Barracuda Spam Firewall User's Guide

Copyright

Trademarks

Contents

Chapter 1 Introduction

This chapter provides an overview of the Barracuda Spam Firewall and includes the following topics:

- Overview (on this page).
- Barracuda Spam Firewall Models (page 10).
- Technical Support (page 10).
- Warranty Policy (page 10).
- Locating Information in this Document (page 11).

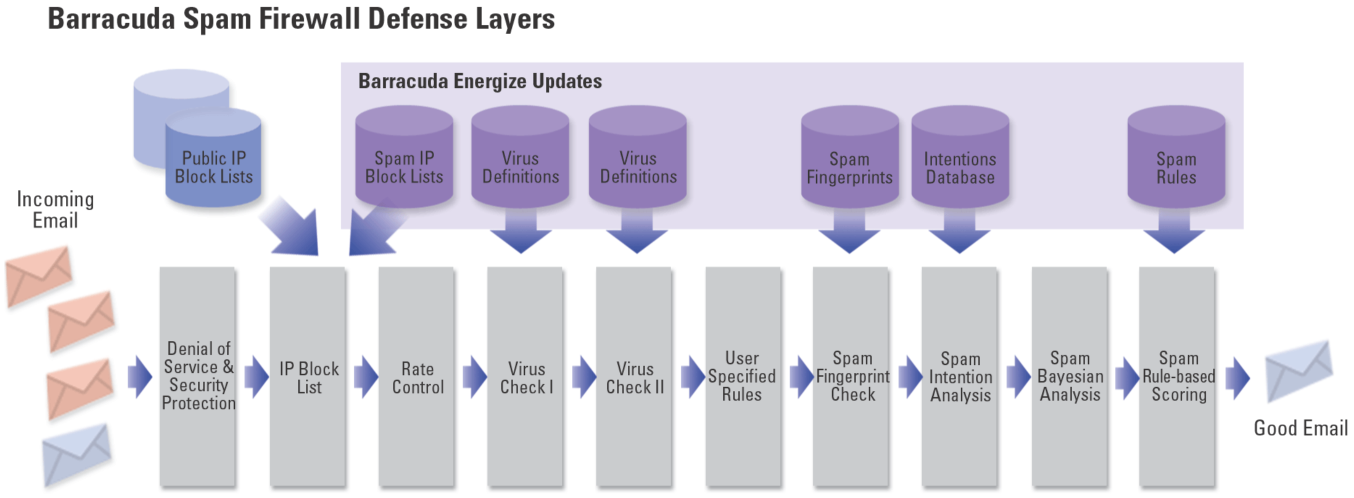
Overview

The Barracuda Spam Firewall is an integrated hardware and software solution that provides powerful and scalable spam and virus-blocking capabilities that do not bog down your email servers. The system has no per-user license fee and can scale to support tens of thousands of active email users.

Using the web-based administration interface, you can configure up to ten defense layers that protect your users from spam and viruses. The ten defense layers are:

- Denial of service and security protection
- IP block list
- Rate control
- Virus check with archive decompression
- Proprietary virus check
- User-specified rules
- Spam fingerprint check
- Intention analysis
- Bayesian analysis
- Rule-based spam scoring

The following figure shows each of these defense layers in action.



Energize Updates Minimize Administration and Maximize Protection

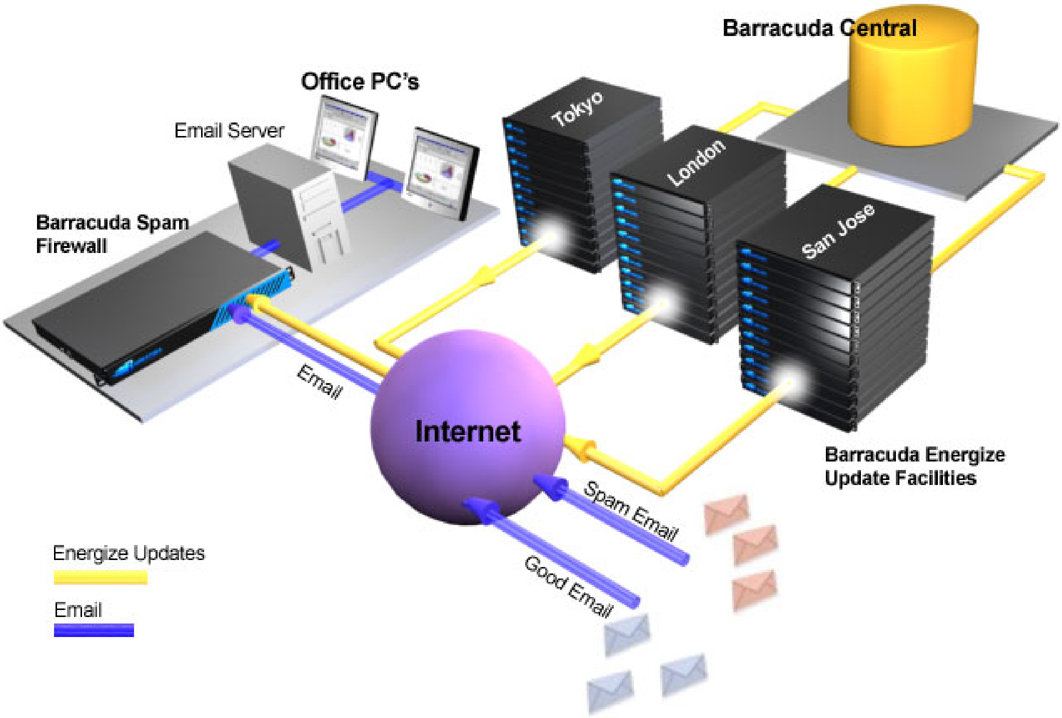
To provide you with maximum protection against the latest types of spam and virus attacks, Barracuda Networks maintains a powerful operations center called Barracuda Central. From this center, engineers monitor the Internet for trends in spam and virus attacks and post updated definitions to Barracuda Central. These updates are then automatically retrieved by your Barracuda Spam Firewall using the Energize Update feature.

By spotting spam trends early on, the team at Barracuda Central can quickly develop new and improved blocking techniques and virus definitions that are quickly made available to your Barracuda Spam Firewall.

Energize Updates provide your Barracuda Spam Firewall with the following benefits:

- Access to known offending IP addresses
- Known spam messages instantly blocked
- Known spam content blocked
- Virus definitions constantly updated

The following figure shows how Barracuda Central provides the latest spam and virus definitions through the Energize Update feature.



Understanding Spam Scoring

The Barracuda Spam Firewall examines all the characteristics of a message and uses a complex system of scores to determine whether a message is spam. When an email reaches the spam scoring filter, the Barracuda Spam Firewall assigns scores to all the properties of the message.

For example, the Barracuda Spam Firewall examines:

- A message's header and subject line for offending characters or words
- The percentage of HTML in the message
- Whether a message contains an 'unsubscribe' link

These properties (along with many others) help the Barracuda Spam Firewall determine a message's spam score, which is displayed on the Message Log page of the administration interface.

The Energize Update feature keeps the spam rules and scores up-to-date so the Barracuda Spam Firewall can quickly counteract the latest techniques used by spammers.

Barracuda Spam Firewall Models

The Barracuda Spam Firewall comes in four models. Refer to the following table for the capacity and features available on each.

Feature	Model 200	Model 300	Model 400	Model 600
Email capacity per day	1 million	4 million	10 million	25 million
Active email users	1,000	2,000	10,000	25,000
Domains	50	250	500	5,000
Compatible with all email servers	✓	✓	✓	✓
Hardened and secure OS	✓	✓	✓	✓
Spam blocking	✓	✓	✓	✓
Virus scanning	✓	✓	✓	✓
Web-based administration interface	✓	✓	✓	✓
Per-user settings and quarantine		✓	✓	✓
MS Exchange/LDAP Accelerator		✓	✓	✓
Syslog support		✓	✓	✓
Clustering			✓	✓
Redundant Disk Array (RAID)			✓	✓
SNMP Support			✓	✓
Per-user score settings				✓
Customizeable Branding				✓

Technical Support

To contact Barracuda technical support:

- By phone, call (408) 342-5400, (888) Anti-Spam, or (888) 268-4772
- By email, use *support@barracudanetworks.com*
- User forum: *http://forum.barracudanetworks.com*

Warranty Policy

The Barracuda Spam Firewall has a 90 day warranty against manufacturing defects.

Locating Information in this Document

Refer to the following table to locate information for a specific page in the administration interface.

Admin Interface Page	Refer to...
BASIC Tab	
Status	Viewing System Status and Statistics on page 22
Message Log	Monitoring and Classifying Incoming Messages on page 24
Spam Scoring	Configuring the Spam Settings on page 28
Virus Checking	Enabling and Disabling Virus Checking and Notification on page 29
Quarantine	Setting Up Quarantine on page 29
IP Configuration	Configuring System IP Information on page 32
Administration	Controlling Access to the Administration Interface on page 33 Resetting and Shutting Down the System on page 34 Automating the Delivery of System Reports on page 35 Viewing Message Details on page 27
Bayesian/Fingerprinting	Changing the Fingerprinting Behavior on page 46 Classifying Messages From Mail Clients on page 26 *(not supported in model 200)* Resetting the Bayes Database on page 35
BLOCK/ACCEPT Tab	
External Blacklists	Subscribing to Blacklist Services on page 36
IP Block/Accept	Filtering by IP Address/Network on page 37
Sender Domain Block/Accept	Filtering by Sender Domain on page 38
Email Sender Block/Accept	Filtering by Sender Email Address on page 38
Email Recipient Block/Accept	Filtering by Recipient Email Address on page 39
Attachment Filtering	Filtering by Attachment Type on page 39
Subject Filtering	Filtering by Subject Line on page 40
Body Filtering	Filtering by Body Contents on page 41
Header Filtering	Filtering by Header Contents on page 41
USERS Tab	
Account View	Viewing User Accounts on page 57
User Features	Assigning Features to User Accounts on page 59
User Add/Update	Creating New User Accounts on page 60
User Backup/Restore	Backing Up and Restoring User Settings on page 60
DOMAINS Tab	
Domain Manager	Managing and Configuring Domains on page 54 Editing Domain Settings on page 54 *(not supported in models 200/300)* Preventing Dictionary Attacks Using Barracuda MS Exchange Accelerator on page 55 *(not supported in model 200)*

Admin Interface Page	Refer to...
ADVANCED Tab	
Email Protocol Checking	Setting Email Protocol Checking on page 47
Rate Controls	Configuring Message Rate Control on page 49
Explicit Users	Activating Individual Accounts on page 49.
Configuration Backup/Restore	Backing Up and Restoring System Configuration on page 42
Energize Updates	Updating Spam and Virus Definitions Using Energize Updates on page 44
Firmware Update	Updating the System Firmware Version on page 49
Appearance	Customizing the Appearance of the Administration Interface on page 45 *(not supported in models 200/300/400)*
Syslog	Using a Syslog Server to Centrally Manage System Logs on page 50 *(not supported in model 200)*
Clustering	Setting Up Clustered Environments on page 51 *(not supported in model 200/300)*
Single Sign-on	Implementing Single Sign-on on page 52 *(not supported in model 200/300)*
SSL	Enabling SSL on page 60
Spam Rule Management	Localizing the Spam Settings on page 53
Bounce/NDR Messages	Customizing Non-Delivery Reports (NDRs) on page 62
Troubleshooting	Troubleshooting on page 63

Chapter 2 Setting Up the Barracuda Spam Firewall

To set up your Barracuda Spam Firewall, follow the process below:

1. Install the Barracuda Spam Firewall (in the next section).
2. Set the System IP Address (page 14).
3. Configure the Barracuda Spam Firewall (page 14).
4. Configure your Corporate Firewall and Update the Firmware (page 16).
5. Route Incoming Email by Modifying MX Records (page 17).
6. Post-Installation Steps (page 17).

The end of this chapter also provides example installation scenarios you can use as a reference to help integrate the Barracuda Spam Firewall into your network environment.

Installing the Barracuda Spam Firewall

To physically install the Barracuda Spam Firewall:

1. Install the Barracuda Spam Firewall in a standard 19-inch rack or other stable location.

   Warning: Do not block the cooling vents located on the front and rear of the unit.

2. Connect a CAT5 Ethernet cable to the back of the Barracuda Spam Firewall.

   The Barracuda Spam Firewall supports both 10BaseT and 100BaseT Ethernet. We recommend a 100BaseT connection for best performance.

   Note: The Barracuda Spam Firewall 600 supports Gigabit Ethernet and has two usable LAN ports. On the 600 model, plug the Ethernet cable into the LAN 2 port.

   Do not connect any other cables to the other connectors on the unit. These connectors are for diagnostic purposes.

3. Connect a power cord to the unit.

4. Press the **Power** button located on the front of the unit

   The power light on the front of the system turns on. For a description of each indicator light, refer to Understanding the Indicator Lights on page 22.

Setting the System IP Address

The Barracuda Spam Firewall is given a default IP address of 192.168.200.200. You can change this address by doing either of the following:

- Connecting directly to the Barracuda Spam Firewall and specifying a new IP address through the console interface, or
- Pushing and holding the RESET button on the front panel. Holding the RESET button for 8 seconds changes the default IP address to 192.168.1.200. Holding the button for 12 seconds changes the IP address to 10.1.1.200.

To connect directly to the Barracuda Spam Firewall to set a new IP address:

1. Attach a standard VGA monitor and PS2 keyboard to the back panel of the Barracuda Spam Firewall.

   The “Barracuda login:” prompt displays on the monitor.

2. Enter **admin** for the login and **admin** for the password.

   The User Confirmation Requested window displays the current IP configuration of the system.

3. Using your Tab key, select **Yes** to change the IP configuration.
4. Enter the new IP address, netmask and default gateway for the Barracuda Spam Firewall, and select **OK** when finished.
5. Select **No** when prompted if you want to change the IP configuration.

Configuring the Barracuda Spam Firewall

After specifying the IP address of the system, you need to configure the Barracuda Spam Firewall from the administration interface. Make sure the computer from which you are configuring the Barracuda Spam Firewall is connected to the same network and the appropriate routing is in place to allow connection to the Barracuda Spam Firewall’s IP address via a web browser.

To configure the Barracuda Spam Firewall:

1. From a web browser, enter the IP address of the Barracuda Spam Firewall that you specified in the previous section, followed by port 8000.

   Example: *http://192.168.200.200:8000*

2. If you are prompted for login information, enter **admin** for the username and **admin** for the password.

3. Go to the BASIC-->IP Configuration page and enter the required information.

   The following table describes the fields you need to populate.

