HTTPS Filtering With the Barracuda Web Security Gateway

https://campus.barracuda.com/doc/45712498/

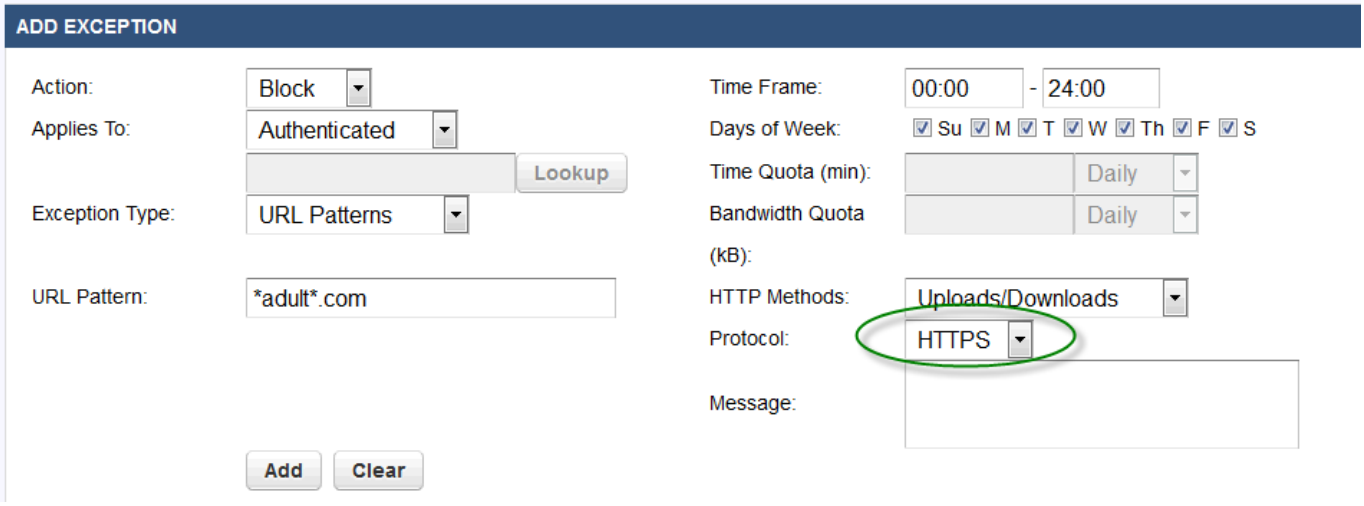
This feature is an effective alternative to SSL Inspection for the following cases:

- For the Barracuda Web Security Gateway 210 or 310 if you want to block some or all HTTPS traffic by domain or by content category. The Barracuda Web Security Gateway 210 does not support SSL Inspection, and limited SSL Inspection is available on the Barracuda Web Security Gateway 310, only for Safe Search. Note: SSL Inspection is *not* available on the Barracuda Web Security Gateway 310Vx virtual machine.
- For the Barracuda Web Security Gateway 410 and higher, as a less resource-intensive tool than SSL Inspection if you only need to block some or all HTTPS traffic by domain or by domain/content category.

You can create block, warn and monitor exceptions for HTTPS web traffic on the **BLOCK/ACCEPT > Exceptions** page with content category filters, and/or domain filters. Unlike SSL Inspection, this feature does not decrypt and inspect the URL content; rather it identifies domains and content categories for use in creating block/warn/allow policies. You can also use URL pattern filters with Exceptions applied to the HTTPS protocol, but only the unencrypted portion of the requested URL can be checked. When HTTPS access is denied, the user will only be presented with a block page if you also set **Enable HTTPS Blockpage** to *Yes* on the **BLOCK/ACCEPT > Configuration** page. Otherwise, the user will not be presented with a block page. For more about block pages, see Block Pages, SSL Inspection and HTTPS Filtering.

Note that, with firmware 14.1 and above, the user is always served a block page per policy when SSL Inspection is enabled. With older versions of firmware, there are occasional conditions when a block page is *not* served per policy when HTTPS Filtering is enabled *and* SSL Inspection is enabled in Transparent mode. See Block Pages, SSL Inspection and HTTPS Filtering for more information.

Example: Block authenticated users from all domains that contain a specific URL pattern, accessed over HTTPS.



This option is disabled on the Barracuda Web Security Gateway by default. To enable, go to the **BLOCK/ACCEPT > Configuration** page and set **Enable HTTPS Filtering** to **Yes**.

Figures

1. HTTPSExceptions.png