



Version

Barracuda Spam Firewall Administrator's Guide

Barracuda Networks Inc.
385 Ravendale Drive
Mountain View, CA 94043
<http://www.barracudanetworks.com>

Copyright Notice

Copyright 2005, Barracuda Networks
www.barracudanetworks.com
v3.2.22

All rights reserved. Use of this product and this manual is subject to license. Information in this document is subject to change without notice.

Trademarks

Barracuda Spam Firewall is a trademark of Barracuda Networks. All other brand and product names mentioned in this document are registered trademarks or trademarks of their respective holders.

Chapter 1 – Introduction 9

Overview	10
Energize Updates Minimize Administration and Maximize Protection	10
Understanding Spam Scoring	11
Inbound and Outbound Modes	12
Technical Support	12
Warranty Policy	12
Barracuda Spam Firewall Models.	13
Locating Information in this Document	14
Basic Tab	14
Block/Accept Tab	15
Users Tab	15
Domains Tab	15
Advanced Tab	16

Chapter 2 – Pre-installation 19

Deployment Types	20
Standard Network Configuration Deployment.	21
ISP Installation Deployment 22	
High Availability Deployment	23

Chapter 3 – Setup 25

Step 1. Verify you Have the Necessary Equipment	25
Step 2. Choose a Setup Type	26
Step 3. Install the Barracuda Spam Firewall	26
Step 3. Configure the System IP Address and Network Settings	27
Step 4. Configure your Corporate Firewall	27
Step 5. Configure the Barracuda Spam Firewall	28
Step 6. Update the System Firmware	29
Step 7. Verify your Subscription Status	29
Step 8. Route Incoming Email to the Barracuda Spam Firewall.	31
Port Forwarding	31
MX Records	31
Step 9. Tune the Default Spam Settings	31
Installation Examples	32
Barracuda Spam Firewall Behind Corporate Firewall	32
Barracuda Spam Firewall in the DMZ	33
Configuring your System for Outbound Mode.	33
Outbound Mode Configuration Process.	34
Changing to Outbound Mode	34
Setting up your Email Server as a Smart/Relay Host	34

Chapter 4 – Basic Tab 37

Monitoring System Status	37
Using the Status page	37
Email Statistics	37
Performance Statistics	38
Subscription Status	39
Hourly and Daily Mail Statistics	39
Understanding the Indicator Lights	39
Monitoring the Message Log	40
Legend	41
Classifying Messages	41
Overview of the Message Log.	43
Changing the Viewing Preferences of the Message Log	43
Viewing Message Details	44
Clearing the Message Log	44
Configuring the Global Spam Scoring Limits	44
Specifying the Subject Text and Priority of Tagged Messages	45
Enabling and Disabling Virus Checking and Notification	46
Setting Up Quarantine Policies	46
Specifying the Quarantine Type	47
Specifying the Global Quarantine Settings	48
Specifying the Per-User Quarantine Settings	48
Configuring System IP Information	49
Controlling Access to the Administration Interface	51
Changing the Password of the Administration Account	51
Limiting Access to the Administration Interface and API	51
Changing the Web Interface Port and Session Expiration Length	52
Shutting Down the System	52
Resetting the System Using the Front Panel	53
Automating the Delivery of System Alerts and Notifications	53
Changing the Operation Mode of the System.	53
Enabling Users to Classify Messages from a Mail Client	54
Using the Microsoft Outlook and Lotus Notes Plug-in.	55
Managing the Bayesian Database	55
Resetting the Bayes Database	55
Sending Spam Messages to Barracuda Networks	56
Synchronizing the Bayesian Database	56
Enabling Intent Analysis.	56
Reducing Backscatter	57
Changing the Language of the Administration Interface	57

Chapter 5 – Using the Block and Accept Filters 59

Subscribing to Blacklist Services	59
Blacklist Services Descriptions	60
What Happens if your Domain or IP Address is on a Blacklist	61
IP Address Filters	61
Sender Domain Filters	62
Sender Email Address Filter	63
Recipient Email Address Filter	63
Attachment Type Filter	64

Subject Line Filter	65
Body Filter	66
Header Filter	66

Chapter 6 – Managing Accounts and Domains 69

How the Barracuda Spam Firewall Creates New Accounts	69
Viewing User Accounts	69
Using Filters to Locate Accounts	70
Editing User Accounts	71
Removing Invalid User Accounts	72
Assigning Features to User Accounts	72
Overriding the Quarantine Settings for Specific User Accounts	73
Example	74
Overriding Quarantine Settings	74
Backing Up and Restoring User Settings	74
Setting Retention Policies	75
Adding New Domains	75
Editing Domain Settings	76
Using LDAP to Authenticate Message Recipients	77
Using LDAP for User Authentication	77
Impact of a Down LDAP Server	80
Common LDAP Settings for Standard Mail Servers	80

Chapter 7 – Advanced Administration 83

Modifying the Email Protocol Settings	83
Configuring Message Rate Control	85
Activating Individual Accounts	86
Backing Up and Restoring System Configuration	86
Performing Desktop Backups	87
Automating Backups (inbound mode only)	87
Restoring from a Backup File	88
Updating Spam and Virus Definitions Using Energize Updates	89
Spam Definition Updates	89
Virus Definition Updates	90
Updating the System Firmware Version	90
Customizing the Appearance of the Administration Interface	91
Using a Syslog Server to Centrally Manage System Logs	92
Setting up Trusted Relays and SASL/SMTP Authentication	93
Customizing the Outbound Footer	94
Configuring the Network Interfaces on Models 600 and Above	95
Setting Up Clustered and Standby Systems	95
Cluster Set up Process	95
Data Propagated to the Clustered Systems	96
Field Descriptions for the Clustering Page	97
Impact of Changing the IP Address of a Clustered System	98
Implementing Single Sign-on	99
Enabling SSL	100
Detecting Spam in Chinese and Japanese Messages	102
Customizing Non-Delivery Reports (NDRs)	102
Troubleshooting	104

Generating System Reports	105
Displaying and Emailing Reports	105
Automating the Delivery of Daily System Reports	106
Specifying Report Properties	106
Example Report	107
Enabling SMTP over TLS/SSL	107
Using the Task Manager to Monitor System Tasks	108
Replacing a Failed System	108
Rebooting the System in Recovery Mode	108
Tasks to Perform Before Rebooting in Recovery Mode	109
Performing a System Recovery or Hardware Test	109
Reboot Options	109

Chapter 8 – Outbound 111

Tabs and Pages Supporting Outbound Mode	111
About Outbound Mode	112
Viewing Outbound Messages in the Message Log	113
Changing the Footers on Outbound Messages	113
Specifying Allowed Senders	114
Specifying Allowed Senders by Domain and IP Address	114
Specifying Allowed Senders Using SMTP Authentication	115
Additional Email Protocol Settings for Outbound Mode	115
Enabling Intent Analysis and Spam Scoring	116
Managing the Quarantine Box	117
Sending NDRs for Quarantined Messages	117
Viewing and Classifying Quarantined Messages	117
Using Filters to Locate Specific Messages	118
Configuring Message Rate Control	118
Adding a Relay Server	119
Setting Up Subject and Body Filtering	120

Chapter 9 – Managing Your Quarantine Inbox 121

Receiving Messages from the Barracuda Spam Firewall	121
Greeting Message	121
Quarantine Summary Report	122
Using the Quarantine Interface	122
Logging into the Quarantine Interface	122
Managing your Quarantine Inbox	123
Changing your User Preferences	124
Changing your Account Password	124
Changing Your Quarantine Settings	124
Enabling and Disabling Spam Scanning of your Email	125
Adding Email Addresses and Domains to Your Whitelist and Blacklist	126
Changing the Language of the Quarantine Interface	127

Appendix 1 – Regular Expressions 129

Using Special Characters in Expressions	130
Examples	130

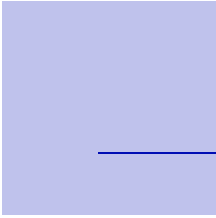
Appendix 2 – Limited Warranty and Licensing 133

Exclusive Remedy 133
Exclusions and Restrictions 134
Open Source Licensing 134

Appendix 3 – Compliance 137

Notice for the USA 137
Notice for Canada 137
Notice for Europe (CE Mark) 137

Index 139



Chapter 1

Introduction

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

<i>Overview</i>	10
<i>Barracuda Spam Firewall Models</i>	13
<i>Energize Updates Minimize Administration and Maximize Protection</i>	10
<i>Inbound and Outbound Modes</i>	12
<i>Technical Support</i>	12
<i>Warranty Policy</i>	12
<i>Locating Information in this Document</i>	14

Overview

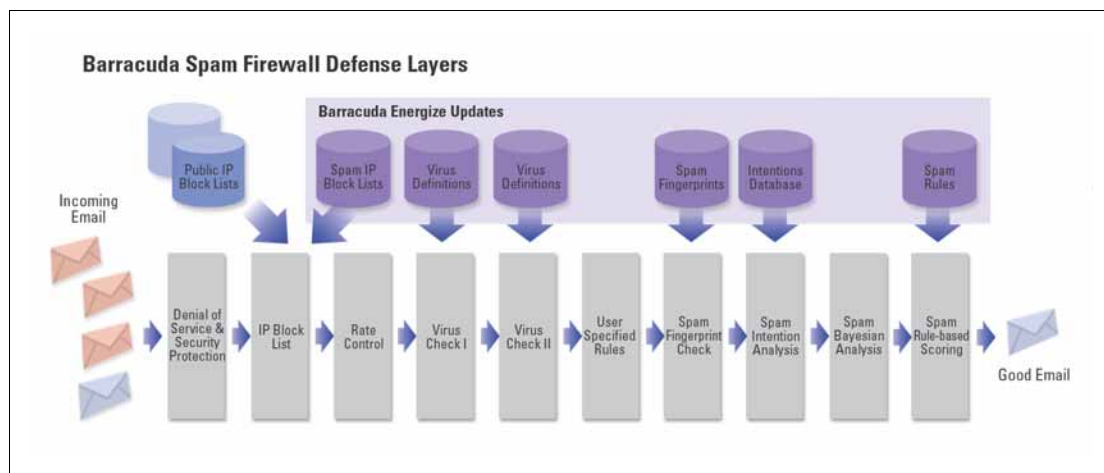
The Barracuda Spam Firewall is an integrated hardware and software solution that provides powerful and scalable spam and virus-blocking capabilities that do not impede the performance of your e-mail servers. The system has no per-user license fee and can be scaled to support tens of thousands of active e-mail 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:

Figure 1.1:



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.

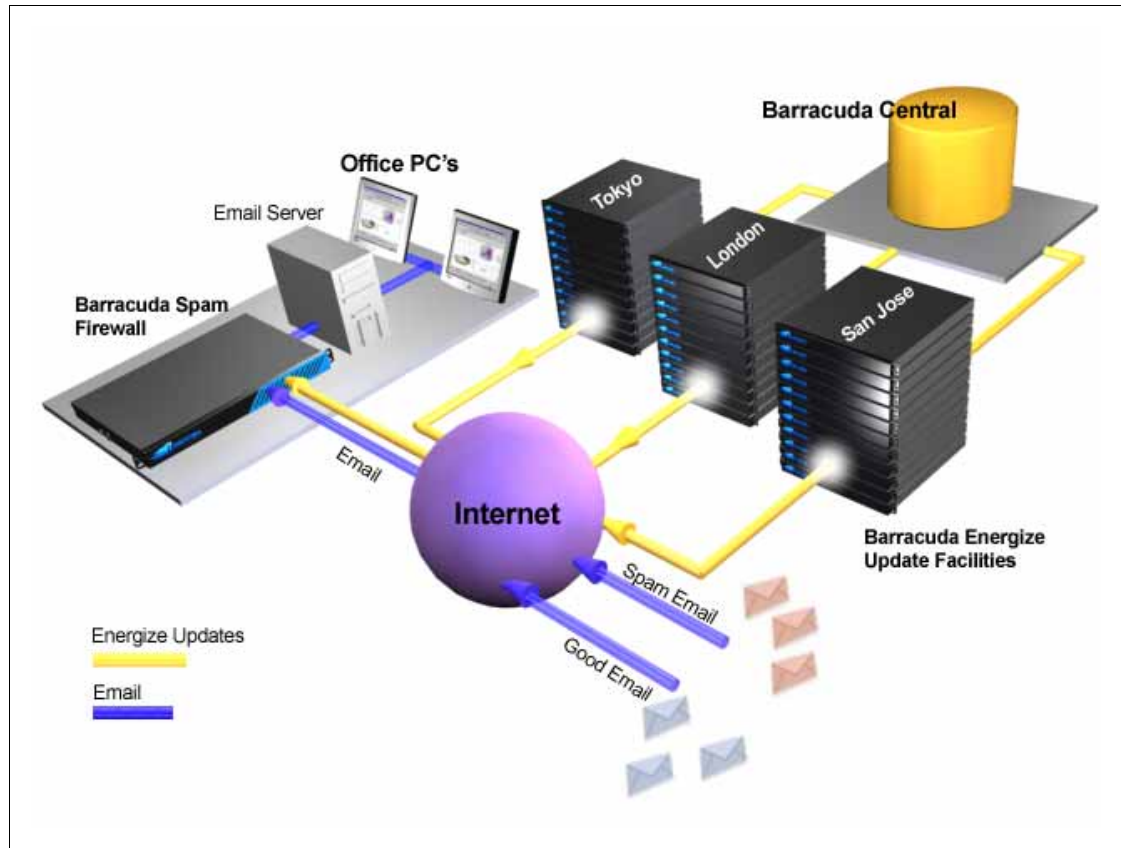
By identifying spam trends at an early stage, the team at Barracuda Central can quickly develop new and improved blocking techniques and virus definitions that are quickly made available to your Barracuda Spam Firewall.

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 Energize.

Figure 1.2:



Understanding Spam Scoring

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

For example, the Barracuda Spam Firewall scrutinizes:

- A message's header and subject line for offensive 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 the spam score for a message that is displayed on the Message Log page of the administration interface.

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

Inbound and Outbound Modes

The Barracuda Spam Firewall can be configured in one of the following two modes:

- Inbound Mode (default) scans all incoming messages for viruses and spam probability. This mode ensures all e-mail delivered to your users is virus-free and legitimate.
- Outbound Mode scans all outgoing messages (from your users) for viruses and spam probability. This mode ensures all e-mail *leaving* your network is virus-free and legitimate.

Your Barracuda Spam Firewall can only operate in one of these two modes. By default, all Barracuda Spam Firewalls are configured for inbound mode when shipped.

For information on how to configure your Barracuda Spam Firewall for outbound mode, refer to *Configuring your System for Outbound Mode* on page 33. For information about the specific features relating to outbound mode, refer to *Chapter 8*.

Technical Support

To contact Barracuda Networks technical support:

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

Warranty Policy

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

Barracuda Spam Firewall Models

The Barracuda Spam Firewall comes in a variety of models. Refer to the following table for the capacity and features available on each model:

Table 1.1:

Feature	Model 200	Model 300	Model 400	Model 600	Model 800	Model 900
Email capacity per day	1 million	2 million	5 million	10 million	15 million	20 million
Active e-mail users	1–500	300–1,000	1,000–5,000	3,000–10,000	8,000–22,000	18,000–25,000
Domains	50	250	500	5,000	5,000	5,000
Compatible with all e-mail servers	✓	✓	✓	✓	✓	✓
Hardened and secure OS	✓	✓	✓	✓	✓	✓
Spam blocking	✓	✓	✓	✓	✓	✓
Virus scanning	✓	✓	✓	✓	✓	✓
Web-based administration interface	✓	✓	✓	✓	✓	✓
Outbound mode	✓	✓	✓	✓	✓	✓
STARTTLS encryption support	✓	✓	✓	✓	✓	✓
SSL support	✓	✓	✓	✓	✓	✓
Per-user settings and quarantine		✓	✓	✓	✓	✓
MS Exchange/LDAP Accelerator		✓	✓	✓	✓	✓
Syslog support		✓	✓	✓	✓	✓
SNMP/API			✓	✓	✓	✓
Per Domain Settings			✓	✓	✓	✓
Clustering			✓	✓	✓	✓
Redundant Disk Array (RAID)			✓	✓	✓	✓
Per-user score settings				✓	✓	✓
Customizeable Branding				✓	✓	✓

Table 1.1:

Feature	Model 200	Model 300	Model 400	Model 600	Model 800	Model 900
Hot Swap Redundant Disk Array (RAID)					✓	✓
Hot Swap Redundant Power Supply					✓	✓
Network Storage						✓

Locating Information in this Document

- This section lists the topics associated with each page in the administration interface.

Basic Tab

The following table lists the topics associated with each page on the Basic tab.

Table 1.2:

Admin Interface Page	Refer to...
Status	<i>Monitoring System Status on page 37</i>
Message Log	<i>Monitoring the Message Log on page 40</i>
Spam Scoring (inbound mode only)	<i>Configuring the Global Spam Scoring Limits on page 44</i> <i>Specifying the Subject Text and Priority of Tagged Messages on page 45</i>
Virus Checking	<i>Enabling and Disabling Virus Checking and Notification on page 46</i>
Quarantine	<i>Setting Up Quarantine Policies on page 46</i>
IP Configuration	<i>Configuring System IP Information on page 49</i>
Administration	<i>Controlling Access to the Administration Interface on page 51</i> <i>Shutting Down the System on page 52</i> <i>Automating the Delivery of System Alerts and Notifications on page 53</i> <i>Changing the Operation Mode of the System on page 53</i>
Bayesian/Intent (inbound mode only)	<i>Enabling Users to Classify Messages from a Mail Client on page 54</i> <i>Managing the Bayesian Database on page 55</i> <i>Enabling Intent Analysis on page 56</i>

Block/Accept Tab

The following table lists the topics associated with each page on the Block/Accept tab.

Table 1.3:

Admin Interface Page	Refer to...
External Blacklists (inbound mode only)	<i>Subscribing to Blacklist Services on page 59</i>
IP Block/Accept	<i>IP Address Filters on page 61</i>
Sender Domain Block/Accept	<i>Sender Domain Filters on page 62</i>
Email Sender Block/Accept	<i>Sender Email Address Filter on page 63</i>
Email Recipient Block/Accept	<i>Recipient Email Address Filter on page 63</i>
Attachment Filtering	<i>Attachment Type Filter on page 64</i>
Subject Filtering	<i>Subject Line Filter on page 65</i>
Body Filtering	<i>Body Filter on page 66</i>
Header Filtering	<i>Header Filter on page 66</i>

Users Tab

The following table lists the topics associated with each page on the Users tab. This tab is not available in outbound mode or in models 200, 300 and 400).

Table 1.4:

Admin Interface Page	Refer to...
Account View	<i>Viewing User Accounts on page 69</i> <i>Editing User Accounts on page 71</i> <i>Removing Invalid User Accounts on page 72</i>
User Features	<i>Assigning Features to User Accounts on page 72</i>
User Add/Update	<i>Overriding the Quarantine Settings for Specific User Accounts on page 73</i>
User Backup/Restore	<i>Backing Up and Restoring User Settings on page 74</i>
Retention Policies	<i>Setting Retention Policies on page 75</i>

Domains Tab

The following table lists the topics associated with each page on the Domains tab. This tab is not available in models 200 and 300.

Table 1.5:

Admin Interface Page	Refer to...
Domain Manager	<i>Adding New Domains on page 75</i> <i>Editing Domain Settings on page 76</i> <i>Using LDAP to Authenticate Message Recipients on page 77</i>

Advanced Tab

The following table lists the topics associated with each page on the Advanced tab.

Table 1.6:

Admin Interface Page	Refer to...
Email Protocol	<i>Modifying the Email Protocol Settings on page 83</i>
Rate Controls	<i>Configuring Message Rate Control on page 85</i>
Explicit Users (inbound mode only)	<i>Activating Individual Accounts on page 86.</i>
Backup	<i>Backing Up and Restoring System Configuration on page 86</i>
Energize Updates	<i>Updating Spam and Virus Definitions Using Energize Updates on page 89</i>
Firmware Update	<i>Updating the System Firmware Version on page 90</i>
Appearance (inbound mode only)	<i>Customizing the Appearance of the Administration Interface on page 91 (not supported in models 200/300/400)</i>
Syslog	<i>Using a Syslog Server to Centrally Manage System Logs on page 92 (not supported in model 200)</i>
Outbound / Relay (inbound mode only)	<i>Setting up Trusted Relays and SASL/SMTP Authentication on page 93</i>
Outbound Footer	<i>Customizing the Outbound Footer on page 94</i>
Advanced IP Configuration (inbound mode only)	<i>Configuring the Network Interfaces on Models 600 and Above on page 95</i>
Clustering	<i>Setting Up Clustered and Standby Systems on page 95 (not supported in model 200/300)</i>
Single Sign-on (inbound mode only)	<i>Implementing Single Sign-on on page 99 (not supported in model 200/300)</i>
SSL	<i>Enabling SSL on page 100</i>
Regional Settings	<i>Detecting Spam in Chinese and Japanese Messages on page 102</i>
Bounce/NDR Messages	<i>Customizing Non-Delivery Reports (NDRs) on page 102</i>
Troubleshooting	<i>Troubleshooting on page 104</i>

Table 1.6:

Admin Interface Page	Refer to...
Reporting	<i>Generating System Reports on page 105</i>
SMTP / TLS	<i>Enabling SMTP over TLS/SSL on page 107</i>
Task Manager	<i>Using the Task Manager to Monitor System Tasks on page 108</i>



Chapter 2

Pre-installation

This chapter provides an overview of the Barracuda Spam Firewall deployment issues that you must consider before you install the Barracuda Spam Firewall on your network.

- *Deployment Types* on page 20

Deployment Types

When deciding how best to deploy your Barracuda IM Firewall, consider both the capabilities of the Barracuda IM Firewall and the components in your network. You can deploy the appliance in a variety of deployment types depending on your needs. The Barracuda IM Firewall provides the flexibility to meet the needs of complex enterprise networks. It supports multiple external network connections, asymmetric routing, servers containing sensitive and important information, multiple VLANs, and more.

The recommended installation deployment type is the Standard Network Configuration. In this deployment, the Barracuda Spam Firewall is able to scan all inbound and outbound Internet traffic for spam and viruses. The descriptions below give a general information each deployment type.

Note



The deployment for your network may vary.