Fields	Description
TCP/IP Configuration	The IP address, subnet mask, and default gateway of the Barracuda Spam Firewall. TCP port is the port on which the Barracuda Spam Firewall receives inbound email. This is usually port 25.
Destination Mail Server TCP/IP Configuration	The hostname or IP address of your destination email server, for example *mail.yourdomain.com*. This is the mail server that receives email after it has been checked for spam and viruses. You should specify your mail server’s hostname rather than its IP address so the destination mail server can be moved and DNS updated at any time without any changes to the Barracuda Spam Firewall. TCP port is the port on which the destination mail server receives inbound email. This is usually port 25. If you need to set up more than one domain or mail server, refer to Managing and Configuring Domains on page 54.
DNS Configuration	Lists the primary and secondary DNS servers you use on your network. It is strongly recommended that you specify a primary and secondary DNS Server. Certain features of the Barracuda Spam Firewall, such as a Fake Sender Domain detection, rely on DNS availability.
Domain Configuration	Default Hostname is the hostname to be used in the reply address for email messages (non-delivery receipts, virus alert notifications, etc.) sent from the Barracuda Spam Firewall. The hostname is appended to the default domain. Default Domain is the domain name to be used in the reply address for email messages (non-delivery receipts, virus alert notifications, etc.) sent from the Barracuda Spam Firewall.
Allowed Email Recipients Domain(s)	The domains managed by the Barracuda Spam Firewall. Make sure this list is complete. The Barracuda Spam Firewall rejects messages for domains that are not listed. To allow messages for all domains that match your mail server, put an asterisk (*) in this field. *Note: One Barracuda Spam Firewall can support multiple domains and mail servers. If you have multiple mail servers, go to the DOMAINS tab and enter the mail server associated with each domain.*

4. Click **Save Changes**.

   If you changed the IP address, you are disconnected from the Barracuda Spam Firewall and will need to log in again using the new IP address.

5. Go to the BASIC-->Administration page and do the following:
   a. Assign a new administration password to the Barracuda Spam Firewall (optional).
   b. Make sure the local time zone is set correctly.

      Time on the Barracuda Spam Firwewall is automatically updated via NTP (Network Time Protocol) and therefore requires port 123 to be open for inbound and outbound UDP traffic on your firewall (if the Barracuda Spam Firewall is located behind one).

      It is important that the timezone be set correctly because this information is used to determine the delivery times for messages and may appear in certain mail reading programs.
   c. Click **Save Changes**.

Your Barracuda Spam Firewall is now configured and will start filtering all emails it receives and route the good email to your email server.

Configuring your Corporate Firewall and Updating Firmware

If your Barracuda Spam Firewall is located behind a corporate firewall, you need to open specific ports to allow appropriate communication between the system and remote servers. You can then download the latest firmware version (if needed) for the Barracuda Spam Firewall.

To configure your corporate firewall and download the latest firmware version:

1. Configure your corporate firewall. Refer to the following table for the ports that need to be opened.

Port	Direction	Protocol	Usage
22	In	TCP	Remote diagnostics and service (optional)
25[1]	In/Out	TCP	Email and email bounces
53	Out	TCP	Domain Name Server (DNS)
80	Out	TCP	Virus, firmware and spam rule updates
123	Out	UDP	NTP (Network Time Protocol)
2703	Out	TCP	Incoming email fingerprints
6277	Out	TCP	Incoming email fingerprints

[1] When your Barracuda Spam Firewall is behind a corporate firewall, you need to do a port redirection (also called port forwarding) of incoming SMTP traffic (port 25) to the Barracuda Spam Firewall.

2. If appropriate, change the NAT routing of your corporate firewall to route incoming email to the Barracuda Spam Firewall. Consult your corporate firewall documentation or your corporate firewall administrator to make the necessary changes.

3. Upgrade the firmware on the Barracuda Spam Firewall:

    a. Go to the ADVANCED-->Firmware Update page.

    b. Click **Download Now** to begin downloading the latest firmware version.

    Updating the firmware may take several minutes. Do not turn off the unit during this process.

    The **Download Now** button will be disabled if the system already has the latest firmware version.

4. Backup the system configuration as described in Backing Up System Data on page 42.

Routing your Incoming Email by Modifying MX Records

If your Barracuda Spam Firewall is in the DMZ (not protected by your corporate firewall), change your DNS MX Records to route incoming email to the Barracuda Spam Firewall.

Warning: Do not try to route outgoing email through the Barracuda Spam Firewall. The unit cannot route or operate as a mail relay for outgoing mail. You need to route your outbound email through your existing email server. The only outbound email from the Barracuda Spam Firewall will be bounced or rejected messages.

Changing your DNS MX Record is normally done at your DNS server or DNS service. If you are changing your DNS MX Record you need to create a DNS entry for the Barracuda Spam Firewall.

The following example shows a DNS entry for a Barracuda Spam Firewall with a name of *barracuda* and an IP address of *66.233.233.88*:

```
barracuda.yournetwork.com     IN A          66.233.233.88
```

The following example shows the associated MX record with a priority number of 10:

```
IN MX 10    barracuda.yournetwork.com
```

Post-Installation Tasks

After you install the Barracuda Spam Firewall, the unit begins filtering incoming email based on the default system settings. For example, the unit automatically checks incoming email for viruses and uses the Barracuda blacklist service to identify spam.

These default settings allow the system to filter out most spam. However, you should customize some of the settings based on your unique environment.

The following table describes the most common tasks you should perform when first setting up your system. Refer to the next chapter for a complete list of configuration tasks.

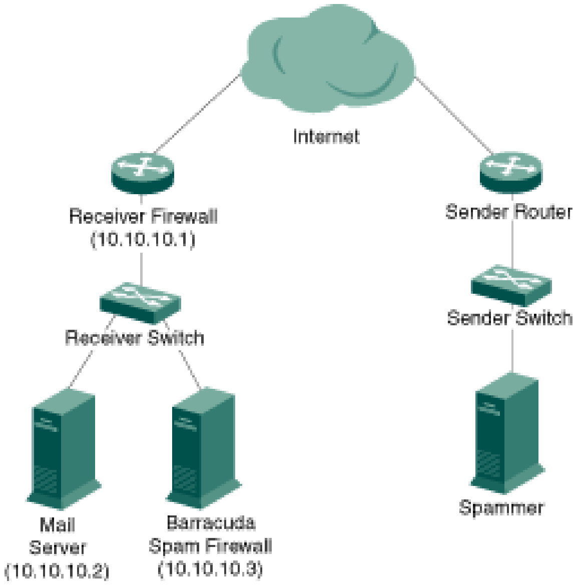
Task	Refer to
Monitor and Classify Incoming Emails	Monitoring and Classifying Incoming Messages on page 24
Verify the Spam Scoring Defaults	Configuring the Spam Settings on page 28
Set Up Quarantine (optional)	Setting Up Quarantine on page 29
Block Messages from Specific IP Addresses, Domains or Email Accounts	Using the Block/Accept Filters on page 37

Installation Examples

This section provides example installation types you can reference to help you determine the best way to integrate the Barracuda Spam Firewall into your network environment.

Barracuda Spam Firewall Behind Corporate Firewall

The figure below shows the Barracuda Spam Firewall behind your corporate firewall. In this example, the Mail Server has an IP address of 10.10.10.2 and the Barracuda Spam Firewall has an IP address of 10.10.10.3.



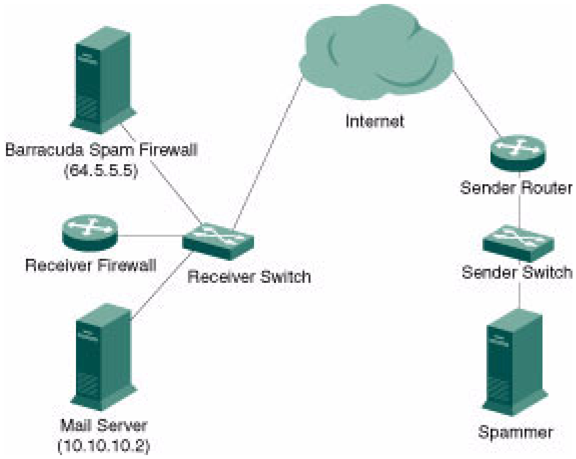
In this type of setup, you would need to do the following:

- Forward (port redirection) incoming SMTP traffic on port 25 to the Barracuda Spam Firewall at 10.10.10.3.
- Configure the Barracuda Spam Firewall to forward filtered traffic to the destination mail server at 10.10.10.2.

There is no need to modify any MX records for this type of setup.

Barracuda Spam Firewall in Front of Corporate Firewall

The figure below shows the Barracuda Spam Firewall in front of your corporate firewall. In this example, the Mail Server has an IP address of 10.10.10.2 and the Barracuda Spam Firewall has a public IP address of 64.5.5.5.



In this type of setup, you would need to do the following:

- Assign an available external IP address to the Barracuda Spam Firewall.
- Change the MX (Mail Exchange) records on the DNS (Domain Name Server) to direct traffic towards the Barracuda Spam Firewall. Create an A record and MX record on your DNS for the Barracuda.

  The following example shows a DNS entry for a Barracuda Spam Firewall with a name of *barracuda* and an IP address of *64.5.5.5.*

  ```
  barracuda.yourdomain.com   IN   A   64.5.5.5
  ```

  The following example shows the associated MX record with a priority number of 10:

  ```
  IN MX 10  barracuda.yournetwork.com
  ```

Chapter 3 Managing the Barracuda Spam Firewall

This chapter describes how to manage and configure your Barracuda Spam Firewall. The following tasks are discussed:

Viewing System Status and Statistics

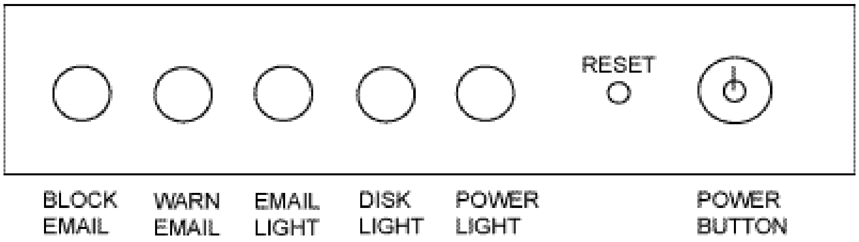
This section contains the following topics:

- Understanding the Indicator Lights on this page.
- Viewing System Statistics on page 23.

Understanding the Indicator Lights

The Barracuda Spam Firewall has five indicator lights on the front panel that blink when the system processes email.

The following figure displays the location of each of the lights.



The following table describes each indicator light.

Light	Color	Description
Block Email	Red	Blinks when email is blocked from either spam or virus detection.
Warn Email	Yellow	Blinks for each email that is either tagged as spam or quarantined.
Email	Green	Blinks when the unit receives email.
Disk	Green	Blinks during disk activity.
Power	Green	Displays a solid green light when the system is powered on.

Viewing System Statistics

The BASIC-->Status page provides email statistics, system environmental conditions and hourly and daily email statistics.

Email Statistics

The following table describes the email statistics displayed on the BASIC-->Status page.

Statistic	Description
Blocked	Number of virus and spam messages blocked by the system.
Blocked: Virus	Number of virus messages blocked by the system.
Quarantined	Number of messages quarantined by the system. This includes messages sent to the global quarantine address and the number of messages quarantined by users. By default, the system does not quarantine messages. To turn on the quarantine feature, refer to Setting Up Quarantine on page 29.
Allowed: Tagged	Number of messages tagged by the system. Tagged messages have their subject line modified based on the settings on the Spam Scoring page (described on page 28).
Allowed	Number of messages delivered to the intended recipient without being blocked or modified.
Total	Statistics for the system since installation or the last reset.
Today	Statistics for the current calendar day (from midnight to midnight).
This Hour	Statistics beginning at the top of the current hour. For example, if it is currently 10:45am, the statistics are for the time period from 10:00am to 10:45am.

Performance Statistics

This section on the BASIC-->Status page displays system environmental conditions, such as:

- Mail queue size for inbound and outbound messages.

  The mail queue size is displayed as a ratio, such as (10/5), with the first statistic representing the number of inbound mail and the second representing the number of outbound mail in the queue.

- Current state of the system fans, processor and redundancy (if applicable).
- Average amount of delay (latency) it takes the system to filter incoming email
- How long ago the last message was delivered.

Information is displayed in red when a value exceeds the normal threshold.

Note: Only the Barracuda Spam Firewall 400 and 600 come with redundant disks; therefore, the redundancy statistics do not appear for the 200 and 300 models.

The firmware and mail/log storage shows the percent of space used on each partition. The Barracuda Spam Firewall emails a system alert when utilization approaches 90% on either of these partitions. *Contact Barracuda Networks technical support if a partition reaches this threshold.*

Hourly and Daily Mail Statistics

Shows the number of messages blocked, quarantined, and allowed for the last 25 days and 24 hours.

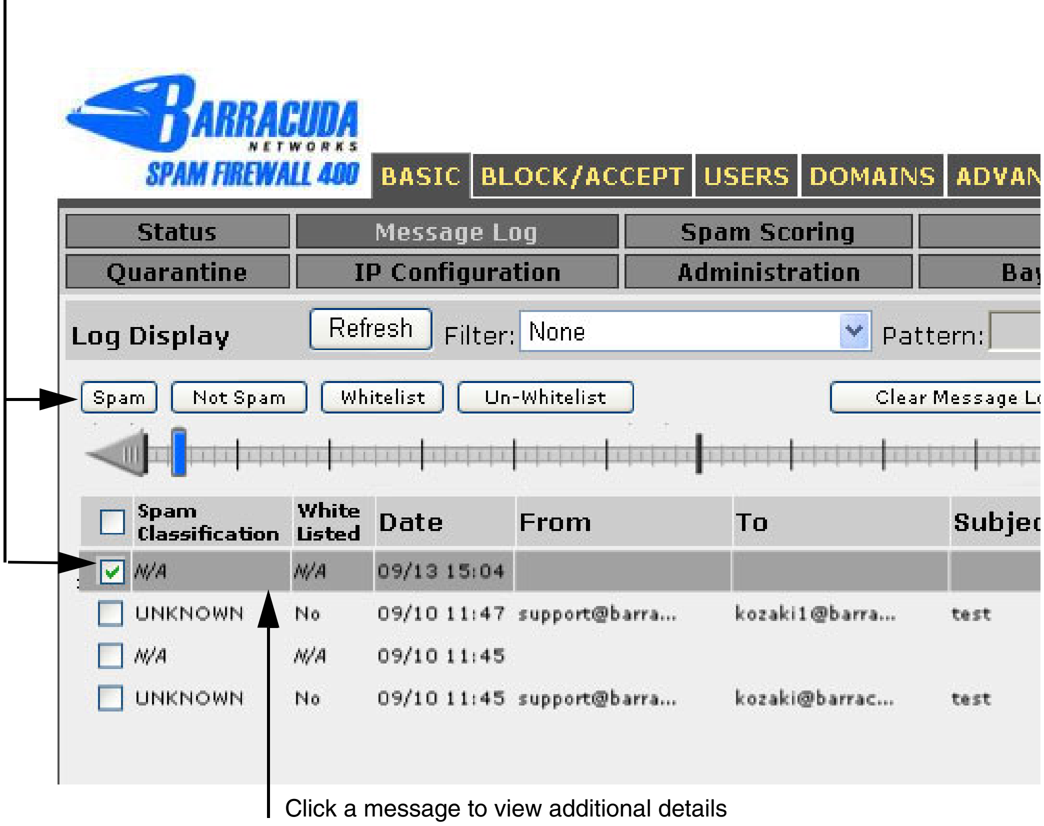
Monitoring and Classifying Incoming Messages

On a regular basis you should monitor incoming messages on the BASIC-->Message Log page, and classify as many messages as you can as spam or not spam, as well as add messages to your whitelist.

