Barracuda Email Security Gateway 30-Day Evaluation Guide

https://campus.barracuda.com/doc/24215924/

Where to start

Begin with the Getting Started section for installation and setup instructions, or use the 2-sided 8.5 x 11" Barracuda Email Security Gateway Quick Start booklet that is included in the box with Barracuda Email Security Gateway. If you have the Barracuda Email Security Gateway Vx virtual machine, start with Virtual Deployment , then return to this page to find hints and guidelines for your 30-day evaluation process.

If you have a Barracuda Email Security Gateway model 600 or higher, a sales engineer is automatically assigned to help you make the most of your 30-day evaluation of Barracuda Email Security Gateway. If you have not yet been contacted by a Barracuda sales engineer, call your reseller or sales representative .

Initial Setup

1. Choose your Deployment Option.
2. Determine whether or not you want to use the Quarantine feature of the Barracuda Email Security Gateway. See Quarantine Options for more details about each quarantine option listed below. By default, the Barracuda Email Security Gateway does *not* quarantine incoming messages, but you may want to enable quarantine if, for example, your organization requires it, or if you want to reduce load on the mail server while giving users a chance to determine what they consider to be "spam" or "not spam". Choose between:
   - Global quarantine – Administrator manages one general quarantine mailbox for all users.
   - Per-user quarantine – Each user has a personal quarantine inbox and can have multiple email accounts associated with that quarantine account. Configure on the **BASIC > Quarantine** page. You might want to try out global quarantine first, adjust scoring and test out block/accept policies, and then configure per-user quarantine if that is the ultimate configuration you want.
   - Quarantine OFF – Turning quarantine off reduces administrator tasks.

Common Use Cases

You are encouraged to work with your Barracuda reseller or sales representative if you have questions about your inital setup, or feel free to call Barracuda Networks Technical Support to discuss how to best deploy and test the Barracuda Email Security Gateway in your network.

Here are a few common use cases and guidelines to prepare you for success.

Use Case: Spam And Virus Protection

The twelve layers of spam and virus protection are, by default, set up for basic protection of your mail server and network.

1. You can further calibrate settings for spam scoring, tagging, blocking and quarantine levels on the **BASIC > Spam Scoring** page.
2. Set filters for attachments, content, recipient and sender rules on the **BLOCK/ACCEPT** pages.

Test Spam and Virus Scanning With a Local User Set

From the **ADVANCED > Explicit Users** page, you have the option to use the **Explicit Users to Scan For** feature to test a subset of locally defined users before fully deploying the Barracuda Email Security Gateway.
To tune your spam settings, continue with How to Tune and Monitor the Default Spam and Virus Settings.

Configure routing of outbound mail

If you will be routing outbound mail through the Barracuda Email Security Gateway, continue with Routing Outbound Mail

Use Case: Email Continuity

The Cloud Protection Layer is included as a cloud-based feature of the Barracuda Email Security Gateway that protects your mail server from malware and DoS attacks, providing email continuity (spooling of email) for up to 4 days if your mail server goes down. The CPL processes mail before it arrives at the Barracuda Email Security Gateway and filters out normal spam before it ever touches the network's perimeter. The CPL saves resources to maximize performance of the appliance. The administrator can view a status (dashboard) page showing email statistics for both the CPL and the Barracuda Email Security Gateway. To use the CPL, see How to Set Up Your Cloud Protection Layer.

Use Case: Data Loss Prevention (DLP)

For health care providers, governmental agencies and other entities who need to protect private,

sensitive and valuable information communicated via email, the Barracuda Email Security Gateway provides optional DLP (Data Loss Prevention) with your Energize Updates subscription. DLP enables your organization to satisfy email compliance filtering for corporate policies and government regulations such as HIPAA. Advanced content scanning is applied for keywords inside the subject line, message body or commonly used text attachments, as well as email encryption.You can configure email encryption per domain. Encryption applies to *outbound* mail.

While encryption is configured at the per-domain level, actual encryption *policy* (by sender domain, email address, recipient, etc.) is only configurable at the global level using the **BLOCK/ACCEPT** pages. These global encryption policies will apply to all domains from which encrypted email messages are sent.

To test DLP Encryption:

1. Configure encryption per the **ADVANCED > Email Encryption** page for each domain.
2. Set your encryption policies for outbound mail using the **BLOCK/ACCEPT** pages.
3. Create two user accounts and send some email from one user to the other that tests your encryption policies.
4. Use the Barracuda Message Center to check for the encrypted email.