- **Standard Network Configuration:** The Barracuda Spam Firewall is connected to your core Internet network components and all network traffic to the Internet passes through the Barracuda Spam Firewall.
- **ISP Installation:** This deployment is used by Internet Service Providers. In this deployment the Barracuda Spam Firewall is configured to interact with these ISPs.
- **High Availability:** The Barracuda Spam Firewall is installed and configured in separate networks and are then clustered to interact with each other.

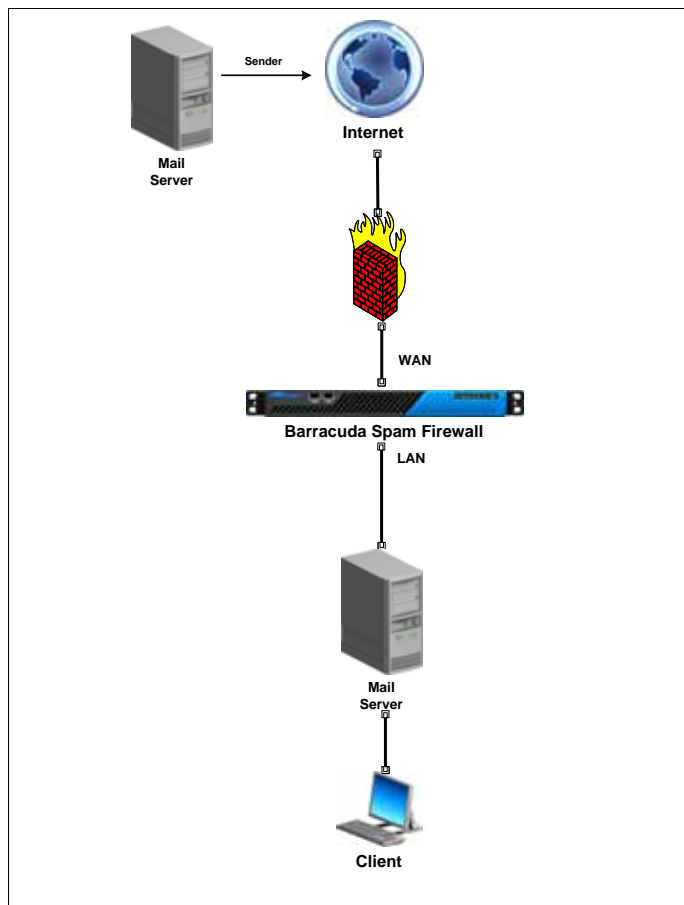
Standard Network Configuration Deployment

Standard Network Configuration requires all Internet requests to pass through the Barracuda Spam Firewall. The Barracuda Spam Firewall is installed directly to the Internet firewall/router. With the Barracuda Spam Firewall connected to your core Internet network components, it is able to filter and scan all Internet traffic requests. It performs content filtering and scans downloads for spam and viruses. It also detects and blocks outbound spam protocol requests, which identifies infected clients on your network.

The most straightforward deployment of the Barracuda Spam Firewall is the Standard Network Configuration Deployment. The Barracuda Spam Firewall scans all outbound traffic for spam activity on all ports to detect infected clients.

Figure 2.1 illustrates a basic installation using the Standard Network Configuration.

Figure 2.1: Standard Network Configuration Deployment

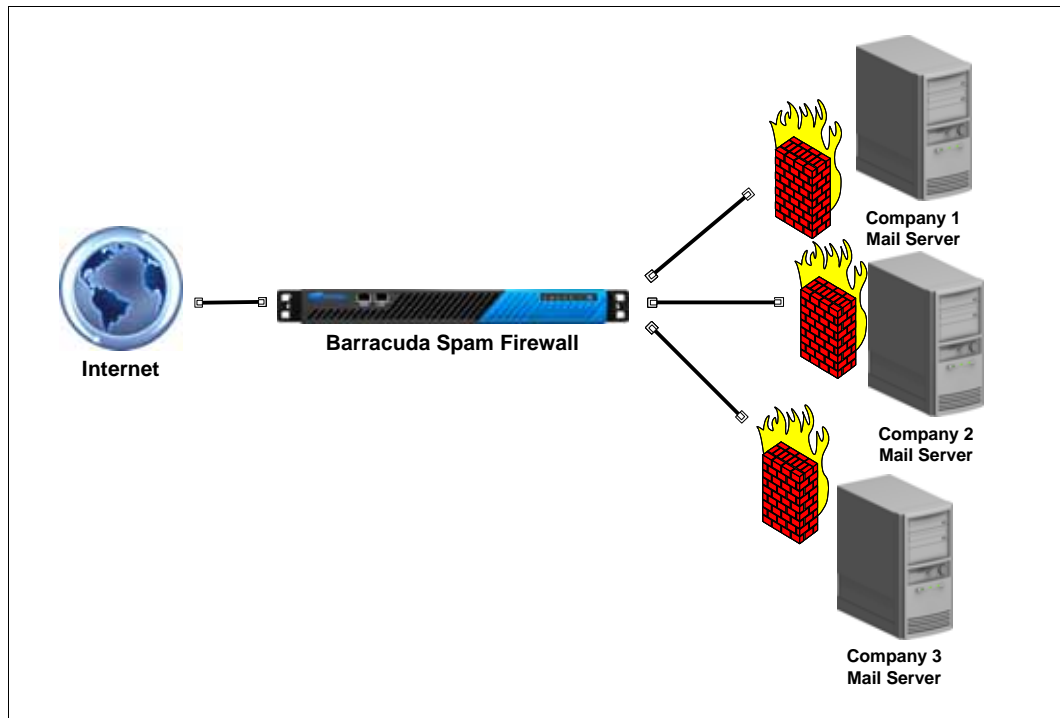


ISP Installation Deployment

This deployment type is typically used by Internet Service Providers. The Barracuda Spam Firewall is configured to interact with these providers.

In this deployment, the Barracuda Spam Firewall detects all network traffic. The proxy server connects directly to the Barracuda Spam Firewall LAN port. The Barracuda Spam Firewall scans for all inbound and outbound HTTP traffic from the proxy server. All outbound traffic on other ports are scanned for normal spam communication. *Figure 2.2* illustrates the ISP Installation Deployment. .

Figure 2.2: ISP Installation Deployment

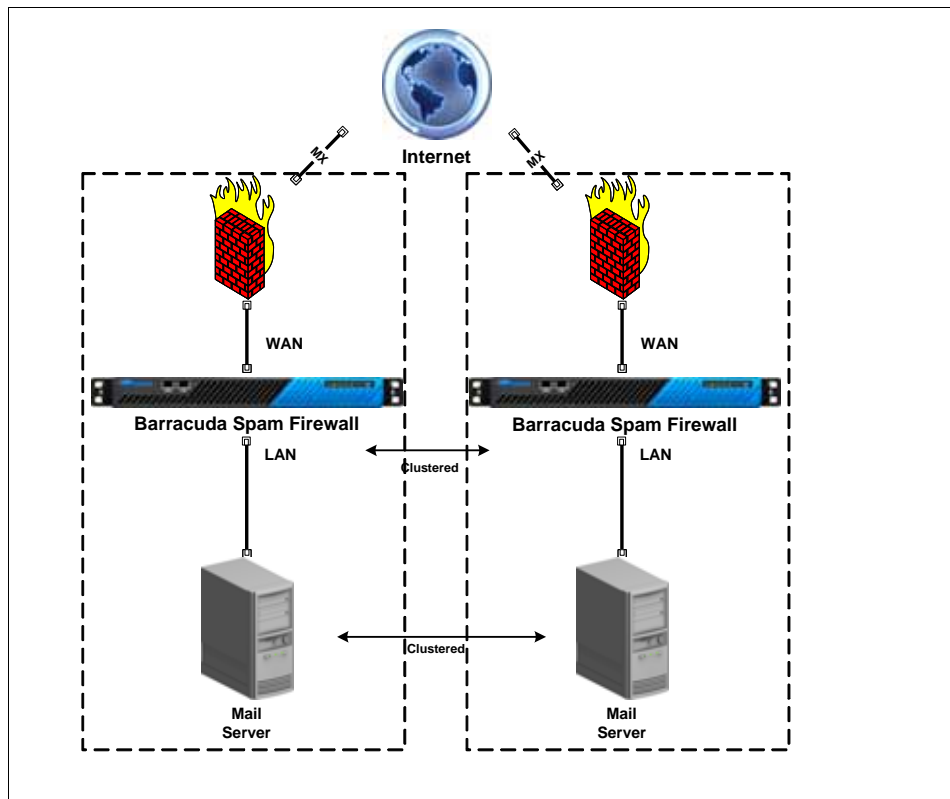


High Availability Deployment

The High Availability deployment is configured in two separate networks and these networks are then clustered to interact with one another. You can combine the Barracuda Spam Firewall appliance with other nodes and appliances into a cluster. One node within the cluster functions as the master node, and the others act as slaves. You can access and configure all nodes in the cluster from the same Web GUI. You can configure cluster parameters on the master node, which then propagate to the slave nodes. The Barracuda Spam Firewall scans the HTTP traffic for spam and viruses; it also provides content filtering.

Figure 2.3 illustrates a basic installation using the High Availability Deployment.

Figure 2.3: High Availability Deployment



This chapter covers:

<i>Installation Examples</i>	32
<i>Barracuda Spam Firewall Behind Corporate Firewall</i>	32
<i>Barracuda Spam Firewall in the DMZ</i>	33
<i>Configuring your System for Outbound Mode</i>	33
<i>Outbound Mode Configuration Process</i>	34
<i>Changing to Outbound Mode</i>	34
<i>Setting up your Email Server as a Smart/Relay Host</i>	34

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

1. Verify you have the necessary equipment (on this page)
2. Choose the inline or pass through method for your Barracuda Spam Firewall installation.
3. Install the Barracuda Spam Firewall (*page 26*)
4. Configure the system IP address and network settings (*page 27*)
5. Configure your corporate firewall (*page 27*)
6. Configure the Barracuda Spam Firewall (*page 28*)
7. Update the system firmware (*page 29*)
8. Verify your subscriptions are active (*page 29*)
9. Route incoming e-mail to the Barracuda Spam Firewall (*page 31*)
10. Tune the default spam settings (*page 31*)

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

Note



If you use your Barracuda Spam Firewall to scan outgoing messages instead of incoming messages, refer to Configuring your System for Outbound Mode on page 33 before you start installing the system.

Step 1. Verify you Have the Necessary Equipment

Before installing your Barracuda Spam Firewall, make sure you have the following equipment:

- Barracuda Spam Firewall (check that you have received the correct model)
- AC power cord

- Ethernet cables
- Mounting rails (models 600, 800, and 900 only)
- VGA monitor (recommended)
- PS2 keyboard (recommended)

Step 2. Choose a Setup Type

Choose the Standard Network Configuration, the ISP Installation, or the High Availability Configuration Deployment..

Step 3. Install the Barracuda Spam Firewall

To physically install the Barracuda Spam Firewall:

1. Fasten the Barracuda Spam Firewall to 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 from your network switch to the Ethernet port on the back of your Barracuda Spam Firewall.

The Barracuda Spam Firewall supports both 10BaseT and 100BaseT Ethernet. Barracuda Networks recommends using a 100BaseT connection for best performance.

Note



The Barracuda Spam Firewall 600 and 800 support Gigabit Ethernet and has two usable LAN ports. On these models, 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 the following to your Barracuda Spam Firewall:
 - Power cord
 - VGA monitor
 - PS2 keyboard

After you connect the AC power cord the Barracuda Spam Firewall may power on for a few seconds and then power off. This is standard behavior.

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

The login prompt for the administrative console is displayed on the monitor, and the light on the front of the system turns on. For a description of each indicator light, refer to *Understanding the Indicator Lights* on page 39.

Step 3. Configure the System IP Address and Network Settings

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. At the `barracuda login` prompt enter `admin` for the login and `admin` for the password. The User Confirmation Requested window displays the current IP configuration of the system.
2. Using the Tab key, select **Yes** to change the IP configuration.
3. Enter the new IP address, netmask, and default gateway for your Barracuda Spam Firewall, and select **OK** when finished.
4. Select **No** when prompted if you want to change the IP configuration.
The new IP address and network settings are applied to the Barracuda Spam Firewall.

Step 4. Configure your Corporate Firewall

If your Barracuda Spam Firewall is located behind a corporate firewall, you need to open specific ports to allow communication between the Barracuda Spam Firewall and remote servers.

To configure your corporate firewall:

1. Using the following table as a reference. Open the specified ports on your corporate firewall:

Table 3.1:

Port	Direction	Protocol	Used for...
22	In	TCP	Remote diagnostics and technical support services (optional)
25	In/Out	TCP	Email and e-mail bounces
53	Out	TCP/UDP	Domain Name Server (DNS)
80	Out	TCP	Virus, firmware and spam rule updates
123	In/Out	UDP	NTP (Network Time Protocol)

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

Step 5. Configure the Barracuda Spam Firewall

After specifying the IP address of the system and opening the necessary ports on your firewall, you need to configure the Barracuda Spam Firewall from the administration interface. Make sure the computer from which you configure 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 followed by port 8000.
Example: <http://192.168.200.200:8000>
2. Log in to the administration interface by entering `admin` for the username and `admin` for the password.
3. Select **Basic > IP Configuration** and enter the required information.
The following table describes the fields you need to populate.

Table 3.2:

Fields	Description
TCP/IP Configuration	The IP address, subnet mask, and default gateway of your Barracuda Spam Firewall. TCP port is the port on which the Barracuda Spam Firewall receives inbound e-mail. This is usually port 25.
Destination Mail Server TCP/IP Configuration	The hostname or IP address of your destination e-mail server, for example <i>mail.yourdomain.com</i> . This is the mail server that receives e-mail 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 e-mail. This is usually port 25. If you need to set up more than one domain or mail server, refer to <i>Adding New Domains</i> on page 75.
DNS Configuration	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 e-mail 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 e-mail messages (non-delivery receipts, virus alert notifications, etc.) sent from the Barracuda Spam Firewall.

Table 3.2:

Fields	Description
Allowed Email Recipients Domain(s)	<p>The domains managed by the Barracuda Spam Firewall. Make sure this list is complete. The Barracuda Spam Firewall rejects all incoming messages addresses to domains not in this list.</p> <p>To allow messages for all domains that match your mail server, put an asterisk (*) in this field.</p> <p><i>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.</i></p>

4. Click **Save Changes**.

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

5. Select **Basic > Administration** and perform the following tasks:

5a. Assign a new administration password to the Barracuda Spam Firewall (optional).

5b. Make sure the local time zone is set correctly.

Time on the Barracuda Spam Firewall 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 time zone be set correctly because this information is used to determine the delivery times for messages and may appear in certain mail reading programs.

6. Click **Save Changes**.

Step 6. Update the System Firmware

To upgrade the firmware on the Barracuda Spam Firewall:

1. Select **Advanced > Firmware Update**.

2. Click **Download Now** and then **OK** on the download duration window.

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

If the system has the latest firmware version downloaded, the **Download Now** button disables.

The system begins downloading the latest firmware version. A message displays once the download is complete.

3. Click **Apply Now** when the download completes.

4. Click **OK** when prompted to reboot the system.

5. Read the release notes to learn about the latest features and fixes provided in the updated firmware version. You can access the release notes from the **Advanced > Firmware Update**.

Step 7. Verify your Subscription Status

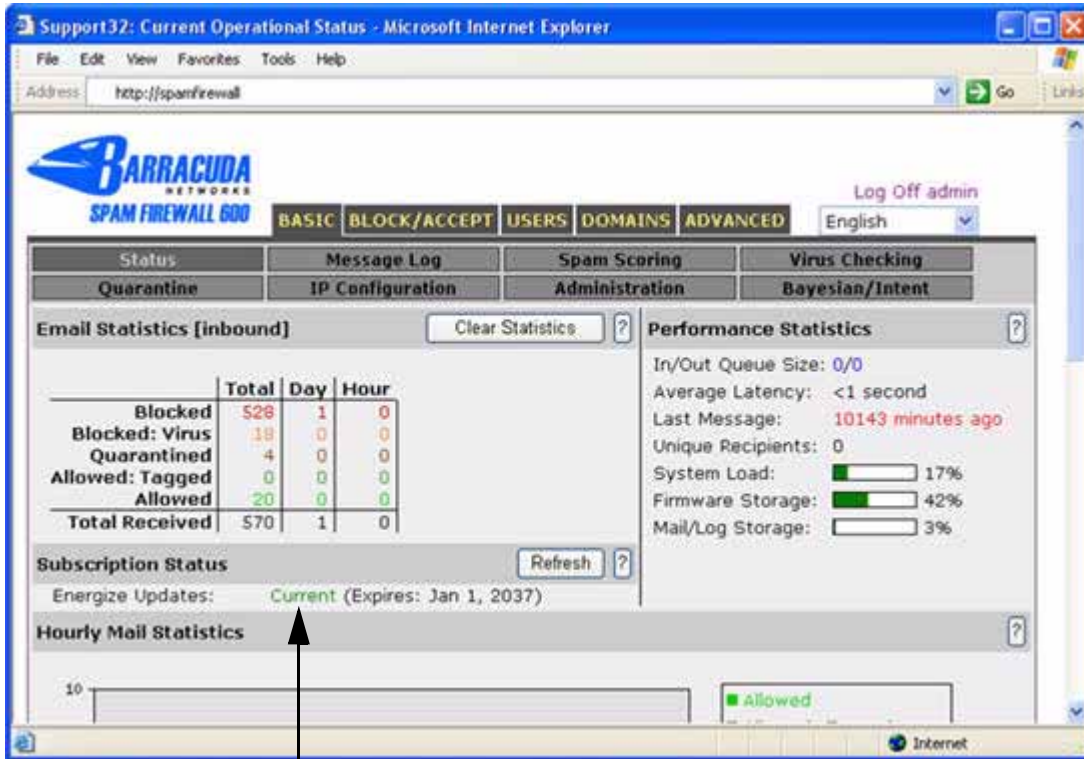
Once you install the Barracuda Spam Firewall, your Energize Update and Instant Replacement subscriptions are active. However, it is important you verify the subscription status so your Barracuda

Spam Firewall receives the latest virus and spam updates from Barracuda Central. The Energize Update service is responsible for downloading these virus and spam definitions to your system.

To check your subscription status:

1. Select **Basic > Status**.
2. In the Subscription Status section, verify the word *current* appears next to Energize Updates and Replacement Service (if purchased).

The following graphic shows the location of the Subscription Status section.



Verify your subscriptions are current

3. If the status of your subscription is Not Activated, do the following:
 - 3a. Click the activate link as shown in the following example. This opens the product activation page.



- 3b. On the product activation page, fill in the required fields and click **Activate**. A confirmation page opens that displays the terms of your subscription.
 - 3c. After a couple minutes, click **Refresh** in the Subscription Status section of the **Basic > Status** page. The status of your subscriptions should now be displayed as *Current*.

Note



If your subscription status does not change to *Current*, or if you have trouble filling out the product activation page, call Barracuda Networks at 888-ANTISPAM and ask for a sales or support representative.

Step 8. Route Incoming Email to the Barracuda Spam Firewall

The next step in setting up your Barracuda Spam Firewall is to route incoming e-mail to the system so it can scan incoming messages for spam and viruses. You can use either of the following methods to route messages to your Barracuda Spam Firewall:

- Port forwarding (used when your Barracuda Spam Firewall is behind a corporate firewall)
- MX records (used when your Barracuda Spam Firewall is in the DMZ)

Note



Do not try to route outgoing e-mail through the Barracuda Spam Firewall unless you have configured the Relay operation or are using the Barracuda Spam Firewall in outbound mode.

After you route incoming e-mail to the Barracuda Spam Firewall, it will start filtering all e-mails it receives and route the good e-mail to your e-mail server.

Port Forwarding

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.

For more information about port forwarding, refer to your firewall documentation or administrator.

