Block Pages, SSL Inspection and HTTPS Filtering

https://campus.barracuda.com/doc/46203173/

If you only need to apply block policies by domain and/or domain (content) categories, you can enable HTTPS filtering on the 210 or higher as opposed to using SSL Inspection. Unlike SSL Inspection, HTTPS filtering does not decrypt the encrypted portion of URLs. This prevents monitoring or capturing of social media interactions such as posts, chat, comments, shares, etc. See How to Configure SSL Inspection Version 12 and Above for requirements around using SSL inspection.

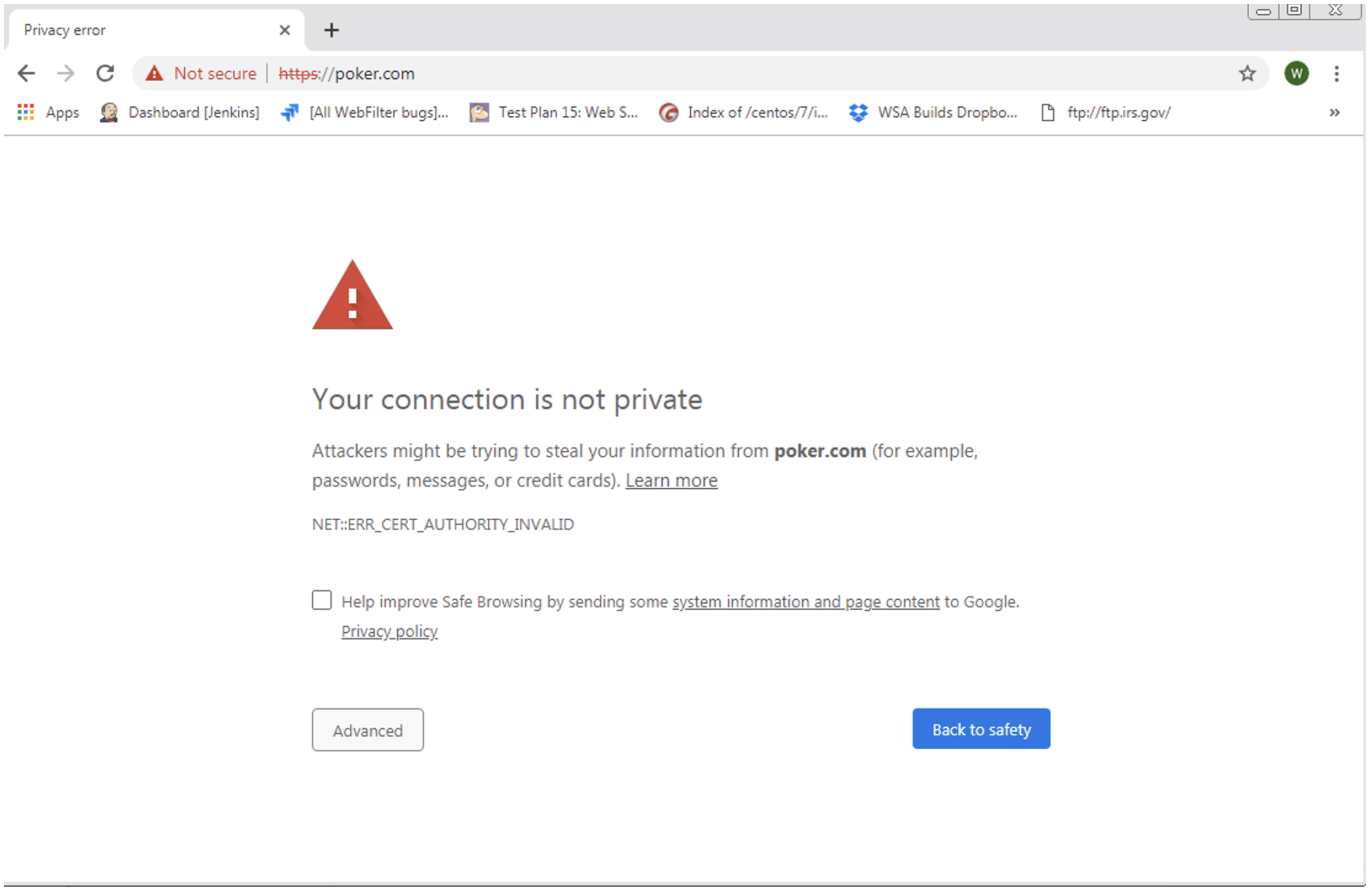
HTTPS Filtering and Block Pages

- 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.
- If client traffic is not using Server Name Indication (SNI) (i.e. using SSLv3 and lower), then immediately after you enable this option, any client machines that had previously established an HTTPS session are communicating with an IP address and will not be blocked. In this situation, the HTTPS website IP address remains in the DNS client resolver cache (as well as in the DNS table on the core router or domain controller) until the DNS request time-to-live (TTL) expires. This can take up to a day or two, depending upon how the HTTPS sites configure TTL.
- If the HTTPS site is using Strict Transport Security (HSTS):
  - The Barracuda Web Security Gateway does not supply a block page unless you are using SSL inspection.
  - With HSTS you should use SSL inspection (available on model 310 and up).

