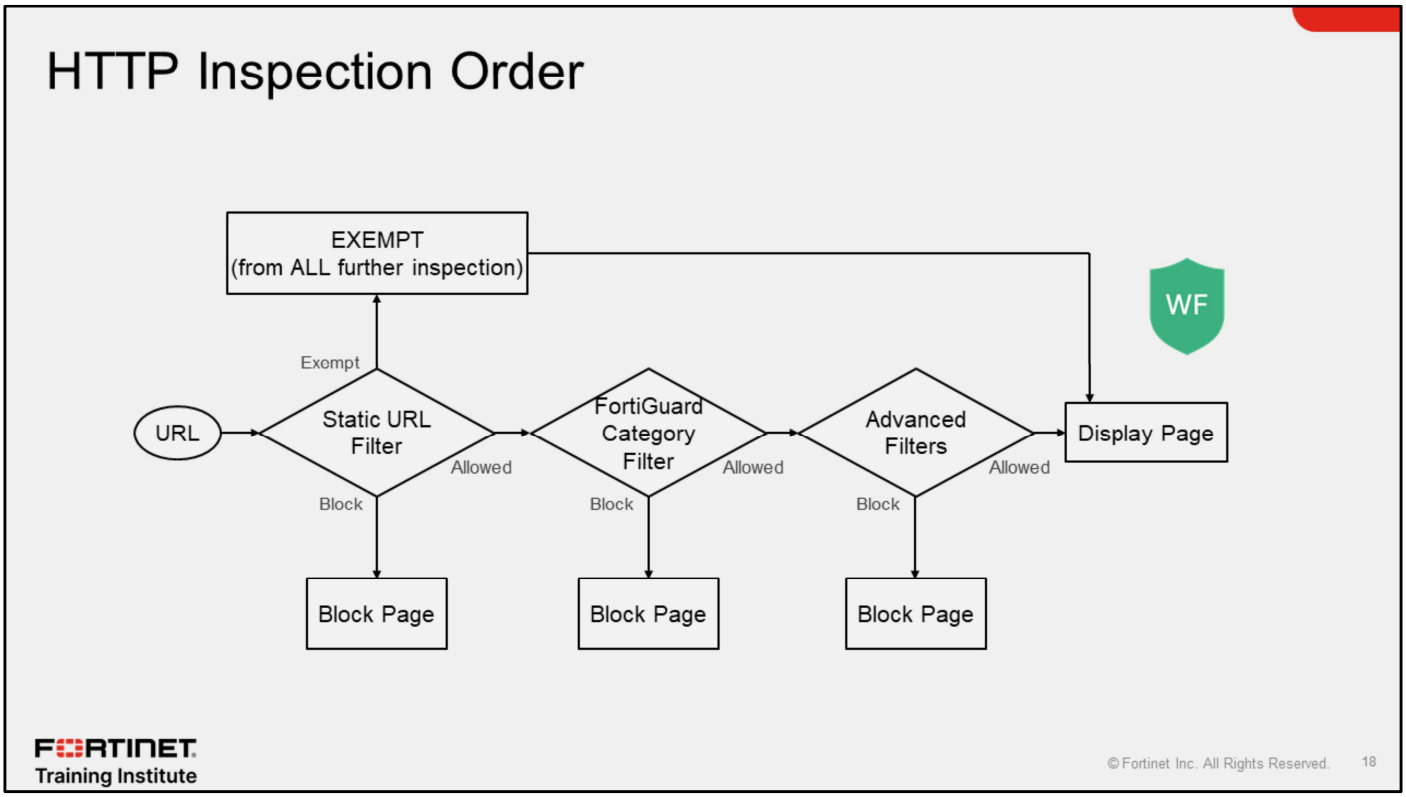
Remember that changing categories does not automatically result in a different action for the website. This depends on the settings within the web filter profile.



Static URL filtering is another web filter feature, which provides more granularity. Configured URLs in the URL filter are checked from top to bottom against the visited websites. If FortiGate finds a match, it applies the configured action. You can configure one of four actions:

- **Exempt** allows the traffic from trusted sources to bypass all security inspections.
- **Block** denies the attempt and the user receives a replacement message.
- **Allow** permits access. The traffic is passed to the remaining operations, including FortiGuard web filter, web content filter, web script filters, and antivirus scanning.
- **Monitor** allows the traffic while creating log entries. The traffic is still subject to all the other security profile inspections.