MX Records

If your Barracuda Spam Firewall is in the DMZ (not protected by your corporate firewall), do the following to route incoming messages to the system:

1. Create a DNS entry for your 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
```

2. Change your DNS MX Records.

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

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

Step 9. Tune the Default Spam Settings

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

Initially, your Barracuda Spam Firewall is configured to tag most spam by adding the word “[BULK]” to the subject line of messages. Once you have more experience with the Barracuda Spam Firewall you can adjust how aggressively the system deals with spam. For example, you may decide to quarantine spam instead of blocking it.

The following table describes the most common tasks you should perform when first tuning your system.

Table 3.3:

Task	Refer to
Monitor and Classify Incoming Emails	<i>Classifying Messages</i> on page 41
Verify the Spam Scoring Defaults	<i>Configuring the Global Spam Scoring Limits</i> on page 44
Set Up Quarantine (optional)	<i>Setting Up Quarantine Policies</i> on page 46
Block Messages from Specific IP Addresses, Domains or Email Accounts	<i>Chapter 5 Using the Block and Accept Filters</i>

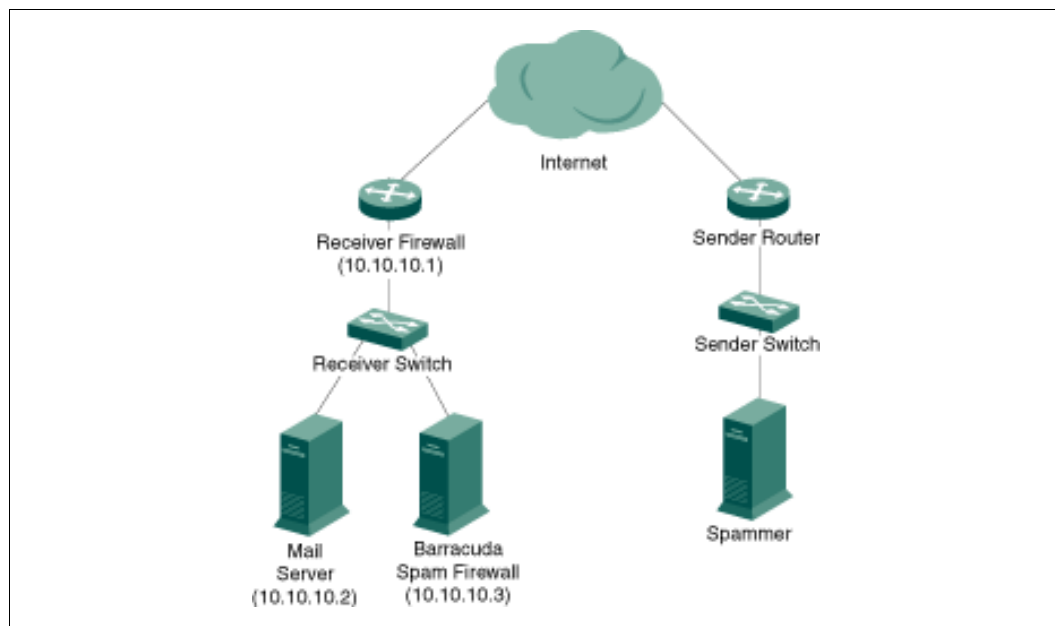
Installation Examples

This section provides example installation scenarios you can reference to help 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.

Figure 3.1:



In this type of setup, perform the following tasks:

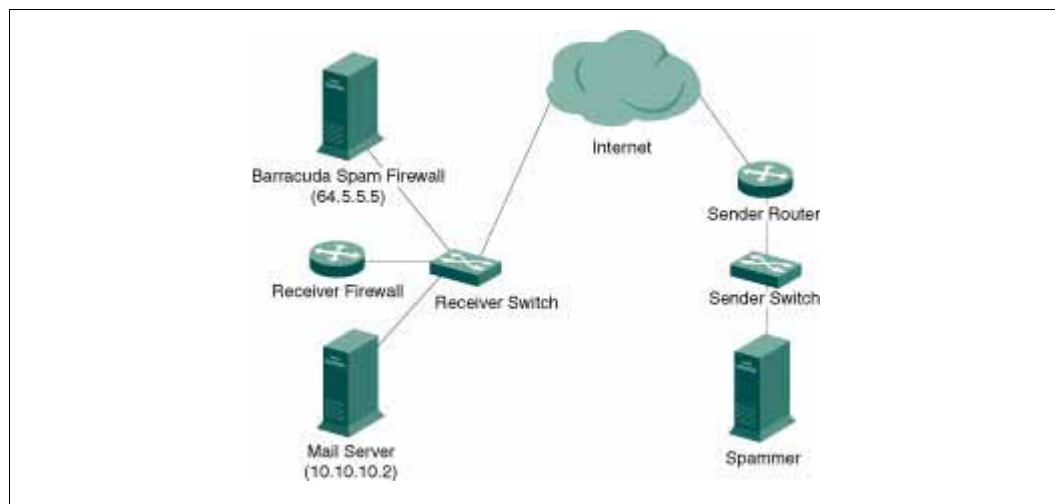
- Forward (port redirection) incoming SMTP traffic on port 25 to the Barracuda Spam Firewall at 10.10.10.3.
- Configure the Barracuda Spam Firewall to forward filtered messages to the destination mail server at 10.10.10.2.

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

Barracuda Spam Firewall in the DMZ

The figure below shows the Barracuda Spam Firewall in front of your corporate firewall in the DMZ. 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.

Figure 3.2:



In this type of setup, perform the following tasks:

- 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 10barracuda.yournetwork.com
```

Configuring your System for Outbound Mode

Your Barracuda Spam Firewall can operate in one of the following two modes:

- Inbound Mode (default) scans all incoming messages for viruses and spam probability.
- Outbound Mode scans all outgoing messages (from your users) for viruses and spam probability. This mode ensures all e-mail leaving your network is virus-free and legitimate.

Outbound Mode Configuration Process

Your Barracuda Spam Firewall can only operate in one of these two modes. By default, all Barracuda Spam Firewalls are configured for inbound mode when shipped.

Follow this general process to set up your Barracuda Spam Firewall for outbound mode:

1. Complete steps 1-7 described earlier in this chapter.
2. Change the mode of your Barracuda Spam Firewall from inbound to outbound (described on *page 34*).
3. Set up your e-mail server as a smart/relay host.

Changing to Outbound Mode

Before you change the mode from inbound to outbound, consider the following:

- All your message log data and quarantine messages are deleted.
- System configuration remains in tact. However, you should verify that the configuration options are appropriate for outbound mode.

If you are changing the mode on a brand new system you do not have to worry about these considerations. However, if your Barracuda Spam Firewall has been operating for a while in inbound mode, you need to consider the impact of changing modes.

To change from inbound to outbound mode:

1. Select **Basic** > **Administration**.
2. In the Operation Mode section, click **Convert**.
3. Click **OK** to confirm you want to change your Barracuda Spam Firewall to outbound mode.

A status bar displays the progress of switching your Barracuda Spam Firewall to outbound mode. Once the switchover completes, your Barracuda Spam Firewall automatically reboots.

Setting up your Email Server as a Smart/Relay Host

The last step in setting up your Barracuda Spam Firewall for outbound mode is to configure your internal mail server to deliver all outgoing messages to the Barracuda Spam Firewall before those messages are sent out. This is done by setting up your e-mail server as a smart/relay host.

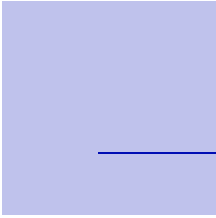
The following Web sites provide instructions on how to set up specific e-mail servers as a smart/relay host. For additional information, consult your e-mail server administrator and documentation.

Table 3.4:

Email Server	Refer to...
Microsoft Exchange Server 2003	http://support.microsoft.com/kb/265293
Novell Groupwise Server	http://www.novell.com/documentation/gw55/index.html?page=/documentation/gw55/gw55ia/data/a2zi22h.html

Table 3.4:

Email Server	Refer to...
Lotus Domino Server	http://www-12.lotus.com/ldd/doc/domino_notes/Rnext/help6_admin.nsf/f4b82fbb75e942a6852566ac0037f284/14cdfeaa188fa90a85256c1d003955af?OpenDocument



Chapter 4

Basic Tab

This chapter covers basic administration tasks, most of which can be performed from the BASIC tab.

- Monitoring System Status* 37
- Using the Status page* 37
- Email Statistics* 37
- Performance Statistics* 38
- Subscription Status* 39
- Hourly and Daily Mail Statistics* 39
- Understanding the Indicator Lights*..... 39
- Monitoring the Message Log*..... 40
- Legend*..... 41
- Classifying Messages*..... 41

Monitoring System Status

You can monitor the status of your Barracuda Spam Firewall by viewing the following:

- **Basic > Status** page in the administration interface
- Indicator lights on the front of the system

Using the Status page

The **Basic > Status** page provides an overview of the health and performance of your Barracuda Spam Firewall. From this page you can view:

- E-mail statistics that display how many messages the system has blocked and quarantined
- Performance statistics

Email Statistics

The following table describes the e-mail statistics displayed on the Status page.

Table 4.1:

Statistic	Description
Blocked	Number of virus and spam messages blocked by the system.

Table 4.1:

Statistic	Description
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 <i>Setting Up Quarantine Policies</i> on page 46.
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 44).
Allowed	Number of messages delivered to the intended recipient without being blocked or modified.
Total	Email statistics for the system since installation or the last reset.
Day	Email statistics for the current calendar day (from midnight to midnight).
Hour	Email 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

The following table describes the system environmental conditions displayed on the Status page.

Note



Statistics displayed in red signify that the value exceeds the normal threshold.

Table 4.2:

Statistic	Description
In/Out Queue Size	Displayed as a ratio, such as 10/5. The first number represents the amount of inbound mail, which includes accepted messages waiting for virus and spam scanning. The second number represents the amount of outbound mail in the queue. Click on the inbound or outbound number to see a summary of the messages currently in the queue.
Average Latency	Average elapsed time it takes the system to tag, quarantine, or deliver a message.
Last Message	How long ago the last message was delivered.
Unique Recipients	Number of unique recipients receiving e-mail during the last 24 hours. This number does <i>not include</i> recipients that were rejected.

Table 4.2:

Statistic	Description
System Load	Estimate of the CPU and disk load on the system. 100% system load is not unusual, especially when the incoming queue is large. However, 100% load for long periods of time could indicate an internal system issue, especially if the incoming queue continues to grow.
Redundancy	Status of the RAID system. <i>Note: The redundancy statistics do not appear for the 200 and 300 models.</i>
Firmware Storage	Amount of disk storage used for various system components.
Mail/Log Storage	Amount of disk storage used for messages and log store.

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

Subscription Status

This section identifies if the following subscriptions are current or expired:

- Energize update
- Instant Replacement (*optional service*)

If one of these subscriptions has expired, contact your Barracuda Networks sales representative to re-activate your subscription.

Hourly and Daily Mail Statistics

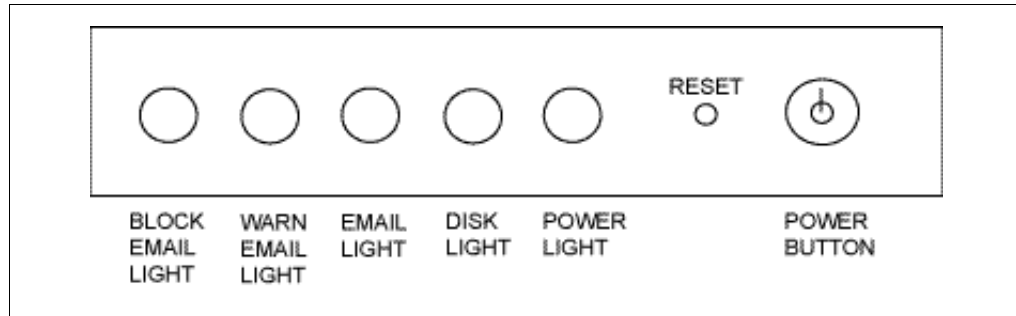
Shows the number of messages blocked, quarantined, and allowed for the last 25 days and 24 hours.

Understanding the Indicator Lights

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

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

Figure 4.1:



The following table describes each indicator light.

Table 4.3:

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

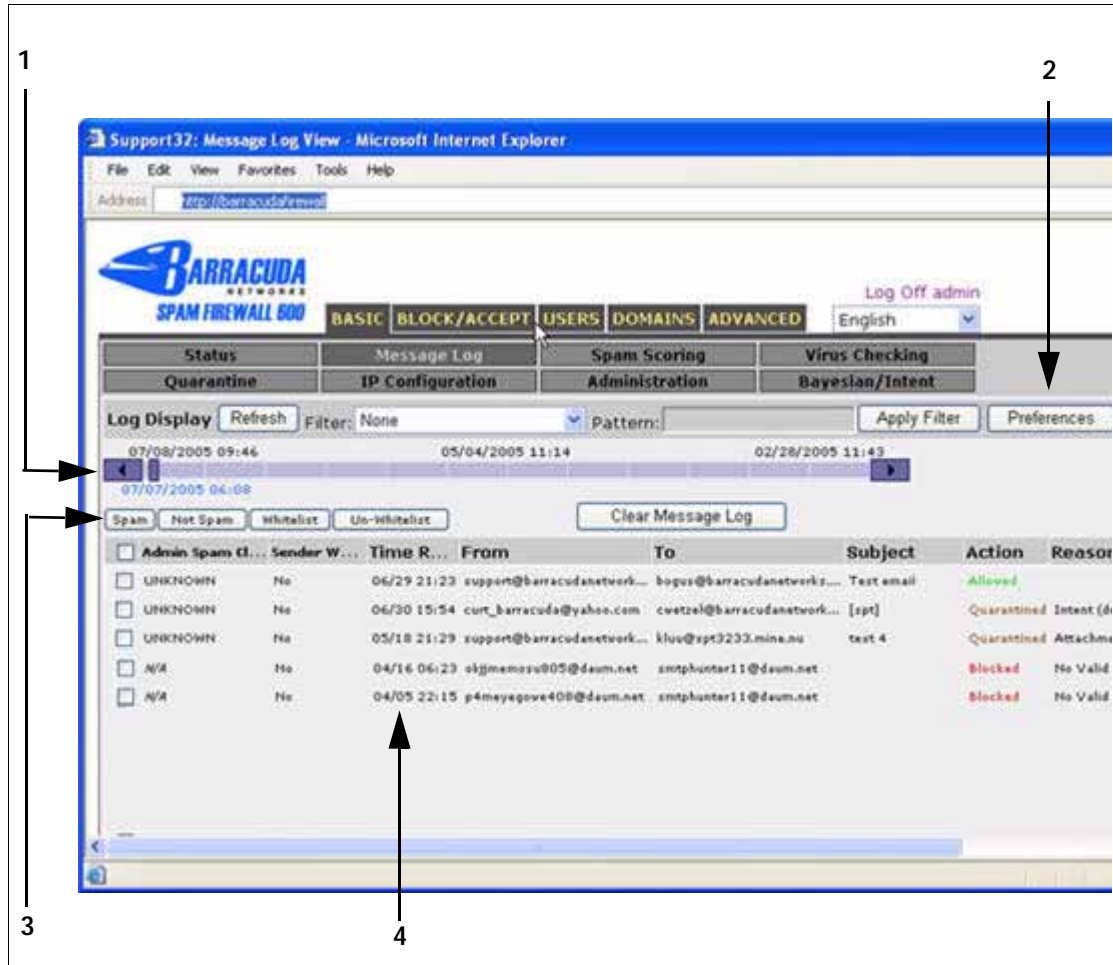
Monitoring the Message Log

On a regular basis you should monitor incoming messages from the Message Log page, and classify as many messages as you can as spam or not spam, as well as add messages to the global whitelist.

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

The following figure identifies the main elements of the Message Log.

Figure 4.2:



Legend

1. Slider bar lets you select the time frame of the message log.
2. Preferences button lets you customize the message log display.
3. Classification buttons let you mark messages as spam and not spam and add senders to the global whitelist.
4. List of all messages for the specified time frame. Click an entry to view the message details.

Classifying Messages

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 Message Log page.

Table 4.4:

Button	Description
Spam	<p>Classifies the message as spam in the Bayesian database.</p> <p>The Bayesian database becomes active once 200 spam messages and 200 not spam messages have been classified. At that time, the Barracuda Spam Firewall begins scanning messages to determine how closely they match the messages identified as spam. This comparison determines a message's spam score.</p> <p>If per-user quarantine is enabled, message classification performed by each individual user is also applied to the Bayesian database.</p> <p>To view the number of messages currently classified as Spam, go to the BASIC--> Bayesian/Intent page.</p> <p><i>Note: 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/Intent page covered on page 56.</i></p>
Not Spam	<p>Classifies the message as Not Spam in the Bayesian database.</p> <p>The Bayesian database becomes active once 200 spam messages and 200 not spam messages have been classified. At that time, the Barracuda Spam Firewall begins scanning messages to determine how closely they match the messages identified as not spam. This comparison determines a message's spam score.</p> <p>If per-user quarantine is enabled, message classification performed by each individual user is also applied to the Bayesian database.</p> <p>To view the number of messages currently classified as Not Spam, go to the BASIC-->Bayesian/Intent page.</p>
Whitelist	<p>Adds the sender of the message to the global whitelist. Messages from whitelisted senders do not receive a spam score.</p> <p>Messages from whitelisted senders still go through:</p> <ul style="list-style-type: none"> • Virus checking • Attachment type filtering (covered on page 64) • Blocking filters for header, body and subject content (covered Chapter 5 Using the Block and Accept Filters)
Un-Whitelist	<p>Removes the sender of the message from the global whitelist.</p>
Clear Message Log	<p>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.</p>

Overview of the Message Log

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

Table 4.5:

Column	Description
Admin 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.
Sender Whitelisted	Identifies if the sender is included in the global whitelist. All messages from whitelisted senders are allowed unless a virus is detected or the message contains an unallowed attachment type.
Time Received	The date and time the Barracuda Spam Firewall received the e-mail.
From / To	The e-mail 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	<p>The reason for the action, such as the sender is on your blacklist or the message has been identified as spam.</p> <p>In some cases this column may show "Message Size" as the reason an e-mail 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.</p> <p>Even though messages over 65k in size are not scanned for spam, they are always scanned for viruses.</p>
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.
Delivery Status	The status of the message in the outbound queue if the message is being delivered to the destination server.
Delivery Detail	Details on the outbound status of the message.

Changing the Viewing Preferences of the Message Log

To change the format of the message log, click **Preferences** on the right side of the page so you can:

- Hide columns you do not want displayed.
- Change the order of the columns so more important columns appear first.
- Increase or decrease the width of the columns.

- Show messages from the local Barracuda Spam Firewall only (clustered environments).
The default behavior is for the message log to display messages from all the Barracuda Spam Firewalls in your clustered environment. If **Only view local messages** is set to **Yes**, then the message log will not show messages received by other Barracuda Spam Firewalls in the cluster. Showing only local messages allows the administrator to only view the messages that they can classify, as opposed to messages from other systems in the cluster that the administrator cannot classify because the administrator is not logged into those other systems.

Viewing Message Details

To view more information about a message on the 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 e-mail 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 *Body Filter* on page 66.

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

Clearing the Message Log

Clicking **Clear Message Log** clears all messages from the Message Log, but does not clear the Bayesian database.

It may take 2 hours to 4 days to completely purge the messages from the system drive. During this time, disk usage may or may not drop at a noticeable rate.

Note



DO NOT use this functionality to free space on the drive unless no further e-mail is flowing in. In many cases, e-mail arrives faster than it is purged, thus negating the clearing of the Message Log for space reasons. If drive space continues to be a problem, contact Barracuda Networks Technical Support.

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 spam scoring settings on the **Basic > Spam Scoring** page. A setting of 10 for any setting disables that option.

Note

On the Barracuda Spam Firewall 400 or above you can set the spam scoring values on a per-domain basis from the DOMAINS tab. For more information, refer to *Editing Domain Settings* on page 76.

Table 4.6:

Setting	Description
Tag score	<p>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.</p> <p>You can change the default text added to the subject line by entering new text in the Spam Tag Configuration section (discussed in the next section).</p> <p>Any message with a score below the tag threshold is automatically allowed. The default value is 3.5.</p>
Quarantine score	<p>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 <i>Specifying the Global Quarantine Settings</i> on page 48.</p> <p>The default setting is 10 (quarantine disabled).</p> <p>To enable quarantine, this setting must have a value lower than the block threshold. For more information, refer to <i>Setting Up Quarantine Policies</i> on page 46.</p>
Block score	<p>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.</p>

Specifying the Subject Text and Priority of Tagged Messages

Basic > Spam Scoring allows 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 *Chapter 5 Using the Block and Accept Filters*.

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

By default, the Barracuda Spam Firewall sends a notification to senders when their e-mails 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** to configure the virus checking and notification settings described in the following table. Click **Save Changes** after making any modifications.

Table 4.7:

Setting	Description
Virus Scanning Enabled:	<p>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.</p> <p><i>Note: On the Barracuda Spam Firewall 400 or above you can enable and disable virus checking on a per-domain basis from the DOMAINS tab. For more information, refer to Editing Domain Settings on page 76.</i></p>
Notify Sender of Virus Interception:	<p>Determines whether the Barracuda Spam Firewall notifies the sender that their e-mail has been blocked because it contained a virus.</p> <p>You should keep this option set to No to prevent the Barracuda Spam Firewall from sending mass e-mail notification traffic in the event of a widespread virus outbreak.</p>

Setting Up Quarantine Policies

By default, the Barracuda Spam Firewall does not quarantine incoming messages, but you may want to enable quarantine because it can provide additional security. Unlike tagged messages, quarantined messages are not delivered to the intended recipients, thus minimizing the risk of a user opening an infected message and spreading a virus throughout your network.

To set up quarantine policies on your system:

Note



To enable quarantine on an outbound mode system, refer to *Chapter 8 Outbound*.

1. Enable quarantine using the Spam Scoring Limits on the BASIC-->Spam Scoring page. For more information, refer to *Configuring the Global Spam Scoring Limits* on page 44.
2. Select **Basic > Quarantine**.
3. Select the quarantine type, as described on *page 47*.
4. Do one of the following:
For global quarantine type, enter the global quarantine delivery address, as described on *page 48*.
For per-user quarantine type, configure the per-user quarantine settings, as described on *page 48*.
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 user's quarantine inbox.

Note



If you have the Barracuda Spam Firewall 400 or above you can specify the quarantine type on a per-domain basis by going to the DOMAINS tab and clicking Edit Domains.

The following table describes the differences between the two quarantine types:

Table 4.8:

Quarantine Type	Location of Quarantined Messages	Quarantine Responsibility
Per User <i>(not available on model 200)</i>	Stores quarantined messages in a user's quarantine inbox on the Barracuda Spam Firewall. The Barracuda Spam Firewall automatically creates user accounts with quarantine inboxes when this type is selected.	Each end manages their quarantined messages from their own personal quarantine inbox. For information about the tasks a user can perform from their quarantine interface, refer to <i>Chapter 9 Managing Your Quarantine Inbox</i> .
Global	Delivers all quarantined messages to a global address you specify.	The Barracuda Spam Firewall administrator manages quarantined messages from the global quarantine location.

Specifying the Global Quarantine Settings

The following table describes the global quarantine configuration fields on the [BASIC-->Quarantine](#) page.

Table 4.9:

Field	Description
Quarantine Delivery Address	<p>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.</p> <p><i>Note: If you have the Barracuda Spam Firewall 400 or above you can specify the quarantine delivery address on a per-domain basis by going to the DOMAINS tab and clicking the Edit Domains link.</i></p>
Quarantine Subject Text	<p>Enter the text you want placed at the beginning of the subject line of a quarantined message. The default text is [SPAM].</p> <p>This allows you to identify quarantined messages when you have them delivered to a mailbox that also receives non-quarantine messages.</p>

Specifying the Per-User Quarantine Settings

The following table describes the Per-User Quarantine Configuration settings on the [Basic > Quarantine](#) page. This section does not appear on the Barracuda Spam Firewall 200.

Table 4.10:

Setting	Description
Quarantine Reply-To Address	<p>The from address that appears in all correspondence sent to users about their Per User quarantine area. If a user replies to this correspondence, the reply is sent to this address.</p>
Quarantine Host	<p>The IP address or hostname that will be sent to users in all quarantine correspondence so they can access their quarantine inbox.</p> <p>Leave this field blank to use the Barracuda Spam Firewall as the quarantine host.</p> <p>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.</p>

Table 4.10:

Setting Description	
Quarantine Default	<p>The default state that quarantine accounts are created with.</p> <p>If set to Enabled, all new accounts will have per-user quarantine functionality.</p> <p>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.</p> <p>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 <i>Configuring System IP Information</i> on page 49.</p>
Link Domains	<p>Determines whether different domains share the same per-user preferences and quarantine inbox.</p> <p>If set to Enabled, the same per-user preferences and quarantine inbox is used for all e-mail addresses with the same name, but different domains. For example, with domain linking enabled, <i>someuser@yourdomain.com</i>, <i>someuser@yourdomain.net</i>, and <i>someuser@corp.yourdomain.com</i> will all share the same preferences and quarantine inbox.</p> <p>Note the following about this feature:</p> <ul style="list-style-type: none"> • Link Domains is a global setting. You cannot activate domain linking for only certain domains or certain users. • This feature does not work for e-mail addresses that have the same domain, but a different handle. For example, <i>someuser@yourdomain.com</i> cannot be linked to <i>s.user@yourdomain.com</i>.
Notification Interval	<p>The interval at which the Barracuda Spam Firewall notifies users about messages in their quarantine.</p>
Notification Start Time	<p>The time of day (in hh:mm format) that the Barracuda Spam Firewall sends the quarantine reports. Changes to this setting take effect the next day.</p>

Configuring System IP Information

Basic > **IP Configuration** contains the network and mail server configuration for your Barracuda Spam Firewall.