Classifying messages creates rules in the Bayesian database that determine how the Barracuda Spam Firewall handles similar messages in the future.

*Note: Click the **Preferences** button to change the message log display by hiding or changing the order of the columns. You can also increase or decrease the width of the columns.*

Classify incoming messages as spam, not spam, or add them to the whitelist



□	Spam Classification	White Listed	Date	From	To	Subjec
☑	N/A	N/A	09/13 15:04			
□	UNKNOWN	No	09/10 11:47	support@barra...	kozaki1@barra...	test
□	N/A	N/A	09/10 11:45			
□	UNKNOWN	No	09/10 11:45	support@barra...	kozaki@barrac...	test

Click a message to view additional details

Classifying Messages from the Administration Interface

Classifying messages is one of the easiest ways to set up rules that determine how the Barracuda Spam Firewall handles incoming messages. The following table describes the buttons to use when classifying messages on the BASIC-->Message Log page.

Button	Description
Spam	Classifies the message as spam in the Bayesian database. The Bayesian database becomes active once 200 spam messages and 200 not spam messages have been classified. At this point, the Barracuda Spam Firewall begins scanning messages for any matchings to affect the scoring of the messages. If per-user quarantine is enabled, message classification performed by each individual user is also applied to the Bayesian database. To view the number of messages currently classified as Spam, go to the BASIC--> Bayesian/Fingerprinting page. *Note: Messages marked as Spam are sent to Barracuda Networks for analysis unless the Submit Email to Barracuda Networks field is set to No on the BASIC-->Bayesian/Fingerprinting page discussed on page 46.*
Not Spam	Classifies the message as Not Spam in the Bayesian database. The Bayesian database becomes active once 200 spam messages and 200 not spam messages have been classified. At this point, the Barracuda Spam Firewall begins scanning messages for any matchings to affect the scoring of the messages. If per-user quarantine is enabled, message classification performed by each individual user is also applied to the Bayesian database. To view the number of messages currently classified as Not Spam, go to the BASIC-->Bayesian/Fingerprinting page.
Whitelist	Adds the sender of the message to your whitelist. Messages from whitelisted senders do not receive a spam score. Messages from whitelisted senders still go through: • Virus checking • Attachment type filtering (discussed on page 39) • Blocking filters for header, body and subject content (discussed on page 40)
Un-Whitelist	Removes the sender of the message from the whitelist.
Clear Message Log	Clears all the logs that are currently displayed. This does not clear the Bayesian database that contains the rules you have set up for incoming messages.

Classifying Messages From Mail Clients

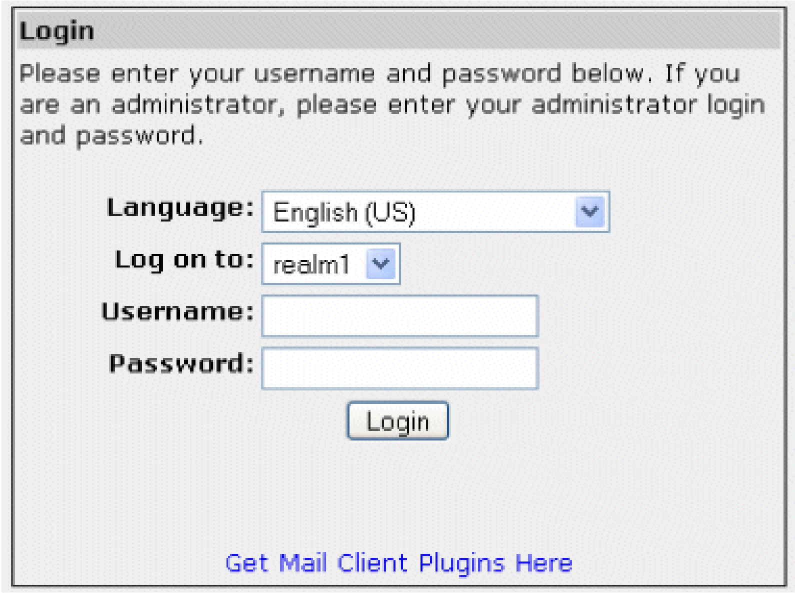
End users can classify their own messages as Spam and Not Spam directly from Microsoft Outlook using a client plug-in. This feature is only available with the Barracuda Spam Firewall 300, 400 and 600.

To make the Outlook client plug-in available to your users:

1. On the BASIC-->Bayesian/Fingerprinting page, set the **Allow Users to Download Plugins** field to **Yes**.

2. Click **Save Changes**.

   A link to the mail plug-in appears at the bottom of the Administration interface login page, as shown below.



Login

Please enter your username and password below. If you are an administrator, please enter your administrator login and password.

Language: English (US)

Log on to: realm1

Username:

Password:

After downloading and installing the plug-in, users can begin classifying messages using these buttons in their mail client: 🟥 🟩 . The first (red) button marks messages as spam and the second (green) button marks messages as not spam.

Note: Once the plug-in has been installed, a user can set various options that affect what happens to messages identified as spam and not spam. To configure these options, select Tools-->Options from the Microsoft Outlook client of the user.

Understanding the Message Log

The following table describes each column displayed in the message log table.

Column	Description
Spam Classification	Identifies when a message has been classified as Spam or Not Spam. When you mark a message as Spam or Not Spam using the buttons at the top of the Message Log, that classification is shown in this column.
White Listed	Identifies if the sender is included in your whitelist. All messages from whitelisted senders are allowed unless a virus is detected or the message contains an unallowed attachment type.
Date	The date when the Barracuda Spam Firewall received the email.
From / To	The email address of the sender and receiver.
Subject	The contents of the message subject line.
Action	The action taken on the message (Allowed, Tagged, Blocked or Quarantined).
Reason	The reason for the action, such as the sender is on your blacklist or the message has been identified as spam. In some cases this column may show “Message Size” as the reason an email is allowed. When this reason appears it means the Barracuda Spam Firewall did not scan the message for spam because the message was over 65k in size. It is extremely rare for a spam message to exceed this size limit and scanning large messages that have such a low spam probability is an inefficient use of system resources. Even though messages over 65k in size are not scanned for spam, they are always scanned for viruses.
Score	The spam score of the message. This score can range from 0 (definitely not spam) to 10 or greater (definitely spam).
Source IP	The IP address or hostname of the sender.

Viewing Message Details

To view more information about a message on the BASIC-->Message Log page, click a message to display the details window.

From the details window, click the following:

- **View Message** tab to view the contents of the message
- **View Source** tab to view the contents including email headers.
- **Deliver** link to send the message to the intended recipient.

Viewing the message body can help you identify words or characters that you may want to include in body filtering. For example, if you notice a series of messages that advertise “as seen on TV” in the body, you can add “as seen on” as keywords that will either block, quarantine or tag messages containing those words. For more information on body filtering, refer to Filtering by Body Contents on page 41.

If you do not want the body of the email displayed for privacy reasons, you can select to hide the body content using the **Message Log Privacy** setting on the BASIC-->Administration page.

Configuring the Spam Settings

The BASIC-->Spam Scoring page lets you modify the global scoring values and specify the subject tag for spam messages. Click **Save Changes** after making any changes to this page.

Configuring the Global Spam Scoring Limits

Once a message passes through the block/accept filters, it is then scored for its spam probability. This score ranges from 0 (definitely not spam) to 10 or higher (definitely spam).

Based on this score, the Barracuda Spam Firewall either tags, quarantines, blocks or allows the message.

The following table describes the settings associated with spam scoring. A setting of 10 for any setting disables that option.

Note: On the Barracuda Spam Firewall 400 and 600 you can set the spam scoring values on a per-domain basis from the DOMAINS tab. For more information, refer to Managing and Configuring Domains on page 54.

Setting	Description
Tag score	Messages with a score above this threshold, but below the quarantine threshold, are delivered to the sender with the word [BULK] added to the subject line. You can change the default text added to the subject line by entering new text in the Spam Tag Configuration section (discussed at the bottom of this page). Any message with a score below the tag threshold is automatically allowed. The default value is 3.5.
Quarantine score	Messages with a score above this threshold, but below the block threshold, are forwarded to the quarantine mailbox you specify. For information on specifying the quarantine mailbox, refer to Specifying the Global Quarantine Settings on page 30. The default setting is 10 (quarantine disabled). To enable quarantine, this setting must have a value lower than the block threshold.
Block score	Messages with a score above this threshold are not delivered to the recipient and the Barracuda Spam Firewall sends a non-delivery receipt (NDR/bounce message) to the sender. The default value is 7.

Specifying the Subject Text and Priority for Tagged Messages

The BASIC-->Spam Scoring page lets you enter the text that appears at the beginning of the subject line of tagged messages. The default text is “[BULK]”.

The system tags a message when:

- The message’s spam score is over the tag threshold (but below the quarantine threshold).
- The block/accept filters identify a message that should be tagged. For information on setting up the block/accept filters to tag messages, refer to Using the Block/Accept Filters on page 37.

If **Set Low Priority** is set to **Yes**, any messages that are tagged are marked as low priority.

By default, the Barracuda Spam Firewall sends a notification to senders when their emails are tagged as spam and not delivered to the recipient. To turn off automatic notification, set **Send Bounce** to No.

Note: You can create rules in many mail clients to place tagged messages in a separate mail folder. For example, when your users receive spam messages with a subject tag of “[BULK]”, you can configure their mail clients to deliver these messages to a folder called Possible Spam.

Enabling and Disabling Virus Checking and Notification

Virus scanning is automatically enabled on the Barracuda Spam Firewall, and the system checks for definition updates on a regular basis (hourly by default).

Use the BASIC-->Virus Checking page to configure the virus checking and notification settings described in the following table. Click **Save Changes** after making any modifications to this page.

Setting	Description
Virus Scanning Enabled:	When virus scanning is enabled, all messages are automatically scanned for viruses. The Barracuda Spam Firewall always blocks a message that contains a virus. The message is never quarantined and is not delivered to the intended recipient even if the sender has been whitelisted. It is recommended you keep virus scanning enabled. *Note: On the Barracuda Spam Firewall 400 and 600 you can enable and disable virus checking on a per-domain basis from the DOMAINS tab. For more information, refer to Managing and Configuring Domains on page 54.*
Notify Intended Recipient of Virus Interception:	Determines whether the Barracuda Spam Firewall notifies a recipient when an incoming email is blocked because the message contained a virus.
Notify Sender of Virus Interception:	Determines whether the Barracuda Spam Firewall notifies the sender that their email has been blocked because it contained a virus. You should keep this option set to No to prevent the Barracuda Spam Firewall from sending mass email notification traffic in the event of a widespread virus outbreak.

Setting Up Quarantine

By default, the Barracuda Spam Firewall does not come configured to quarantine messages.

To set up quarantine functionality on your system:

1. Enable quarantine functionality using the Spam Scoring Limits. Refer to Configuring the Global Spam Scoring Limits on page 28 for more information.
2. Go to the BASIC-->Quarantine page.
3. Select the quarantine type, as described on page 30.
4. Do one of the following:
   - For global quarantine type, enter the global quarantine delivery address, as described on page 30.
   - For per-user quarantine type, configure the per-user quarantine settings, as described on page 31.
5. Click **Save Changes**.

Specifying the Quarantine Type

The Quarantine Type determines if the Barracuda Spam Firewall delivers a quarantined message to the global Quarantine Delivery Address, or to a per-user quarantine box.

Note: If you have the Barracuda Spam Firewall 400 or 600, you can specify the quarantine type on a per-domain basis from the ADVANCED-->Advanced Domain Setup page.

The following table describes the two quarantine types.

Quarantine Type	Description
Per User	Delivers a personalized Quarantine Summary report to each user's email account. This report is sent out daily at 3:30pm and contains a link to the system where users can log in and perform the following tasks: • Specify whether they wish to receive their quarantine mail with "Quarantine Subject Text" in the subject line, or have quarantined mail stored on the Barracuda Spam Firewall (the default). • Turn off all spam scanning for their mailbox. • Set up personal whitelists and blacklists. The Per User quarantine type is not available on the Barracuda Spam Firewall 200.
Global	Delivers all quarantined messages to a global address you specify.

Specifying the Global Quarantine Settings

The following table describes the global quarantine configuration fields.

Field	Description
Quarantine Delivery Address	Specify the mailbox to which all quarantined messages should be delivered. This mailbox can either be on the mail server that the Barracuda Spam Firewall protects (i.e. yourname@yourdomain.com) or a remote mail server. *Note: If you have the Barracuda Spam Firewall 400 or 600, you can specify the quarantine delivery address on a per-domain basis from the ADVANCED -->Advanced Domain Setup page.*
Quarantine Subject Text	Enter the text you want placed at the beginning of the subject line of a quarantined message. The default text is [SPAM]. This allows you to identify quarantined messages when you have them delivered to a mailbox that also receives non-quarantine messages.

Specifying the Per-User Quarantine Settings

The following table describes the Per-User Quarantine Configuration settings. This section does not appear on the Barracuda Spam Firewall 200.

Setting	Description
Quarantine Reply-To Address	The from address used in all correspondence sent to users about their Per User quarantine area. Any replies to that correspondence are sent to this address.
Quarantine Host	The IP address or hostname that will be sent to users in all quarantine correspondence for login to the system. Leave this field blank to use the Barracuda Spam Firewall as the quarantine host. If your users need to access a server with an external IP address and the Barracuda Spam Firewall is not configured with one, you need to select another server as the quarantine host and enter that server's external address in this field.
Quarantine Default	The default state that quarantine accounts are created with. If set to **Enabled**, all new accounts will have per-user quarantine functionality. If set to **Disabled**, users do not receive messages in their quarantine inbox. Instead, messages are delivered to that user's general inbox tagged with the Quarantine Subject Text in the subject line. To enable some users with per-user quarantine functionality (but have this functionality disabled for all others), set this field to Disabled and follow the instructions in Overriding the Per-User Quarantine Account Settings on page 32.
Link Domains	Determines whether different domains share the same per-user preferences and quarantine inbox. If set to **Enabled**, the same per-user preferences and quarantine inbox is used for all email addresses with the same name, but different domains. For example, with domain linking enabled, *someuser@yourdomain.com*, *someuser@yourdomain.net*, and *someuser@corp.yourdomain.com* will all share the same preferences and quarantine inbox. Note the following about this feature: • Link Domains is a global setting. You cannot activate domain linking for only certain domains or certain users. • This feature does not work for email addresses that have the same domain, but a different handle. For example, *someuser@yourdomain.com* cannot be linked to *s.user@yourdomain.com*.
Notification Interval	The interval at which the Barracuda Spam Firewall notifies users about messages in their quarantine.