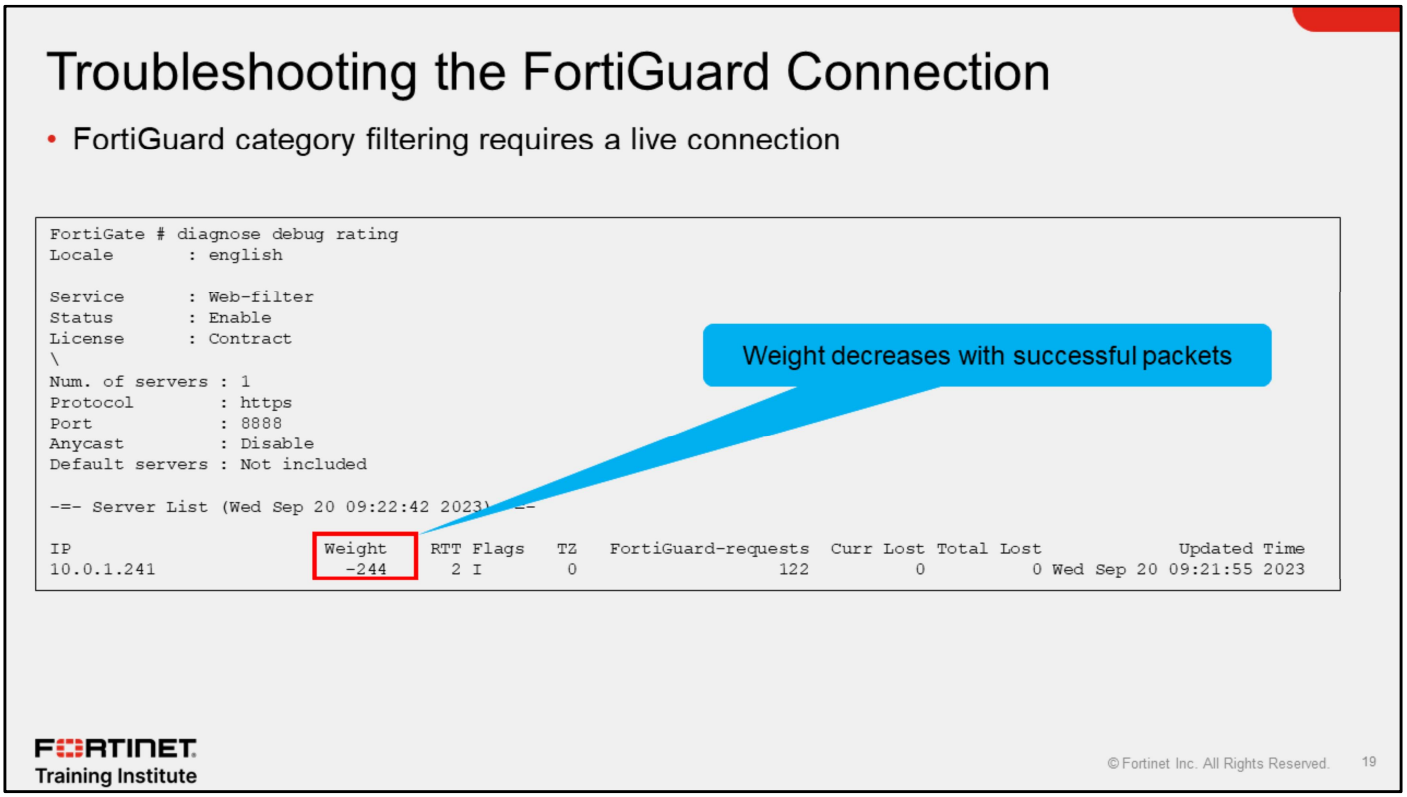
To find the exact match, URL filtering has three pattern types: **Simple**, **Regular Expressions**, and **Wildcard**.