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

Table 4.11:

Test Configuration (inbound mode only)	<p>Click Begin Test to verify that the IP information you entered for your Barracuda Spam Firewall is correct. A status report displays the results of the tests.</p>
---	--

Table 4.11:

TCP/IP Configuration	<p>The IP address, subnet mask, and default gateway of the Barracuda Spam Firewall.</p> <p>TCP port is the port on which the Barracuda Spam Firewall receives inbound e-mail. This is usually port 25.</p> <p><i>Note: If your Barracuda Spam Firewall is running firmware version 3.1.x or earlier and is part of a clustered environment, then changing the IP address of the system removes it from the cluster. You will need to add the system back into the cluster after you change the IP address. If your Barracuda Spam Firewall is running firmware version 3.2.x or above, the system remains part of its cluster after its IP address changes.</i></p>
Destination Mail Server TCP/IP Configuration (inbound mode only)	<p>Server Name/IP: The hostname or IP address of your destination e-mail server, for example <i>mail.yourdomain.com</i>. This is the mail server that receives e-mail after it has been checked for spam and viruses.</p> <p>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.</p> <p>TCP port is the port on which the destination mail server receives inbound e-mail. This is usually port 25.</p> <p>Valid Test Email Address: To test that the Barracuda Spam Firewall can successfully send e-mail messages, enter an address in this field and click Test SMTP Connection. The system sends a message to the e-mail address you specify. The From address in this e-mail is <i>smtptest@barracudanetworks.com</i>.</p>
DNS Configuration	<p>The primary and secondary DNS servers you use on your network.</p> <p>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.</p>
Proxy Server Configuration (optional) (inbound mode only)	<p>If your Barracuda Spam Firewall is behind a proxy server, then you may need to enter one or more of the following parameters so the system can download Firmware and Energize Updates. Incorrect proxy settings can cause your updates to fail.</p> <ul style="list-style-type: none"> • Server Name/IP - The IP address or hostname of the proxy server. • TCP Port - The port (usually 8080) used for proxy client authentication. • Username - The proxy username (if any) assigned to your Barracuda Spam Firewall. • Password - The proxy password (if any) assigned to your Barracuda Spam Firewall.
Domain Configuration	<p>Default Hostname is the hostname to be used in the reply address for e-mail messages (non-delivery receipts, virus alert notifications, etc.) sent from the Barracuda Spam Firewall. The hostname is appended to the default domain.</p> <p>Default Domain is the domain name used in the reply address for e-mail messages (non-delivery receipts, virus alert notifications, etc.) sent from the Barracuda Spam Firewall.</p>

Table 4.11:

Allowed Email Recipients Domain(s) <i>(inbound mode only)</i>	<p>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.</p> <p>To allow messages for all domains that match your mail server, put an asterisk (*) in this field.</p> <p><i>Note: One Barracuda Spam Firewall can support multiple domains and mail servers. If you have multiple mail servers, go to the DOMAINS tab and click the Edit Domains link to set up a different mail server for each domain.</i></p>

Controlling Access to the Administration Interface

This section covers the following tasks you can perform from the BASIC-->Administration page:

- Changing the Password of the Administration Account on this page.
- Limiting Access to the Administration Interface and API on this page.
- *Changing the Web Interface Port and Session Expiration Length* on page 52.

Changing the Password of the Administration Account

The 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 and API

Basic > Administration allows you limit the IP addresses that can access the administration interface and API, and establish an SNMP connection to the system. The following table describes these options:

Table 4.12:

Setting	Description
Administrator IP/Range	The 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 invalid login error.
Allowed SNMP and API IP/Range <i>(inbound mode only)</i>	<p>The range of IP addresses from which users can change configuration information through the Barracuda API, or access SNMP on the Barracuda Spam Firewall.</p> <p>For more information regarding the API, refer to the documentation on Barracuda Networks Web site under Support -->Documentation.</p>

Additional information:

- To add an individual IP address (instead of an entire network), use a netmask of 255.255.255.255.
- If you do not specify any IP addresses or networks, all systems are granted access.

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.

Table 4.13:

Field	Description
Web Interface HTTP Port	<p>The port used to access the administration interface from your Web browser (default is HTTP port 80). To change this value:</p> <ol style="list-style-type: none"> 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	<p>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:</p> <ol style="list-style-type: none"> 1. Enter the number of minutes a session can remain active. 2. Click Save Changes.

Shutting Down the System

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

Caution



Shutting down, restarting, or reloading the system can cause interruptions in e-mail delivery.

The following table describes each of these options.

Table 4.14:

Button	Description
Shutdown	Shuts down and powers off the system.

Table 4.14:

Button	Description
Restart	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.

Caution



Shutting down, resetting, or reloading the system can cause interruptions in e-mail delivery.

Automating the Delivery of System Alerts and Notifications

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

Enter the e-mail addresses (comma separated) in the provided field 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.

Changing the Operation Mode of the System

Your Barracuda Spam Firewall can operate in one of two modes: inbound mode or outbound mode. The most commonly used mode is the inbound mode, which scans incoming messages for spam and viruses. If your organization has a reason to scan outgoing messages from your users, you can configure your system to operate in outbound mode.

A Barracuda Spam Firewall can only be configured for one mode.

If you choose to change the mode from inbound to outbound (or vice versa), note the following:

- All your message log data and quarantine messages are deleted.
- System configuration remains in tact. However, you should verify that the configuration options are appropriate for outbound mode.

To change the mode of your Barracuda Spam Firewall:

1. Go to the BASIC-->Administration page.
2. In the Operation Mode section, click **Convert**.
3. Click **OK** to confirm you want to change the mode of your Barracuda Spam Firewall.

A status bar displays the progress of switching your Barracuda Spam Firewall to outbound mode. Once the switchover completes, your Barracuda Spam Firewall automatically reboots.

Enabling Users to Classify Messages from a Mail Client

- The Barracuda Spam Firewall provides access to a mail client plug-in that lets end users mark messages as spam and not spam directly from their Outlook or Lotus Notes client. In addition, the plug-in also automatically creates and maintains a personalized whitelist based on the user's behavior.
- The whitelist generated by the plug-in and the classifications made by the user only affect that user's individual Bayesian database and not the global Bayesian database. Changes to the global Bayesian database can only be accomplished by the administrator on the **Basic > Message Log** page.
- This feature is not available on the Barracuda Spam Firewall 200.

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

1. On the Bayesian/Intent page, set the **Allow Users to Download Plugins** field to **Yes**.
2. If you're enabling the Outlook plug-in, select the Outlook plug-in version you want your users to download.

Table 4.15:

Outlook Plu-In	Description
Version 1	Allows users to classify messages as spam and not spam from their Microsoft Outlook client.
Version 2	Contains all the functionality of version 1 and adds the automatic whitelist feature. This feature automatically adds e-mail addresses to the user's individual whitelist based on the user's behavior. The Outlook plug-in version 2 automatically whitelists the following: <ul style="list-style-type: none">• The recipient address within each message sent by the user after the new Outlook plug-in is installed. This only applies to messages sent outside of the local mail server.• The sender's e-mail address for messages that the user classifies as "not spam".• All e-mail addresses the user adds to their Contact list in Outlook.

3. Click **Save Changes**.

A link to the mail plug-in appears at the bottom of the Administration interface login page so users can download the plug-in, as shown in the following example:

Figure 4.3:

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:

Login

[Get Mail Client Plugins Here](#)

Using the Microsoft Outlook and Lotus Notes Plug-in

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

Version 2 of the Outlook Plug-in is configured to automatically:

- Whitelist e-mail addresses associated with sent messages and new contacts
- Move spam-declared messages to the Deleted Items folder in the user's Outlook client
- Whitelist the 'From:' e-mail address within 'Not-Spam'-declared messages.

An individual can change the default behavior of the Outlook plug-in by going to the Tools menu in their Outlook client and selecting Options | Spam Firewall tab.

Managing the Bayesian Database

Basic > **Bayesian/Intent** allows you to manage the Bayesian database by performing the tasks described in this section.

Resetting the Bayes Database

The Bayesian/Intent 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**.

Sending Spam Messages to Barracuda Networks

- When you classify messages as spam in the Message Log the Barracuda Spam Firewall sends a copy of the spam message to Barracuda Networks for further analysis. This allows Barracuda Networks to improve the spam definitions and intent analysis provided in the Energize Updates.
- To configure the system to not send spam messages to Barracuda Networks, go to the **Basic > Bayesian/Intent** page and set the Submit Email to Barracuda Networks field to **No**.

Synchronizing the Bayesian Database

- If one of your Barracuda Spam Firewalls has a Bayesian database that is superior to the other systems in the cluster, you can click **Synchronize** on the **Basic > Bayesian/Intent** page to copy the database to the other systems.
- When synchronizing databases, make sure you are logged into the Barracuda Spam Firewall that has the database you want to propagate. After you click Synchronize, the Bayesian databases on the other clustered systems will be replaced.
- The most common time to synchronize databases is when you add a new system to a cluster. In this case, you would first add the new system to the cluster, then log into an existing system in the cluster that has the best Bayesian database, and click **Synchronize** to propagate the database to the new system (and all others in the cluster).
- Synchronization is quicker than backing up an existing Bayesian database and restoring it onto the new system.

Enabling Intent Analysis

Intention Analysis attempts to match URLs in a message against a database of URLs known for sending spam. By enabling intent analysis you can block messages that contain such URLs and significantly reduce the amount of spam received by your users.

Table 4.16:

Field	Description
Intent Analysis	Whether messages that contain offending URLs should be tagged, quarantined, or blocked. Selecting to tag or quarantine a message may result in reduced system performance because the Barracuda Spam Firewall will continue to process the message in an attempt to filter possible spam using stricter rules. To disable intent analysis, select Off (not recommended).
Realtime Intent Analysis	In addition to using the database of URLs that the Barracuda Spam Firewall receives from the Energize Updates on an hourly basis, your system can also communicate with Barracuda Central in realtime to check against the latest lists and block even the newest spam. <i>Note: Turning this option on can cause a slight increase in mail scanning time as network (DNS) lookups will need to be performed.</i>
URL Exemptions	Exemptions can be made for specific URLs from Intention Analysis. Any messages containing the exempted URLs will still be scanned, but the messages will not be blocked, quarantined or tagged.

Reducing Backscatter

By default, your Barracuda Spam Firewall is configured to send a bounce notification (also known as a non-delivery report) to a sender when the Barracuda Spam Firewall blocks their e-mail. This is done to alert legitimate senders that their message has not been delivered to the recipient. However, if the e-mail came from an illegitimate source like a spammer then sending a bounce notification is not necessary. Sending bounce messages to illegitimate senders is known as backscatter.

Backscatter can increase the load on your Barracuda Spam Firewall and may generate a lot of e-mail to fake addresses.

If your Barracuda Spam Firewall rarely blocks a legitimate e-mail, consider turning off bounce notification to reduce backscatter.

To turn off notifications:

1. Turn off virus notification:
 - 1a. On the **Basic > Virus Checking** page, set the two Virus Notification settings to **No**.
 - 1b. Click **Save Changes**.
2. Turn off bounce notifications:
 - 2a. On the **Basic > Spam Scoring** page, set the Send Bounce field to **No**.
 - 2b. Click **Save Changes**.
3. Turn off attachment notifications:
 - 3a. On the **Block/Accept > Attachment Filtering** page, set the Block Notification fields to **No**.
 - 3b. Click **Save Changes**.

Changing the Language of the Administration Interface

You can change the language of the administration interface by selecting a language from the drop-down menu in the upper right corner of the window. Supported languages include Chinese, Japanese, Spanish, French, and others.

The language you select is only applied to your individual quarantine interface. No other user's interface is affected.

Using the Block and Accept Filters

The Block/Accept tab provides a wide range of filters that enhance the default spam and virus detection capabilities of the Barracuda Spam Firewall. These filters support the use of regular expressions. For more information on using regular expressions, refer to *Appendix 1 Regular Expressions*.

This chapter covers the following filters you can apply from the **Block/Accept** tab:

<i>Subscribing to Blacklist Services</i>	59
<i>Blacklist Services Descriptions</i>	60
<i>What Happens if your Domain or IP Address is on a Blacklist</i>	61
<i>IP Address Filters</i>	61
<i>Sender Domain Filters</i>	62
<i>Sender Email Address Filter</i>	63
<i>Recipient Email Address Filter</i>	63

Subscribing to Blacklist Services

The External Blacklist page (inbound mode only) 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 you receive. 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 sends notifications when it rejects such messages, the sender will be notified and legitimate senders will therefore know to re-send their message.

Subscribing to blacklist services does not hinder the performance of the Barracuda Spam Firewall. Query response time is typically in milliseconds, so delays are negligible. And once the Barracuda Spam Firewall queries a blacklist service, that query is cached on your own local DNS for a period of time, making further queries very fast.

The following table describes each of the blacklist settings on the [Block/Accept > External Blacklist](#) page.

Table 5.1:

Blacklist Setting	Description
Barracuda Blacklist	Whether the blacklist maintained by Barracuda Networks is enabled. The Barracuda blacklist 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	Free or subscription blacklists that you want to use. After entering the external blacklist, specify the action you want performed. Click Add and then Save Changes when finished. You can locate blacklists on the Internet by searching for <i>DNSBL</i> or <i>RBL</i> . However, be cautious and use only trusted blacklists.
Blacklist Options	<p>Delay RBL Check—Determines whether RBL checks are performed after the RCPT TO is given.</p> <p>Setting this option to Yes causes RBL checks to run after the RCPT TO is given in the SMTP transaction. This allows the sender/recipient information to appear in the message log.</p> <p>Setting this option to No results in only the IP being available in the message log entry.</p> <p>Blacklist Using Full Header Scan—Set to Yes to let the Barracuda Spam Firewall scan e-mail headers for blacklisted IP addresses.</p> <p>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.</p>

Blacklist Services Descriptions

The following table describes each blacklist service available.

Table 5.2:

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.

Table 5.2:

Blacklist Service	Description
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 e-mail. By accessing this list, system administrators are allowed to choose to accept or deny e-mail 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.

What Happens if your Domain or IP Address is on a Blacklist

If your domain or IP address is on a blacklist that you subscribe to, then your Barracuda Spam Firewall will not deliver messages from users on that domain. There could be several reason why your domain is on the list:

- Your mail server may have been hijacked by a spammer to be used for spamming.
- Your mail server is an open relay meaning any one can use it to send e-mails to any recipient without any authentication.
- Spammers used your domain as a fake sender to send spam to recipients.
 - If your domain or IP address is on a blacklist, you will need to contact the blacklist provider to have it removed.

IP Address Filters

IP Block/Accept allows you to filter messages based on the sender's IP network.

The following table describes the filters on this page.

Table 5.3:

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, but do go through virus, attachment, body, and subject filters. Click Add after adding each entry, followed by Save Changes .

Table 5.3:

Filter	Description
Blocked IP Range	<p>Add any IP addresses or networks to your blacklist. To add an individual IP address, use a netmask of 255.255.255.255. To help you calculate the correct subnet mask for a range of addresses, use a subnet mask calculator.</p> <p>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.</p> <p>Click Add after adding each entry, followed by Save Changes.</p>

Note



Use the Comment field to add any notes about the blocked IP address. This is useful if more than one person manages your Barracuda Spam Firewall.

Sender Domain Filters

Sender Domain Block/Accept allows you to filter messages based on the sender's e-mail address.

The following table describes the filters on this page.

Table 5.4:

Filter	Description
Allowed Sender Domain/Subdomain	<p>Add any domains or subdomains that you wish to include in your whitelist. Whitelisting a domain automatically whitelists all subdomains. For example, adding <i>customer.com</i> allows messages from <i>joe@customer.com</i> as well as <i>joe@office1.customer.com</i>.</p> <p>Do not use wildcards (such as *) or the @ sign when entering a domain. For example, just enter <i>customer.com</i> instead of <i>*@customer.com</i>.</p> <p>Whitelisted domains/subdomains bypass spam scoring as well as all other blacklists, but do go through virus, IP block/accept and body/subject filters.</p> <p>Click Add after adding each entry, followed by Save Changes.</p>
Blocked Sender Domains/Subdomain	<p>Add any domains or subdomains that you wish to block. Blocking a domain automatically blocks all subdomains. For example, adding <i>spammer.com</i> blocks messages from <i>joe@spammer.com</i> as well as <i>joe@server1.spammer.com</i>.</p> <p>Do not use wildcards (such as *) or the @ sign when entering a domain. For example, just enter <i>customer.com</i> instead of <i>*@customer.com</i>.</p> <p>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.</p> <p>Click Add after adding each entry, followed by Save Changes.</p>

Note

If more than one person manages your Barracuda Spam Firewall, you may want to add an explanation in the Comment field that describes why the specified domains are whitelisted or blocked.

Sender Email Address Filter

Email Sender Block/Accept allows you to filter messages based on the sender's e-mail address. The following table describes the filters on this page.

Table 5.5:

Filter	Description
Allowed Email Addresses	<p>Add the e-mail address of each sender to include in the global whitelist. Click Add after adding each entry, followed by Save Changes.</p> <p>Whitelisted e-mail addresses bypass spam scoring, Intention Analysis, Bayesian filtering, and keyword filters, but still go through the IP address filters, virus scanning, External Blacklists check, and attachment filters.</p>
Blocked Email Addresses	<p>Add the e-mail address of each sender to include in your blacklist, and specify whether the sender should be blocked, quarantined or tagged.</p> <p>All e-mail addresses in this list will be blocked unless the whitelist also contains the same e-mail address. In this case, the message will not be blocked.</p> <p>Click Add after adding each entry, followed by Save Changes.</p>

Note

If more than one person manages your Barracuda Spam Firewall, you may want to add an explanation in the Comment field that describes why the specified addresses are whitelisted or blocked.

Recipient Email Address Filter

Email Recipient Block/Accept allows you to filter messages based on a recipient's e-mail address.

The following table describes the filters on this page.

Table 5.6:

Filter	Description
Allowed Email Addresses	<p>Add the e-mail address for each recipient you want to include in the whitelist.</p> <p>Recipients added to this list will never have their incoming messages scored for spam, but these messages still go through virus scanning and attachment filters. Whitelisted recipients can have their incoming messages blocked if the sender's IP address, domain, or e-mail address is blacklisted.</p> <p>Click Add after adding each entry, followed by Save Changes.</p>
Blocked Email Addresses	<p>Add the e-mail address for each recipient that you want to include in your blacklist, and specify whether the recipient's incoming message should be blocked, quarantined or tagged.</p> <p>A common reason to block a recipient's e-mail address is if that user is no longer with your company and you want to keep their account active on your mail server.</p> <p>Recipients added to this list never receive messages unless an accept filter has been set up for the sender's IP address, domain, or e-mail address.</p> <p>Click Add after adding each entry, followed by Save Changes.</p>

Note



If more than one person manages your Barracuda Spam Firewall, you may want to add an explanation in the Comment field that describes why the specified domains are whitelisted or blocked.

Attachment Type Filter

Attachment Filtering allows you to block and quarantine messages if they contain attachments with certain file extensions.

The maximum attachment size allowed by you Barracuda Spam Firewall is 100 megabytes. If a message exceeds this size, the Barracuda Spam Firewall rejects the message and the sending server notifies the sender that their message did not go through. Contact Barracuda Networks technical support to change this maximum.

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).

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

Table 5.7:

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 e-mail has been blocked because it contained a banned file extension.
Notify sender of Banned File Interception	Select Yes to notify senders when one of their e-mails 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 e-mail 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.

Subject Line Filter

Subject Filtering allows you to 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.

Table 5.8:

Subject Blocking	Enter the words, regular expressions, or characters that will cause a message to be blocked if they appear in the subject line.
------------------	---

Table 5.8:

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 (<i>inbound mode only</i>)	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.

Body Filter

Body Filtering allows you to 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.

Table 5.9:

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 (<i>inbound mode only</i>)	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.

Header Filter

Header Filtering allows you to filter messages based on the contents of a message's header.

The following table describes the parameters on this page. Click [Save Changes](#) after making any changes.

Table 5.10:

Header Blocking	Enter the words, regular expressions, or characters that will cause a message to be blocked if they appear in the e-mail header.
Header Quarantine	Enter the words, regular expressions, or characters that will cause a message to be quarantined if they appear in the e-mail header.
Header Tagging <i>(inbound mode only)</i>	Enter the words, regular expressions, or characters that will cause a message to be tagged if they appear in the e-mail header.
Header Whitelisting	Enter the words, regular expressions, or characters that will cause a message to be whitelisted if they appear in the e-mail 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.

Managing Accounts and Domains

This chapter covers the following tasks that you can perform from the Users and Domains tabs (inbound mode only):

<i>How the Barracuda Spam Firewall Creates New Accounts</i>	69
<i>Viewing User Accounts</i>	69
<i>Using Filters to Locate Accounts</i>	70
<i>Editing User Accounts</i>	71
<i>Assigning Features to User Accounts</i>	72
<i>Overriding the Quarantine Settings for Specific User Accounts</i>	73
<i>Overriding Quarantine Settings</i>	74

How the Barracuda Spam Firewall Creates New Accounts

The Barracuda Spam Firewall automatically creates a new user account when the following occurs:

- You enable quarantine and set the type to per-user. For more information on enabling quarantine, refer to *Setting Up Quarantine Policies* on page 46.
- The Barracuda Spam Firewall receives an e-mail that needs to be quarantined.

