

How to Configure SSL Inspection Version 12 and Above

<https://campus.barracuda.com/doc/68354870/>

This article applies to the Barracuda Web Security Gateway 310 and higher running version 12.0 and above. For background information, see [Using SSL Inspection With the Barracuda Web Security Gateway](#). If you are using Google Chrome browser, see [How to Configure SSL Inspection for Google Chrome Browser](#) to prevent certificate errors users might encounter.

IMPORTANT NOTES:

- If you want to use SSL Inspection with Google consumer apps, see [Google Workspace Control Over HTTPS](#).
- Spydef policies (see **ADVANCED > Energize Updates**) take precedence over SSL Inspection as enabled for Domains / Categories / Source Networks / Users or Groups / Destination IPs. Once SSL Inspection is enabled, Spyware defs will be applied, even to exemptions you configure on that page.
- When SSL Inspection is enabled, all traffic is inspected. As a result, when certain applications need to send their traffic over port 443, this can cause issues with the application and prevent it from working properly.

Applications known to have these issues are listed below and should be exempted from SSL Inspection.

- Skype
- UPS Worldship

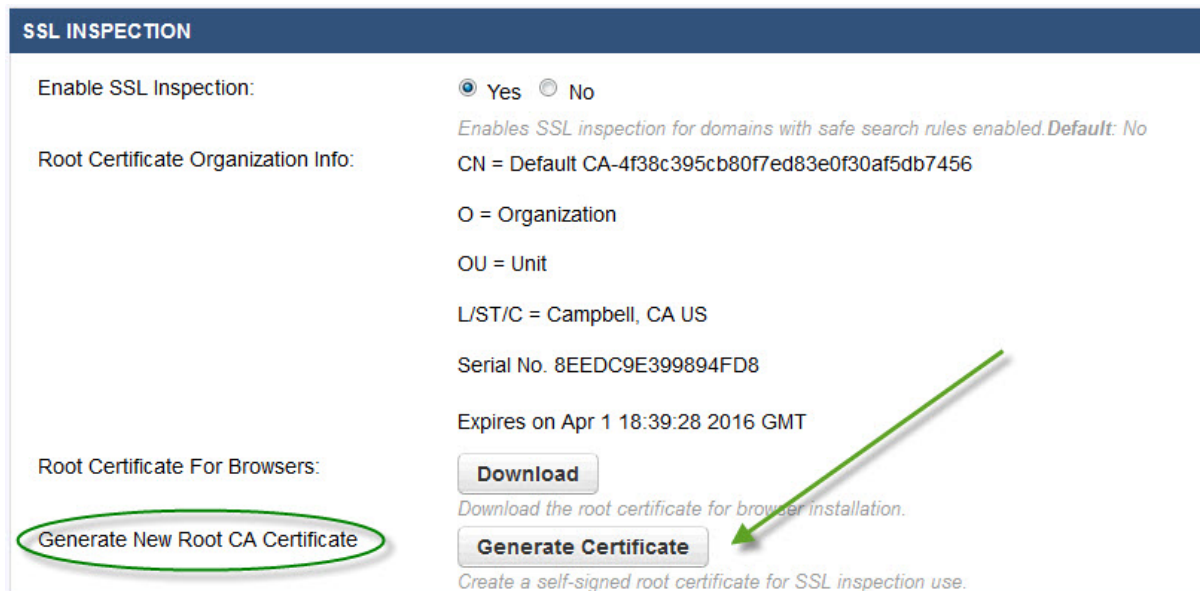
Use the Barracuda Web Security Gateway as a secure intermediary between HTTPS requests and destination web servers to apply granular control to applications and sub applications you want to block or allow. If you only need to block domains and content categories, then you can use the HTTPS Filtering feature instead. See [HTTPS Filtering With the Barracuda Web Security Gateway](#). SSL Inspection is a resource-intensive feature, and it can, under certain configurations, result in an impact on performance.

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.

Configure SSL Inspection for Barracuda Web Security Gateway 310

The Barracuda Web Security Gateway 310 Vx virtual machine does NOT support SSL Inspection.

