Using SSL Inspection With the Barracuda Web Security Gateway

https://campus.barracuda.com/doc/6160443/

Due to recent vulnerabilities discovered with the SSL protocol, Barracuda strongly recommends that you upgrade to 8.1.0.005 before using this feature. Available with the Barracuda Web Security Gateway 310 (limited) and higher.

For configuration steps, see How to Configure SSL Inspection. This feature is supported for the Barracuda Web Security Gateway version 7.0 and higher. For information about SSL Inspection features supported for appliances and Vx models, see the documentation for the version you are running.

Why SSL Inspection Is Important

Social media sites like Facebook and YouTube are now typically accessed over HTTPS, the encryption protocol used to protect online banking sessions and user logins for services of all kinds on the web.

By enabling the Barracuda Web Security Gateway to decrypt, inspect and re-encrypt web traffic at the URL level, administrators have fine grained control over the use of web-based applications. This allows administrators to choose to block certain portions of web based applications such as Facebook Chat and Facebook Sharing, while enabling other portions, such as the rest of Facebook. Since Facebook, Twitter, various search engines such as Google, and many web-based applications run over HTTPS, SSL Inspection is required for this level of monitoring and blocking. With this control the administrator can define what they deem permissible on their network and need not block all of Facebook, Twitter, G Suite and other popular web-based applications.

Additionally, since block pages cannot always be served when just using HTTPS filtering, using SSL Inspection almost guarantees presentation of a block page when needed.

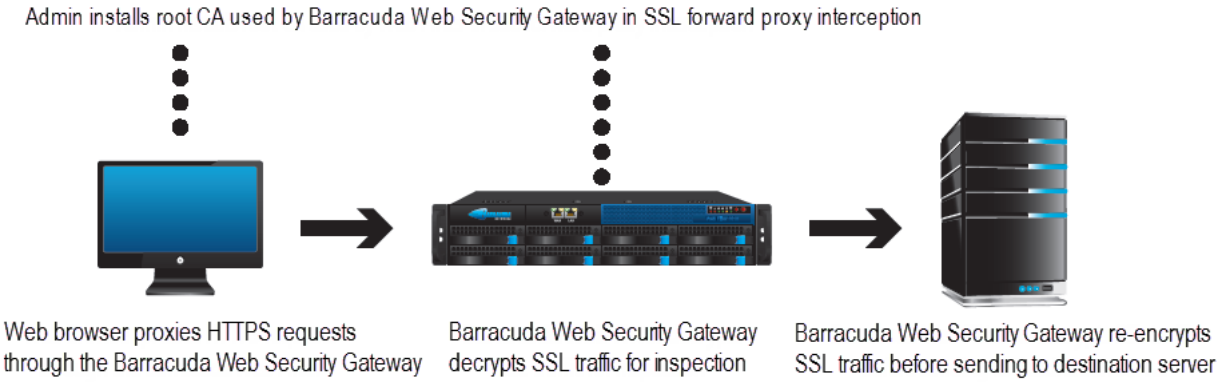
How SSL Inspection Works

With SSL Inspection, the content of a URL over HTTPS can be scanned. This allows the Barracuda Web Security Gateway to apply policies and detect malware and viruses at the URL level for traffic you designate for SSL Inspection.

The Barracuda Web Security Gateway acts as a secure intermediary between user HTTPS web requests and the destination web server (i.e. Facebook.com, YouTube.com, yourdomain.com, etc.). HTTPS content in user web requests is decrypted and scanned by the Barracuda Web Security

Gateway, which then detects malware and enforces web policies configured on the **BLOCK/ACCEPT** pages. After processing, this HTTPS traffic will be re-encrypted on the fly by the Barracuda Web Security Gateway and routed to the destination web server as shown in Figure 1.

Figure 1: SSL Inspection



To use this feature, the administrator installs a root certificate in client browsers from the Barracuda Web Security Gateway. The Barracuda Web Security Gateway can then intercept and inspect the HTTPS connections by presenting the client a CA derived from this root CA. If you have a high availability deployment, you must install the same root certificate on each Barracuda Web Security Gateway.

SSL Inspection Versus HTTPS Filtering

If you only need to block by domain and/or domain (content) categories, you can enable **HTTPS filtering** on the 210 and higher. See HTTPS Filtering With the Barracuda Web Security Gateway for details. Unlike SSL Inspection, HTTPS filtering does not decrypt the encrypted portion of URLs. This prevents monitoring or capturing of social media interactions such as chat, comments, shares, etc. HTTPS Filtering is a good choice when:

- You have a Barracuda Web Security Gateway 210, which currently does not support SSL Inspection.
- You have a Barracuda Web Security Gateway 310, which supports limited SSL Inspection (Safe Search).
- Your organization policies only require blocking web traffic over HTTPS by domain or domain categories.
- Saving system resources for traffic processing other than SSL Inspection is important for your application. HTTPS filtering is a much less resource intensive option than SSL Inspection.

SSL Accelerator Hardware

SSL functions are offloaded to an SSL accelerator card if included in your Barracuda Web Security Gateway appliance model. Presence and enabling of this hardware results in improved overall system performance. See SSL Accelerator Hardware for details and to determine if your Barracuda Web Security Gateway appliance includes this hardware.

Popular Use Cases of SSL Inspection

Use case: Suspicious Keyword Tracking on Social Media

Monitor social messaging over HTTP/HTTPS in real time, with keyword alert emails to teachers or administrators to trigger immediate responses to emerging cases of bullying, harassment, or loss of confidential data. The Suspicious Keyword Tracking feature only requires the use of SSL Inspection if traffic is over HTTPS (which is typical for Facebook, G Suite, etc.) and is available on the Barracuda Web Security Gateway 410 and higher. Database of keywords is embedded in the Barracuda Web Security Gateway, is frequently updated, and can be customized. See the **BLOCK/ACCEPT > Web App Monitor** page to configure.

Use case: G Suite Control Over HTTPS

Perform granular regulation of G Suite tools over HTTPS; for example, allow business Gmail account access, but block personal Gmail account access. See G Suite Control Over HTTPS. For Chromebooks, see How to Get and Configure the Barracuda Chromebook Security Extension.

Use case: Facebook Control Over HTTPS

Regulate and archive Facebook application interactions (chat, posting, games, etc.). See Facebook Control Over HTTPS.

Use cases: Safe Search Over HTTPS

Users or groups you specify will *not* see search engine content that contains objectionable thumbnail images in the search results; only filtered thumbnails are displayed in the search results. See Creating Block and Accept Policies. Available with the Barracuda Web Security Gateway 310 and higher. See also How to Configure SSL Inspection.

Use case: Secure Uploads and Downloads Via Web-Based Email

Popular for schools. Allow access to web-based email applications, but prevent potentially dangerous

uploads and downloads.

Figures