When these two circumstances occur, the system does the following:

1. Checks the recipient e-mail address against its database.
To increase security, you can configure the Barracuda Spam Firewall to validate the receiving e-mail address (using LDAP or the SMTP command RCPT TO) before it creates an account. This helps prevent the Barracuda Spam Firewall from creating accounts for invalid users.
2. If the address does not exist, the system creates a new user account for the recipient.
The Barracuda Spam Firewall uses the e-mail address of the recipient as the username of the account and then auto-generates a password.
3. Sends the user the login information so they can access their quarantine inbox.
4. Places the quarantined message in the recipient's quarantine inbox.
5. Sends a quarantine summary report to the user.
Because the Barracuda Spam Firewall automatically creates user accounts, you should never need to manually add new accounts to the system.

Viewing User Accounts

The USERS-->Account View page displays a list of all user accounts on your Barracuda Spam Firewall. From this page you can:

- Edit a user's account settings by logging in to their quarantine interface
- Delete user accounts
- Change the password of specific accounts.

The following table describes each column on this page.

Table 6.1:

Column	Description
Account Address	The e-mail address of the account.
Notify Interval	How often the system sends the quarantine summary message to the 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.
Size (KB)	The current size of the user's quarantine area. This is a good indicator of which users are not cleaning out their quarantine areas and taking up system disk space.
Message Count	The current number of messages in a user's quarantine area. This is another indicator to use when determining which users need to clean out their quarantine area.
Oldest Message	The oldest message in a user's quarantine area.
Admin Actions	Click Edit Account to view that user's quarantine account so you can troubleshoot issues and change the user's preferences and spam scoring values. Click Change Password to change the user's password. Click Delete to remove the quarantine account from the system including all of the user's settings and quarantined messages.
Remove All Invalid Accounts (button)	For more information, refer to <i>Overriding the Quarantine Settings for Specific User Accounts</i> on page 73.

Using Filters to Locate Accounts

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

Table 6.2:

Filter	Description
None	Displays all accounts on the system with the newest ones listed first.
"Account" (e-mail address)	Displays only the accounts for the e-mail addresses entered in the Pattern textbox.

Table 6.2:

Filter	Description
"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. <i>Note: The wildcard is applied to the right of the pattern. This means if you search for 'bob' then bob@domain.com and bobby@domain.com will match, but not billybob@domain.com.</i>
"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. <i>Note: The wildcard is applied to the left of the pattern. This means if you search for 'domain.com' then user@domain.com and user@corp.domain.com will match, but not user@domain1.com.</i>
"Quarantined Enabled"	Displays all accounts with quarantined enabled.
"Quarantined 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.

Editing User Accounts

In some cases you may need to edit the settings of a specific user account to:

- Check the messages within a user's quarantine inbox.
- Modify a user's spam and quarantine settings.
- Add e-mail addresses to a user's whitelist or blacklist to resolve why that user is not receiving legitimate mail or receiving a large amount of spam.

To make changes to a user's account:

1. Select [Users](#) > [Accounts View](#).
2. In the Administrator Actions column, click [Edit Account](#) next to the account you want to modify.

A new page opens that displays the end user quarantine interface.

3. Use the [Quarantine Inbox](#) and [Preferences](#) tabs to make the necessary changes.

Removing Invalid User Accounts

From the **Users > Accounts View** page you can remove existing user accounts on your Barracuda Spam Firewall that your mail server or LDAP server (if enabled) consider to be invalid.

To begin removing invalid accounts, click **Remove All Invalid Accounts**. A status page then appears with an overview of the accounts that are being removed.

Before removing invalid accounts, note the following:

- It can take many hours to remove all invalid accounts. It takes the system about 1-2 seconds to verify each valid account and about 3-5 seconds to remove an invalid account.
- To stop the removal process, click the stop button in the status/log display that pops up when the process begins.
- You can close the administration interface at any time without disrupting the account removal process.
- The Barracuda Spam Firewall also removes all messages stored in an invalid user's quarantine.

Assigning Features to User Accounts

Users > User Features allows you to specify which features your users can control from their quarantine interface.

Note



When assigning features to accounts remember that the settings configured by end users override the default and domain settings configured by the Barracuda administrator.

The following table describes the features on this page.

Table 6.3:

User Feature	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: <ul style="list-style-type: none">• The quarantine type configured on the BASIC-->Quarantine page, or• The per-domain quarantine type configured on the DOMAINS tab by clicking Edit Domain. For more information, refer to <i>Editing Domain Settings</i> on page 76. <p><i>Note: If you set this value to No, the quarantine settings configured by the user do not take effect.</i></p>

Table 6.3:

User Feature	Description
Spam Scan Enable/Disable Ability	<p>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:</p> <ul style="list-style-type: none"> • The settings configured on the BASIC-->Spam Scoring page, or • The per-domain settings configured on the DOMAINS tab by clicking Edit Domain. For more information, refer to <i>Editing Domain Settings</i> on page 76. <p><i>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.</i></p>
Notification Change Ability	<p>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.</p> <p><i>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.</i></p>
Whitelist/Blacklist Ability	<p>Determines whether your users can add e-mail addresses and domains to their personal whitelist and blacklist.</p> <p><i>Note: If this value is set to Yes and a user adds entries to their whitelist and blacklist, those additions are ignored when you change Whitelist/Blacklist Ability to No.</i></p>
Use Bayesian Ability	<p>Determines whether your users can view and edit their Bayesian database.</p>
Scoring Change Ability	<p>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:</p> <ul style="list-style-type: none"> • The settings configured on the BASIC-->Spam Scoring page, or • The per-domain settings configured on the DOMAINS tab by clicking Edit Domain. For more information, refer to <i>Editing Domain Settings</i> on page 76. <p><i>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.</i></p>
User Features Override	<p>Use this section to provide specific user accounts with different features than specified in the Default User Features section.</p> <p>In the User Accounts box, enter the e-mail addresses for the accounts you want to override, and then specify the features for these accounts. Click Save Changes when finished.</p>

Overriding the Quarantine Settings for Specific User Accounts

The only time you should need to use the **Users > User Add/Update** page is when you want to override the quarantine settings for specific users. You should almost never need to create new user accounts because the Barracuda Spam Firewall automatically creates accounts when you enable the per-user quarantine feature. For more information, see *How the Barracuda Spam Firewall Creates New Accounts* on page 69.

Example

One of the most common scenarios for overriding quarantine settings is when you want to provide a few users with a quarantine inbox on the Barracuda Spam Firewall, and have the rest of your users receive quarantine messages in their standard e-mail inbox.

Providing a user with a quarantine inbox gives them greater control over how their messages are quarantined, but also requires them to manage their quarantine queue. For this reason, you may only want to provide a quarantine inbox to a subset of power users.

In this example, you would do the following:

- Set the quarantine type to per user (for more information, see *Specifying the Quarantine Type* on page 47)
- Set the quarantine default to disabled so users are not set up with a quarantine inbox on your Barracuda Spam Firewall (for more information, see *Specifying the Per-User Quarantine Settings* on page 48)
- Enter the e-mail addresses of the users you want to have a quarantine inbox and set Enable Quarantine Inbox to **Yes**. Refer to the next section for more information.

Overriding Quarantine Settings

To override the quarantine settings for specific users:

1. In the User Account(s) box, enter the e-mail addresses (one per line) of the user accounts you want to override.
2. Select whether the user accounts you listed are enabled with the user quarantine feature.
For a description of the user quarantine feature, refer to *Specifying the Quarantine Type* on page 47.

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 e-mail login information to the new users. To view an example greeting e-mail that contains login information, refer to *Greeting Message* on page 121.
4. Click **Save Changes**.

For information on assigning additional features to user accounts, refer to *page 72*.

Backing Up and Restoring User Settings

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

To backup user settings:

1. 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.
2. Save the user setting backup file (*pu_config.tgz*) to your local system.

To restore user settings:

1. From the **Users > User Backup/Restore** page, click **Browse**.
2. Locate the user settings backup file (*pu_config.tgz*) and click **Upload Now**.

Setting Retention Policies

Retention policies help you automatically manage your users' quarantine areas by controlling how much space is available on the Barracuda Spam Firewall for a user's quarantine messages.

You can control the amount of space used for quarantine areas using:

- Size restrictions that determine the size each user's quarantine
- Age restrictions that determine the period of time messages are kept in a user's quarantine area

It is recommended you train your users to manage their own quarantine areas and not rely on the retention policies to automatically remove messages. Relying on the Barracuda Spam Firewall to automatically manage quarantine areas can impact system performance.

In addition to using retention policies to manage quarantine areas, you can also select **User > Accounts View** to view the size of each user's quarantine area. You can then contact users directly if they have a large quarantine area that they need to manage.

Note



When you enable retention policies, keep in mind that if your system has been accumulating mail without retention policies then the first day retention policies that are enabled may have an impact on system performance. The longer a system runs without retention policies the larger the performance impact. After the first day or two, the load stabilizes as the system is able to keep large quarantine fluctuations to a minimum. Retention policies are run starting at approximately 02:30 AM.

Adding New Domains

- If your Barracuda Spam Firewall is responsible for filtering messages for more than one e-mail server or domain, you need to enter the domains associated with each mail server on the **Domains > Domain Manager** page.
- If you have the Barracuda Spam Firewall 400, 600, or 800 you can also set spam scoring, quarantine type and spam/virus checking on a per-domain basis.

To add and configure domains:

1. Select **Domains > Domain Manager**.
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 76.

Editing Domain Settings

To edit the settings for a specific domain:

1. Select **Domains > Domain Manager**, 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 above.

Note



Setting values on a per-domain basis overrides the values configured elsewhere in the administration interface.

Table 6.4:

Destination Server and Destination Port	The hostname and destination port of the mail server associated with the selected domain.
Use MX Records	Whether MX lookups are performed on the specified Destination Server.
Valid Test Email Address	Enter a valid e-mail 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 e-mail address. The test e-mail has a "from" address of <i>smtpstest@barracudanetworks.com</i> .
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 <i>Configuring the Global Spam Scoring Limits</i> on page 44. <i>Note: These domain settings override the global settings configured on the BASIC-->Spam Scoring page. But the individual spam scoring settings configured by the user in their PREFERENCES-->Spam Settings page override the domain settings.</i>
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 <i>Specifying the Quarantine Type</i> on page 47.

Table 6.4:

Global Quarantine Email Address	Specifies the address for the global quarantine e-mail address for the domain. For more information, refer to <i>Specifying the Global Quarantine Settings</i> on page 48.
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 e-mail addressed from a domain for which the Barracuda Spam Firewall receives e-mail. You should only enable this option if all e-mail from your domains goes directly to your mail server and not through the Barracuda Spam Firewall.

3. Click **Save Changes**.

Using LDAP to Authenticate Message Recipients

This section describes how to configure your Barracuda Spam Firewall to use an LDAP server for user authentication. LDAP allows your Barracuda Spam Firewall to verify that the recipients of incoming e-mail are valid users.

This section contains the following topics:

- *Using LDAP for User Authentication* on page 77
- *Impact of a Down LDAP Server* on page 80
- *Common LDAP Settings for Standard Mail Servers* on page 80

Using LDAP for User Authentication

To enable your Barracuda Spam Firewall to authenticate users using LDAP:

1. Select **Domains > Domain Manager**.
2. In the Actions column, click **Edit LDAP** next to the domain that you want to use LDAP authentication.
3. Scroll to **Edit LDAP** settings section and fill in the required information.

The following table describes the fields on this page.

Table 6.5:

LDAP Server	<p>The name of your LDAP server to use for authenticating message recipients.</p> <p>To specify two LDAP servers for failover purposes, enter the IP address of each LDAP server separated by a space. The username, password, filers, search base, and port need to be the same for both LDAP servers.</p>
Exchange Accelerator Enabled	<p>Controls whether LDAP lookups are performed for recipient verification. If set to Yes, the LDAP settings will be used. If set to No, the Barracuda Spam Firewall defaults to SMTP verification through RCPT TO commands.</p> <p>For more information about the Exchange Accelerator feature, read the text located above this field in the administration interface.</p>
Unify Email Aliases	<p>Whether the Barracuda Spam Firewall unifies all e-mail aliases for a single user. Selecting Yes makes all messages sent 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.</p> <p>This feature is not available in the Barracuda Spam Firewall 200.</p> <p>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.</p>
SSL/TLS Mode	<p>LDAP supports two modes for secure communications.</p> <ul style="list-style-type: none"> • LDAPS—The original mode typically used with version 2 of the LDAP protocol. LDAPS is a traditional out-of-band SSL/TLS connection where SSL/TLS is first negotiated and then the LDAP protocol is spoken over this channel. The port for LDAPS is usually 636. • StartTLS—Introduced with version 3 of the LDAP protocol. In this mode, an unsecured LDAP connection is initially made. The client then tells the server it wishes to upgrade to SSL/TLS. If the server supports it and its policy allows StartTLS, then SSL/TLS is negotiated and all further communication occurs securely. The StartTLS capability can be offered on the same port as plain-text LDAP and therefore is typically the default port 389. <p>If SSL/TLS is off, then LDAP communications will occur in plain-text. This is often desirable if the network between your Barracuda Spam Firewall and your LDAP server(s) is private and/or anonymous authentication is used (meaning no username/DN and password is sent). Plain-text LDAP is significantly more efficient than LDAP over SSL/TLS because SSL/TLS can introduce significant processing delays, especially when connecting to the LDAP server.</p>

Table 6.5:

SMTP over TLS/SSL settings	<p>If SMTP over TLS/SSL is enabled then passwords will not be sent in clear text if both sending and receiving systems support TLS/SSL. If one system does not support TLS/SSL, then traffic between the systems will not be secured/encrypted.</p> <p>If you enable this option and an LDAP connection cannot be made or the StartTLS LDAP command is not supported or disallowed, then the LDAP connection fails.</p>
LDAP Port	The LDAP port used to communicate with the Exchange server. By default, this port is 389.
LDAP / Exchange Username	<p>The username for the LDAP/Exchange server.</p> <p>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.</p>
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	<p>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.</p> <p>If you have two domains under one forest, and you want to authenticate both domains using the same LDAP server, use an LDAP search base of DC=com and LDAP port of 3268. This allows for a complete search under the .com domain and a Global Catalog default connection.</p>
LDAP UID	This specifies an attribute of the LDAP container found using the LDAP filter and which provides the Barracuda a unique identifier to associate with user accounts on the Barracuda. This is primarily used for Alias Unification and Single-signon. Typically this is <i>uid</i> , or on more recent Active Directory schemas <i>sAMAccountName</i> .
LDAP Primary Email Alias	When Unify Email Aliases is enabled this LDAP container attribute provides the account name under which quarantined messages are stored and for which the actual recipient address is an alias of. For Single-Signon using LDAP (and when Unify Email Aliases is enabled), this is the account that users will be directed to when logging in with any of their aliases. This attribute is almost always <i>mail</i> , and should be a fully qualified address with a local part, an "@" sign, and a domain component which is configured on the Barracuda as a valid domain.
Canary Email	This email address is used to determine if LDAP lookups are properly locating valid and invalid email addresses for this domain during the normal operation of the Barracuda. If at anytime the provided canary address is not found in the LDAP directory then LDAP recipient verification (Exchange Accelerator) and Unify Email Aliases will be disabled for the duration of the failure.

Table 6.5:

Valid Email (for testing)	This e-mail address is used in conjunction with the "Test LDAP" button to determine whether the LDAP settings can locate the provided address, and whether the proper attributes for LDAP UID and LDAP Primary Email Alias have been provided.
---------------------------	--

4. Click **Save Changes**.

Impact of a Down LDAP Server

If your LDAP server goes down for any reason, your Barracuda Spam Firewall cannot authenticate message recipients and the system creates an invalid account for each recipient that receives a message. The system creates the invalid accounts until the LDAP server is back up.

To remove invalid accounts once the LDAP server is back up, refer to *Overriding the Quarantine Settings for Specific User Accounts* on page 73. If you are using Unify Email Aliases, the Barracuda Spam Firewall returns a 421 retry message to the connecting sending server because the primary e-mail value cannot be found. This prevents duplicate user account from being created.

Common LDAP Settings for Standard Mail Servers

The following table provides common values you can use for the LDAP username, LDAP filter and search base for standard mail servers.

Table 6.6:

Mail Server	LDAP Setting
Microsoft Exchange 5.x	LDAP username: cn=<username>,dc=<domain>,cn=admin Example: cn=username,cn=users,dc=domain,dc=com <Domain> should be the NT domain name and not the e-mail domain (unless they are the same). The "admin" suffix is necessary to validate hidden recipients. Leave the LDAP filter and Search Base at the default setting.
Microsoft Exchange 2003	One of the best filters is: ((proxyaddresses=smtp:\${recipient_email}))(mail=\${recipient_email}))
Lotus Domino receiving messages for one domain	LDAP username: username@domain.com LDAP filter: ((mail=\${recipient_email})(cn=\${recipient_local_part})(shortname=\${recipient_local_part}))(fullname=\${recipient_local_part}))

Table 6.6:

Mail Server	LDAP Setting
Lotus Domino receiving messages for two domains	<p>If your Lotus Domino server receives messages for two domains, but the Name and Address book is only configured with a single Internet address for each user, use the following filter so LDAP can authenticate both domains:</p> <pre data-bbox="703 394 1463 447">((mail=\${recipient_email})(cn=\${recipient_email})(uid=\${recipient_email}))</pre> <p>Example: UserName@abc.com can receive mail addressed to UserName@abc.com OR UserName@xyz.com and performing an LDAP test works on UserName@abc.com but fails on UserName@xyz.com. Using this filter enables LDAP to authenticate both domains.</p>
Novell Groupwise	<p>LDAP username: cn=username,o=organization Leave the LDAP filter and Search Base the same.</p>

Advanced Administration

This chapter covers the following tasks that you can perform from the ADVANCED tab:

- Modifying the Email Protocol Settings*..... 83
- Configuring Message Rate Control* 85
- Activating Individual Accounts*..... 86
- Backing Up and Restoring System Configuration* 86
- Performing Desktop Backups* 87
- Automating Backups (inbound mode only)*..... 87
- Restoring from a Backup File*..... 88
- Updating Spam and Virus Definitions Using Energize Updates* 89

Note



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.

Modifying the Email Protocol Settings

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

Table 7.1:

Mail Protocol (SMTP) Checking	
SMTP HELO Required	<p>Whether mail clients connecting to the Barracuda Spam Firewall need to introduce themselves with a SMTP HELO command.</p> <p>Selecting Yes for this option may stop automated spam-sending programs used by spammers.</p> <p>The default setting is No.</p>

Table 7.1:

Enforce RFC 821 Compliance	<p>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.</p> <p>Setting this option to Yes stops messages sent from spam senders but also from some Windows mail programs (such as Microsoft Outlook) that do not adhere to the RFC 821 standard. For this reason, the default setting is No.</p>
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 e-mail sent from domains that do not have an entry in DNS.
Sender Spoof Protection <i>(inbound mode only)</i>	<p>Whether the Barracuda Spam Firewall prevents outside individuals from sending e-mail using this domain as the "from" address. Setting this option to Yes blocks all e-mail addressed from a domain for which the Barracuda Spam Firewall receives e-mail.</p> <p>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.</p>
SPF/Caller ID Configuration <i>(inbound mode only)</i>	
Sender Policy Framework/ Microsoft SenderID Framework:	<p>SPF (Sender Policy Framework) and Microsoft SenderID Framework are checks that can help the Barracuda Spam Firewall distinguish between spam and legitimate messages.</p> <p>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 SenderID 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.</p> <p>How SPF works</p> <p>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.</p>
Trusted Forwarder IP	<p>The Trusted Forwarder IP address is a list that contains the IP addresses of any machines that you have set up to forward e-mail to the Barracuda Spam Firewall from outside sources.</p> <p>The Barracuda Spam Firewall ignores any IP address in this list when performing SPF/SenderID checks. Instead, the next IP address in the Received headers list is tried.</p>
Incoming SMTP Timeout	

Table 7.1:

Incoming SMTP Timeout	<p>Sets a limit on the time spent on an incoming SMTP transaction. The default is 30 seconds.</p> <p>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 of <i>timeout</i>.</p>
SMTP Messages Per Session (<i>inbound mode only</i>)	
Messages per SMTP session	<p>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 of <i>Per-Connection Message Limit Exceeded</i>.</p>
SMTP Welcome Banner	
SMTP Welcome Banner	<p>Whether the Welcome Banner is presented to the SMTP client connecting to the Barracuda Spam Firewall.</p> <p>This value should be unique to make it easy for you to identify the system presenting the Welcome Banner.</p> <p>This value can be left blank for the Barracuda Spam Firewall to manage the setting.</p>
Barracuda Headers	
Remove Barracuda Headers	<p>Removes Barracuda's custom X-headers that are applied before a message leaves the system.</p> <p>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.</p>

Configuring Message Rate Control

Rate Controls allows you to 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 e-mail 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.

Table 7.2:

Setting	Description
Rate Control	<p>Specifies the maximum number of connections allowed from the same IP address in a half-hour timeframe. This setting is only taken into consideration when over five unique IP addresses are connected to the Barracuda Spam Firewall.</p> <p>When the number goes over the Rate Control threshold, the Barracuda Spam Firewall blocks further connections/messages.</p> <p>Legitimate sending e-mail 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 e-mail when they do not get through.</p>
Rate Control Exclude IP/Range	<p>Specifies the 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.</p>

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. Select **Advanced** --> **Explicit Users**.
2. In the Email Address field, enter the e-mail 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.

Backing Up and Restoring System Configuration

On a regular basis you should back up your system configuration in case you need to restore this information on a replacement Barracuda Spam Firewall or in the event your current system data becomes corrupt.

There are two types of backup you can perform from the **Advanced** > **Backup** page:

- Desktop backup—A one-time only backup that stores the backup file on your local desktop.
- Automated backups (recommended)—Recurring backups that you schedule.

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 (barracuda.conf) contains a checksum that prevents the file from being uploaded to the system if any changes are made.

The following information is not included in the desktop or automated backup:

- System password
- System IP information
- DNS information

Performing Desktop Backups

To perform a desktop backup:

1. From the Desktop Backup section on the **Advanced > Backup** page, select the components you want to backup. The following table describes each component.

Table 7.3:

Component	Description
Configuration	All global and system settings (less system password, system IP, and DNS information)
User Settings	All user settings except the individual user Bayesian databases
Bayesian Data	All global Bayesian data
Quarantine Data	All quarantine data

2. Click **Backup** and save the configuration file to a directory on your local system.

Automating Backups (*inbound mode only*)

To configure your Barracuda Spam Firewall to automatically backup your system and user configuration on a regular basis, go to the **Advanced > Backup** page and fill in the fields located in the Automated Backups section.

The following table describes the fields in the Automated Backups section.