So, with these different features, what is the inspection order? If you have enabled many of them, the inspection order flows as follows:

1. The local static URL filter
2. FortiGuard category filtering (to determine a rating)
3. Advanced filters (such as safe search or removing Active X components)

For each step, if there is no match, FortiGate moves on to the next check enabled.



Category-based filtering requires a live connection to FortiGuard.

You can verify the connection to FortiGuard servers by running the `diagnose debug rating` CLI command. This command displays a list of FortiGuard servers you can connect to, as well as the following information:

- `Weight`: It is based on the difference in time zones between FortiGate and this server to reduce the possibility of using a remote server.
- `RTT`: Return trip time
- `Flags`: `D` (IP returned from DNS), `I` (Contract server contacted), `T` (being timed), `F` (failed)
- `TZ`: Server time zone
- `FortiGuard-requests`: The number of requests sent by FortiGate to FortiGuard
- `Curr Lost`: Current number of consecutive lost FortiGuard requests (in a row, it resets to `0` when one packet succeeds)
- `Total Lost`: Total number of lost FortiGuard requests

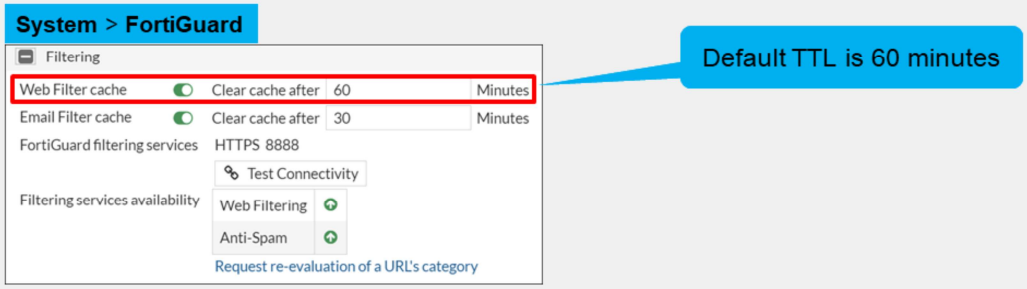
The list is of variable length depending on the FortiGuard Distribution Network and the FortiGate configuration.

Troubleshooting the FortiGuard Connection (Contd)

- Change default FortiGuard or FortiManager communications from HTTPS port 443:
  - Disable FortiGuard anycast setting on CLI to use UDP ports 443, 53, or 8888

```
config system fortiguard
    set fortiguard-anycast {enable|disable}
    set protocol {udp|https}
    set port {8888|53|443}
end
```