Overriding the Per-User Quarantine Account Settings

The Per-User Quarantine Account Override section on the BASIC-->Quarantine page lets you change the default quarantine configuration on a per-user basis.

For example, if the default quarantine configuration is set to disabled, you can enable per-user quarantine functionality for specific users by listing their email addresses in this section.

This feature is not available on the Barracuda Spam Firewall 200.

To override the default quarantine configuration:

1. In the User Accounts box, enter the email addresses of the users whose quarantine settings you want to override.
2. For the Enable User(s) Quarantine option, select one of the following:
   - **Yes** to enable quarantine for the specified user accounts.
   - **No** to disable quarantine for those users.
3. Click **Save Changes**.

Configuring System IP Information

The BASIC-->IP Configuration page contains the network and mail server configuration for your Barracuda Spam Firewall.

The following table describes each of the sections on this page.

Section	Description
TCP/IP Configuration	The IP address, subnet mask, and default gateway of the Barracuda Spam Firewall. TCP port is the port on which the Barracuda Spam Firewall receives inbound email. This is usually port 25.
Destination Mail Server TCP/IP Configuration	**Server Name/IP:** The hostname or IP address of your destination email server, for example *mail.yourdomain.com.* This is the mail server that receives email after it has been checked for spam and viruses. You should specify your mail server’s hostname rather than its IP address so the destination mail server can be moved and DNS updated at any time without any changes to the Barracuda Spam Firewall. TCP port is the port on which the destination mail server receives inbound email. This is usually port 25. **Valid Test Email Address:** To test that the Barracuda Spam Firewall can successfully send email messages, enter an address in this field and click **Test SMTP Connection**. The system sends a message to the email address you specify. The From address in this email is *smtptest@barracudanetworks.com*.
DNS Configuration	Lists the primary and secondary DNS servers you use on your network. You should specify a primary and secondary DNS Server. Certain features of the Barracuda Spam Firewall, such as Fake Sender Domain detection, rely on DNS availability.

Section	Description
Domain Configuration	Default Hostname is the hostname to be used in the reply address for email messages (non-delivery receipts, virus alert notifications, etc.) sent from the Barracuda Spam Firewall. The hostname is appended to the default domain. Default Domain is the domain name used in the reply address for email messages (non-delivery receipts, virus alert notifications, etc.) sent from the Barracuda Spam Firewall.
Allowed Email Recipients Domain(s)	Lists the domains managed by the Barracuda Spam Firewall. Make sure this list is complete. The Barracuda Spam Firewall rejects messages for domains that are not listed here. To allow messages for all domains that match your mail server, put an asterisk (*) in this field. *Note: One Barracuda Spam Firewall can support multiple domains and mail servers. If you have multiple mail servers, go to the ADVANCED--> Advanced Domain Setup page and enter the mail server associated with each domain.*

Controlling Access to the Administration Interface

This section covers the following topics:

- Changing the Password of the Administration Account on this page.
- Limiting Access to the Administration Interface on this page.
- Changing the Web Interface Port and Session Expiration Length on page 34.

Changing the Password of the Administration Account

The BASIC-->Administration page lets you change the password used to access the administration interface by entering the information requested and clicking **Save Password**.

Limiting Access to the Administration Interface

The Administrator IP / Range section on the BASIC-->Administration page lets you specify a range of IP addresses from which users can access the administration interface. Users attempting to log in to the administration interface from an unallowed IP address receive an error that their login is invalid.

Note: To add an individual IP address (as opposed to an entire network), specify a netmask of 255.255.255.255.

If you do not specify any IP addresses or networks, all systems are granted access with the correct password.

Changing the Web Interface Port and Session Expiration Length

The following table describes the settings in the Web Interface HTTP Port section on the BASIC-->Administration page.

Field	Description
Web Interface HTTP Port	The port used to access the administration interface from your web browser (default is HTTP port 80). To change this value: 1. Enter a new port number in the field. 2. Click **Restart Interface**. You are automatically logged out of the administration interface. 3. In your Web browser, change the port used to access the administration interface.
Session Expiration Length	The length of time users can be logged into the administration interface before being automatically logged off (default is 60 minutes). To change this value: 1. Enter the number of minutes a session can remain active. 2. Click **Save Changes**.

Resetting and Shutting Down the System

This section covers the following topics:

- Shutting Down the System on this page.
- Resetting the System Using the Front Panel on this page.
- Resetting the Bayes Database on page 35.

Shutting Down the System

The System Reset/Shutdown section on the BASIC-->Administration page lets you shutdown, reset, and reload the Barracuda Spam Firewall.

Warning: Shutting down, resetting, or reloading the system can cause interruptions in email delivery.

The following table describes each of these options.

Button	Description
Shutdown	Shuts down and powers off the system.
Reset	Reboots the system.
Reload	Re-applies the system configuration should the recent changes not take effect.

Resetting the System Using the Front Panel

Pressing the RESET button located on the front panel of the Barracuda Spam Firewall does the following:

- Reboots the system
- Resets the firmware version to the factory setting

Do not push and hold the RESET button for longer than a few seconds as this changes the IP address of the system. Pushing and holding the RESET button for 8 seconds changes the default IP address to 192.168.1.200. Holding the button for 12 seconds changes the IP address to 10.1.1.200

Warning: Shutting down, resetting, or reloading the system can cause interruptions in email delivery.

Resetting the Bayes Database

The BASIC-->Bayesian/Fingerprinting page lets you reset the Bayes database, which contains all the rules you have configured from the Message Log page, such as the messages you consider to be spam and not spam. The Bayes database significantly improves the spam identification process.

If you want to reset the Bayes database and purge the rules you have configured, click **Reset**.

Automating the Delivery of System Reports

The BASIC-->Administration page lets you configure the Barracuda Spam Firewall to automatically email daily system status reports and system alerts to the email addresses you specify.

Enter the email addresses (comma separated) in the provided fields and click **Save Changes**. The daily system status reports are sent out nightly and the system alerts on an as-needed basis.

The daily system status report shows the number of messages blocked, quarantined, tagged and allowed for each hour of that day.

Subscribing to Blacklist Services

The BLOCK/ACCEPT-->External Blacklist page lets you subscribe to various blacklist services. External blacklists, sometimes called DNSBLs or RBLs, are lists of Internet addresses from which potential spam originates. The Barracuda Spam Firewall uses these lists to verify the authenticity of the messages received. If the system receives a message from a sender on a blacklist, the message is either blocked, quarantined or tagged depending on the blacklist settings.

By default, the Barracuda Spam Firewall uses the Barracuda blacklist service and the spamhaus.org external blacklist service.

Blacklists can generate false-positives (legitimate messages that are blocked). However, because the Barracuda Spam Firewall rejects such messages when they are identified, the sender will be notified and legitimate senders will therefore know to re-send their message.

Blacklist Setting	Description
Barracuda Blacklist	Enable or disable the blacklist maintained by Barracuda Networks, which contains servers that are manually verified for sending large amounts of spam.
Common External Blacklists	Activate or deactivate blacklist services that are built into the Barracuda Spam Firewall by changing the selected action for the given blacklist(s) and clicking the **Save Changes** button.
Custom External Blacklists	Enter any additional free or subscription blacklists you want to use and specify the action you want performed. Click **Add** and then **Save Changes** when finished.
Blacklist Using Full Header Scan	Set to **Yes** to let the Barracuda Spam Firewall scan email headers for blacklisted IP addresses. Scanning headers can impact system performance because the Barracuda Spam Firewall needs to do a DNS lookup for each header. For this reason, you should only enable this feature if mail from the Internet is not delivered directly to the Barracuda Spam Firewall.

About the Blacklist Services

The following table describes each blacklist service available.

Blacklist Service	Description
sbl.spamhaus.org	Spamhaus tracks the Internet's Spammers, Spam Gangs and Spam Services, provides dependable realtime anti-spam protection for Internet networks, and works with Law Enforcement to identify and pursue spammers worldwide
xbl.spamhaus.org	To help stop the increase of spam from illegal exploits, Spamhaus released the Exploits Block List (XBL). This list is a realtime DNS-based database of IP addresses of illegal third-party exploits, including open proxies, worms/viruses with built-in spam engines, and other types of trojan-horse exploits used by spammers.
relays.ordb.org	ORDB.org is the Open Relay Database. ORDB.org is a non-profit organization that stores IP-addresses of verified open SMTP relays. These relays are likely to be used as conduits for sending unsolicited bulk email. By accessing this list, system administrators are allowed to choose to accept or deny email exchange with servers at these addresses.
bl.spamcop.net	SpamCop is a more aggressive spam service that often errs on the side of blocking mail. Many mail servers can operate with blacklists in a tag-only mode, which may be preferable when using SpamCop.

Using the Block/Accept Filters

The IP BLOCK/ACCEPT tab provides a wide range of filters that enhance the default spam and virus detection capabilities of the Barracuda Spam Firewall.

The Barracuda Spam Firewall supports the use of regular expressions in the block/accept filters. For more information on using regular expressions, refer to Appendix A.

The following table lists the various block/accept filters.

Block/Accept Filter	Refer to
Sender IP address	page 37
Sender domain	page 38
Sender email address	page 38
Recipient email address	page 39
Attachment type	page 39
Subject line content	page 40
Body content	page 41
Header content	page 41

Filtering by IP Address/Network

The BLOCK/ACCEPT-->IP Block/Accept page lets you filter messages based on the sender's IP network.

The following table describes the fields on this page.

Filter	Description
Allowed IP Range	Add any IP addresses or networks that you wish to add to your whitelist. To add an individual IP address, use a netmask of 255.255.255.255. Whitelisted IP addresses bypass spam scoring as well as all other blacklists with the exception of attachment, body, and subject filters. Use the comment field to add any notes about the allowed IP address. Click **Add** after adding each entry, followed by **Save Changes**.
Blocked IP Range	Add any IP addresses or networks to your blacklist. To add an individual IP address, use a netmask of 255.255.255.255. Blacklisted IP addresses/networks bypass all whitelists with the exception of IP address/network-based whitelists. You can specify whether the IP/Range should be blocked, quarantined or tagged. Use the comment field to add any notes about the blocked IP address. Click **Add** after adding each entry, followed by **Save Changes**.

Filtering by Sender Domain

The BLOCK/ACCEPT-->Sender Domain Block/Accept page lets you filter messages based on the sender's email address.

The following table describes the parameters on this page.

Filter	Description
Allowed Sender Domain/Subdomain	Add any domains or subdomains that you wish to include in your whitelist. Whitelisting a domain automatically whitelists all subdomains. For example, adding *customer.com* allows messages from *joe@customer.com* as well as *joe@office1.customer.com*. Whitelisted domains/subdomains bypass spam scoring as well as all other blacklists with the exception of IP block/accept and body/subject filters. Click **Add** after adding each entry, followed by **Save Changes**.
Blocked Sender Domains/Subdomain	Add any domains or subdomains that you wish to block. Blocking a domain automatically blocks all subdomains. For example, adding *spammer.com* blocks messages from *joe@spammer.com* as well as *joe@server1.spammer.com*. Blacklisted domains/subdomains bypass all whitelists with the exception of IP address/network and domain/subdomain-based whitelists. You can specify whether the IP/Range should be blocked, quarantined or tagged. Click **Add** after adding each entry, followed by **Save Changes**.

Filtering by Sender Email Address

The BLOCK/ACCEPT-->Email Sender Block/Accept page lets you filter messages based on the sender's email address.

The following table describes the parameters on this page.

Filter	Description
Allowed Email Addresses	Add the email address of each sender to include in your whitelist. Click **Add** after adding each entry, followed by **Save Changes**.
Blocked Email Addresses	Add the email address of each sender to include in your blacklist, and specify whether the sender should be blocked, quarantined or tagged. Click **Add** after adding each entry, followed by **Save Changes**.

Filtering by Recipient Email Address

The BLOCK/ACCEPT-->Email Recipient Domain Block/Accept page lets you filter messages based on a recipient's email address.

The following table describes the parameters on this page.

Filter	Description
Allowed Email Addresses or Domains	Add the email address for each recipient you want to include in your whitelist. Recipients added to this list will never have their messages scored for spam. Whitelisted recipients bypass spam scoring as well as all other blacklists with the exception of IP block/accept, and body/subject filters. Click **Add** after adding each entry, followed by **Save Changes**.
Blocked Email Addresses or Domains	Add the email address for each recipient that you want to include in your blacklist, and specify whether the recipient's message should be blocked, quarantined or tagged. A common reason to block a recipient 's email address is if that user is no longer with your company and you want to keep their account on your mail server. Recipients added to this list never receive messages unless an accept filter has been set up for the sender's IP address, domain, email address, or body/subject/header. Click **Add** after adding each entry, followed by **Save Changes**.

Filtering by Attachment Type

The BLOCK/ACCEPT-->Attachment Filtering page lets you block and quarantine messages if they contain attachments with certain file extensions.

The following table describes the parameters on this page. Click **Save Changes** after making any changes to this page. You can enter multiple lines for each filter, each line containing a type of file extension.

Filter	Description
Attachment Blocking	
Blocked Attachment File Extensions	Add the file extensions (without the preceeding dot ".") to block. The Barracuda Spam Firewall blocks the entire message if it contains an attachment with one of these extensions.
Block Extensions in Archives	Select **Yes** to scan the contents of archive files (such as zip files) for the extensions you want to block. The Barracuda Spam Firewall blocks the entire message if it has an archive file containing one of these extensions.
Block Password Protected Archives	Select **Yes** for the system to block messages that contain password-protected archive files (such as zip files). Password-protected archives cannot be scanned for file extensions. For this reason, you may want to block these type of archives.
Block Notification	
Notify intended receiver of Banned File Interception	Select **Yes** to notify recipients when an incoming email has been blocked because it contained a banned file extension.

Filter	Description
Notify sender of Banned File Interception	Select **Yes** to notify senders when one of their emails has been blocked because it contained a banned file extension.
Attachment Quarantine	
Quarantined Attachment Extensions	Add the attachment extensions (without the “.”) to quarantine. The complete email containing the attachment is sent to the quarantine account.
Quarantine Extensions in Archives	Select **Yes** for the system to scan the contents archive files (such as zip files) for the extensions you want to quarantine. The Barracuda Spam Firewall quarantines the entire message if it has an archive file containing one of these extensions.
Quarantine Password Protected Archives	Select **Yes** for the system to quarantine messages that contain password-protected archive files (such as zip files). Password-protected archives cannot be scanned for file extensions. For this reason, you may want to block these type of archives.

Note: All messages, including those from whitelisted senders, go through attachment filtering. This means that if a sender on your whitelist sends a message containing an unallowed attachment type, that message is either blocked or quarantined (depending on your settings).

Filtering by Subject Line

The BLOCK/ACCEPT-->Subject Filtering page lets you filter messages based on the contents of a message’s subject line.

The following table describes the parameters on this page. Click **Save Changes** after making changes.