Table 7.4:

Field	Description
Server Type	The type of server that will store the backup files. The available options include FTP or SMB (windows shared drive). Selecting a server type enables automated backups. Select Off to disable automated backups.

Table 7.4:

Field	Description
Server Name/IP	The IP address or fully qualified domain name of the backup server.
Port (optional)	The port to use for the FTP or SMB server.
Username	The username that the Barracuda Spam Firewall should use to log into the backup server.
Password	The password that the Barracuda Spam Firewall should use to log into the backup server.
Folder/Path	The folder, path, or share name to store the backup files on the backup server.
Test Backup Server	Before enabling automated backups, we recommend you test the backup settings you specified by clicking Test Backup Server .
Backup Schedule	<p>Lists the components you can include in your backup and the scheduled backup time for each. You can select the following components to back up:</p> <ul style="list-style-type: none">• System Configuration—All global and system settings (less system password, system IP, and DNS information)• User settings—All user settings except the individual user Bayesian databases• Bayesian data—All global Bayesian data• Quarantine data—All quarantine data <p>After selecting the components, specify the frequency of the backups (daily or weekly).</p>
Backups to keep	The number of backups to keep on the backup server at one time. When this limit is reached, the oldest backup file is removed to make room for the latest.

Restoring from a Backup File

To restore system configuration from a backup file:

Note



You should perform a system restore during non-business hours when there is less e-mail 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. Go to the Configuration Restore section on the **Advanced** > **Backup** page.
2. Do one of the following:

Table 7.5:

To restore from...	Then...
A desktop backup file	<ol style="list-style-type: none"> 1. Click Browse next to the Restore Backup File. 2. Locate the configuration backup file (<i>barracuda.conf</i>) and click Restore.
An automated backup file	<ol style="list-style-type: none"> 1. Click Browse near the Restore Auto Backup field. 2. Locate the auto backup file you want to restore based on the timestamp, and click Restore.

3. 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)

Updating Spam and Virus Definitions Using Energize Updates

[Advanced > Energize Updates](#) allows you to 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.

Spam Definition Updates

The following table describes the Spam Definition Updates fields on this page. Click [Save Changes](#) after making any changes.

Table 7.6:

Field	Description
Current 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 .

Table 7.6:

Field	Description
Automatically Update	Determines the frequency at which the Barracuda Spam Firewall checks for updates. To disable automatic updates, select Off . Hourly updates occur at the beginning of each hour. Daily updates occur at 12:20am (twenty after midnight) based on the system time zone. The recommended setting is Hourly .
Energize Updates	Informs you if your Energize Updates are current and when your subscription expires.

Virus Definition Updates

The following table describes the Virus Definition Updates fields on the [Advanced > Energize Updates](#) page. Click **Save Changes** after making any updates to this page.

Table 7.7:

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) based on the system time zone.

Updating the System Firmware Version

[Advanced > Firmware Update](#) allows you to 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:
 - 3a. Log out of the administration interface.
 - 3b. Log back into the administration interface and go to the **Advanced > Firmware Update** page.
 - 3c. Click **Apply**.
When activating the downloaded firmware, the Barracuda Spam Firewall resets. After the reset your e-mail automatically continues to be filtered.

Customizing the Appearance of the Administration Interface

Advanced > Appearance allows you to customize the default image used on the administration interface and in the e-mail quarantine correspondence sent to users. This tab is only displayed on the Barracuda Spam Firewall 600 and above.

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

Table 7.8:

Field	Description
General	
Spam Firewall Name	The system name that appears 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.

Table 7.8:

Field	Description
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 a jpg, gif, or png file under 50k.
Image URL	The URL the user goes to when clicking on the custom image.
Reset	Reverts 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 image to the system.
Upload New Image	To use a custom image in quarantine e-mails, click Browse , select the image, and click Upload Now . The uploaded image appears in the upper left corner of the quarantine e-mail. The recommended image size is 159x64 pixels and must be a jpg, gif, or png file under 100k.
Header Background Color	The color of the table header background used in quarantine e-mails. Use a standard HTML hex code for this value.
Header Font Color	The color of the table header font used in quarantined e-mails. Use a standard HTML hex code for this value.
Reset	Clears custom quarantine settings and reverts back to the default image and colors.

Using a Syslog Server to Centrally Manage System Logs

Advanced > **Syslog** allows you to specify a server to which the Barracuda Spam Firewall sends syslog data. Syslog support is not available on the Barracuda Spam Firewall 200. 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.

The following table describes the two types of data you can send to a syslog server.

Table 7.9:

Syslog Field	Description
Mail Syslog Configuration	<p>The IP address of the syslog server you want to receive data related to e-mail flow. This is the same data used to build the message log.</p> <p>Information such as the connecting IP, from address, to address, and the spam score for the messages are all included. This syslog data appears on the e-mail facility at the debug priority level on the specified syslog server.</p> <p>Click Monitor Mail Syslog to view the mail syslog output in a new window.</p>
Web GUI Syslog Configuration	<p>The IP address of the syslog server you want to receive data related to the administration interface. Some of the actions tracked include:</p> <ul style="list-style-type: none">• User logins• When a user deletes or delivers a message from their quarantine list• Any configuration changes made to your Barracuda Spam Firewall• When system reports are generated <p>This syslog data appears on the local1 facility with login information at info priority, and configuration changes at debug priority.</p> <p>Click Monitor Web Syslog to view the Web syslog output in a new window.</p>

Setting up Trusted Relays and SASL/SMTP Authentication

Advanced > **Outbound/Relay** allows you to setup basic relaying functionality with IP/domain/sender entries.

Table 7.10:

Field	Description
Trusted Relay IP/Range	Enter an IP address range to use as trusted relays on your Barracuda Spam Firewall. If you enter the asterisk (*) wildcard as an allowed e-mail recipient domain, then the default mail server should be configured to trust your Barracuda Spam Firewall as a relay.
Trusted Relay Host/Domain	Enter the host or domain name to use as trusted relays on your Barracuda Spam Firewall.

Table 7.10:

Field	Description
Senders with Relay Permission	Enter the e-mail address or domain name of those users that are permitted to send messages to any e-mail address on the Internet.
Outbound/Relay	Select Yes to only allow outbound messages to be sent from the users specified above. All other outbound messages regardless of the recipient address will not be delivered. The default and recommended setting for this field is No .
Enable SASL/SMTP Authentication	Supported values include: <ul style="list-style-type: none"> • None—SASL/SMTP authentication is disabled. • LDAP—SMTP Authentication/SASL is set to authenticate against LDAP. • SMTP AUTH Proxy—SMTP Authentication/SASL is set to pass the SMTP Authentication command through to another mail server. <p>SMTP AUTH/SASL defines a new SMTP command (AUTH) to authenticate users before allowing them to relay through your Barracuda Spam Firewall. If this authentication is enabled, then users should select 'Use name and password' or a similar option in their e-mail client. Because the password is transmitted in cleartext, it is a good idea to configure SMTP over TLS, as configured on the ADVANCED -->SMTP/TLS page.</p>
Edit LDAP Settings: mine.nu	If you selected LDAP for SASL/SMTP Authentication, then enter the required information about your LDAP server in the fields provided.
SMTP AUTH Server	If you selected to use SMTP AUTH Proxy for SASL/SMTP Authentication, then enter the hostname of the SMTP AUTH server in this field. The username and password provided by the user in the SMTP AUTH command is relayed to the SMTP server you specify in this field. The SMTP server can be any server that is set up to support the SMTP AUTH authentication command (e.g. MS-Exchange or Sendmail).

Customizing the Outbound Footer

By default, the Barracuda Spam Firewall adds a footer to all outbound messages passed through the system. This footer informs the recipient that the message has been scanned for spam and viruses.

Advanced > Outbound Footer allows you to change the default footer behavior. The following table describes the footer settings you can change.

Table 7.11:

Field	Description
Attach Footer	Determines whether a footer is attached to outgoing messages.

Table 7.11:

Field	Description
Text Footer	The footer text attached to text/ASCII-based messages.
HTML Footer	The footer text attached to HTML-based messages.
Footer Exemptions	List of sending e-mail addresses that will not have a footer attached. Enter one e-mail address per line.

Configuring the Network Interfaces on Models 600 and Above

If you have a Barracuda Spam Firewall 600 or above you can configure the second and third network interfaces directly from the [Advanced > Advanced IP Configuration](#) page.

To configure the second and third network interfaces:

1. Enter the IP address and netmask for the appropriate network interface.
2. Select the network interface associated with the IP address you entered.
3. Click **Add** and then **Save Changes**.
4. Repeat these steps for the remaining network interface(s).

Setting Up Clustered and Standby Systems

[Advanced > Clustering](#) allows you to link multiple Barracuda Spam Firewalls together so they can synchronize configuration settings. Clustered systems can be geographically dispersed and do not need to be co-located on the same network.

You can also use the Clustering page to specify standby systems to use in case an active system goes down.

Clustering is available on the Barracuda Spam Firewall 400 and above.

This section includes the following topics:

- *Cluster Set up Process* on page 95
- *Data Propagated to the Clustered Systems* on page 96
- *Field Descriptions for the Clustering Page* on page 97
- *Impact of Changing the IP Address of a Clustered System* on page 98

Cluster Set up Process

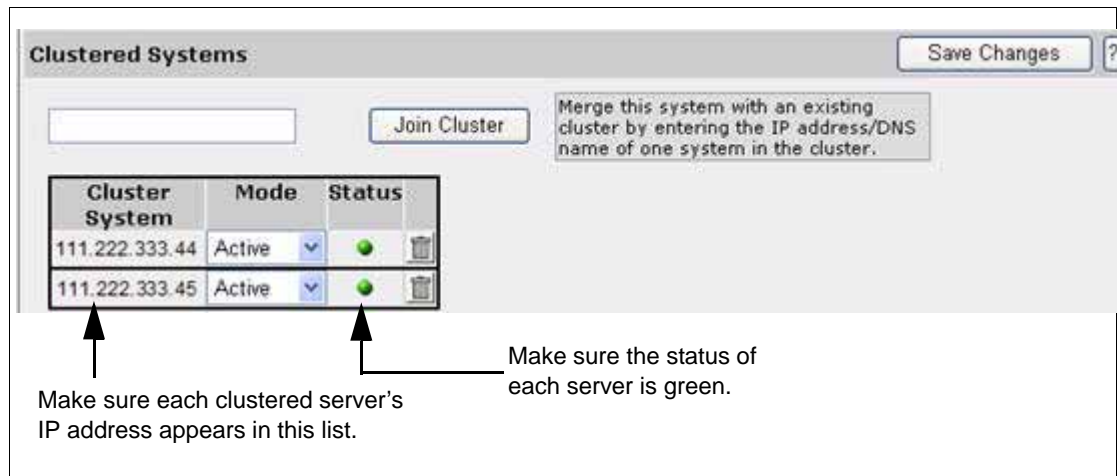
To cluster two Barracuda Spam Firewalls together:

1. Complete the installation process for each system as described in *Chapter 3 Setup*.
2. From the [Advanced > Task Manager](#) page on the Barracuda1 system, verify that no processes are running. Complete this step for the Barracuda2 system as well. No processes should be running when you add a system to a cluster.
3. From the [Advanced > Clustering](#) page on the Barracuda1 system, enter the shared secret password for the cluster, and click **Save Changes**.

4. From the **Advanced > Clustering** page on the Barracuda2 system, do the following:
 - 4a. Enter the same shared secret password, and click **Save Changes**.
 - 4b. In the Clustered Systems section, enter the IP address of the Barracuda1 system and click **Join Cluster**.
 - 4c. Click **Save Changes**.
5. On each Barracuda system, refresh the **Advanced > Clustering** page, and verify that:
 - Each system's IP address appears in the Clustered Systems list
 - The status of each server is green

The following example shows two servers in a cluster with a green status.

Figure 7.1:



6. Complete the following optional tasks:
 - Setup the MX record for each clustered system as a round robin in DNS (requires at least two systems in the cluster to be in an active state).
 - Configure your network switch to balance the load on each clustered system.

Load balancing controls traffic shaping whereas round robin directs traffic to the other clustered system if one fails.

Data Propagated to the Clustered Systems

Clustering not only makes managing multiple Barracuda Spam Firewalls more manageable, but also provides 100% redundant coverage of the propagated data. The following table identifies the data that is propagated to the other clustered systems when a new system joins.

Table 7.12:

Propagated Data	Data Not Propagated
System settings (global and domain) configured through the Administration interface	System IP configuration covered in <i>Configuring System IP Information</i> on page 49.

Table 7.12:

Propagated Data	Data Not Propagated
Per-user quarantine settings configured through a user's quarantine interface	SSL settings covered in <i>Enabling SSL</i> on page 100.
Message logs	
Bayesian databases	
Quarantine inboxes	
User accounts	

Note



A new system propagates its Bayesian database only once when it first joins the cluster. The clustered systems do not synchronize their Bayesian databases with each other. For this reason, you may want to periodically backup each system's Bayesian database and upload the backup file to the other clustered systems so they all have consistent policies. Synchronization will be added to a future firmware release.

Each user account has a primary and backup server in the cluster. The primary is the server that first joins the 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).

Field Descriptions for the Clustering Page

The following table describes the fields on the [Advanced > Clustering](#) page that you must complete to set up a clustered environment.

Table 7.13:

Field	Description
Cluster Settings	
Cluster Shared Secret	<p>The passcode shared by all Barracuda Spam Firewalls in this cluster. All Barracuda Spam Firewalls in a cluster must have the same shared passcode.</p> <p>Make sure a passcode has already been set on an existing system before you try adding this system to the cluster.</p>
Cluster Host Name	<p>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.</p> <p>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 to the cluster.</p>

Table 7.13:

Field	Description
Clustered Systems	
Cluster Field	<p>Enter the IP address or host name of one of the Barracuda Spam Firewalls in the cluster to join, and click Join Cluster.</p> <p>Once this system joins the cluster, the following happens:</p> <ul style="list-style-type: none"> • Configuration settings are pulled from the cluster and some of these settings override the settings on this system. • User lists on this system are synced with the cluster so no user accounts are lost.
Cluster System List	<p>Cluster System lists the other systems in this cluster.</p> <p>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.</p> <p>You must manually switch a standby server to Active if you want the standby server to begin filtering messages. The switchover does <i>not</i> automatically occur when an active server fails.</p> <p>Status displays whether each system is up and running (green dot) or down (red dot).</p>
Local Host Map	
Host Name / IP Address	<p>Maps 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.</p> <p>Use the local host map feature when:</p> <ul style="list-style-type: none"> • 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.

Impact of Changing the IP Address of a Clustered System

If your Barracuda Spam Firewall is running firmware version 3.1.x or earlier and is part of a clustered environment, then changing the IP address of the system removes it from the cluster. You will need to add the system back into the cluster after you change the IP address.

If your Barracuda Spam Firewall is running firmware version 3.2.x or above, the system remains part of its clustered environment after its IP address changes.

Implementing Single Sign-on

Advanced > Single Sign-On allows you to 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 above.

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.

Table 7.14:

Field	Description
Login Realm Selector	Enabling this option displays a realm selection drop-down menu on the login page so users can select their realm and login with just their username.
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 on the login page as well as in the Domain Settings for the administrator. This is a required field.
Auth. Type	Controls the type of realm that is created. Available options include: <ul style="list-style-type: none">• 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 a RADIUS database)• POP (where the password is maintained in an external POP server)
Auth. Host	The name of the LDAP, RADIUS, or POP server that the Barracuda Spam Firewall attempts to connect to for authentication purposes. This field is ignored for LOCAL authentication.
Auth. Port	The port the Barracuda Spam Firewall uses to connect to the LDAP, RADIUS, or POP server for authentication purposes. This field is ignored for LOCAL authentication.

Table 7.14:

Field	Description
Username Template	<p>If using LOCAL authentication, this field is ignored.</p> <p>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 e-mail address and the username portion.</p> <p>If using RADIUS authentication, this field should contain the RADIUS shared secret.</p>
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.

Enabling SSL

Advanced > **SSL** allows you to enable SSL on your Barracuda Spam Firewall. Click **Save Changes** after making any changes.

One of the most common reasons to enable SSL is to ensure user passwords remain secure. When using the Single Sign-on feature (covered in *Implementing Single Sign-on* on page 99), 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.

Table 7.15:

Web Interface HTTPS/SSL Configuration	
HTTPS/SSL access only:	<p>Select Yes to enable SSL and only allow access to the Administration interface via SSL. Select No to use standard HTTP access.</p> <p><i>Note: Once you enable SSL, any user who tries to log into the administration interface using "http" will be automatically redirected to the "https" equivalent address.</i></p>
Use HTTPS links in e-mails	<p>Whether the Barracuda Spam Firewall uses <i>https://</i> (instead of <i>http://</i>) in the links included in system e-mails. This applies to daily system reports, quarantine e-mails, and system alerts that are sent out by the system. This setting does not apply to e-mails sent out by users.</p> <p>This setting is automatically set to Yes when you enable HTTPS/SSL access.</p>
Web Interface HTTPS/SSL port	The SSL port used by the Barracuda Spam Firewall. Default port for SSL is 443.

Table 7.15:

SSL Certificate Configuration	
Certificate Type	<p>Select one of the following certificates for SSL:</p> <ul style="list-style-type: none"> • Default (Barracuda Networks) certificates are free but 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 Web browsers cannot verify the authenticity of the certificate and therefore display a warning every time a user accesses the administration 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	<p>The information stored in your certificates and Certificate Signing Requests. Provide the following information:</p> <p>Common Name is the fully qualified domain name used to access the administration interface. For example: "barracuda.yourdomain.com"</p> <p>Country is the two-letter country code where your organization is located.</p> <p>State or Province Name is the full name of the state or province where your organization is located.</p> <p>Locality Name is the city where your organization is located.</p> <p>Organization Name is the legal name of your company or organization.</p> <p>Organization Unit Name is an optional field in which to specify a department or section within your organization.</p>
Download Certificate Signing Request (CSR)	<p>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.</p>
Download Private key	<p>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.</p>
Download Private Root Certificate	<p>Click Download to obtain the private root certificate and import it into your Web browser. This is recommended if you selected a Private certificate type.</p> <p>Once you have imported the certificate, your Web browser is able to verify the authenticity of the Barracuda Spam Firewall's SSL certificate, and should no longer issue a warning when you visit the administration interface.</p>

Table 7.15:

Trusted Certificate	
Upload Signed Certificate	<p>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.</p> <p>Once you have uploaded your signed certificate, make sure <i>Trusted</i> is selected for the Certificate Type (described above).</p>
Upload Private key	<p>After downloading the private key, browse to the location of the key and click Upload.</p>

Detecting Spam in Chinese and Japanese Messages

Advanced > **Regional Settings** allows you to 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.

Table 7.16:

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

Customizing Non-Delivery Reports (NDRs)

Advanced > **Bounce/NDR Messages** allows you to modify the information in an NDR and select the default language to use in the message.

The Barracuda Spam Firewall sends NDRs to e-mail 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 Spam Firewall 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 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.

Table 7.17:

Field	Description
Select NDR Language	
Default Language	<p>Select the language to use for the default non-delivery reports. The Barracuda Spam Firewall automatically translates the default NDR messages to the language you specify.</p> <p>To customize the information in an NDR:</p> <ol style="list-style-type: none"> 1. From the Default Language drop-down menu, select Custom. 2. Click Save Changes. 3. Enter your customized text in the message boxes provided. 4. Click Save Changes. <p><i>Note: If you customize NDRs and then later switch back to a predefined language, you lose all customization and the Barracuda Spam Firewall reverts back to the default message for the specified language.</i></p>
Customized NDRs	
Banned File (recipient)	When a message containing an attachment type that has been banned is sent to a user, the Barracuda Spam Firewall blocks the incoming message and sends this notice to the intended recipient of the e-mail.
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 e-mail.
Spam (sender)	When the Barracuda Spam Firewall blocks a message because it was determined to be spam, the Barracuda Spam Firewall 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.

Table 7.18:

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.
%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

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

The following table describes each troubleshooting tool provided with the system.

Table 7.19:

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 Spam Firewall 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.

Table 7.19:

Troubleshooting Tool	Description
Telnet Device	<p>Attempts to establish a telnet session from your Barracuda Spam Firewall to the specified system. This session is non-interactive.</p> <p>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.</p>
Dig/NS-lookup Device	<p>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.</p> <p>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 <i>mx mydomain.com</i>.</p>
TCP Dump	<p>Performs a tcpdump on your Barracuda Spam Firewall to monitor network traffic.</p> <p>Enter any information you wish to provide for monitoring the connection (as well as any option to adjust the tcpdump output; for example: <i>-x -X port 53</i>) and click Begin TCP Dump to start the test.</p>
Traceroute Device	<p>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.</p>

Generating System Reports

The Barracuda Spam Firewall has a variety of system reports that can help you keep track of such statistics as the top spam senders and the top viruses detected by the system.

You can either generate a system report on demand, or configure the system to automatically generate the system reports on a daily basis. These settings are available on the [Advanced > Reporting](#) page.

Displaying and Emailing Reports

To display or e-mail a specific report:

1. From the [Advanced > Reporting](#) page, select a report from the Report Type drop-down menu.
2. Select a date and time range for the report.
3. Do one of the following:

Table 7.20:

To..	Then...
Email the report	<p>Enter the e-mail address for each recipient in the field provided and click Email Report. Separate each address by a comma.</p> <p>Emailed reports will be added to a queue shown in the Pending Reports section. Only one report can be created at a time to prevent overloading the Barracuda Spam Firewall. If a report takes a long time to generate you can cancel the report to free up system resources.</p>
Display the report in a separate window	<p>Click Show Report.</p> <p><i>Note: Selecting Show Report (instead of e-mailing the report) can consume a lot of resources on the Barracuda Spam Firewall. As a result, you should use discretion when specifying the span of time for a displayed report. Reports over 7 days in length can only be generated if you select to e-mail the report.</i></p>

Automating the Delivery of Daily System Reports

The Daily Report Email Options section lets you configure the Barracuda Spam Firewall to automatically deliver daily system reports to specific users by entering their e-mail addresses in the field next to each report type.

You can enter as many e-mail addresses as you like for each report as long as each address is separated by a comma. If you do not want a daily report to be distributed, do not enter an e-mail address next to that report type.

Each report covers traffic for one day only.

Specifying Report Properties

The following table describes the report properties you can modify to increase the usefulness of your system reports. These properties apply to reports sent via e-mail, as well as reports generated to screen.