1. Log in to the Barracuda Web Security Gateway web interface, and go to the **BLOCK/ACCEPT > Configuration** page.
2. Set **SSL Inspection** to *ON*.
3. Select whether to use the default Barracuda Networks root certificate or create your own self-signed certificate. Barracuda Networks recommends creating your own self-signed certificate. To create one, click **Create Certificate** and follow instructions.



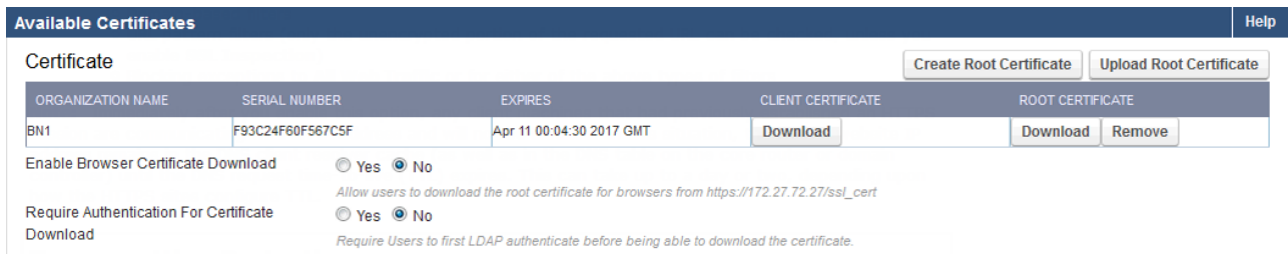
4. Click the **Download** button next to **Root Certificates For Browsers**, and save the file to the Trusted Root Certificate path. If the certificate is installed to the personal path, it will not work correctly. The certificate must be installed on all remote devices that will be SSL inspected.

As an administrator you may have methods of pushing the certificate to managed remote devices. For unmanaged devices, you may want to enable users to install the certificate in their browsers themselves. In this case you will need to provide them access to the certificate file. You can do so by emailing the certificate, or posting it on an internal network share, or posting it on a public or private web server.
5. Install the certificate file as a trusted root certificate in all client browsers. If you want to enable users to install the certificate in their browsers, see the note above.

SSL Inspection will then apply to any SafeSearch selections you make on the **BLOCK/ACCEPT > Content Filters** page.

Configure SSL Inspection for Barracuda Web Security Gateway 410 and higher

1. Log in to the Barracuda Web Security Gateway web interface, and go to the **ADVANCED > SSL Inspection** page.
2. Set **SSL Inspection** to *ON*.
3. Select whether to use the default Barracuda Networks root certificate or create your own self-signed certificate; Barracuda Networks recommends creating your own self-signed certificate. To create one, click **Create Root Certificate** under **Available Certificates** and follow instructions in the wizard. If you are deploying multiple Barracuda Web Security Gateways, you can upload a root certificate from one Barracuda Web Security Gateway to the others in the cluster. Use **Upload Certificate** to install the certificate.



4. Click the **Download** button in the table under **Client Certificate** for the certificate you want to install on clients and save the file to your trusted root certificate path. If the certificate is installed to the personal path, it will not work correctly. The certificate must be installed on all remote devices that will be SSL inspected.
5. Install the certificate file in all client browsers. If you want to enable users to install the certificate in their browsers, set **Enable Browser Certificate Download** to **Yes**. To require users to authenticate before downloading the certificate, set **Enable Browser Certificate Download** to **Yes**.
6. In most use cases, no further configuration is necessary for the Barracuda Web Security Gateway to SSL inspect sites and applications you specify on the **BLOCK/ACCEPT > Web App Control** page and the **BLOCK/ACCEPT > Web App Monitor** page. However, you can also choose to enter specific domains to exempt from SSL Inspection, and/or specific users, domains, networks or content filter categories to SSL inspect.

When to select specific domains or categories to SSL inspect You only need to specify specific domains or categories in the **Domains** or **Content Filter Categories** sections of the **ADVANCED > SSL Inspection** page if you need to SSL inspect web traffic for a domain that is not associated with any applications on the **BLOCK/ACCEPT > Web App Control** page.

7. Optional: configure specific *application of or exemption from* SSL Inspection. Click **Help** on the **ADVANCED > SSL Inspection** page for more configuration details.
 - **Inspected Domains** – Enter domain names that you want inspected and filtered at the URL level. You only need to specify domains to inspect if you want to show entire *URLs* in reports on web requests.
 - **Content Filter Categories** – Using the check boxes in the Categories List, you can add or remove content filter categories to/from the list of categories that you want to be

inspected.