Filter	Description
Subject Blocking	Enter the words, regular expressions, or characters that will cause a message to be blocked if they appear in the subject line.
Subject Quarantine	Enter the words, regular expressions, or characters that will cause a message to be quarantined if they appear in the subject line.
Subject Tagging	Enter the words, regular expressions, or characters that will cause a message to be tagged if they appear in the subject line.
Subject Whitelisting	Enter the words, regular expressions, or characters that will cause a message to be whitelisted if they appear in the subject line.

Note the following about content filtering:

- You can enter multiple lines for each filter, but each line should contain one regular expression or word. Each line is applied independently.
- HTML comments and tags imbedded between characters in the HTML source are filtered out so content filtering applies to the actual words as they appear when viewed in a web browser.

Filtering by Body Contents

The BLOCK/ACCEPT-->Body Filtering page lets you filter messages based on the contents of a message's body.

The following table describes the parameters on this page. Click **Save Changes** after making any changes to this page.

Filter	Description
Message Content Blocking	Enter the words, regular expressions, or characters that will cause a message to be blocked if they appear in the message body.
Message Content Quarantine	Enter the words, regular expressions, or characters that will cause a message to be quarantined if they appear in the message body.
Message Content Tagging	Enter the words, regular expressions, or characters that will cause a message to be tagged if they appear in the message body.
Message Content Whitelisting	Enter the words, regular expressions, or characters that will cause a message to be whitelisted if they appear in the message body.

Note the following about content filtering:

- You can enter multiple lines for each filter, but each line should contain one regular expression or word. Each line is applied independently.
- HTML comments and tags imbedded between characters in the HTML source are filtered out so content filtering applies to the actual words as they appear when viewed in a web browser.

Filtering by Header Contents

The BLOCK/ACCEPT-->Header Filtering page lets you filter messages based on the contents of a message's header content.

The following table describes the parameters on this page. Click **Save Changes** after making any updates to this page.

Filter	Description
Header Blocking	Enter the words, regular expressions, or characters that will cause a message to be blocked if they appear in the email header.
Header Quarantine	Enter the words, regular expressions, or characters that will cause a message to be quarantined if they appear in the email header.
Header Tagging	Enter the words, regular expressions, or characters that will cause a message to be tagged if they appear in the email header.
Header Whitelisting	Enter the words, regular expressions, or characters that will cause a message to be whitelisted if they appear in the email header.

Note the following about content filtering:

- You can enter multiple lines for each filter, but each line should contain one regular expression or word. Each line is applied independently.
- HTML comments and tags imbedded between characters in the HTML source are filtered out so content filtering applies to the actual words as they appear when viewed in a web browser.

Backing Up and Restoring System Configuration

You can backup and restore the following information from the Barracuda administration interface:

- Barracuda Spam Firewall system configuration that includes all the settings configured on the various pages in the administration interface.
- Per-user settings such as the allowed and blocked email lists created by each user, the users' quarantine notification intervals, and the passwords your users have set.
- Bayesian database that includes all the messages that have been configured as Spam or Not Spam.

Backing Up System Data

To backup your system:

1. Backup the system configuration as follows:
   - a. From the ADVANCED-->Configuration Backup/Restore page, click **Backup**.
   - b. Save the configuration file (*barrcuda.conf*) to a directory on your local system.
2. Backup the user settings as follows:
   - a. From the USERS-->User Backup/Restore page, click one of the following:
     - **Download Backup File** to save the last backup file to a specified location.
     - **Create Backup File Now** to create a new backup file instead of saving the backup file that already exists.
   - b. Save the user setting backup file (*pu_config.tgz*) to your local system.
3. Backup the Bayesian database, as follows:
   - a. From the BASIC-->Bayesian/Fingerprinting page, click **Backup**.
   - b. Save the Bayesian backup file (*bayes.tgz*) to your local system.

Note: Do not edit the backup files. Any configuration changes you want to make need to be done through the administration interface. The configuration backup file (barrcuda.conf) contains a checksum that prevents the file from being uploaded to the system if any changes are made to the file.

Restoring System Data

To restore system configuration from a backup file:

Note: You should perform a system restore during non-business hours when there is less email traffic. Performing a restore only takes a few minutes, but the Barracuda Spam Firewall will be out of service during this short amount of time.

1. Restore system configuration as follows:

   a. From the ADVANCED-->Configuration Backup/Restore page, click **Browse**.

   b. Locate the configuration backup file (*barracuda.conf*) and click **Upload Now**.

2. If you are restoring configuration on a replacement Barracuda Spam Firewall, update the following:

   – Virus and spam definitions (from the ADVANCED-->Energize Updates page)

   – Firmware (from the ADVANCED-->Firmware Update page)

3. Restore the user settings as follows:

   a. From the USERS-->User Backup/Restore page, click **Browse**.

   b. Locate the user settings backup file (*pu_config.tgz*) and click **Upload Now**.

4. Restore the Bayesian database as follows:

   a. From the BASIC-->Bayesian/Fingerprinting page, click **Browse**.

   b. Locate the Bayesian backup file (*bayes.tgz*) and click **Upload Now**.

Updating Spam and Virus Definitions Using Energize Updates

The ADVANCED-->Energize Updates page lets you manually update the current spam and virus definitions, as well as change the interval at which the Barracuda Spam Firewall checks for updates.

Energize Updates provide the Barracuda Spam Firewall with the latest spam and virus definitions.

The following table describes the Spam Definition Updates fields on this page. Click **Save Changes** after making any updates to this page.

Field	Description
Current Spam Definition Version	Displays the version that is currently running on the Barracuda Spam Firewall.
Latest Version Available	Displays the latest version that is available. If the current version running on the Barracuda Spam Firewall is not the latest, click **Update** to download the latest version.The Update button is disabled if the system already has the latest version.
Previous Version	Displays the previous version that was running on the system. To go back to this version of the spam definitions, click **Revert**.
Automatically Update Spam Definitions	Determines whether definitions are automatically updated when new versions are available. The recommended setting is **Yes**.
Spam Definition Update Frequency	Determines the frequency at which the Barracuda Spam Firewall checks for updates. The recommended setting is **Hourly**. Hourly updates occur at the beginning of each hour. Daily updates occur at 12:20am (twenty after midnight).

The following table describes the Virus Definition Updates fields on this page. Click **Save Changes** after making any updates to this page.

Field	Description
Current Virus Definition Version	Displays the version that is currently running on the Barracuda Spam Firewall. To view more information about the version, click **view release notes**.
Latest Version Available	Displays the latest version that is available. If the current version running on the Barracuda Spam Firewall is not the latest, click **Update** to download the latest version.The Update button is disabled if the system already has the latest version.
Previous Version	Displays the previous version that was running on the system. To go back to this version of the virus definitions, click **Revert**.
Automatically Update Virus Definitions	Determines whether definitions are automatically updated when new versions are available. The recommended setting is **Yes**.
Virus Definition Update Frequency	Determines the frequency at which the Barracuda Spam Firewall checks for updates. The recommended setting is **Hourly**. Hourly updates occur at the beginning of each hour. Daily updates occur at 12:40am (forty minutes past midnight).

Customizing the Appearance of the Administration Interface

The ADVANCED-->Appearance page lets you customize the default image used on the administration interface and in the email quarantine correspondence sent to users. This tab is only displayed on the Barracuda Spam Firewall 600.

The following table describes the fields on this page. Click **Save Changes** after making any updates to the page.

Field	Description
General	
Spam Firewall Name	Specify the system name you want to appear on the login screen (above the username and password fields). The default name is Barracuda Spam Firewall.
Web Interface	
Image Preview	Shows the current image that will be used in the administration interface. This preview updates once you upload a new image to the system.
Upload New Image	To use a custom image on the administration interface, click **Browse**, specify the image you want to use, and click **Upload Now**. The uploaded image appears in the upper left corner of the administration interface. The recommended image size is 159x64 pixels and must be of type jpg, gif, or png and be under 50k.
Image URL	The URL the user goes to when clicking on the custom image.
Reset	Allows you to revert back to the default image and URL that came with the system. The default image is the Barracuda Networks logo.
Quarantine Email	
Image Preview	Shows the current image that will be used in quarantine messages sent to users. This preview updates once you upload a new quarantine email image to the system.
Upload New Image	To use a custom image in the quarantine emails, click **Browse**, specify the image you want to use, and click **Upload Now**. The uploaded image appears in the upper left corner of the quarantine email. The recommended image size is 159x64 pixels and must be of type jpg, gif, or png and be under 100k.
Header Background Color	Specify the color of the table header background used in quarantine emails. Use a standard HTML hex code for this value.
Header Font Color	Specify the color of the table header font used in quarantined emails. Use a standard HTML hex code for this value.
Reset	Allows you to clear the custom quarantine email settings and revert back to the default image and colors.

Configuring Advanced Settings

This section describes some of the expert settings available on the ADVANCED tab. In most cases you should not need to change any of the default settings described in this section. It is recommended you talk to Barracuda Networks technical support before performing any of these tasks.

This section includes the following topics:

- Changing the Fingerprinting Behavior on page 46.
- Setting Email Protocol Checking on page 47.
- Configuring Message Rate Control on page 49.
- Activating Individual Accounts on page 49.
- Updating the System Firmware Version on page 49.
- Using a Syslog Server to Centrally Manage System Logs on page 50.
- Setting Up Clustered Environments on page 51.
- Implementing Single Sign-on on page 52.

Changing the Fingerprinting Behavior

By default, email fingerprinting is enabled on the Barracuda Spam Firewall. It is recommended you do not change this setting.

Fingerprinting examines the characteristics of messages that have already been identified as spam and uses this information to identify the same or similar messages each time they pass through your Barracuda Spam Firewall.

When an email is identified as spam, by default it is sent to Barracuda Central and “fingerprinted”. This fingerprinting process allows the system to classify other similar emails as spam.

The fingerprinting feature also performs specialized URL analysis that closely examines the URLs contained in suspicious email messages and compares them against Barracuda’s database of known spammer URLs. This lets the Barracuda Spam Firewall eliminate false URLs before reaching your users.

To change the fingerprinting behavior on your system:

1. Go to the BASIC-->Bayesian/Fingerprinting page.
2. Update the settings in the Barracuda Email Fingerprinting section of the page.

   Refer to the following table for description of the fields in this section.

3. Click **Save Changes**.

Field	Description
Check Email Fingerprints	Whether the Barracuda Spam Firewall performs fingerprinting checks on messages. Setting this to **Yes** lets the Barracuda Spam Firewall check incoming messages against Barracuda Networks known fingerprinting database of spam messages.
Intent Analysis	Whether the Barracuda Spam Firewall performs intent analysis of messages. Setting this to **Yes** lets the Barracuda Spam Firewall consider the intent of messages by looking at the URLs they contain.
Tag Intent Analysis Matches	Whether the Barracuda Spam Firewall tags spam messages identified by intent analysis instead of blocking the messages. Recommended setting is **No**.
Submit Email to Barracuda Networks	Whether the Barracuda Spam Firewall sends a copy of messages classified as spam to Barracuda Networks for further analysis. Setting this to **Yes** forwards any message that a user classifies as spam in the message log. This allows Barracuda Networks to analyze the message and improve the spam definitions and intent analysis maintained by the company.

Setting Email Protocol Checking

The ADVANCED-->Email Protocol page lets you change the default settings for SMTP checking.The table below describes each setting on this page. Click **Save Changes** after making any modifications.

Setting	Description
Mail Protocol (SMTP) Checking	
SMTP HELO Required	Whether mail clients connecting to the Barracuda Spam Firewall need to introduce themselves with a SMTP HELO command. Selecting **Yes** for this option may stop automated spam-sending programs used by spammers. The default setting is **No**.
Enforce RFC 821 Compliance	Whether the Barracuda Spam Firewall requires that the SMTP "MAIL FROM" and "RCPT TO" commands contain addresses that are enclosed by '<' and '>'. It also requires that the SMTP "MAIL FROM" and "RCPT TO" commands do not contain RFC 822 style phrases or comments. Setting this option to **Yes** stops messages sent from spam senders but also from some Windows mail programs (such as MS-Outlook) that do not adhere to the RFC 821 standard. For this reason, the default setting is **No**.
Require Fully Qualified Domain Names	Whether the Barracuda Spam Firewall requires fully qualified domain names.
Reject Fake “From” domains	Whether the Barracuda Spam Firewall rejects mail sent from domains that do not have an entry in DNS.
Sender Spoof Protection	Whether the Barracuda Spam Firewall prevents outside individuals from sending mail using this domain as the “from” address. Setting this option to **Yes** blocks all mail addressed from a domain for which the Barracuda Spam Firewall receives mail. You should only enable this option if all mail from your domains goes directly to your mail server and not through the Barracuda Spam Firewall.

Setting	Description
SPF/Caller ID Configuration	
Sender Policy Framework/ Microsoft Caller ID:	SPF (Sender Policy Framework) and Microsoft Caller ID are checks that can help the Barracuda Spam Firewall distinguish between spam and legitimate messages. How SPF works—Domain owners identify the addresses of their sending mail servers in DNS. When an SMTP receiver (like the Barracuda Spam Firewall) gets a message, it checks the sending mail server address contained in the message against the domain owner’s DNS records. If this check does not find a record for the sending mail server, the message is assumed to be spam. Enabling this feature impacts the performance of the Barracuda Spam Firewall due to the multiple DNS queries needed to retrieve a domain's SPF or Caller ID record (if it exists). Turning on this option causes messages that fail this test to be blocked. The default setting for this setting is No.
Trusted Forwarder IP	The Trusted Forwarder IP address is a list that contains the IP addresses of any machines that you have set up to forward mail to the Barracuda Spam Firewall from outside sources. The Barracuda Spam Firewall ignores any IP address in this list when performing SPF/Caller ID checks. Instead, the next IP address in the Received headers list is tried.
Incoming SMTP Timeout	
Incoming SMTP Timeout	Sets a limit on the time spent on an incoming SMTP transaction. The default is 30 seconds. Setting a time limit on SMTP transactions prevents spammers from maintaining open connections to the Barracuda Spam Firewall that can impact system resources. Messages in SMTP transactions that go over this threshold show up on the Message Log page as being "blocked" with a reason "timeout".
SMTP Messages Per Session	
Messages per SMTP session	Sets a limit on the number of messages in one SMTP session. If the number of messages in one session exceeds this threshold the rest of the messages are blocked and show up in the message log as being "blocked" with a reason "Per-Connection Message Limit Exceeded".
SMTP Welcome Banner	
SMTP Welcome Banner	Determines the Welcome Banner presented to the SMTP client connecting to the Barracuda Spam Firewall. This value must be unique across your network. If this value is not unique and a message attempts to go to a server with the same welcome banner, the message fails to be delivered. This value can be left blank for the Barracuda Spam Firewall to manage the setting.
Barracuda Headers	
Remove Barracuda Headers	Removes Barracuda’s custom X-headers that are applied before a message leaves the system. It is recommended you do not remove Barracuda headers because they contain the reason a message is tagged, quarantined or blocked. This information makes it easier to troubleshoot message handling issues.