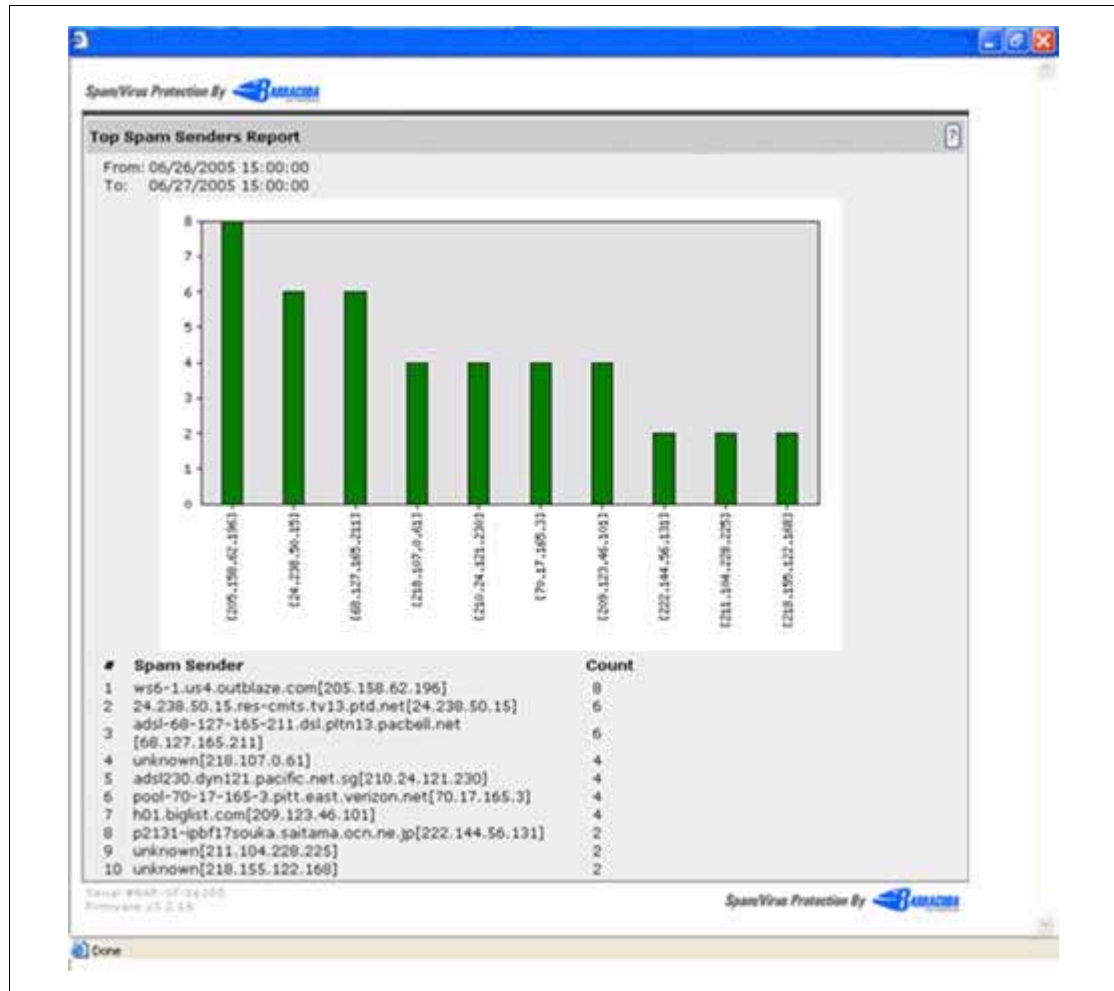
Table 7.21:

Report Property	Description
Top Count	<p>Determines the maximum number of records (rows) displayed in each report. For example, if you enter 10 in this field then the Top Spam Senders report would show the top 10 originators of spam messages.</p> <p>A pie chart cannot display more than 50 records.</p>
Chart Type	<p>The format used to display each report. The supported options are pie, vertical bars, and horizontal bars.</p>

Example Report

The following example shows a Top Spam Senders report in a vertical bars format.

Figure 7.2:



Enabling SMTP over TLS/SSL

Advanced > SMTP/TLS allows you to enable SMTP over TLS/SSL, which lets you encrypt mail over the Internet when both the sender and recipient are using a Barracuda Spam Firewall or other STARTTLS-capable mail server.

The new SMTP command known as STARTTLS advertises and negotiates an encrypted channel with the peer for this SMTP connection. STARTTLS is the standard SMTP feature for encryption of e-mail communications.

If you select **Yes** for this option, then SMTP over TLS will be enabled for incoming connections and SMTP over TLS will be attempted for outgoing connections, but requires the receiver server to support it.

Using the Task Manager to Monitor System Tasks

Advanced > **Task Manager** provides a list of tasks that are in the process of being performed, and also displays any errors encountered when performing these tasks.

Some of the tasks that the Barracuda Spam Firewall tracks include:

- Clustered environment setup
- Configuration and Bayesian data restoration
- Invalid users removal

If a task takes a long time to complete, you can click the **Cancel** link next to the task name and then run the task at a later time when the system is less busy.

The Task Errors section will list an error until you manually remove it from the list. The errors are not phased out over time.

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 Spam Firewall. For more information about these tools, refer to *Troubleshooting* on page 104.

In the event that a Barracuda Spam Firewall 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 14*.

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

Barracuda Networks
385 Ravendale Drive
Mountain View, CA 94043

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 86.

Rebooting the System in Recovery Mode

If your Barracuda Spam Firewall experiences a serious issue that impacts its core functionality, you can use diagnostic and recovery tools that are available at the reboot menu to return your system to an operational state.

Tasks to Perform Before Rebooting in Recovery Mode

Before you use the diagnostic and recovery tools, perform the following tasks:

Use the built-in troubleshooting tools to help diagnose the problem. For more information, see *Troubleshooting* on page 104.

Perform a system restore from the last known good backup file.

Contact Barracuda Networks Technical Support for additional troubleshooting tips.

- As a last resort, you can reboot your Barracuda Spam Firewall and run a memory test or perform a complete system recovery, as described in this section.

Performing a System Recovery or Hardware Test

To perform a system recovery or hardware test:

1. Connect a monitor and keyboard directly to your Barracuda Spam Firewall.
2. Reboot the system by doing one of the following:
 - Clicking the **Restart** button on the Basic > **Administration** page.
 - Pressing the Power button on the front panel to turn off the system, and then pressing the Power button again to turn back on the system.
The Barracuda splash screen displays with the following three boot options:
Barracuda
Recovery
Hardware_Test

3. Use your keyboard to select the desired boot option, and press `Enter`.

You must select the boot option within three seconds of the splash screen appearing. If you do not select an option within 3 seconds, the Barracuda Spam Firewall defaults to starting up in the normal mode (first option).

For a description of each boot option, refer to *Reboot Options* on page 109

Note



Reboot your Barracuda Spam Firewall to stop the hardware test.

Reboot Options

The following table describes the options available at the reboot menu.

Table 7.22:

Reboot Option	Description
Barracuda	Starts the Barracuda Spam Firewall in the normal (default) mode. This option is automatically selected if no other option is specified within the first three seconds of the splash screen appearing.
Recovery	Displays the Recovery Console where you can select the following options: <ul style="list-style-type: none">• Perform Filesystem Repair—Repairs the file system on XFS-based Barracuda Spam Firewalls. Select this option only if the serial number on your Barracuda Spam Firewall is below 24364; otherwise select the Perform Full System Re-image option.• Perform Full System Re-image—Restores the factory settings on your Barracuda Spam Firewall s and clears out the Bayesian database as well as quarantine e-mail and configuration information. Select this option if the serial number on your Barracuda Spam Firewall is 24364 or above.• Enable remote administration—Turns on reverse tunnel that provides Barracuda Networks technical support to access the system. Another method for enabling remote administration is to click Establish Connection to Barracuda Central on the Advanced->Troubleshooting page.• Run diagnostic memory test—Runs a diagnostic memory test from the operating system. If problems are reported when running this option, we recommend running the Hardware_Test option next.
Hardware_Test	Performs a thorough memory test that shows most memory related errors within a two-hour time period. The memory test is performed outside of the operating system and can take a long time to complete.

Note



Recover options are available only in the Barracuda Spam Firewall newer models.

Chapter 8

Outbound

This chapter describes the additional features that are provided when your Barracuda Spam Firewall is configured for outbound mode. For information on configuring your system for outbound mode, refer to *Configuring your System for Outbound Mode* on page 33.

Most of the inbound mode features documented in the other chapters are also supported when your system is in outbound mode. However, some pages do not appear in outbound mode while some other unique pages are added when your Barracuda Spam Firewall is configured for outbound mode.

<i>Tabs and Pages Supporting Outbound Mode</i>	<i>111</i>
<i>About Outbound Mode.....</i>	<i>112</i>
<i>Viewing Outbound Messages in the Message Log.....</i>	<i>113</i>
<i>Changing the Footers on Outbound Messages.....</i>	<i>113</i>
<i>Specifying Allowed Senders.....</i>	<i>114</i>
<i>Specifying Allowed Senders by Domain and IP Address.....</i>	<i>114</i>
<i>Specifying Allowed Senders Using SMTP Authentication.....</i>	<i>115</i>

Tabs and Pages Supporting Outbound Mode

The following table describes the tabs and pages that are unique to outbound mode. For information about the tabs and pages not mentioned in this table, refer to the other chapters in this guide.

Table 8.1:

BASIC-->Message Log	The Message Log in outbound mode provides a slightly different view of your outbound messages. For more information, refer to <i>Viewing Outbound Messages in the Message Log</i> on page 113.
BASIC-->Footer	The Footer page is unique to outbound mode. For more information, refer to <i>Changing the Footers on Outbound Messages</i> on page 113.
BASIC-->Allowed Senders	The Allowed Senders page is unique to outbound mode. For more information, refer to <i>Specifying Allowed Senders</i> on page 114.
POLICY	The POLICY tab contains many of the same pages that reside on the BLOCK/ACCEPT tab on the inbound mode. For information about the pages on the POLICY tab, refer to <i>Chapter 5</i> .

Table 8.1:

ADVANCED-->Email Protocol	The Email Protocol page provides a few features unique to outbound mode. For more information, refer to <i>Additional Email Protocol Settings for Outbound Mode</i> on page 115.
ADVANCED-->Rate Control	The Rate Control page contains slightly different settings in outbound mode. For more information, refer to <i>Configuring Message Rate Control</i> on page 118.
ADVANCED-->Relays	The Relay page is unique to outbound mode. For more information, refer to <i>Adding a Relay Server</i> on page 119.
ADVANCED-->Spam Scoring	The Spam Scoring page on the ADVANCED tab is unique to outbound mode. For more information, refer to <i>Enabling Intent Analysis and Spam Scoring</i> on page 116.
QUARANTINE BOX	The QUARANTINE BOX tab is unique to outbound mode. For more information, refer to <i>Managing the Quarantine Box</i> on page 117.

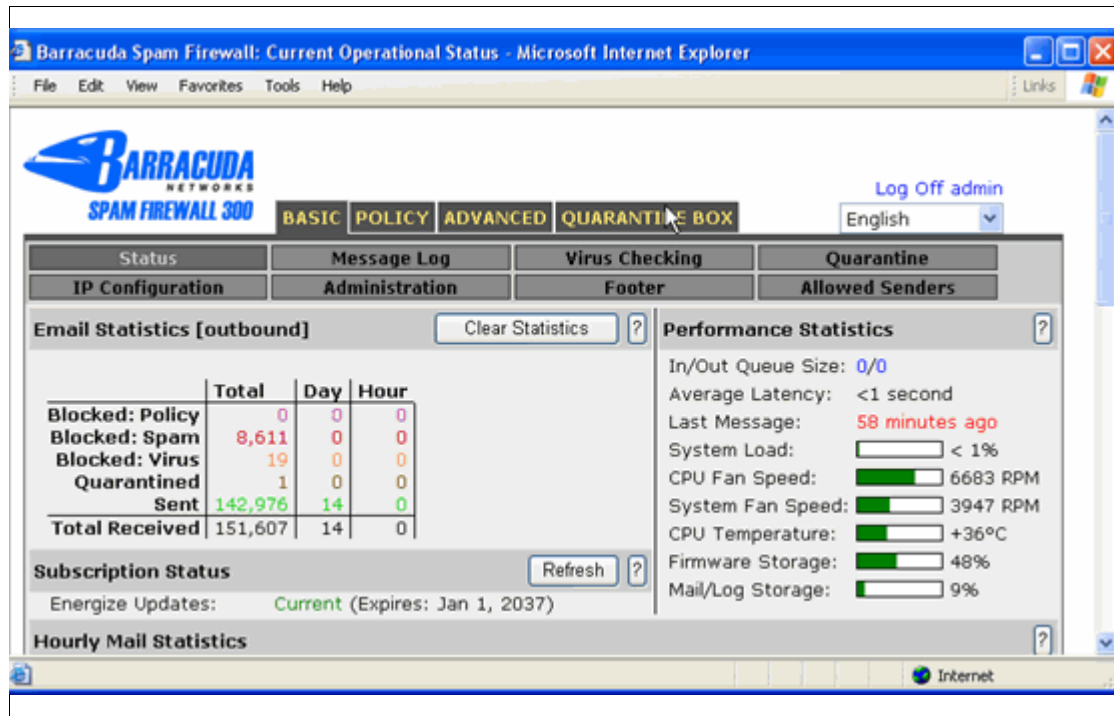
About Outbound Mode

Outbound Mode ensures that all e-mail leaving your network is virus-free and legitimate. It prevents individuals from unintentionally or intentionally using your organization's network to send viruses or spam. A Barracuda Spam Firewall can be configured for either inbound or outbound mode, but not both.

Once you configure your system for outbound mode, any outgoing message that contains a virus is automatically blocked and placed in the Quarantine Box. By default, outgoing messages are not scanned for intent analysis or spam scoring, but you can turn on this functionality if desired.

The easiest way to determine if your system is in outbound or inbound mode is to look on the **Basic > Status** page where the mode of your system appears next to the E-mail Statistics section, as show in the following example:

Figure 8.1:



Viewing Outbound Messages in the Message Log

If your Barracuda Spam Firewall is configured for outbound mode, the **Basic > Message log** page displays slightly different information about the outgoing messages.

For example, some common values for the Action column include:

- Sent—Occurs when the outgoing message is successfully sent to the intended recipient.
- Aborted—Occurs when the receiving e-mail server is down, the recipient e-mail address is incorrect or no longer valid.
- Deferred—Occurs when the rate control threshold is exceeded. For more information about rate control, refer to *Configuring Message Rate Control* on page 118.

The Action column also shows when an outgoing message has been quarantined or blocked due to a policy violation.

For a description of the other columns that also appear with inbound mode, refer to *Monitoring the Message Log* on page 40.

Changing the Footers on Outbound Messages

By default, the Barracuda Spam Firewall adds a footer to all outbound messages passed through the system. This footer informs the recipient that the message has been scanned for spam and viruses.

The BASIC-->Footer page lets you change the default footer behavior. The following table describes the footer settings you can change.

Table 8.2:

Field	Description
Attach Footer	Determines whether a footer is attached to outgoing messages.
Text Footer	The footer text attached to text/ASCII-based messages.
HTML Footer	The footer text attached to HTML-based messages.
Footer Exemptions	List of sending e-mail addresses that will not have a footer attached. Enter one e-mail address per line.

Specifying Allowed Senders

Basic > Allowed Senders allows you to control which messages are allowed to be relayed through your Barracuda Spam Firewall. You can control which messages are relayed by specifying:

- Allowed sending domains
- Allowed IP addresses
- SMTP authentication

Specifying Allowed Senders by Domain and IP Address

The following table describes the fields that allow you to control the domains and IP addresses that can send messages through your Barracuda Spam Firewall.

Table 8.3:

Field	Description
Sending Domains	Enter each domain that should be allowed to send e-mail through your Barracuda Spam Firewall. Click Add after entering each domain. If you leave this list empty, only the allowed IP addresses (described below) are used to verify allowed senders.
Allowed Sender IP Address	Enter each IP address (or network range using netmask) that should be allowed to send e-mail through your Barracuda Spam Firewall. If you leave this list empty: <ul style="list-style-type: none">• All IP addresses are allowed to send e-mail through the system.• Only the allowed Sending Domains (described above) are used to verify allowed senders.

Specifying Allowed Senders Using SMTP Authentication

Instead of specifying the IP addresses or domains that can send messages through your Barracuda Spam Firewall, you can enable SMTP authentication to authenticate users before their messages are allowed through the system.

To enable SMTP authentication to control allowed senders, fill in the following fields on the [Basic > Allowed Senders](#) page.

Table 8.4:

Field	Description
Enable SASL/SMTP Authentication	Supported values include: <ul style="list-style-type: none">• None—SASL/SMTP authentication is disabled.• LDAP—SMTP Authentication/SASL is set to authenticate against LDAP.• SMTP AUTH Proxy—SMTP Authentication/SASL is set to pass the SMTP Authentication command through to another mail server. SMTP AUTH/SASL defines a new SMTP command (AUTH) to authenticate users before allowing them to relay through your Barracuda Spam Firewall. If this authentication is enabled, then users should select 'Use name and password' or a similar option in their e-mail client. Because the password is transmitted in cleartext, it is a good idea to configure SMTP over TLS, as configured on the ADVANCED-->SMTP/TLS page.
Edit LDAP Settings: affinitypath.com	If you selected LDAP for SASL/SMTP Authentication, then enter the required information about your LDAP server in the fields provided.
SMTP AUTH Server	If you selected to use SMTP AUTH Proxy for SASL/SMTP Authentication, then enter the hostname of the SMTP AUTH server in this field. The username and password provided by the user in the SMTP AUTH command is relayed to the SMTP server you specify in this field. The SMTP server can be any server that is set up to support the SMTP AUTH authentication command (e.g. MS-Exchange or Sendmail).

Additional Email Protocol Settings for Outbound Mode

The outbound mode of the Barracuda Spam Firewall contains a few additional settings on the [Advanced > Email Protocol](#) page. The following table describes these settings:

Table 8.5:

Field	Description
Maximum Message Size	Determines the maximum message size (in bytes) accepted by the Barracuda Spam Firewall. Messages that exceed this limit are automatically blocked and an NDR notification goes out to the sender.

Table 8.5:

Field	Description
Messages per SMTP Session	<p>Sets a limit on the number of messages allowed in one SMTP session. If the number of messages in one session exceeds this threshold the rest of the messages are temporarily blocked and show up in the message log as being Deferred with a reason of <i>Per-Connection Message Limit Exceeded</i>.</p> <p>The sender is required to make a new connection to continue sending messages, which may ultimately trigger a Rate Control block.</p>

Enabling Intent Analysis and Spam Scoring

By default, intent analysis and spam scoring are disabled in outbound mode so your outgoing messages are not scanned for spam probability or offending URLs.

To change this default behavior, select **Advanced** > **Spam Scoring** to enable intent analysis and spam scoring of outgoing messages.

The following table describes the fields on this page.

Table 8.6:

Spam Scoring Limits	
Spam Scoring	<p>Whether spam scoring is turned on or off. Spam scoring is turned off when a Barracuda Spam Firewall is configured for outbound mode.</p> <p>After turning on spam scoring, you should configure the quarantine and block scores described below.</p>
Quarantine Score	<p>Messages with a score above this threshold, but below the block threshold, are forwarded to the quarantine inbox described in <i>Managing the Quarantine Box</i> on page 117.</p> <p><i>Note: Spam Scoring must to set to Yes for the quarantine score to take effect.</i></p>
Block Score	<p>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.</p> <p><i>Note: Spam Scoring must to set to Yes for the quarantine score to take effect.</i></p>
Intent Analysis	
Intent Analysis	<p>When Intent Analysis is turned on, your Barracuda Spam Firewall tries to match the URLs contained in outgoing messages against a local database of URLs known for sending spam.</p> <p>If the system finds a match, the outgoing message that contains the offending URL is automatically blocked.</p> <p>Systems configured for outbound mode have Intent Analysis turned off by default.</p> <p><i>Note: The local database that contains the list of offending URLs is updated on a regular basis by Energize Updates.</i></p>

Table 8.6:

Realtime Intent Analysis	<p>When this option is set to Yes, your Barracuda Spam Firewall tries to match the URLs contained in outgoing messages against the live Barracuda Central database that contains the latest list of URLs known for sending spam.</p> <p>The Barracuda Central database can be slightly more up-to-date than the local database used when Intent Analysis is turned on. However, using real-time intent analysis can increase the time it takes to scan messages.</p>
URL Exemptions	<p>Lists the URLs that should not be classified as offending URLs even if there is a match found during intent analysis. It is recommended you enter URLs that are commonly included in your outgoing messages.</p> <p><i>Note: You do not need to include "http://" in front of the URLs you add to this list.</i></p>
Spam Bounce (NDR) Configuration	
Send Bounce	<p>By default, the Barracuda Spam Firewall sends an NDR (non-delivery report) to senders when their message is blocked and not delivered. You can turn off this automatic notification by selecting No.</p>

Managing the Quarantine Box

When the Barracuda Spam Firewall detects a virus in an outgoing message, that message is automatically placed in the Quarantine Box so the system administrator can take appropriate action (such as scanning the sender's computer for a virus). If spam scanning has been enabled, then spam messages may also be sent to the Quarantine Box.

Sending NDRs for Quarantined Messages

- After the Barracuda Spam Firewall quarantines a message, it sends an NDR (non-delivery report) to the sender informing them that their message was not sent.
- To stop the Barracuda Spam Firewall from sending NDRs when an outgoing message is quarantined, select **Basic** > **Quarantine** and **No** next to this option.

Viewing and Classifying Quarantined Messages

The **Quarantine Inbox** tab lists the messages that the Barracuda Spam Firewall has quarantined. To view the contents of a message, click on the message entry.

After viewing the messages in the quarantine inbox you may decide to remove the message from the inbox or deliver the message to the intended recipient. The following table describes the actions you can take after selecting a message:

Table 8.7:

Button	Action
Deliver	Sends the message to the intended recipient. Note that if a virus has been detected in the message that you decide to deliver, the virus is not removed.
Whitelist	Adds the sending e-mail address to the whitelist and delivers the message. All future e-mail from this sender are not quarantined.
Delete	Removes the message from the quarantine box without sending it to the recipient.
Reject	Sends an NDR to the sender and deletes the message from the quarantine box.
Forward	Forwards the message to the specified address. Use this feature when you want to further examine the e-mail from another system.

