
Securing the Barracuda Web Security Gateway

<https://campus.barracuda.com/doc/54264981/>

Secure Deployment

You can deploy your Barracuda Web Security Gateway either behind your corporate firewall or in front of your corporate firewall in the DMZ. However, for maximum security, Barracuda Networks recommends deploying the Barracuda Web Security Gateway behind a corporate firewall. See [Deployment Options](#).

Securing Network Access

To secure your Barracuda Web Security Gateway on your network, begin by locking down the user interface ports. Barracuda Networks recommends using the non-standard port 8000 for internal access to the web interface, which is configured on the **BASIC > Administration** page. From that page you can also further limit access to the web interface by IP address with the **Administrator/IP Range** setting. If no IP address is specified in this field, all systems are granted access with the correct administrator password.

You can secure external access to the Barracuda Web Security Gateway with the **Web Interface HTTPS/SSL Port** setting on the **ADVANCED > Secure Administration** page. The recommended port is 443 because it is a standard **HTTPS/SSL** port used for secure web browser communication and because the identity of the remote-connected server can be verified with significant confidence. When this feature is enabled, all non-SSL connection requests coming through the web interface HTTP port (as designated on the **BASIC > Administration** page) are automatically re-directed to the **Web Interface HTTPS/SSL Port** you designate. To configure SSL-only access to the web interface, see [How to Enable SSL for Administrators and Users](#).

SSL Certificates

As described above, limiting user interface access to HTTPS provides further security and can also be configured on the **ADVANCED > Secure Administration** page along with the use of SSL certificates. There are three types of SSL certificates to choose from:

- Default (Barracuda Networks)
- Private (self-signed)
- Trusted certificate - a certificate signed by a trusted certificate authority (CA)

For more information about the types of certificates and how to configure them, click **Help** on the **ADVANCED > Secure Administration** page.

Limiting Access to the API

The Barracuda set of APIs provides for remote administration and configuration of the Barracuda Web Security Gateway. By using the Barracuda Web Security Gateway APIs, IT administrators can easily manage large blocks of usernames, create local or IP groups, and configure some single global variables. For more information, see [Barracuda Web Security Gateway API Guide](#).

To limit access to the API, use the **Allowed SNMP and API IP/Range** setting on the **BASIC > Administration** page. The IP addresses you enter in that field can also establish an SNMP connection to the system. To secure use of the API, you must also create an API password, which can be entered on the same page.

© Barracuda Networks Inc., 2019 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.