Securing the Barracuda Email Security Gateway

https://campus.barracuda.com/doc/9011839/

Secure Deployment

You can deploy your Barracuda Email Security Gateway behind your corporate firewall or in front of your corporate firewall in the DMZ. However, for maximum security, Barracuda Networks recommends deploying the Barracuda Email Security Gateway behind a corporate firewall as described in Deployment Behind the Corporate Firewall.

Securing Network Access

To secure your Barracuda Email 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 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, then all systems are granted access with the correct administrator password.

Barracuda Networks strongly recommends securing external access to the Barracuda Email Security Gateway by using the **Web Interface HTTPS/SSL Port** setting on the **ADVANCED > Secure Administration** page. Barracuda Networks recommends using port 443 because it is a standard **HTTPS/SSL** port that is used for secure web browser communication, and the identity of the remotely connected server can be verified with significant confidence. To configure SSL-only access to the web interface, see How to Enable SSL for Administrators and Users.

> If per-user quarantine is enabled as well as HTTPS, users will be redirected to HTTPS access if they are trying to access their quarantine inbox.

Integration with External Systems and Services - Security Considerations

The Barracuda Email Security Gateway integrates with other systems and services in your environment, like your LDAP server and mail servers. Barracuda Networks recommends creating separate service accounts for these integration points, rather than personal accounts, and then using the principle of least privilege. This integration strategy is part of an overall security policy.

See Security for Integrating with Other Systems - Best Practices for more information.

SSL Certificates

As described above, Barracuda Networks stronglyrecommends limiting user interface access to HTTPS to provide the best security, and can 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)

Configuring SSL certificates is described in How to Enable SSL for Administrators and Users as well as in the online help of the **ADVANCED > Secure Administration** page.

Secure Links in Notification Emails

If **Per-User quarantine** (as opposed to Global) is configured on the **BASIC > Quarantine** page, Barracuda Networks recommends securing hyperlinks in quarantine correspondence emails that are sent from the Barracuda Email Security Gateway to users and administrators. Setting **Use HTTPS Links in Emails** to *Yes* on the **ADVANCED > Secure Administration** page ensures that these emails sent from the Barracuda Email Security Gateway contain only HTTPS links.

Use the Cloud Protection Layer

Using the Cloud Protection Layer (CPL) feature means that all email going into your organization is pre-filtered for spam, viruses, phishing and other malware threats before it reaches your network. This feature requires using Barracuda Cloud Control and validating your domain ownership with the cloud service. To use this feature, please see Cloud Protection Layer for details on configuration.

Limiting Access to the API

The Barracuda Networks set of APIs provides for remote administration and configuration of the Barracuda Email Security Gateway. See the Barracuda Email Security Gateway API Guide for more detailed information. Common settings, such as IP addresses and spam scoring levels, that you can

set by clicking the **Save Changes** button in the web interface, can be configured via the APIs.

To limit access to the APIs, 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.

Help Users to Avoid Potentially Malicious Senders

To warn recipients in the organization to exercise caution when clicking on links or attachments in messages from potentially unknown and/or malicious senders, set the **Inbound External Sender Warning** option on the **BASIC > Administration** page to *Yes.* Enabling this option means that a header with following text is added to an inbound email if it is from a domain that is not configured on the Barracuda Email Security Gateway:

CAUTION: This email originated from outside your organization. Exercise caution when opening attachments or clicking links from unknown senders.

You can customize this text by entering the message you want to use for the header in the **Custom Header Text** box as well as in HTML format in the **Custom Header HTML** box. If the email part is text, the *text* template will be used. If the email part is HTML, the HTML part will be used.

Tracking Changes to the Configuration and User Login Activities

The syslog function of the Barracuda Email Security Gateway provides two kinds of logs, capturing:

- User login activities and any configuration changes made on the device.
- Data related to mail flow. This data is the same information as that used to build the Message Log in the Barracuda Email Security Gateway.

From the **ADVANCED > Troubleshooting** page, click **Monitor Web Syslog** to view the web syslog output. You can also configure a syslog server as described in Using a Syslog Server to Centrally Monitor System Logs.

Limiting User Access

Securing User Access With Single Sign-On

Single Sign-On is a per-domain setting available on the Barracuda Email Security Gateway 400 and higher.

With **Single Sign-On** (SSO), users can log into their quarantine inbox via the web interface using their domain passwords instead of a password managed separately by the Barracuda Email Security Gateway. **Single Sign-On** is configured at the domain level by either the Administrator or a Domain Admin. See Roles and Navigating the Web Interface for more detail about how roles work.

Note that, if you are using LDAP authentication for single sign-on, you can either use the same LDAP server and settings for user authentication as the one you're using for recipient verification (configured on the **USERS > LDAP Configuration** page), or you can configure a separate LDAP server for single sign-on from the **USERS > Single Sign-On** page. Please see the help on that page for specifics about LDAP server settings to understand how they affect user logins and access to their quarantine inbox.

Important

If enabling **Single Sign-On** for a domain, you should also configure **HTTPS/SSL Access Only** at the global level on the **ADVANCED > Secure Administration** page to protect the transmission of network passwords. See How to Enable SSL for Administrators and Users to configure SSL access only to the web interface of the Barracuda Email Security Gateway.

User Account Authentication

You can configure the Barracuda Email Security Gateway to authenticate user accounts using an LDAP, POP, or RADIUS server. This feature is available on the Barracuda Email Security Gateway 400 and higher and is configured at the domain level, not as a global setting. These user account authentication mechanisms are configured from the **DOMAINS** tab by selecting the Domains page and clicking the **Manage Domain** link for a particular domain.

To configure authentication, navigate to the **USERS > Single Sign-On** page for the selected domain and select the **Authentication Type**. For RADIUS and POP, fill in the server settings on the page. To require users to log in to the Barracuda Email Security Gateway web interface (as opposed to single sign on) to view and manage their account, select *Local* for Authentication Type.

LDAP and User Account Authentication

Configure LDAP settings on the **USERS > LDAP Configuration** page. LDAP server types supported include Active Directory, Open LDAP, Novell eDirectory and Domino Directory. You can configure

LDAPS (SSL/TLS) for encryption of LDAP queries between the Barracuda Email Security Gateway and your LDAP server. LDAPS can optionally be required. As stated above, these settings are domain-specific.

If you select LDAP authentication, you can configure the **Exchange Accelerator/LDAP Verification** feature on the **USERS > LDAP Configuration** page as follows:

- Setting to *Yes* means that LDAP lookups for recipient verification for the domain will be performed based on settings on the page.
- Setting to *No* means that the Barracuda Email Security Gateway will default to SMTP verification through RCPT TO commands.

See also: Roles and Navigating the Web Interface