Using Filters to Locate Specific Messages

If your quarantine box contains many messages, you may need to use the Filter menu to search for specific messages. These filters include:

- **From contains**—Searches the From field in all quarantined messages for the specified text.
- **Subject contains**—Searches the Subject line in all quarantined messages for the specified text.
- **Message contains**—Searches the message body in all quarantined messages for the specified text. This filter may fail or take an exceptionally long period of time with a large Message Log.

Configuring Message Rate Control

Rate Control allows you to 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 e-mail to your server in a small amount of time.

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

Table 8.8:

Setting	Description
Rate Control	<p>Specifies the rate threshold for the following:</p> <ul style="list-style-type: none">• Maximum number of connections allowed from the same IP address in a half-hour timeframe. This setting takes affect when over 5 unique IP addresses are connected to the Barracuda Spam Firewall.• Maximum SMTP sessions allowed from the same e-mail address. This setting takes affect after 5 unique e-mail addresses have been sent through the system. <p>When the number of connections or SMTP sessions goes over the specified rate, the Barracuda Spam Firewall blocks further outgoing messages from the sending IP address or SMTP session.</p>
Rate Control Exclude IP/Range	The IP address range you wish to exclude from rate control. To enter a single IP address (instead of a range), enter a netmask of 255.255.255.255.
Rate Control Exclude Sender Email Address	The sending e-mail addresses (one per line) that should not be subject to rate control.

Adding a Relay Server

Advanced > Relay allows you to add relay servers or 'smart hosts' for certain domains. Adding a relay server is necessary if you want to redirect messages for certain domains to another relay server or to another mail server in your network

To add a relay server:

1. In the Relay Server Configuration field, enter the relay server domain name and click **Add Domain**.
2. Enter the relay server's IP address and destination port.
3. Specify whether you want to use MX records.
4. Click **Save Changes**.
5. Enter a valid e-mail address in the provided field, and click **Test**.
6. The Barracuda Spam Firewall sends an e-mail to the relay server.
7. Check the relay server to verify the test message was received. If the message is not delivered, verify the relay server information you just entered.

This page also lets you specify a single mail relay server, as follows:

1. Enter an asterisk (*) as the domain name and click **Add Domain**.
2. Remove all other entries from the domain name list by clicking the trash can icon next to each one.

The asterisk wildcard domain causes all outbound e-mails forwarded to the Barracuda Spam Firewall to be sent to a single mail server to another relay server specified on the **Advanced > Relay**.

Setting Up Subject and Body Filtering

You can use compliance buttons to filter information containing credit card, information, privacy, or HIPAA information that are confidential or sensitive material for outbound mail. These buttons contain pre-set patterns. When selected, they are inserted as keyword listings that have precoded patterns that contain regular expressions. Outbound e-mails that contain these patterns are blocked. This information include:

- **Credit Cards:** Messages sent through the Barracuda Outbound Spam Firewall containing recognizable Master Card, Visa, American Express, Diners Club or Discover card numbers are blocked or quarantined when this pattern is used.
- **Social Security:** Messages sent with valid social security numbers are blocked or quarantined when using this pattern.
- **Privacy:** Messages are blocked or quarantined for privacy if they contain two or more of the following information: Address, Birthday, Social Security number, credit card number, driver's license number, phone number, or expiration date.
- **HIPAA:** Messages are blocked or quarantined if they are identified by the Privacy option above or these messages contain two or more phrases indicative of private medical information.

These patterns help minimize the misuse of confidential information for outbound mails but they do not guarantee that these patterns cannot be overridden or that misuse of confidential be completely prevented. These patterns cannot take away the importance of educating your employees on recognizing misuse of confidential information.

Managing Your Quarantine Inbox

This chapter describes how you can check your quarantined messages, classify messages as spam and not spam, and modify your user preferences using the Barracuda Spam Firewall interface. This chapter is intended for the end user and contains the following topics:

- Receiving Messages from the Barracuda Spam Firewall in the next section.
- *Using the Quarantine Interface* on page 122.
- *Changing your User Preferences* on page 124.

Receiving Messages from the Barracuda Spam Firewall

The Barracuda Spam Firewall sends you the following two types of messages:

- Greeting Message
- Spam Quarantine Summary Report

Greeting Message

The first time the Barracuda Spam Firewall quarantines an e-mail 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: <*your e-mail address*>

Password: <*your 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 e-mail 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.

Figure 9.1:

The screenshot shows an email from Barracuda Spam Firewall. The header includes: From: Barracuda Spam Firewall [support@barracudanetworks.com], To: nguyen@affinitypath.com, Cc: (empty), Subject: Daily Spam Quarantine Summary, Sent: Tue 1/13/13. The main body features the Barracuda logo and the title "Spam Quarantine Summary". It addresses "nguyen@affinitypath.com" and states there are 3 messages in the quarantine inbox. A list of instructions follows: "Click on the **Deliver** link to have a message delivered to your mailbox.", "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.", and "Click the **Delete** link to have the message deleted from your quarantine (message will be automatically for spam learning)". Below this is a table of quarantined messages:

Date	From	Subject	Actions
01/12 13:01	"Khoa Nguyen" <khoa_barracu...>	welcome to paris you 1	Deliver Whitelist Delete
01/07 09:26	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

At the bottom, it says "To view your entire quarantine inbox or manage your preferences, [click here](#)." and includes the "Spam/Virus Protection By BARRACUDA NETWORKS" logo. Two arrows point from text above to the "click here" link and the "Actions" column of the table.

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 your 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 e-mail displays the message.

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

Table 9.1:

Action	Description
Deliver	Delivers the selected message to your standard e-mail inbox. <i>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 your quarantine list.</i>
Whitelist	Adds the selected message to your whitelist so all future e-mails from this sender are not quarantined unless the message contains a virus or banned attachment 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 <i>mail3.abcbank.com</i> , and a subsequent message may come from <i>mail2.abcbank.com</i> . 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. <i>Note: Some bulk commercial e-mail may be considered useful by some users and spam by others. Instead of classifying bulk commercial e-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).</i>
Classify as Spam	Classifies the selected message as spam.

Changing your User Preferences

After logging into your quarantine interface, you can use 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 your quarantine interface, go to **Preferences > Password**. This option is not available if single sign on has been enabled via LDAP or Radius.

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 will 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.

Table 9.2:

Quarantine Setting	Description
Enable Quarantine	<p>Whether the Barracuda Spam Firewall quarantines your messages.</p> <p>If you select Yes, the Barracuda Spam Firewall does not deliver quarantined messages to your general e-mail inbox, but you can view these messages from the quarantine interface and quarantine summary reports.</p> <p>If you select No, all messages that would have been quarantined for you are delivered to your general e-mail inbox with the subject line prefixed with [QUAR]:. The Barracuda Spam Firewall administrator can modify this prefix.</p>
Notification Interval	<p>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 e-mails have been quarantined.</p> <p>If you select Never, you can still view your quarantined messages from the quarantine interface, but you will not receive quarantine summary reports.</p>

Table 9.2:

Quarantine Setting	Description
Notification Address	The e-mail address the Barracuda Spam Firewall should use to deliver your quarantine summary report.
Default Language	The language in which you want to receive your quarantine notifications. This setting also sets the default encoding for handling unknown character sets during filtering. All e-mail notifications from the Barracuda Spam Firewall are in UTF8 encoding.

Enabling and Disabling Spam Scanning of your Email

If you do not want the Barracuda Spam Firewall scanning your e-mails 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 e-mails are tagged, quarantined or blocked.

When the Barracuda Spam Firewall receives an e-mail 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.

The following table describes the fields on the [Preferences > Spam Settings](#) page.

Setting	Description
Spam Filter Enable/Disable	
Enable Spam Filtering	Select Yes for the Barracuda Spam Firewall to scan your e-mails 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.
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.
Barracuda Bayesian Learning	

Setting	Description
Reset Bayesian Database	Click Reset to remove your Bayesian rules learned by the Barracuda Spam Firewall from the point of installation.
Bayesian Database Backup	
Backup Bayesian Database	Click Backup to download a copy of your Bayesian database to your local system. This backup copy can then be uploaded to any Barracuda Spam Firewall, including this one, in the case of a corrupt Bayesian installation.
Restore Database	Click Browse to select the backup file containing your Bayesian database, and then click Upload Now to load the Bayesian settings to this Barracuda Spam Firewall. The backup file does not need to have originated from this Barracuda Spam Firewall, nor from the same user database.

Adding Email Addresses and Domains to Your Whitelist and Blacklist

[Preferences](#) > [Whitelist/Blacklist](#) allows you to specify e-mail addresses and domains from which you do or do not want to receive e-mails.

List Type	Description
Whitelist	The list of e-mail addresses or domains from which you always wish to receive messages. The only time the Barracuda Spam Firewall blocks a message from someone on your whitelist is when the message contains a virus or a disallowed attachment file extension.
Blacklist	The 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. The only time a blacklisted e-mail address is delivered is if the same e-mail address also appears in your whitelist.

To whitelist or blacklist senders, follow these steps:

1. Select [Preferences](#) > [Whitelist/Blacklist](#).
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 e-mail 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.

Changing the Language of the Quarantine Interface

You can change the language of your quarantine interface by selecting a language from the drop-down menu in the upper right corner of the **Quarantine Inbox** and **Preferences** tabs. Supported languages include Chinese, Japanese, Spanish, French, and others.

The language you select is only applied to your individual quarantine interface. No other user's interface is affected.



Appendix 1

Regular Expressions

The Barracuda Spam Firewall allows you to 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.

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 130.
- All matches are not case sensitive.

Table 1.1 describes the most common regular expressions supported by the Barracuda Spam Firewall.

Table 1.1: Common Regular Expressions

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 new line
[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]

Table 1.1: Common Regular Expressions

Expression	Matches...
\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 prepended by a backward slash (\) when you want them interpreted literally:

Table 1.2: Special Characters

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

Examples

Table 1.3 provides some examples to help you understand how regular expressions can be used.

Table 1.3: Regular Expressions

Example	Matches...
viagra	viagra, VIAGRA or viaGRa
d+	One or more digits: 0, 42, 007
(bad good)	letters 'bad' or matches the letters 'good'
^free	letters 'free' at the beginning of a line
v[i1]agra	viagra or v1agra
v(ia 1a)gra	viagra or v1agra
v agra	v agra
v(i 1 \)?agra	vagra, viagra, v1agra or v agra

Table 1.3: Regular Expressions

Example	Matches...
FREE	*FREE*
FREE V.*GRA	*FREE* VIAGRA, *FREE* VEHICLEGRA, etc

Limited Warranty and Licensing

Barracuda Networks, Inc., or the Barracuda Networks, Inc. subsidiary or authorized Distributor selling the Barracuda Networks product, if sale is not directly by Barracuda Networks, Inc., ("Barracuda Networks") warrants that commencing from the date of delivery to Customer (but in case of resale by a Barracuda Networks reseller, commencing not more than sixty (60) days after original shipment by Barracuda Networks, Inc.), and continuing for a period of ninety (90) days: (a) its products (excluding any software) will be free from material defects in materials and workmanship under normal use; and (b) the software provided in connection with its products, including any software contained or embedded in such products will substantially conform to Barracuda Networks published specifications in effect as of the date of manufacture. Except for the foregoing, the software is provided as is. In no event does Barracuda Networks warrant that the software is error free or that Customer will be able to operate the software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Barracuda Networks does not warrant that the software or any equipment, system or network on which the software is used will be free of vulnerability to intrusion or attack. The limited warranty extends only to you the original buyer of the Barracuda Networks product and is non-transferable.

Exclusive Remedy

Your sole and exclusive remedy and the entire liability of Barracuda Networks under this limited warranty shall be, at Barracuda Networks or its service centers option and expense, the repair, replacement or refund of the purchase price of any products sold which do not comply with this warranty. Hardware replaced under the terms of this limited warranty may be refurbished or new equipment substituted at Barracuda Networks option. Barracuda Networks obligations hereunder are conditioned upon the return of affected articles in accordance with Barracuda Networks then-current Return Material Authorization ("RMA") procedures. All parts will be new or refurbished, at Barracuda Networks discretion, and shall be furnished on an exchange basis. All parts removed for replacement will become the property of the Barracuda Networks. In connection with warranty services hereunder, Barracuda Networks may at its discretion modify the hardware of the product at no cost to you to improve its reliability or performance. The warranty period is not extended if Barracuda Networks repairs or replaces a warranted product or any parts. Barracuda Networks may change the availability of limited warranties, at its discretion, but any changes will not be retroactive. IN NO EVENT SHALL BARRACUDA NETWORKS LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE, OR ITS DOCUMENTATION.

Exclusions and Restrictions

This limited warranty does not apply to Barracuda Networks products that are or have been (a) marked or identified as "sample" or "beta," (b) loaned or provided to you at no cost, (c) sold "as is," (d) repaired, altered or modified except by Barracuda Networks, (e) not installed, operated or maintained in accordance with instructions supplied by Barracuda Networks, or (f) subjected to abnormal physical or electrical stress, misuse, negligence or to an accident.

EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS MAKES NO OTHER WARRANTY, EXPRESS, IMPLIED OR STATUTORY, WITH RESPECT TO BARRACUDA NETWORKS PRODUCTS, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, AVAILABILITY, RELIABILITY, USEFULNESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. EXCEPT FOR THE ABOVE WARRANTY, BARRACUDA NETWORKS'S PRODUCTS AND THE SOFTWARE IS PROVIDED "AS-IS" AND BARRACUDA NETWORKS DOES NOT WARRANT THAT ITS PRODUCTS WILL MEET YOUR REQUIREMENTS OR BE UNINTERRUPTED, TIMELY, AVAILABLE, SECURE OR ERRORFREE, OR THAT ANY ERRORS IN ITS PRODUCTS OR THE SOFTWARE WILL BE CORRECTED. FURTHERMORE, BARRACUDA NETWORKS DOES NOT WARRANT THAT BARRACUDA NETWORKS PRODUCTS, THE SOFTWARE OR ANY EQUIPMENT, SYSTEM OR NETWORK ON WHICH BARRACUDA NETWORKS PRODUCTS WILL BE USED WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK.

Open Source Licensing

Barracuda products may include programs that are covered by the GNU General Public License (GPL) or other "open source" license agreements. The GNU license is re-printed below for your reference. These programs are copyrighted by their authors or other parties, and the authors and copyright holders disclaim any warranty for such programs. Other programs are copyright by Barracuda Networks.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public

License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Source Code Availability

Per the GPL and other "open source" license agreements the complete machine readable source code for programs covered by the GPL or other "open source" license agreements is available from Barracuda Networks at no charge. If you would like a copy of the source code or the changes to a particular program we will gladly provide them, on a CD, for a fee of \$100.00. This fee is to pay for the time for a Barracuda Networks engineer to assemble the changes and source code, create the media, package the media, and mail the media. Please send a check payable in USA funds and include the program name. We will mail the packaged source code for any program covered under the GPL or other "open source" license.



Appendix 3

Compliance



Notice for the USA

Compliance Information Statement (Declaration of Conformity Procedure) DoC FCC Part 15: This device complies with part 15 of the FCC Rules.

Operation is subject to the following conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received including interference that may cause undesired operation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try one or more of the following measures:
 - Reorient or relocate the receiving antenna.
 - Increase the separation between the equipment and the receiver.
 - Plug the equipment into an outlet on a circuit different from that of the receiver.
 - Consult the dealer or an experienced radio/ television technician for help.

Notice for Canada

This apparatus complies with the Class B limits for radio interference as specified in the Canadian Department of Communication Radio Interference Regulations.



Notice for Europe (CE Mark)

This product is in conformity with the Council Directive 89/336/EEC, 92/31/EEC (EMC).

Index

A

- Account View page 69
- accounts
 - activating for individuals 86
 - creating 69
 - deleting 69
 - editing 71
 - overriding settings 73
- activating individual accounts 86
- adding domains 75
- administration interface
 - branding 91
 - logging in 28
- Administration page 51
- Advanced Domain Setup page 75
- Advanced IP Configuration page 95
- aliases, unifying 78
- allow email recipient domains 51
- allowed email recipient domains 29
- allowed IP range 51
- Allowed Senders page (outbound mode) 113
- allowed SNMP range 51
- Appearance page 91

B

- backscatter, reducing 57
- backup
 - automatic 86
 - desktop 86
 - system data 86
- Barracuda Central 11
- Barracuda headers, removing 85
- Barracuda Spam Firewall
 - configuring 28
 - features 13
 - installing 26
 - model comparison 13
 - overview 10
 - warranty policy 12
- Bayesian database
 - resetting 55
 - restoring 88
- blacklist services 59, 60

- block email setting 45, 125
- BLOCK/ACCEPT tab 59
- Body Filtering page 66
- branding the administration interface 91

C

- caller ID 84
- certificates, signing 101
- changing, password 51
- character tags 133
- Clear Log button 42
- clustering Barracuda Spam Firewalls 95, 96, 97, 99, 100, 102, 104, 105
- Clustering page 95, 96, 97, 99, 100, 102, 104, 105
- configuring
 - Barracuda Spam Firewall 28
 - domains 75
- contacting technical support 12
- creating new accounts, about 69
- customizing
 - administration interface 91

D

- daily mail statistics 39
- defense layers 10
- deleting
 - user accounts 69
- destination mail server setting 50
- diagnostic memory test 110
- disabling
 - spam scoring 125
 - virus checking 46
 - virus notification 46
- DNS configuration 28
- DNSBLs 59
- domain configuration 28
- Domain Manager page 76
- domains
 - adding 75
 - configuring 50
 - editing 76

E

- editing
 - accounts 71
 - domains 76
- email
 - routing 31
 - servers 75
 - statistics 37
- email aliases, unifying 78
- Email Protocol page 83
- email protocol settings (outbound mode) 115
- Email Recipient Block/Accept page 63
- enabling
 - spam scoring 125
 - virus checking 46
 - virus notification 46
- Energize Updates 10
- equipment, required 25
- Exchange Accelerator feature 78

F

- failed system, replacing 108
- file attachments
 - quarantining 65
- file extensions
 - quarantining 65
- firewall, configuring 27
- firmware
 - updating 29
- Footers page (outbound mode) 113
- full header scan 60

G

- generating reports 105
- global quarantine
 - settings 48
 - types 47
- greeting message 121

H

- hardware test 110
- header
 - blocking 67
 - quarantining 67
 - tagging 67
 - whitelisting 67
- headers (Barracuda), removing 85
- hourly mail statistics 39
- HTTPS access 100

I

- incoming SMTP timeout setting 85

- indicator lights 39
- installation examples 32
- installing, Barracuda Spam Firewall 26
- Instant Replacement service 108
- Intent Analysis, enabling 56
- IP address, setting 27
- IP Configuration page 49

L

- language, changing in administration interface 57
- LDAP 77
- LDAP, common settings 80
- LEDs (on front panel) 39
- lights (on front panel) 39
- link domains 49
- logging into quarantine interface 122
- Lotus Notes plug-in 54

M

- mail client 54
- mail statistics 39
- mail syslog 92
- managing, quarantine inbox 123
- message content
 - blocking 66
 - quarantining 66
 - tagging 66
 - whitelisting 66
- message details 44
- Message Log page 40, 43, 54
- message log privacy 44
- mode, changing (inbound/outbound) 53
- monitoring
 - message log 40
 - system status 37
- multiple domains, configuring 75
- MX records 31, 76

N

- network interfaces, configuring 95
- network settings, configuring 27
- network time protocol 29
- not spam, classifying messages as 42
- notification interval, quarantine 49
- NTP 29

O

- ORDB blacklist 61
- Outbound Footer page 94

- outbound mode 12
 - about 112
 - configuring 33
 - features 111
- Outbound Relay page 93
- Outlook plug-in 54
- overriding
 - account settings 73
 - quarantining settings 73

P

- password (user), changing 124
- password, changing 51
- per-domain settings 76
- performance statistics 38
- per-user quarantine settings 48
- per-user quarantine type 47
- port forwarding 31
- post-installation tasks 31
- preferences, changing 124
- proxy server configuration 50
- pu_config.tgz 75

Q

- quarantine
 - email setting 45, 125
 - notification interval 49
 - overriding settings 73
 - setting up 46
 - types 47
- quarantine inbox, managing 123
- quarantine interface, logging in 122
- Quarantine page 48
- quarantine summary report 122

R

- RAID 13
- Rate Control page 85
- Rate Control page (outbound mode) 118
- RBLs 59
- reboot options 108
- recovery mode 108
- regular expressions, about 129
- re-imaging system, enabling
 - remote administration 110
- relays, setting up 93
- removing Barracuda headers 85
- repairing, file system 110
- replacing a failed system 108
- replacing failed system 108
- Reporting page 105
- RESET button, using 53

- resetting Bayesian database 55
- restoring
 - Bayesian database 88
 - system configuration 88
 - system data 86
 - user settings 88
- retention policies, setting 75
- RFC 821 compliance 83
- routing incoming email 31

S

- SASL authentication 94
- Send Bounce field 45
- Sender Email Address page 63
- Sender Policy Framework (SPF) 84
- setting up, quarantine 46
- SMTP authentication 94
- SMTP HELO 83
- SMTP settings 83
- spam
 - classification 43
 - classifying messages as 42
- Spam Bounce (NDR) Configuration 45
- spam scoring
 - enabling and disabling 125
 - overview 11
- spamcop blacklist 61
- Spamhaus 60
- SPF 83, 84
- spoof protection 77, 84
- StartTLS 78
- Subject Filtering page 65
- subject line
 - blocking 65
 - quarantining 65
 - tagging 65
 - whitelisting 65
- subscription status 39
- subscription status, verifying 29
- synchronizing databases in a cluster 56
- Syslog page 92
- system alerts, enabling 53
- system notifications, enabling 53
- system status, monitoring 37

T

- tag email setting 125
- tag score 45
- TCP ports 27
- TCP/IP configuration 50
- technical support, contacting 12
- testing memory 110
- TLS, enabling 78

U

- UDP ports 27
- unifying email aliases 78
- un-whitelist 42
- updating
 - firmware 29
- Use MX Records field 76
- user preferences, changing 124
- user settings
 - restoring 88

V

- viewing message details 44
- Virus Checking page 46
- virus checking, enabling and disabling 46
- virus notification, enabling and disabling 46

W

- warranty policy 12
- Web GUI syslog 92
- Web interface port, configuring 52
- whitelist, adding messages to 42