Configuring Message Rate Control

The ADVANCED-->Rate Controls page lets you configure how many connections are allowed from the same IP address in a half-hour time period. Rate control protects you from spammers or spam-programs that send large amounts of email to your server in a small amount of time.

The table below describes each setting on this page. Click **Save Changes** after making any modifications.

Setting	Description
Message Rate Control	Specifies the maximum number of connections allowed from the same IP address in a half-hour timeframe. When the number goes over this threshold, the Barracuda Spam Firewall blocks further connections/ messages. Legitimate sending email servers will act on this message and inform the sender or sending mail server to try again later. Spam senders probably will not do anything with this message and will stop sending email when they do not get through.
Rate Control Exclude IP/Range	Enter any IP address range that you wish to exclude from rate control. To enter a single IP address (rather than a range), enter 255.255.255.255 for the netmask.

Activating Individual Accounts

When you first start using the Barracuda Spam Firewall you may prefer to only activate a few accounts so you can familiarize yourself with the system and train a few users before rolling out the new capabilities to your entire organization.

To activate an individual account:

1. Go to the ADVANCED --> Explicit Users page.
2. In the Email Address field, enter the email address of the account to activate.
3. Click **Add**.

Note: Only accounts added to the Email Address list receive spam and virus protection. However, RBLs, rate control, and recipient validation are applied to all incoming mail regardless of this list.

Updating the System Firmware Version

The ADVANCED-->Firmware Update page lets you manually update the firmware version of the system or revert to a previous version.

The only time you should revert back to an old firmware version is if you recently downloaded a new version that is causing unexpected problems. In this case, call Barracuda Networks technical support before reverting back to a previous firmware version.

To manually load the latest firmware version:

Note: Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-business hours.

1. Read the release notes of the latest firmware version to learn about the new features.

2. Click **Download Now**.

   This button will be disabled if the Barracuda Spam Firewall already has the latest firmware version.

3. After downloading the firmware version, activate it by doing the following:

   a. Log out of the administration interface.

   b. Log back into the administration interface and go to the ADVANCED-->Firmware Update page.

   c. Click **Apply**.

   When activating the downloaded firmware, the Barracuda Spam Firewall resets. After the reset your email automatically continues to be filtered.

Using a Syslog Server to Centrally Manage System Logs

The ADVANCED-->Syslog page lets you specify a server to which the Barracuda Spam Firewall sends syslog data. The following table describes the two types of data you can send to a syslog server.

Syslog Field	Description
Mail Syslog Configuration	Enter the IP address of the syslog server you want to receive data related to mail flow. This data consists of the same data that is used to build the message log. Information such as the connecting IP, from address, to address, and the spam score for the messages is all included. This syslog data appears on the mail facility at the debug priority level on the specified syslog server.
Web GUI Syslog Configuration	Enter the IP address of the syslog server you want to receive data related to the web interface. This data consists of information about when a user logs in, as well as any configuration changes made to your Barracuda Spam Firewall. This syslog data appears on the local1 facility with login information at info priority, and configuration changes at debug priority.

Syslog is a standard UNIX/Linux tool for sending remote system logs and is available on all UNIX/ Linux systems. Syslog servers are also available for Windows platforms from a number of free and premium vendors.

Barracuda Networks has tested with a Windows freeware syslog server from Kiwi Enterprises (www.kiwisyslog.com). Barracuda Networks makes no guarantees that your Barracuda Spam Firewall will be completely compatible with this syslog server.

Syslog support is not available on the Barracuda Spam Firewall 200.

Setting Up Clustered Environments

The ADVANCED-->Clustering page lets you link multiple Barracuda Spam Firewall systems together so they can synchronize configuration settings. You can also use this page to specify standby systems to use in case an active system goes down.

Clustering is available on the Barracuda Spam Firewall models 400 and 600.

Clustering not only makes managing multiple Barracuda Spam Firewall systems more manageable, but also provides 100% redundant coverage of the propagated data.

The following table lists the information that is and is not propagated to the other clustered systems.

Propagated Data	Data Not Propagated
System settings (global and domain) configured through the Administration interface	System IP configuration described on page 32.
Per-user quarantine settings configured through a user's quarantine interface	SSL settings described on page 60.
Message logs	
Bayesian databases	
Quarantine inboxes	

Each user account has a primary and backup server in the cluster. The primary is the server that first to joins cluster, and the secondary is the next server joining the cluster. There are always two servers at all times that have the same information (configuration and quarantine messages).

The following table describes the settings on the ADVANCED-->Clustering page.

Field	Description
Cluster Settings	
Cluster Shared Secret	The passcode shared by all Barracuda Spam Firewall systems in this cluster. All Barracuda Spam Firewalls in a cluster must have the same shared passcode. Make sure a passcode has already been set on an existing system before you try adding this system to the cluster.
Cluster Host Name	The host name for this system. The other systems in this cluster use this host name when communicating with this system. When this field is blank, the system IP address is automatically used. If this host name cannot be resolvable by DNS, create an entry in the Local Host Map field at the bottom of this page on each Barracuda Spam Firewall in the cluster **before** adding this machine into the cluster.
Clustered Systems	
Cluster Field	Enter the IP address or host name of one of the Barracuda Spam Firewall systems in the cluster you want to join, and click **Join Cluster**. Once this system joins the cluster, configuration settings are pulled from the cluster that is joined and override the settings on this system. User lists are synced between the cluster and this machine so that any users on this machine are not lost, but integrated into the cluster. A system successfully joins a cluster when the IP address of each system in the cluster appears in an active state with a green status light.

Field	Description
Cluster System List	**Cluster System** lists the other systems in this cluster. **Mode** specifies whether a system is Standby or Active. Designate a server as Standby if you want a spare system to switch to in the event another system goes down. Only Active servers filter incoming messages. You must manually switch a standby server to Active if you want the standby server to begin filtering messages. The switchover does *not* automatically occur when an active server fails. **Status** displays if the system is up and running (green dot).
Local Host Map	
Host Name / IP Address	Map a local host name to an IP address for a system in the cluster. This mapping results in a local override of DNS hostname-to-IP address lookups.Click **Add** after specifying each new entry. This mapping is not synchronized with other systems in the cluster. Use the local host map feature in the following situations: • There are clustered Barracuda Spam Firewalls on different private networks and systems on the same private network must communicate using the private IP address of the other systems while systems on different networks must communicate using the public IP address of the other systems. • Different clustered Barracuda Spam Firewalls need to forward to different destination mail servers. In this case, the Destination Server field on the Domain configuration page could be "localmail" and each Barracuda Spam Firewall in the cluster would have a different IP address assigned to "localmail" in the Local Host Map field.

Implementing Single Sign-on

The ADVANCED-->Single Sign-On page lets you configure the Barracuda Spam Firewall to authorize user accounts using an LDAP or Active Directory server. This feature is available in the Barracuda Spam Firewall 400 and 600 models.

With single sign-on, users can automatically log into their quarantine interface or the administration interface using their domain passwords instead of a password managed separately by the Barracuda Spam Firewall.

The following table describes the fields on the ADVANCED-->Single Sign-On page.

Field	Description
Login Realm Selector	Enabling this option displays a realm selection drop-down menu on the login screen so users can select their realm and login with just their username. This is used to support single sign on.
Local Realm Name	The realm name as displayed for local authentication (where the password is generated and stored on the Barracuda Spam Firewall).
Advanced Single Sign-on Configuration	
Realm Name	The name of the realm as displayed to the users in the Realm Selector as well as in the Domain Settings for the administrator. This is a required field.

Field	Description
Auth. Type	Controls the type of realm that is created. Available options include: • LOCAL (where the Barracuda Spam Firewall controls the password), • LDAP (where the password is maintained in an external LDAP database), • RADIUS (where the password is maintained in the RADIUS database).
Auth. Host	The name of the LDAP server or RADIUS server that the Barracuda Spam Firewall attempts to connect to for authentication purposes. It is ignored for LOCAL authentication.
Auth. Port	The port the Barracuda Spam Firewall uses to connect to the LDAP server or RADIUS server for authentication purposes. It is ignored for LOCAL authentication.
Username Template	If using LOCAL authentication, this field is ignored. If using LDAP authentication, this field contains the template for the username the Barracuda Spam Firewall attempts to bind with (for example: cn=__USERNAME__,dc=mydomain,dc=com). The __USERNAME__ is replaced with both the full email address and the username portion. If using RADIUS authentication, this field should contain the RADIUS shared secret.
Auth. Default	Determines which realm is used as the default if a user does not select one or they fail login at their selected realm.

Localizing the Spam Settings

The ADVANCED-->Spam Rule Management page lets you enhance the Barracuda Spam Firewall’s ability to detect spam in Chinese and Japanese language messages. The following table describes the options on this page.

Option	Description
Chinese (PRC) Government Compliance	This option may need to be enabled if your Barracuda Spam Firewall resides in the Peoples Republic of China (PRC). Set this option to **No** if your Barracuda Spam Firewall is located outside the PRC.
Chinese Language Spam Rules	Enable this option if your company receives a significant amount of valid Chinese language email. Otherwise, this option should be disabled.
Japanese Language Spam Rules	Enable this option if your company receives a significant amount of valid Japanese language email. Otherwise, this option should be disabled.

Managing and Configuring Domains

The DOMAINS-->Domain Manager page lets you add new domains and make changes on a per-domain basis.

Adding New Domains

If your Barracuda Spam Firewall is responsible for filtering messages for more than one email server and domain, you need to enter the domains associated with each server on the DOMAINS-->Domain Manager page.

If you have the Barracuda Spam Firewall 400 or 600, you can also set spam scoring, quarantine type and spam/virus checking on a per-domain basis.

To add and configure domains:

1. Go to the DOMAINS-->Domain Manager page.
2. In the Advanced Domain Configuration section, enter the domain associated with your other mail server, and click **Add Domain**.

   The domain appears in the table.
3. Click **Edit Domain** next to the domain you just added.

   The Domain Edit page opens.
4. Configure the domain settings, as described in Editing Domain Settings on page 54.

Editing Domain Settings

To edit the settings for a specific domain:

1. On the DOMAINS-->Domain Manager page, click **Edit Domain** next to the domain to edit.

   The Domain Edit page opens.
2. Specify the per-domain settings described in the following table. These settings are only available on the Barracuda Spam Firewall 400 and 600.

   Note: Setting values on a per-domain basis override the values configured elsewhere in the administration interface.

Setting	Description
Destination Server and Port	The hostname and destination port of the mail server associated with the selected domain.
Use MX Records	Controls whether or not MX lookups are performed on the Destination Server specified
Valid Test Email Address	Enter a valid email address to test whether the Barracuda Spam Firewall can filter messages for the selected domain, and click **Test SMTP Connection**. Then check the Message Log and verify the test message appears in the log and make sure the message is delivered to the test email address. The test email has a "from" address of *smtptest@barracudanetworks.com*.

Setting	Description
Realm Name	The name of the realm as displayed to users in the Realm Selector as well as in the Domain Settings for administrators. A realm is a database of usernames and passwords that identify valid users, plus the list of roles associated with each valid user.
Tag Score, Quarantine Score, Block Score	For information on spam scoring, refer to Configuring the Global Spam Scoring Limits on page 28.
Per-User Quarantine	Determines the quarantine type for the domain. Selecting **Yes** sets the quarantine type to Per-User. Selecting **No** sets the quarantine type to Global. For information on quarantine types, refer to Specifying the Quarantine Type on page 30.
Global Quarantine Email Address	Specifies the address for the global quarantine email address for the domain. For more information, refer to Specifying the Global Quarantine Settings on page 30.
Spam Scan Enabled, Virus Scan Enabled	Lets you enable or disable spam and virus checking for the domain.
Spoof Protection	Whether the Barracuda Spam Firewall prevents outside individuals from sending mail using your domains as the “from” address. Setting this option to **Yes** blocks all mail addressed from a domain for which the Barracuda Spam Firewall receives mail. You should only enable this option if all mail from your domains goes directly to your mail server and not through the Barracuda Spam Firewall.

3. Click **Save Changes**.

Preventing Dictionary Attacks Using Barracuda MS Exchange Accelerator

A "Dictionary" or NDR (Non-Delivery Report) attack occurs when a spammer tries to delivery a series of messages to every possible recipient name on an email server.

Microsoft Exchange attempts to protect against dictionary attacks by accepting messages for all recipients rather than rejecting invalid recipients and letting a spam sender know which accounts are valid. Unfortunately, this often causes the Exchange server to experience a high CPU load because the server still attempts to send one or more non-delivery notifications for every invalid recipient.

The Barracuda MS Exchange Accelerator feature uses the LDAP service built into Exchange to verify recipients before delivering messages to the MS Exchange server and consuming valuable resources. If the recipient cannot be verified, the Barracuda Spam Firewall does not deliver the message. This premium service is recommended for all MS Exchange configurations.

Note: The LDAP protocol must be enabled on your Exchange server in order to use the Barracuda MS Exchange Accelerator. LDAP is automatically on by default in most MS Exchange installations.

To set up the Barracuda MS Exchange Accelerator service:

1. Go to the DOMAINS-->Domain Manager page.
2. Click **Edit LDAP** in the Actions column.

3. Enter the required information for each listed domain.

   The following table describes the fields on this page.

Field	Description
LDAP Server	The name of the LDAP server for your MS Exchange server.
Exchange Acclerator Enabled	Whether the Exchange Accelerator feature is enabled for the selected domain.
Unify Email Aliases	Whether the Barracuda Spam Firewall unifies all email aliases for a single user. Selecting **Yes** makes all messages to any of the user's aliases use the same preferences and same quarantine inbox. You must have an LDAP server specified on this page for the Unify Email Aliases feature to work. This feature is not available in the Barracuda Spam Firewall 200. The Unify Alias feature links individual aliases together. For example, if sanderson@acme.com, sandy_anderson@acme.com, and sanderso@acme.com were all associated with one account, then the Barracuda Spam Firewall would link all the aliases to the primary account.
LDAP Port	The LDAP port used to communicate with the Exchange server. By default, this port is 389.
LDAP / Exchange Username	The username for the LDAP/Exchange server. To determine the fully-qualified username, open Active Directory, go into Active Directory Users and Computers and double-click on the user account in question. Under the Account tab, use the User Login Name plus the @xxx.xxx that follows as the LDAP username.
LDAP / Exchange Password	The password for the LDAP/Exchange server.
LDAP Filter	The custom LDAP filter to apply to this domain (optional).
LDAP Search Base	Enter a value that controls the starting search point in the LDAP tree. The default value looks up the 'defaultNamingContext' top-level attribute and uses it as the search base.
Valid Email (for testing)	Enter a valid email address to use to verify that LDAP lookups are working correctly. Click **Test LDAP** after entering this address.

4. Click **Save Changes**.

Replacing a Failed System

Before you replace your Barracuda Spam Firewall, use the tools provided on the ADVANCED-->Troubleshooting page to try to resolve the problem with your Barracuda system. For more information about these tools, refer to Troubleshooting on page 63.

