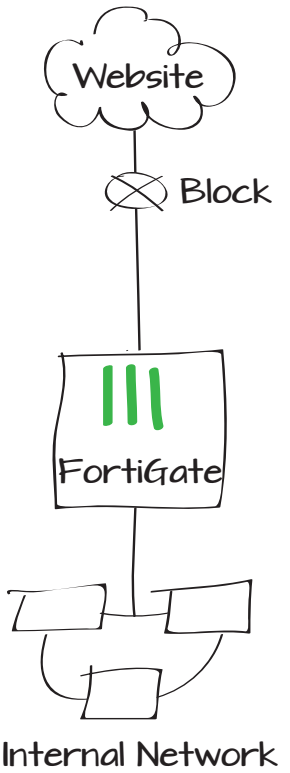
Blocking access to specific websites

This example sets up the FortiGate unit to block users from viewing a specific website using web filtering.

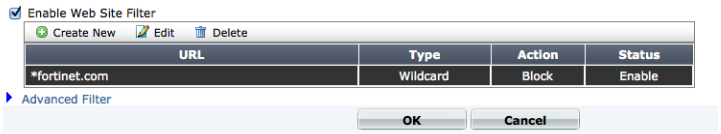
1. Creating a web filter profile
2. Adding the web filter profile to a security policy
3. Results



Creating a web filter profile

Go to **Security Profiles > Web Filter > Profiles**.

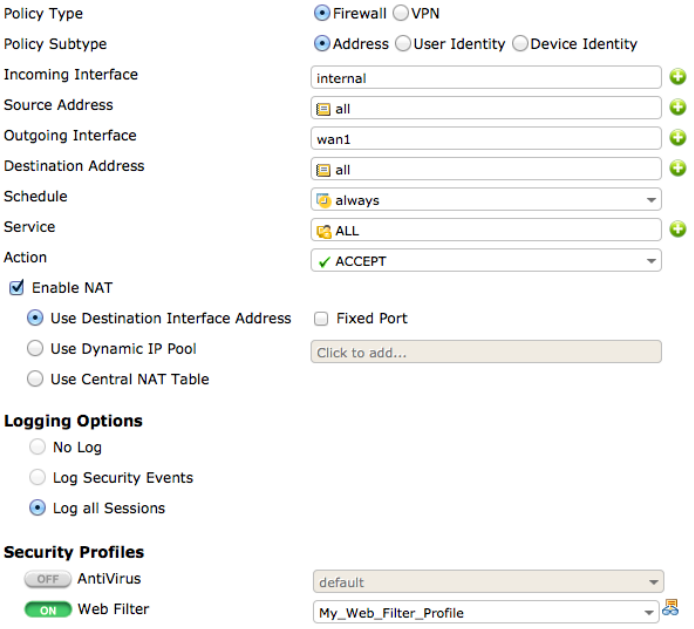
Create a new profile and select **Enable Web Site Filter** and **Create New**. Set the **URL** to *fortinet.com, using * as a wildcard character in order to block all subdomains of the site. Set the **Type** to **Wildcard** and the **Action** to **Block**.



Adding the web filter profile to a security policy

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

Edit the policy controlling the traffic you wish to block from the website. Under **Security Profiles**, enable **Web Filter** and set it to use the new profile.



Results

In a web browser, visit www.fortinet.com and docs.fortinet.com. In both cases, the FortiGate unit displays a message, stating that the website is blocked.

This example will only block HTTP web traffic. In order to block HTTPS traffic as well, see "Blocking HTTPS traffic with web filtering" on page 149.

The URL you requested has been blocked

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

URL = fortinet.com/

The URL you requested has been blocked

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

URL = docs.fortinet.com/fgt.html