Using the Barracuda WSA With the Barracuda Web Security Gateway

https://campus.barracuda.com/doc/39822097/

The Barracuda Web Security Agent is supported for the Barracuda Web Security Gateway 410 and higher.

Filter Traffic from Remote Windows and Macintosh Laptops and Desktops

Use the Barracuda Web Security Agent (WSA) to filter web traffic, detect and block malware, and ensure safe browsing for off-network users. When you deploy the Barracuda WSA on each remote desktop, Mac OSX computer, or laptop, all web traffic for those clients is signed by the Barracuda WSA. The Barracuda WSA intercepts all HTTP/S and FTP traffic through any connection on the remote computer without regard to the type of web browser. This includes Ethernet, wireless, or dial-up connections. Browsing policies created on the Barracuda Web Security Gateway are then applied to that traffic as it is returned to the client in one of two ways:

- The Barracuda WSA proxies all web traffic over the Internet through a specified Barracuda Web Security Gateway, which can monitor traffic and apply web security policies before routing that traffic to the internet. With the Barracuda Web Security Gateway version 7.1 and higher, SSL Inspection is also available for this type of deployment on the Barracuda Web Security Gateway 410 and higher.
  - OR -
- The Barracuda WSA looks up and applies company policies to client web traffic before routing it to the internet, without the need to pass the traffic through the Barracuda Web Security Gateway. For this option, enable **Policy Lookup Only** mode from the **ADVANCED > Remote Filtering** page of the Barracuda Web Security Gateway. Note that when using **Policy Lookup Only** mode, SSL Inspection of HTTPS traffic is not available. See Policy Lookup Only Mode With the Barracuda Web Security Agent.

You can download the files required to install the Barracuda WSA for Windows or Macintosh and configure how it filters traffic for your remote users via the **ADVANCED > Remote Filtering** page in the Barracuda Web Security Gateway web interface.

The Barracuda WSA works with LDAP authenticated users.

Figure 1: The Barracuda WSA proxies off-network users' web traffic to the Barracuda Web Security Gateway.

Installing the Barracuda WSA

See How to Install the Barracuda WSA with the Barracuda Web Security Gateway for information on installing the Barracuda WSA on a Windows machine or a Macintosh OSX machine. Then, continue with the section below to configure the agent during and after installation.

- If you are installing on a Windows machine, please read the Release Notes - Barracuda Web Security Agent for Windows.
- If you are installing on a Macintosh, please read the Release Notes - Barracuda Web Security Agent for Macintosh.

Configuring Settings for the Barracuda WSA

All of the following settings, except for **Policy Lookup Only** Mode, can be configured from the Barracuda WSA client using the Configuration tool. The tool exposes the same settings that are configured from the administrative web interface of the Barracuda Web Security Gateway **ADVANCED > Remote Filtering** page.

However, each Sync event synchronizes the Barracuda WSA settings to those configured on the Barracuda Web Security Gateway **ADVANCED > Remote Filtering** page. A sync event is triggered by any of the following:

- User logging into Barracuda WSA
- A network change
- On the Macintosh client - Clicking the **Synchronize Settings** button in the WSA Preferences; on the Windows client - clicking on the Barracuda WSA icon in the task tray and selecting **Sync** to update local settings

For more information about the Configuration tool, see:

- For Windows: Configuration Tool for Barracuda WSA Windows Client 4.x or Configuration Tool for

Barracuda WSA Windows Client 5.0 and Above
- For Mac: Configuring Preferences for Barracuda WSA Macintosh Client.

Exceptions to Filtering with the Barracuda WSA

From the **ADVANCED > Remote Filtering** page, you can specify domains or subnets that should bypass filtering by the Barracuda Web Security Gateway as well as any existing proxies on the client's LAN for which traffic should bypass filtering.

Begin initial configuration of your Barracuda WSA installation by identifying all of your internal IP addresses and proxies, then entering those in the **Bypass Filter** and **Proxy Exception** text boxes on the **ADVANCED > Remote Filtering** page. This will exempt these IP addresses from traffic redirection. If you have a PAC or WPAD driven proxy setup, ensure that the proxy hosts are also listed as Proxy Exceptions. Also make sure to identify the external IP address of your Barracuda Web Security Gateway in the External Hostname/IP field so that the Barracuda WSA can direct user web traffic to that IP address.

Application Filtering with the Barracuda WSA

The Barracuda WSA automatically forwards web browser traffic on all ports, and forwards traffic from all other applications on ports 80 and 443. On the **ADVANCED > Remote Filtering** page you can specify how the Barracuda WSA filters application traffic by default (Default Filter Settings):

- Filter ports 80 and 443 for all applications
- Filter specified applications and allow all others
- Filter specified applications and block all others

If you have specific applications that use other ports, you can add them to the **Applications to Filter** (All Ports) list on the **ADVANCED > Remote Filtering** page. You can also list specific applications to always block, or specific applications to filter.

The Barracuda Web Security Gateway Vx virtual appliance does not support application blocking.

Using SSL Inspection for HTTPS Traffic With the Barracuda WSA

SSL Inspection of Barracuda WSA client traffic is currently available:

- Performed by the Barracuda Web Security Gateway. See instructions below to configure.
  - OR -
- SSL inspection is available *on the client itself*. This offloads resource intensive processing from the Barracuda Web Security Gateway:
  - When running version 2.0 or higher of the Barracuda WSA for Mac and version 11.0 or higher of the Barracuda Web Security Gateway. See Client-side SSL inspection with the Barracuda WSA to configure.
  - When running version 5.0 or higher of the Barracuda WSA for Windows and version 12.0 or higher of the Barracuda Web Security Gateway.

To filter and inspect HTTPS traffic such as Facebook posts, Google search terms, Skype chat and other encrypted traffic at the URL level, you can enable the SSL Inspection feature on the Barracuda Web Security Gateway.:

1. Go to the **ADVANCED > SSL Inspection** page to enable SSL Inspection. Follow instructions in the page to create, upload or use the default certificate, and then install it in the browsers of all remote machines running the Barracuda WSA.
2. Synchronize the Barracuda WSA client on all remote machines:
   1. On Windows clients: click on the Barracuda WSA icon in the task tray. **Sync Settings** to synchronize the client with the new setting on the Barracuda Web Security Gateway.
   2. On Macintosh clients: From the context menu, select **WSA Preferences**. On the **Barracuda Web Security Gateway** tab, click the **Synchronize Settings** button.

Note that, when SSL inspection is configured ON the Barracuda Web Security Gateway, Policy Lookup Only Mode must be set to **No** on the **ADVANCED > Remote Filteringg** page. For more information about SSL Inspection, see Using SSL Inspection With the Barracuda Web Security Gateway.

Figures

1. RemoteFilteringDiagram.png