In the event that a Barracuda Spam Firewall system fails and you cannot resolve the issue, customers that have purchased the Instant Replacement service can call technical support and receive a new unit within 24 hours. The technical support numbers are listed on page 10.

After receiving the new system, ship the failed Barracuda Spam Firewall back to Barracuda Networks at the address below. Barracuda technical support can provide details on the best way to return the unit.

Barracuda Networks
10040 Bubb Road
Cupertino, CA 95014

(408)342-5400

Note: To quickly configure the new system so it behaves the same as your failed system, use the system configuration, Bayesian database, and user settings backup files from the failed system and restore that data on the new system. For information on restoring data, refer to Backing Up and Restoring System Configuration on page 42.

Managing User Accounts

The USERS tab (available on the Barracuda Spam Firewall 300, 400 and 600 models) lets you do the following:

- View user accounts
- Assign features to user account
- Add and delete user accounts
- Backup and restore user settings

Viewing User Accounts

The USERS-->Account View page lets you view each user's account settings, log in to their quarantine interface to change their personal preferences, and delete any per-user quarantine accounts on the system.

The following table describes each column on this page.

Column	Description
Account Address	The email address of the account.
Notify Interval	How often the system sends the quarantine summary message to the user.
User Quarantine?	Whether the user has their quarantine account enabled. If this is set to **No**, all quarantine messages are delivered to the user with the subject line altered instead of being placed in quarantine.
Spam Scan?	Whether the user has spam scoring enabled. If this is set to **No**, this user's messages are not scanned for spam.

Column	Description
Admin Actions	Click **Edit Account** to view that user's quarantine account so you can troubleshoot issues and change the user's preferences. Click **Delete** to remove the quarantine account from the system including all of the user's settings and quarantined messages.
Remove All Invalid Accounts	Click this button to have the Barracuda Spam Firewall check each user account against the recipient verifier and remove any accounts that are currently invalid.

To limit the accounts displayed on this page, use any of the filters described in the following table.

Filter	Description
None	Displays all accounts on the system with the newest ones listed first
"Account" (email address)	Displays only the accounts for the email addresses entered in the Pattern textbox.
"Account (pattern*)	Displays only the accounts that match the full or partial usernames entered in the Pattern textbox. The matches apply across all domains on the Barracuda Spam Firewall. *Note: the wildcard is on the right of the pattern. This means if you search for 'bob' -- bob@domain.com and bobby@domain.com will match, but not billybob@domain.com.*
"Account (*pattern)	Displays only the accounts that match the full or partial usernames entered in the Pattern textbox. The matches apply across all domains on the Barracuda Spam Firewall. *Note: the wildcard is on the left of the pattern. This means if you search for 'domain.com' -- user@domain.com and user@corp.domain.com will match, but not user@domain1.com.*
"Quarantined Enabled"	Displays all accounts with quarantined enabled.
"Quarntined Disabled"	Displays all accounts with quarantined disabled.
"Spam Scan Enabled"	Displays all accounts with spam scanning enabled.
"Spam Scan Disabled"	Displays all accounts with spam scanning disabled.

Assigning Features to User Accounts

The USERS-->User Features page lets you specify which features your users can control from their quarantine interface.

The following table describes the settings on this page.

User Features	Description
Quarantine Enable/Disable Ability	Determines whether your users can enable/disable their quarantine inbox. If you set this value to **No**, all messages are quarantined based on: • The quarantine type configured on the BASIC-->Quarantine page, or • The per-domain quarantine type configured on the ADVANCED-->Advanced Domain Setup page. For more information, refer to Managing and Configuring Domains on page 54. *Note: If you Set this value to **No**, the quarantine settings configured by the user do not take affect.*
Spam Scan Enable/Disable Ability	Determines whether your users can enable/disable spam scanning of their incoming messages. If you set this value to **No**, all users' messages are scanned for spam based on: • The settings configured on the BASIC-->Spam Scoring page, or • The per-domain settings configured on the ADVANCED-->Advanced Domain Setup page. For more information, refer to Managing and Configuring Domains on page 54. *Note: If this value is set to **Yes** and a user has disabled spam scanning, that user's spam scanning will be re-enabled when you change Spam Scan Enable/Disable Ability to **Yes**.*
Notification Change Ability	Determines whether your users can change how often they receive the quarantine summary notification. If you set this value to **No**, all users receive notifications based on the frequency specified in the Quarantine Notification setting on the BASIC-->Quarantine page. *Note: If this value is set to **Yes**, and a user changes their notification interval, that user's change is preserved when you change the Notification Change Ability to **No**.*
Whitelist/ Blacklist Ability	Determines whether your users can add email addresses and domains to their personal whitelist and blacklist. *Note: If this value is to **Yes** and a user adds entries to their whitelist and blacklist, those additions are ignored when you change Whitelist/Blacklist Ability to **No**.*
Scoring Change Ability	Determines whether your users can change the levels at which their messages are tagged, quarantined, or blocked. If you set this value to **No**, all messages are scored based on: • The settings configured on the BASIC-->Spam Scoring page, or • The per-domain settings configured on the ADVANCED-->Advanced Domain Setup page. For more information, refer to Managing and Configuring Domains on page 54. *Note: If this value is set to **Yes** and a user changes their spam scoring, that user's changes are not preserved when you change Scoring Change Ability to **No**.*
User Features Override	Use this section to provide specific user accounts with a different feature set than specified in the Default User Features section. In the User Accounts box, enter the email addresses for the accounts you want to override, and then specify the features for these accounts. Click **Save Changes** when finished.

Creating New User Accounts

The USERS-->User Add/Update page lets you create new user accounts with specific settings. To add a new user account to the system:

1. In the User Account(s) box, enter the email addresses (one per line) of the new user accounts.
2. Specify whether the new user accounts are enabled with the user quarantine feature.

   For a description of the user quarantine feature, refer to Specifying the Quarantine Type on page 30.

   Note: If you enable the user quarantine, you should disable aliases and public folders so no per-user accounts are created for these items.
3. Select the option to email login information to the new users. To view an example greeting email that contains login information, refer to Greeting Message on page 65.
4. Click **Save Changes**.

   For information on assigning additional features to user accounts, refer to page 59.

Backing Up and Restoring User Settings

The USERS-->Backup/Restore page lets you save user settings to a text file and restore those settings if needed. User settings include configuration such as the allowed and blocked email lists created by each user, the users' quarantine notification intervals, and the passwords your users have set.

For information on backing up and restoring the user settings, refer to Backing Up and Restoring System Configuration on page 42.

Enabling SSL

The ADVANCED-->SSL page lets you enable SSL on your Barracuda Spam Firewall. Click **Save Changes** after making any modifications to this page.

One of the most common reasons to enable SSL is to ensure user passwords remain secure. When using the Single Sign-on feature (described on page 60), you should also use SSL because Single Sign-on may require passwords be passed to the Barracuda Spam Firewall in their original, unencrypted form. If you are not using Single Sign-On, SSL is not required to keep your passwords secure.

SSL not only ensures that your passwords are encrypted, but also ensures that the rest of the data transmitted to and received from the administration interface is encrypted as well.

The following table describes the fields on the ADVANCED-->SSL page.

Field	Description
Web Interface HTTPS/SSL Configuration	
HTTPS/SSL access only:	Select **Yes** to enable SSL and only allow access to the Administration interface via SSL. Select **No** to use standard HTTP access.
Use HTTPS links in emails	Whether the Barracuda Spam Firewall uses *https://* (instead of *http://*) in the links included in system emails. This applies to daily system reports, quarantine emails, and system alerts that are sent out by the system. This setting does not apply to emails sent out by users. This setting is automatically set to **Yes** when you enable HTTPS/SSL access.

Field	Description
Web Interface HTTPS/SSL port	The SSL port used by the Barracuda Spam Firewall. Default port for SSL is 443.
SSL Certificate Configuration	
Certificate Type	Select one of the following certificates for SSL: • **Default (Barracuda Networks)** used for SSL connections that will generate browser alerts. The default certificate is signed by Barracuda Networks and provided free as the default type of certificate. • **Private (self-signed)** certificates provide strong encryption without the cost of purchasing a certificate from a trusted certificate authority (CA). However your web browser cannot verify the authenticity of the certificate, and display a warning every time you access the Admin interface. To avoid this warning, download the Private Root Certificate and import it into your browser. • **Trusted** certificates are issued by trusted Certificate Authorities (CA), which are usually recognized by your Web browser so no additional configuration is required.
Certificate Generation	
Organization Info	The information stored in your certificates and Certificate Signing Requests. Provide the following information: **Common Name** is the fully qualified domain name used to access the Administration interface. For example: "barracuda.yourdomain.com" **Country** is the two-letter country code where your organization is located. **State or Province Name** is the full name of the state or province where your organization is located. **Locality Name** is the city where your organization is located. **Organization Name** is the legal name of your company or organization. **Organization Unit Name** is an optional field in which to specify a department or section within your organization.
Download Certificate Signing Request (CSR)	Click **Download** to obtain a certificate signing request that is required to purchase a signed certificate from a trusted certificate authority. The certificate is generated with a 1024 bit key length.
Download Private key	Click **Download** to obtain a copy of the private key used for the CSR. The certificate authority where you purchased your certificate may ask for this key, which is only available after you download a CSR.
Download Private Root Certificate	Click **Download** to obtain the private root certificate and import it into your web browser. Once you have imported the certificate, your web browser is able to verify the authenticity of the Barracuda system’s SSL certificate, and should no longer issue a warning when you visit the administration interface.
Trusted Certificate	
Upload Signed Certificate	After purchasing the certificate using the CSR, browse to the location of the certificate and click **Upload**. Once you upload the certificate, your Barracuda Spam Firewall automatically begins using it. Once you have uploaded your signed certificate, make sure *Trusted* is selected for the Certificate Type (described above).
Upload Private key	After downloading the private key, browse to the location of the key and click **Upload**.

Customizing Non-Delivery Reports (NDRs)

The ADVANCED-->Bounce/NDR Messages page lets you modify the information in an NDR and select the default language to use in the message.

The Barracuda Spam Firewall sends NDRs to email recipients and senders when one of their messages is blocked. The NDR contains a brief explanation of why the Barracuda Spam Firewall blocked the message. Information that you may want to add to an NDR includes the contact information of the Barracuda system administrator so internal users know who to contact if they have questions about a blocked message.

Note: The Barracuda Spam Firewall only sends out Non-Delivery Reports if these notifications have been enabled on the BASIC-->Spam Scoring and BASIC-->Virus Checking pages.

The following table describes the settings on the ADVANCED-->Bounce/NDR Messages page.

Field	Description
Select NDR Language	
Default Language	Select the language to use for the Non-Delivery Reports. The Barracuda Spam Firewall automatically translates the default NDR messages to the language you specify. To customize the information in an NDR, select **Custom** and enter your customized text in the Customized NDRs section. *Note: If you customize NDRs and then later switch back to a predefined language, you lose all customization and the Barracuda system reverts back to the default message for the specified language.*
Customized NDRs	
Banned File (recipient)	When a message containing an attachment type that has been band is sent to a user, the Barracuda Spam Fire blocks the incoming message and sends this notice to the intended recipient of the email.
Banned File (sender)	When someone sends a message containing an attachment type that has been banned, the Barracuda Spam Firewall blocks the outgoing message and sends this notice to the sender of the email.
Spam (sender)	When the Barracuda Spam Firewall blocks a message because it was determined to be spam, the Barracuda system sends this notice back to the message sender.
Virus (recipient)	When the Barracuda Spam Firewall determines that a message contains a virus, it sends this notice to the intended recipient of the blocked message.
Virus (sender)	When the Barracuda Spam Firewall determines that a message contains a virus, it sends this notice to the sender of the message.

The following table describes the supported macros you can use in NDRs.

Macro	Description
%f	The Barracuda Spam Firewall administrator's e-mail address (typically used in 'From:' header of NDRs).
%C	The list of recipients to be used in the Copy To (Cc:) header of the NDR.
%d	RFC 2822 date-time (current time).
%m	The 'Message-ID' header field body.

Macro	Description
%j	The Subject header field body.
%s	The original envelope sender, rfc2821-quoted and enclosed in angle brackets.
%S	The address that receives sender notification. This is normally a one-entry list containing sender address (%s), but may be unmangled/reconstructed in an attempt to undo the address forging done by some viruses.
%v	The output of the (last) virus checking program.
%F	The list of banned file names.

Troubleshooting

The ADVANCED-->Troubleshooting page provides various tools that help troubleshoot network connectivity issues that may be impacting the performance of your Barracuda Spam Firewall.

The following table describes the fields on the ADVANCED-->Troubleshooting page.

Troubleshooting Tool	Description
Support Diagnostics	
Establish Connection to Barracuda Central	If you need help troubleshooting and diagnosing an issue, click this button to establish a connection to Barracuda Central and provide the Barracuda Networks support engineer with the serial number displayed. You can click the **Stop** button to terminate all connections to your Barracuda system when the work is complete.
Network Connectivity	
Ping Device	Sends a ping request from your Barracuda Spam Firewall to the specified system. Enter the IP address or hostname of the system you wish to ping (as well as any ping options you want to provide) and click **Begin Ping** to start the test.
Telnet Device	Attempts to establish a telnet session from your Barracuda Spam Firewall to the specified system. This session is non-interactive. Use this test to verify connectivity and initial response from a remote server. Enter the IP address or hostname you wish to telnet to (as well as any options you wish to provide), and click **Begin Telnet** to start the test.
Dig/NS-lookup Device	Performs a "dig" command on your Barracuda Spam Firewall. Dig is a more advanced nslookup command that you can use to lookup any type of DNS record. Enter the IP address or hostname you wish to perform a dig against (as well as any options you wish to provide), and click **Begin Dig** to start the test. For example to lookup mx records, enter *mx mydomain.com*.
TCP Dump	Performs a tcdump on your Barracuda Spam Firewall to monitor network traffic. Enter any information you wish to provide for monitoring the connection (as well as any option to adjust the tcpdump output; for example: -x -X port 53) and click **Begin TCP Dump** to start the test.
Traceroute Device	Performs a traceroute from the Barracuda Spam Firewall to the specified system to determine routes used. Enter the IP address or hostname of the destination server and click **Begin Traceroute** to start the test.

Chapter 4 Using the Barracuda Spam Firewall to Filter Your Emails

This chapter describes how end users interact with the Barracuda Spam Firewall to check their quarantined messages, classify messages as spam and not spam, and modify their user preferences. This chapter contains the following topics:

- Receiving Messages from the Barracuda Spam Firewall in the next section.
- Using the Quarantine Interface on page 66.
- Changing your User Preferences on page 68.