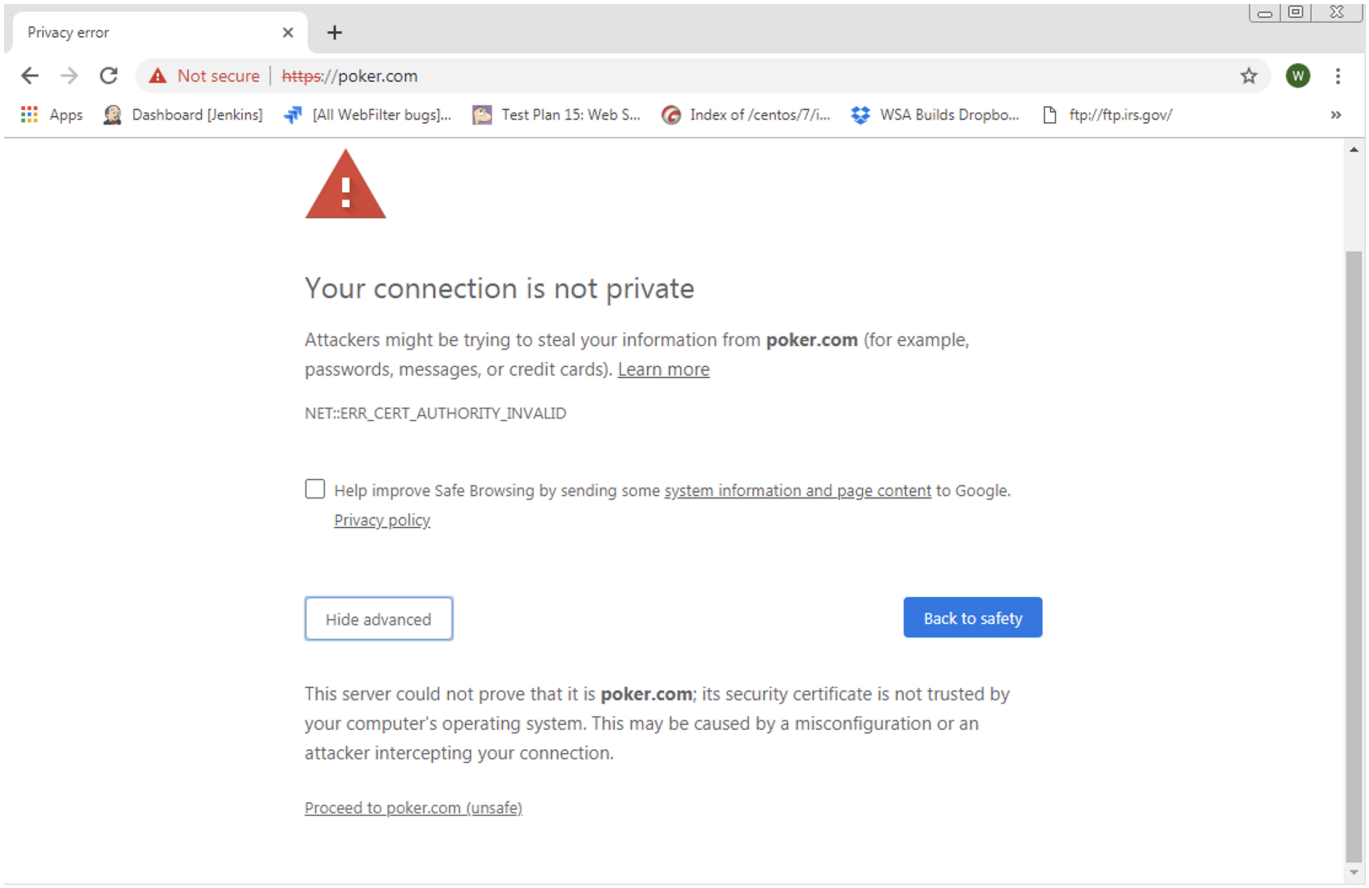
When HTTPS access is denied, the user is only presented with a block page if you also set **Enable HTTPS Blockpage** to *Yes* on the **BLOCK/ACCEPT > Configuration** page. Otherwise, the user is not presented with a block page. Note that the user will get an error message in their browser when attempting to visit blocked domains over HTTPS with the following configuration:

- SSL Inspection is disabled, *and*
- The SSL certificate has been removed from / not installed in the user's browser, *and*
- The **Enable HTTPS Blockpage** feature is set to *YES* on the **BLOCK/ACCEPT > Configuration** page.

