Extra help: Web filtering

This section contains tips to help you with some common challenges of FortiGate web filtering.

The Web Filter option does not appear in the GUI.

Go to **Config > System > Features** and enable **Web Filter**.

New Web Filter profiles cannot be created.

Go to **Config > System > Features** and select **Show More**. Enable **Multiple Security Profiles**.

Web Filtering has been configured but is not working.

Make sure that web filtering is enabled in a policy. If it is enabled, check that the policy is the policy being used for the correct traffic. Also check that the policy is getting traffic by going to the policy list and adding the Sessions column to the list.

An active FortiGuard Web Filtering license displays as expired/unreachable.

First, ensure that web filtering is enabled in one of your security policies. The FortiGuard service will sometimes show as expired when it is not being used, to save CPU cycles.

If web filtering is enabled in a policy, go to **System > Config > FortiGuard** and click the blue arrow beside **Web Filtering**. Under Port Selection, select **Use Alternate Port (8888)**. Select **Apply** to save the changes. Check whether the license is shown as active. If it is still inactive/expired, switch back to the default port and check again.

Websites blocked using the FortiGuard Categories are not consistently blocked (for example, traffic is only blocked using certain browsers).

In your web filter profile, make sure that **Scan Encrypted Connections** is selected. Next, create an SSL Inspection profile and add it to the security policy. Traffic should now be blocked consistently.

SSL Inspection is causing certificate errors.

Download the Fortinet_CA_SSLProxy certificate and install it on your web browser. For more information, see “Preventing security certificate warnings when using SSL inspection” on page 230.