- **Inspected Users/Groups** – If you want to add specific domains to inspect, you must first choose one or more users or groups (e.g. **All Users**, **Authenticated Users**, etc.) for which you want to apply SSL Inspection. Note that if you choose **Unauthenticated Users**, SSL Inspection will not be applied to Barracuda WSA clients because they are always authenticated with the Barracuda Web Security Gateway. Additionally, if you select an LDAP group, any Barracuda WSA users not in that group will not be subject to SSL Inspection.
- **Inspected Networks** – Enter the IP address and Netmask in the table for any network(s) for which you want to ssl inspect traffic.
- **Exempt Domains** – Optionally add any domains you want to bypass SSL Inspection. For example, if you have enabled any of the **SafeSearch** categories in the **Safe Browsing** section of the **BLOCK/ACCEPT > Content Filter** page, you might want to exempt one or more domains from Safe Search.

Advanced Settings

These features are configured in the **SSL Inspection Options** section of the **ADVANCED > SSL Inspection** page.

- **Enable SSLv2 Proxy Support** – To mitigate the risk of SSLv2 related POODLE vulnerability on the *internal* interface of the Barracuda Web Security Gateway, SSLv2 is turned off by default. If you have a legacy browser or web client inside the organization that is being SSL inspected and supports only SSLv2 or below, you could possibly experience an outage. Setting this feature to **Yes** enables SSLv2 for your legacy browser or web clients that use it, avoiding an outage.
- **Enable SSLv3 Proxy Support** – To mitigate the risk of SSLv3 related POODLE vulnerability on the *internal* interface of the Barracuda Web Security Gateway, SSLv3 is turned off by default. If you have a legacy browser or web client inside the organization that is being SSL inspected and supports only SSLv3 or below, you could possibly experience an outage. Setting this feature to **Yes** enables SSLv3 for your legacy browser or web clients that use it, avoiding an outage.
- **Use TLSv1 for SSL Inspection** – Client browsers can use either TLSv1.0, v1.1 or v1.2, in general, to connect to the Barracuda Web Security Gateway proxy. The proxy uses TLSv1.2 to connect to servers. This feature relates to the Barracuda Web Security Gateway server side setting and should be set to **Yes** if you want to perform selective SSL Inspection for websites that only support TLSv1.0. Otherwise, set to **No**.
- **Validate Certificates** – Setting to **Yes** means that, when doing SSL Inspection, the Barracuda Web Security Gateway will perform validation of the certificate of the server (website) the client is visiting in order to verify the identity of the server. Setting to **No** means that this check will not be performed. You might set this option to **No** if your firewall already performs this function.
- **Server Domain Checking** – Setting to **Yes** means that, when doing SSL Inspection with the **Validate Certificates** feature enabled, the Barracuda Web Security Gateway will check the **CN** field (Common Name) - or the **SAN** field (Subject Alternative Name), if present - in the server certificate, and verify whether or not it matches the domain name of the server. Setting to **No**

means that this check will not be performed. You might set this option to *No* if your firewall already performs this function.

SSL Inspection Modes by Model

Table 1.

MODEL COMPARISON	310	410	410 Vx	610	610 Vx	810	910	1010 / 1011
Remote Filtering Tab (WSA)	-	X	X	X	X	X	X	X
Safe Search	X(1)	X	X	X	X	X	X	X
Web Application Control	-	X	X	X	X	X	X	X
Web Application Monitoring	-	X		X	X	X	X	X

(1) Available with version 10.0 and above

The Barracuda Web Security Gateway 310 Vx does not support SSL Inspection.

Using SSL Inspection With the Barracuda Web Security Agent

If you have remote users with Macs or Windows laptops outside the network running the [Barracuda Web Security Agent \(WSA\)](#) with the Barracuda Web Security Gateway, you can configure the Barracuda Web Security Gateway to SSL Inspect HTTPS traffic. See [SSL Inspection With the Barracuda Web Security Agent](#).

Figures

1. 410SSIGenerateCert.jpg
2. SSLCertsTable12.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.