



Version 3 Features Overview

Barracuda Spam Firewall

Due in great part to input from our customers, the Barracuda Spam Firewall has been greatly enhanced in the latest firmware release. Because of the number of new features, we have created this document to provide an overview of this newly added functionality. If you have any questions or comments after reading this document, please call us at (408) 342-5400 or email us at support@barracudanetworks.com.

Feature List

The following features are new to the Barracuda Spam Firewall version 3. Note that some features may not be available on all models. A short summary of each feature follows.

- Alias Linking
- Single Sign-On
- Secure Sockets Layer (SSL) Support
- Cluster Synchronization
- Internationalization/User Interface Localization
- Customizable Non-Delivery Report (NDR) Messages
- Full Regular Expression Support For Subject/Header Filters
- Sender Policy Framework (SPF)/Caller-ID (aka Sender ID)
- Troubleshooting Tools

Alias Linking (Account Unification)

In prior firmware releases, unless domain linking was enabled, a user needed to manage a separate quarantine account for every email address they were receiving mail for. Using alias linking, a user with multiple email addresses need only manage one quarantine inbox and one set of preferences. Alias linking uses LDAP to automatically determine if multiple email addresses belong to the same user.

Single Sign-On

A common problem in many organizations is password management. The Barracuda Spam Firewall contains functionality to manage user passwords locally, but this requires users to maintain a separate password for their quarantine area. With the new Single Sign-On functionality, users can log into the Barracuda using their domain passwords through LDAP/Active Directory. RADIUS support for single sign-on will be available in an upcoming release.

SSL

Support for SSL is now included in the web-based interface. Although unnecessary for keeping passwords secure in prior releases because they were "hashed" prior to transmission to the server, session encryption has become important since Single Sign-On may require that passwords be passed to the server in their original form. If you are not utilizing Single Sign-On, then SSL is not required to keep your passwords secure. SSL not only ensures that the passwords are encrypted, but also ensures that the rest of the data transmitted and received is encrypted as well.

The Barracuda Spam Firewall ships with a default certificate used for SSL connections that will generate browser alerts. If you wish to remove this warning, you can generate a signing request for upload to a certificate authority. The validated certificate can then be loaded into the Barracuda for use in your SSL connections.



Version 3 Features Overview

Barracuda Spam Firewall

Cluster Synchronization

The Barracuda Spam Firewall will now synchronize configuration settings, for both global and per user preferences, between machines in a defined cluster. This allows a user to make changes on one “master” machine and have those changes propagate to all other “slave” machines automatically. It also provides 100% redundant coverage of user settings, Message Logs and Bayesian databases.

Internationalization/User Interface Localization

The interface used in the Barracuda now fully supports languages other than English (including some multi-byte languages). Currently supported languages include: English, Japanese, Chinese (Traditional and Simplified), and German. Other languages are being developed and will be available in upcoming firmware releases.

Customizable NDR Messages

Bounce messages that are sent out are now customizable. Separate text can be created for a virus notification to the sender, a virus notification to the recipient, a spam notification to the sender, a Banned File notification to the sender, and a Banned File notification to the recipient.

Full Regular Expressions Support For Subject/Header Filtering

Prior versions of the Barracuda Spam Firewall limited the subject and header filters to a small subset of regular expressions. They have been enhanced to support the full set of regular expressions in the same way as Body Filtering.

Sender ID

Support for SPF and Microsoft’s Caller-ID, now often referred to as Sender ID, are included in the Barracuda Spam Firewall. This functionality allows the firewall to test the validity of an email server that is sending mail from a particular domain. If enabled by the sender, the firewall can locate a list of the sender’s “valid” email server IP’s and then verify that the email originated from a valid email server. If this feature is enabled, and the Barracuda Spam Firewall determines that the email wasn’t sent from an authorized email server, it will block that email.

Troubleshooting Tools

Support for various tools for troubleshooting network problems are now available in the web GUI. The available tools include:

- A way to initiate a diagnostic session for Barracuda Support personnel
- A way to initiate a ping command
- A way to initiate a telnet command (although non-interactive, can be used to test connectivity)
- A way to initiate a Dig/NS-Lookup command
- A way to initiate a TCP Dump of the network traffic