Receiving Messages from the Barracuda Spam Firewall

The Barracuda Spam Firewall sends the following two types of messages to end users:

- Greeting Message
- SPAM Quarantine Summary Report

Greeting Message

The first time the Barracuda Spam Firewall quarantines an email intended for you, the system sends you a greeting message with a subject line of “User Quarantine Account Information”. The greeting message contains the following information:

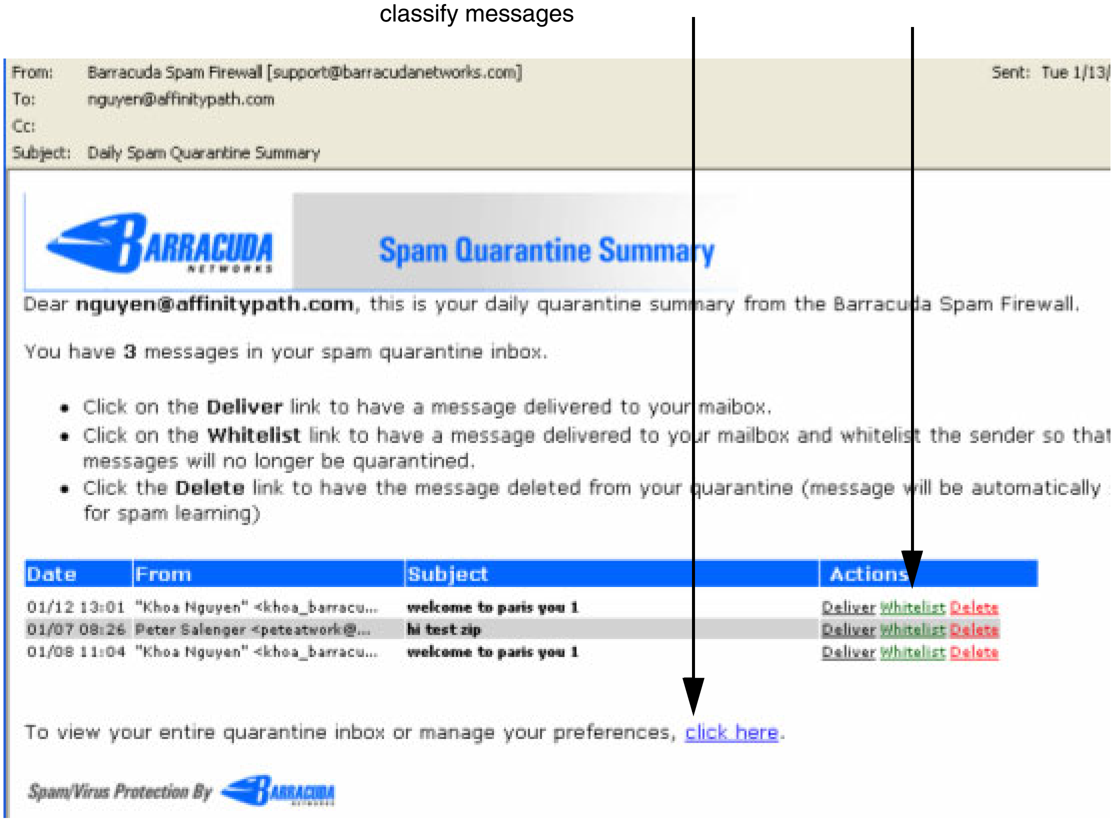
> Welcome to the Barracuda Spam Firewall. This message contains the information you will need to access your Spam Quarantine and Preferences.
>
> Your account has been set to the following username and password:
>
> Username: *<user’s email address>*
>
> Password: *<user’s default password>*
>
> Access your Spam Quarantine directly using the following link:
> http://*<barracuda system address or name>*:8000

The Barracuda Spam Firewall automatically provides your login information (username and password) and the link to access the quarantine interface. You should save this email because future messages from the system do not contain your login information.

Quarantine Summary Report

The Barracuda Spam Firewall sends you a daily quarantine summary report so you can view the quarantined messages you did not receive. From the quarantine summary report you can also add messages to your whitelist, delete messages, and have messages delivered to your inbox.

The following figure shows an example of a quarantine summary report.



Click to access the Quarantine interface to set preferences and classify messages

Select to deliver, whitelist or delete quarantined messages

From: Barracuda Spam Firewall [support@barracudanetworks.com] Sent: Tue 1/13/
To: nguyen@affinitypath.com
Cc:
Subject: Daily Spam Quarantine Summary

Spam Quarantine Summary

Dear **nguyen@affinitypath.com**, this is your daily quarantine summary from the Barracuda Spam Firewall.

You have **3** messages in your spam quarantine inbox.

- Click on the **Deliver** link to have a message delivered to your maibox.
- Click on the **Whitelist** link to have a message delivered to your mailbox and whitelist the sender so that messages will no longer be quarantined.
- Click the **Delete** link to have the message deleted from your quarantine (message will be automatically for spam learning)

Date	From	Subject	Actions
01/12 13:01	"Khoa Nguyen" <khoa_barracu...	**welcome to paris you 1**	Deliver Whitelist Delete
01/07 08:26	Peter Salenger <peteatwork@...	**hi test zip**	Deliver Whitelist Delete
01/08 11:04	"Khoa Nguyen" <khoa_barracu...	**welcome to paris you 1**	Deliver Whitelist Delete

To view your entire quarantine inbox or manage your preferences, click here.

Using the Quarantine Interface

At the end of every quarantine summary report is a link to the quarantine interface where you can set additional preferences and classify messages as spam and not spam.

Logging into the Quarantine Interface

To log into the quarantine interface:

1. Click the link provided at the bottom of the Quarantine Summary Report (displayed above).

   The login page appears.

2. Enter your username and password, and click **Login**.

   Your login information resides in the greeting message sent to you from the Barracuda Spam Firewall.

Managing your Quarantine Inbox

After logging into the quarantine interface, select the QUARANTINE INBOX tab to view a list of your quarantined messages. When you first start using the quarantine interface, you should view this list on a daily basis and classify as many messages as you can.

The Barracuda Spam Firewall has a learning engine that learns how to deal with future messages based on the ones you classify as spam and not spam. The learning engine becomes more effective over time as you teach the system how to classify messages and as you set up rules based on your whitelist and blacklist.

Clicking on an email displays the message.

The following table describes the actions you can perform from this page.

Action	Description
Deliver	Delivers the selected message to your standard email inbox. *Note: If you want to classify a message or add it to your whitelist, make sure to do so before delivering the message to your inbox. Once the Barracuda Spam Firewall delivers a message, it is removed from the quarantine list.*
Whitelist	Adds the selected message to your whitelist so all future emails from this sender are not quarantined unless the message contains a virus or banned file type. The Barracuda Spam Firewall adds the sending e-mail address exactly as it appears in the message to your personal whitelist. Note that some commercial mailings may come from one of several servers such as “mail3.abcbank.com”, and a subsequent message may come from “mail2.abcbank.com”. See the section on managing your whitelists and blacklists for tips on specifying whitelists with greater effectiveness.
Delete	Deletes the selected message from your quarantine list. The main reason to delete messages is to help you keep track of which quarantine messages you have reviewed. You cannot recover messages you have deleted.
Classify as Not Spam	Classifies the selected message as not spam. *Note: Some bulk commercial mail may be considered useful by some users and spam by others. For this reason, classifying such messages may not be very effective because users may counteract each others’ classification. Instead of classifying bulk commercial mail, it may be more effective to add it to your whitelist (if you wish to receive such messages) or blacklist (if you prefer not to receive them).*
Classify as Spam	Classifies the selected message as spam.

Changing your User Preferences

After logging into the quarantine interface, select the PREFERENCES tab to change your account password, modify your quarantine and spam settings, and manage your whitelist and blacklist.

Changing your Account Password

To change your account password, do one of the following:

- On the quarantine interface login page, click **Create New Password**, or
- After logging into the quarantine interface, go to PREFERENCES-->Password.

  In the provided fields, enter your existing password and enter your new password twice. Click **Save Changes** when finished.

Note: Changing your password breaks the links in your existing quarantine summary reports so you cannot delete, deliver, or whitelist messages from those reports. New quarantine summary reports contain updated links that you can use the same as before.

Changing Your Quarantine Settings

The following table describes the quarantine settings you can change from the PREFERENCES-->Quarantine Settings page.

Quarantine Setting	Description
Enable Quarantine	Whether the Barracuda Spam Firewall quarantines your messages. If you select **Yes**, the Barracuda Spam Firewall does not deliver quarantined messages to your general email inbox, but you can view these messages from the quarantine interface and quarantine summary reports. If you select **No**, all messages that would have been quarantined for you are delivered to your general email inbox with the subject line prefixed with “[QUAR]:”. The Barracuda Spam Firewall administrator can modify this prefix.
Notification Interval	The frequency the Barracuda Spam Firewall sends you quarantine summary reports. The default is daily. The Barracuda Spam Firewall only sends quarantine summary reports when one or more of your emails have been quarantined. If you select **Never**, you can still view your quarantined messages from the quarantine interface, but you will not receive quarantine summary reports.
Notification Address	The email address the Barracuda Spam Firewall should use to deliver your quarantine summary report. Leave this field blank to use the email address associated with your user account.

Enabling and Disabling Spam Scanning of your Email

If you do not want the Barracuda Spam Firewall scanning your emails for spam content, you can disable spam filtering from the PREFERENCES-->Spam Settings page. From this page you can also change the default spam scoring levels that determine when your emails are tagged, quarantined or blocked.

When the Barracuda Spam Firewall receives an email for you, it scores the message for its spam probability. This score ranges from 0 (definitely not spam) to 10 or higher (definitely spam). Based on this score, the Barracuda Spam Firewall either allows, quarantines, or blocks the message.

A setting of 10 for any setting disables that option.

Setting	Description
Spam Filter Enable/Disable	
Enable Spam Filtering	Select **Yes** for the Barracuda Spam Firewall to scan your emails for spam. Select **No** to have all your messages delivered to you without being scanned for spam.
Spam Scoring	
Use System Defaults	Select **Yes** to use the default scoring levels. To configure the scoring levels yourself, select **No** and make the desired changes in the Spam Scoring Levels section described below.
Spam Scoring Levels	
Tag score	Messages with a score above this threshold, but below the quarantine threshold, are delivered to you with the word [BULK] added to the subject line. Any message with a score below this setting is automatically allowed. The default value is 3.5.
Quarantine score	Messages with a score above this threshold, but below the block threshold, are forwarded to your quarantine mailbox. The default setting is 10 (quarantine disabled). To enable the quarantine feature, this setting must have a value lower than the block threshold.
Block score	Messages with a score above this threshold are not delivered to your inbox. Depending on how the system is configured, the Barracuda Spam Firewall may notify you and the sender that a blocked message could not be delivered. The default value is 9.

Adding Email Addresses and Domains to Your Whitelist and Blacklist

The PREFERENCES-->Whitelist/Blacklist page lets you specify email addresses and domains from which you do or do not want to receive emails.

List Type	Description
Whitelist	A list of e-mail addresses or domains from which you always wish to receive messages. The only time the Barracuda Spam Firewall filters a message from someone on your whitelist is when the message contains a virus or a disallowed attachment file extension.
Blacklist	A list of senders from whom you never want to receive messages. The Barracuda Spam Firewall immediately discards messages from senders on your blacklist. These messages are not tagged or quarantined and cannot be recovered. The sender does not receive a notice that the message was deleted, and neither do you.

To whitelist or blacklist senders, follow these steps:

1. Go to the PREFERENCES-->Whitelist/Blacklist page.

   A list of your existing whitelisted and blacklisted addresses appears on this page.

2. To delete a whitelist or a blacklist entry, click the trash can icon next to the address.

3. To add an entry, type an e-mail address into the appropriate field, and click the corresponding **Add** button.

Tips on specifying addresses

When adding addresses to your whitelist and blacklist, note the following tips:

- If you enter a full email address, such as *johndoe@yahoo.com*, just that user is specified. If you enter just a domain, such as *yahoo.com*, all users in that domain are specified.

- If you enter a domain such as *barracudanetworks.com*, all subdomains are also included, such as *support.barracudanetworks.com* and *test.barracudanetworks.com*.

- Mass mailings often come from domains that do not resemble the company's web site name. For example, you may want to receive mailings from *historybookclub.com*, but you will find that this site sends out its mailing from the domain *hbcfyi.com*. Examine the From: address of an actual mailing that you are trying to whitelist or blacklist to determine what to enter.

Appendix A About Regular Expressions

The Barracuda Spam Firewall lets you use regular expressions in many of its features. Regular Expressions allow you to flexibly describe text so that a wide range of possibilities can be matched.

Note the following when using regular expressions:

- Be careful when using special characters such as |, *, '.' in your text. For more information, refer to Using Special Characters in Expressions on page 72.
- All matches are case-insensitive.

The following table describes the most common regular expressions supported by the Barracuda Spam Firewall.

Expression	Matches...
Operators	
*	Zero or more occurrences of the character immediately preceding.
+	One or more occurrences of the character immediately preceding.
?	Zero or one occurrence of the character immediately preceding.
|	Either of the characters on each side of the pipe.
( )	Characters between the parenthesis as a group.
Character Classes	
.	Any character except newline
[ac]	Letter 'a' or letter 'c'
[^ac]	Anything but letter 'a' or letter 'c'
[a-z]	Letters 'a' through 'z'
[a-zA-Z.]	Letters 'a' through 'z' or 'A' through 'Z' or a dot
[a-z\-]	Letters 'a' through 'z' or a dash
\d	Digit, shortcut for **[0-9]**
\D	Non-digit, shortcut for **[^0-9]**
\a	Digit, shortcut for **[0-9]**
\w	Part of word: shortcut for **[A-Za-z0-9_]**
\W	Non-word character: shortcut for **[^\w]**
\s	Space character: shortcut for **[\n\r\t]**
\S	Non-space character: shortcut for **[^\s]**
Miscellaneous	
^	Beginning of line
$	End of line
\b	Word boundary
\t	Tab character

Using Special Characters in Expressions

The following characters have a special meaning in regular expressions and should be preprended by a backward slash (\ ) when you want them interpreted literally:

.
[
]
\
*
?
$
(
)
|
^
@

Examples

The following table provides some examples to help you understand how regular expressions can be used.

<table>
<tr><th>Example</th><th>Matches...</th></tr>
<tr><td>viagra</td><td>viagra, VIAGRA or vIaGRa</td></tr>
<tr><td>d+</td><td>One or more digits: 0, 42, 007</td></tr>
<tr><td>(bad|good)</td><td>letters 'bad' or matches the letters 'good'</td></tr>
<tr><td>^free</td><td>letters 'free' at the beginning of a line</td></tr>
<tr><td>v[i1]agra</td><td>viagra or v1agra</td></tr>
<tr><td>v(ia|1a)gra</td><td>viagra or v1agra</td></tr>
<tr><td>v\|agra</td><td>v|agra</td></tr>
<tr><td>v(i|1|\|)?agra</td><td>vagra, viagra, v1agra or v|agra</td></tr>
<tr><td>*FREE*</td><td>*FREE*</td></tr>
<tr><td>*FREE* V.*GRA</td><td>*FREE* VIAGRA, *FREE* VEHICLEGRA, etc</td></tr>
</table>

Index