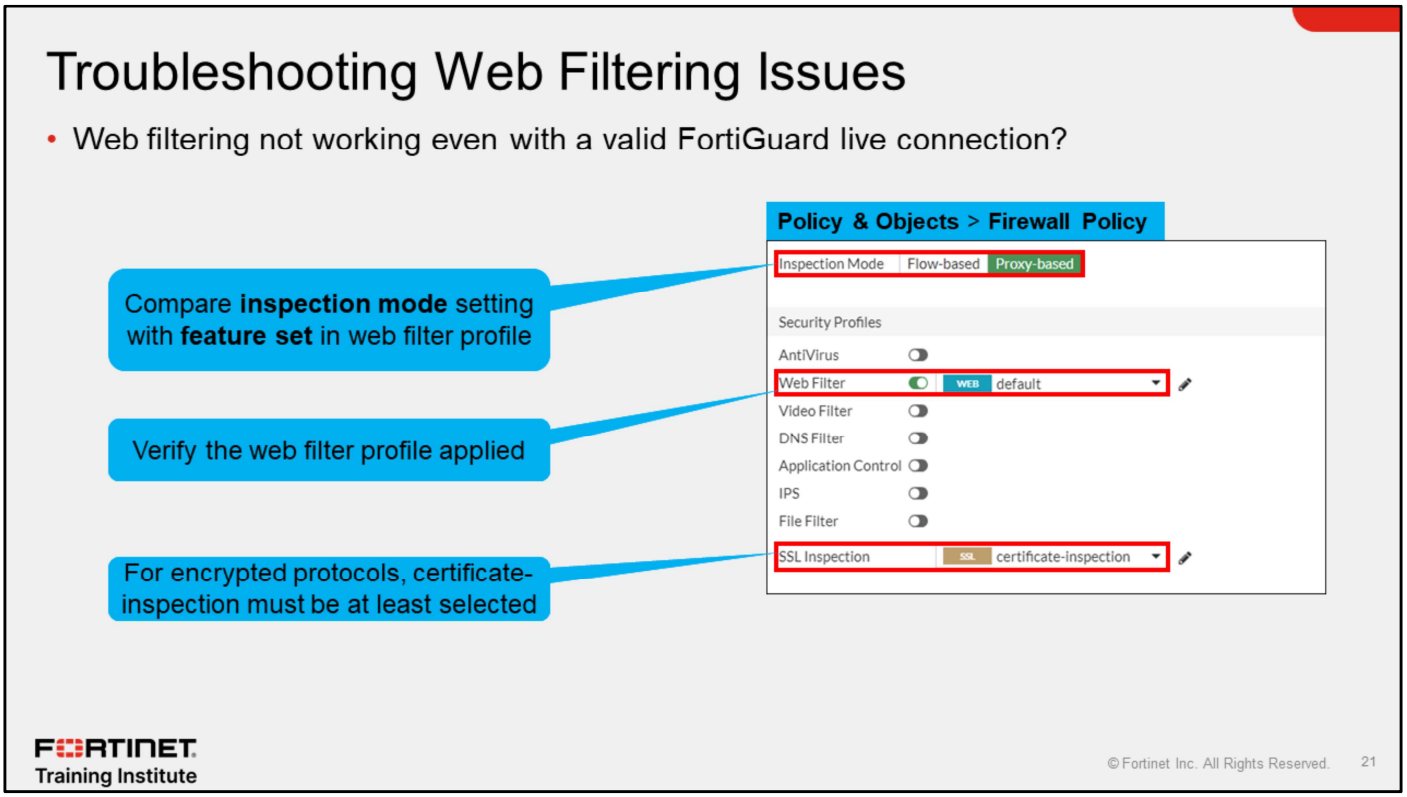
- Enable **Web Filter cache** to reduce requests to FortiGuard



FORTINET Training Institute

By default, FortiGate is configured to enforce the use of HTTPS port 443 to perform live filtering with FortiGuard or FortiManager. When the `fortiguard-anycast` command is `enable`, the FortiGuard domain name resolves to a single anycast IP address, which is the only entry in the list of FortiGuard servers. By disabling the FortiGuard anycast setting on the CLI, other ports and protocols are available. These ports and protocols query the servers (FortiGuard or FortiManager) on HTTPS port 53 and port 8888, UDP port 443, port 53, and port 8888. If you are using UDP port 53, any kind of inspection reveals that this traffic is not DNS and prevents the service from working. In this case, you can switch to the alternate UDP port 443 or port 8888, or change the protocol to HTTPS, but these ports are not guaranteed to be open in all networks, so you must check beforehand.

