How to Configure the Barracuda WSA With the Barracuda Web Security Gateway

https://campus.barracuda.com/doc/39822214/

Initial Configuration

Begin initial configuration of your Barracuda WSA installation by doing the following. After completing the steps in this article, continue with:

- For Windows: Configuration Tool for Barracuda WSA Windows Client 4.x (4.x) or Configuration Tool for Barracuda WSA Windows Client 5.0 and Above.
- For Mac: Configuring Preferences for Barracuda WSA Macintosh Client.

1. Log into the Barracuda Web Security Gateway web interface as **admin**.
2. On the **ADVANCED > Remote Filtering** page, 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. **Note**: It is recommended that you enter the *hostname* of your Barracuda Web Security Gateway in case the IP address of the appliance changes, which would interrupt service for your current Barracuda WSA installations in the field. If you do enter the IP address and must change it at some point, the following procedure is required to ensure minimal service interruptions:
    1. Create the new IP address forward on your network firewall while the existing/old Barracuda Web Security Gateway IP address is still accessible to Barracuda WSA installations.
    2. Enter the new IP address in this field so that the Barracuda WSA in the field can be updated with the new IP address of the Barracuda Web Security Gateway.
    3. Once all of your Barracuda WSA installations are updated with the new IP address, you can expire the old IP address.
3. Identify all of your internal IP addresses and proxies, then entering those in the **Bypass Filter** and **Proxy Exception** text boxes. 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**.
4. Create a port forward on your network firewall on port 8280 to the external IP address of your Barracuda Web Security Gateway (**External Hostname/IP**).
5. Click the **Help** button on the **ADVANCED > Remote Filtering** page for details on the above and other configuration options.

SSL Inspection and the Barracuda WSA

Available with the Barracuda Web Security Gateway 7.1 and higher

SSL Inspection on the Barracuda Web Security Gateway (server-side)

If you want the Barracuda Web Security Gateway to be able to monitor and block web traffic over HTTPS for Facebook applications, YouTube applications, Gmail and other sub-applications that run over HTTPS, you can enable SSL inspection on the Barracuda Web Security Gateway and for remote users running the Barracuda WSA. To configure the Barracuda Web Security Gateway to use SSL Inspection, see How to Configure SSL Inspection and the **ADVANCED > SSL Inspection** page in the Barracuda Web Security Gateway web interface. When you configure SSL Inspection on the Barracuda Web Security Gateway, all traffic from the Barracuda WSA is also subject to SSL Inspection automatically.

Note that SSL Inspection will not work when **Policy Lookup Only Mode** is enabled in the **ADVANCED > Remote Filtering** page on the Barracuda Web Security Gateway.

Client-side SSL Inspection

Client-side SSL Inspection is supported by the Barracuda Web Security Gateway 410 and higher:

- For the Mac: Running version 2.0 and higher of the Barracuda WSA and version 11.0 and higher of the Barracuda Web Security Gateway.
- For Windows: Running version 5.0 and higher of the Barracuda WSA and version 12.0 and higher of the Barracuda Web Security Gateway.

See Client-side SSL inspection with the Barracuda WSA for more information. Client-side SSL Inspection does not support Web Application Monitoring. If you are using that feature, then do not enable client-side SSL Inspection; rather, configure SSL Inspection on the Barracuda Web Security Gateway as described above, and all web traffic from any Barracuda WSA installations will be SSL inspected.

For more about how SSL Inspection works and why it is important, see Using SSL Inspection With the Barracuda Web Security Gateway.

Web Connectivity Issues and the Barracuda WSA

Once the Barracuda WSA is deployed for end users, the administrator can do any of the following to address any web connectivity issues users might have when using the Barracuda WSA on their remote laptops and PCs:

- Temporarily disable the Barracuda WSA if the user is experiencing any problems when they are logging into the network from a hotel or other captive portal. Check to see if the **Captive Portal** feature is enabled on the **BLOCK/ACCEPT > Configuration** page of your Barracuda

Web Security Gateway.

- Stop the Barracuda WSA service on the user’s laptop or PC. Uninstall the Barracuda WSA from the users’s laptop or PC. See related article on uninstalling the agent.
- Configure Fail Open and Fail Closed Modes with the Barracuda WSA.

© 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.