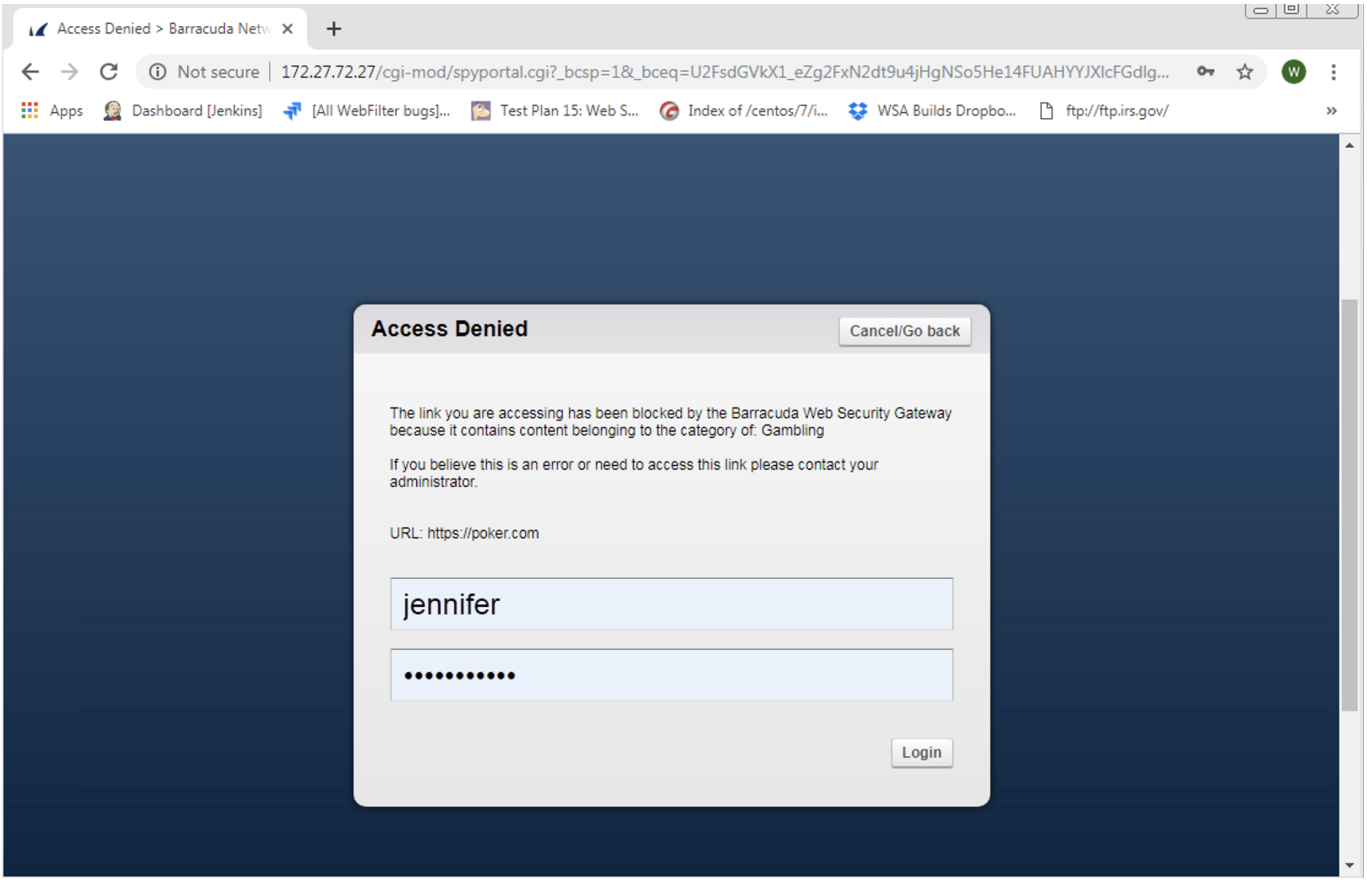
Visiting a blocked HTTPS website with this configuration will result in the following pages presented to the user:



If the user clicks **Advanced**, the following page is served:



If the user clicked **Proceed to <domain name> (unsafe)**, then the a block page is served:



Use cases for this configuration:

- Guest user, internet cafe, hotel, etc.
- Administrator does not want to install certificates in users' browsers.

Note that, with this configuration, each time users try to visit another domain, they will see the warning again.

See also Block Messages and Using SSL Inspection With the Barracuda Web Security Gateway.

Figures

1. HTTPSBLockPage1.png
2. HTTPSBLockPage2.png
3. HTTPSBLockpage3.png