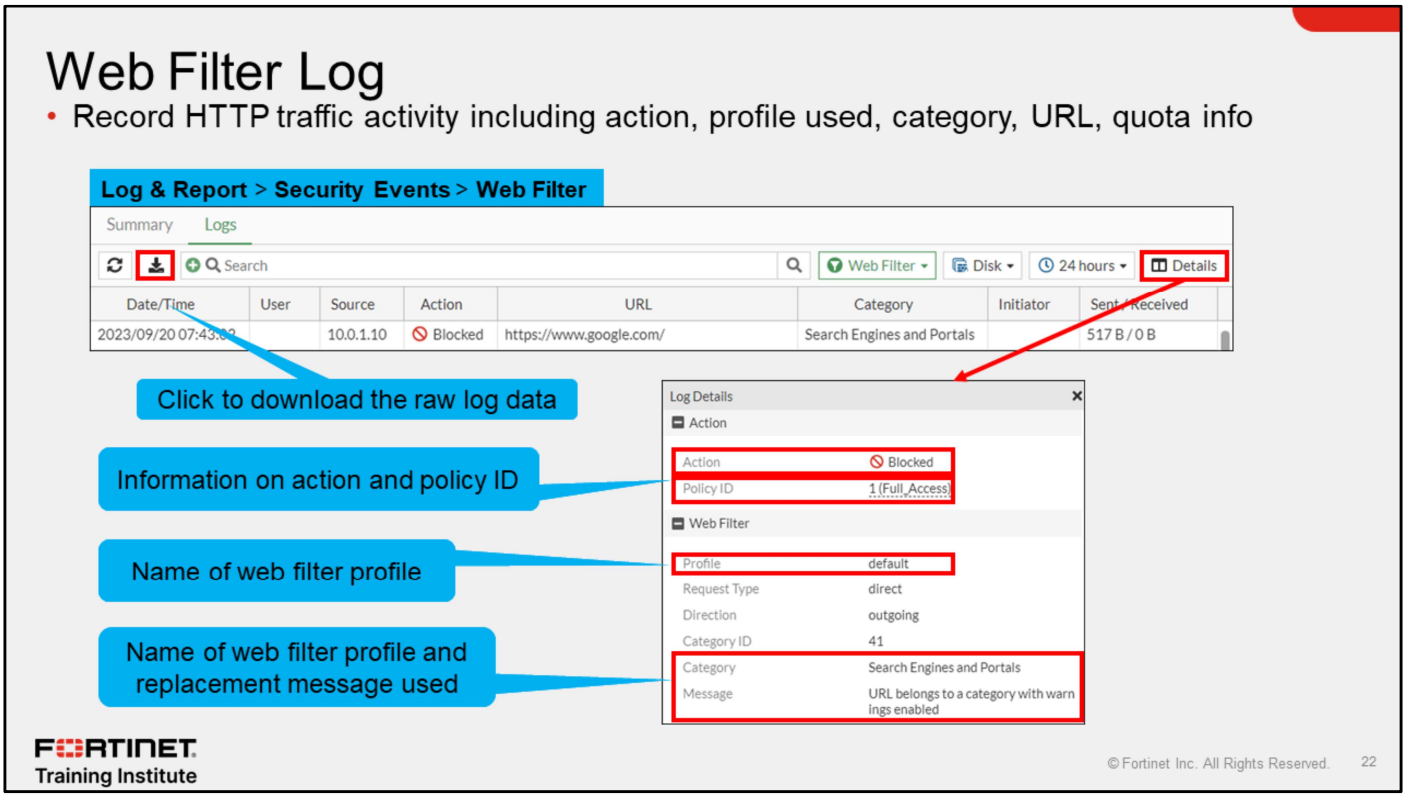
If the number of FortiGuard requests is too high, you can also enable **Web Filter cache.** Once enabled, FortiGate maintains a list of recent website rating responses in memory. So, if the URL is already known, FortiGate doesn't send back a rating request. Caching responses reduces the amount of time it takes to establish a rating for a website. Also, memory lookup is much quicker than packets travelling on the internet.



What if you have a live connection to FortiGuard and configured your security profiles, but they are not performing web inspection?

Most of the time, issues are caused by misconfiguration on the device. You can verify them as follows:

- Make sure that the **SSL Inspection** field includes at least one profile with an SSL certification inspection method.
- Make sure that the correct web filter profile is applied on the firewall policy.
- Verify the inspection mode setting with the feature set in the corresponding web filter profile.



To confirm the correct configuration and web filtering behavior, you can view the web filter logs.

This slide shows an example of a log message. Access details include information about the FortiGuard quota and category (if those are enabled), which web filter profile was used to inspect the traffic, the URL, and more details about the event.

You can also view the raw log data by clicking the download icon at the top of the GUI. The file downloaded is a plain text file in a syslog format.

Knowledge Check

1. Which action in URL filtering bypasses all security profiles?

✓ A. Exempt
B. Allow

2. Which statement about proxy-based web filtering is true?

A. It requires fewer resources than flow-based.
✓ B. It transparently analyzes the TCP flow of the traffic.

Review

- ✓ Describe FortiOS inspection modes
- ✓ Implement a web filter profile in flow-based and proxy-based inspection modes
- ✓ Work with web filter categories
- ✓ Configure a URL filter for further granularity
- ✓ Troubleshoot common web filtering issues
- ✓ Monitor logs for web filtering events

FORTINET Training Institute

This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to configure web filtering on FortiGate to control web traffic in your network.