Chapter 1 – Introduction ........................................ 9

Overview ................................................................. 10
What This Guide Covers .............................................. 10
Easy Administration .................................................... 10
IPv6 Network Support ............................................... 10
12 Layers of Virus and Spam Protection .......................... 11
   Inbound Message Filtering ........................................ 11
   Outbound Message Filtering and Encryption .................... 11
   Internal Virus Scanning ............................................. 12
Energize Updates Maximize Protection ............................ 12
   Barracuda Central .................................................. 12
   How Energize Updates Defeat Spam .............................. 13
Barracuda Spam & Virus Firewall Models ......................... 14
Contacting Technical Support ....................................... 15

Chapter 2 – Barracuda Spam & Virus Firewall Concepts . 17

Twelve Layers of Defense ............................................. 18
Maximizing Efficiency and Performance of Spam Scanning .... 18
Connection Management Layers .................................... 19
   Denial of Service Protection ........................................ 19
   Rate Control .......................................................... 19
   IP Analysis ............................................................ 19
   Sender Authentication ............................................... 20
   Recipient Verification .............................................. 20
Mail Scanning Layers .................................................. 21
   Virus Scanning ........................................................ 21
   User-specified rules (custom policy) .............................. 21
   Fingerprint Analysis ................................................ 21
   Intent Analysis ....................................................... 22
   Image Analysis ....................................................... 22
   Bayesian Analysis ................................................... 22
   Spam Scoring ......................................................... 22
   Predictive Sender Profiling ........................................ 24

Chapter 3 – Getting Started ......................................... 25

Initial Setup .............................................................. 26
   Virtual Machine Deployment ....................................... 26
      Best Practices for Configuring Your Hypervisor .............. 26
   Checklist for Unpacking ............................................ 26
   Installation Examples ................................................ 27
      Barracuda Spam & Virus Firewall Behind Corporate Firewall 27
      Barracuda Spam & Virus Firewall in the DMZ ................ 27
      Clustering the Barracuda Spam & Virus Firewall ............. 28
   Install the Barracuda Spam & Virus Firewall ................... 29
Chapter 4 – Securing the Barracuda Spam & Virus Firewall

Securing Network Access ................................................. 46
SSL Certificates .......................................................... 46
Secure Links in Notification Emails ................................. 46
Use the Cloud Protection Layer ...................................... 46
Limiting Access to the API ............................................... 47
Tracking Changes to the Configuration and User Login Activities ......................................................... 47
Limiting User Access ....................................................... 47
Securing User Access With Single Sign On ....................... 47
User Account Authentication ........................................... 48
LDAP and User Account Authentication ............................ 48
Limiting User Access to a Clustered System ...................... 48
Advanced Email Security Policy ........................................ 48
SMTP/TLS (Transport Layer Security) encryption ............... 48
Securing the Outbound Relay of Email .............................. 49
Invalid Bounce Suppression ............................................. 49

Product Tips ....................................................................... 41
Email Statistics - Inbound ................................................. 42
Email Statistics - Outbound .............................................. 42
Setting up Quarantine ...................................................... 42
# Chapter 5 – Advanced Inbound Spam Filtering Policy

- **Rate Control** ................................................................. 52
- **When Rate Control Takes Effect** ................................. 52
- **Exemptions from Rate Control** ..................................... 52
- **IP Analysis** ..................................................................... 53
- **Trusted Forwarders** ....................................................... 53
- **IP Reputation** ................................................................. 53
- **Barracuda Reputation (BRBL)** ....................................... 53
  - Exempting IP Addresses from the BRBL and Other Blocklists 54
- **Subscribing to External blocklist Services** ........................ 54
- **Sender Whitelisting - Precedence** ................................... 54
- **Reverse DNS Blocking** .................................................. 54
- **Content Analysis - Inbound** ........................................... 55
  - **Custom Content Filters** .............................................. 55
  - **Attachment Filtering** .................................................. 55
  - **Blocking Email by Country** ........................................ 56
  - **Fingerprint Analysis** .................................................. 56
  - **Intent Analysis** ........................................................... 56
  - **Image Analysis** .......................................................... 57
- **Bayesian Analysis** .......................................................... 57
  - How Bayesian Analysis Works ....................................... 57
  - Global Bayesian Filtering Versus Per-User ...................... 57
  - Getting the Best Accuracy From the Bayesian Database ...... 58
  - When to Use Bayesian Analysis ...................................... 58
- **Outlook and Lotus Notes Plugins** .................................... 59

# Chapter 6 – Outbound Filtering Policy

- **Encryption of Outbound Mail** ........................................ 62
- **Secured Message Contents** .......................................... 62
- **Configuring and Using Encryption** ................................. 62
  - Requirements for Using Encryption ................................. 62
  - Setting Encryption Policy for Outbound Mail .................. 62
  - Branding ................................................................. 63
  - Encryption and Quarantine, Blocking and Queuing .......... 63
- **Sending and Receiving Encrypted Messages** ................... 63
- **Spam Filtering and Quarantine of Outbound Mail** .............. 64
  - **Spam Scoring** .......................................................... 64
  - **Managing Outbound Quarantine** ................................ 64
- **Rate Control for Outbound Mail** .................................... 65
- **IP, Domain and Email Address Filtering of Outbound Mail** 65
  - **IP Address Filtering** ................................................. 65
  - **Sender and Recipient Filtering** ................................... 66
  - **Reverse DNS Blocking** ............................................. 66
  - **Attachment Filename and Type Filtering** ..................... 66
- **Content Analysis - Outbound Mail** ................................. 67
  - **Custom Content Filters - Outbound** ............................ 67
  - **Attachment Content Filtering - Outbound** .................. 67
  - **Fingerprint Analysis - Outbound** ............................... 67
  - **Intent Analysis - Outbound** ....................................... 67
  - **Image Analysis - Outbound** ...................................... 68
Chapter 1

Introduction

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

- Overview ........................................................................................................... 10
- Barracuda Spam & Virus Firewall Models ................................................... 14
- Contacting Technical Support........................................................................... 15
Overview

The Barracuda Spam & Virus Firewall is an integrated hardware and software solution that provides powerful and scalable spam and virus-blocking capabilities without affecting the performance of your mail servers. With no per-user license fee, the Barracuda Spam & Virus Firewall can be scaled to support hundreds of thousands of active email users.

In addition to protecting your mail server from malware from the Internet, the Barracuda Exchange Anti-Virus add-in for the MS Exchange Server can secure your internal mail transactions as well, blocking infected messages on your internal network.

What This Guide Covers

This guide provides concepts and general guidance the administrator needs to understand how to best configure the Barracuda Spam & Virus Firewall according to the organization’s deployment needs, policies and email infrastructure. General discussion of the powerful features of the Barracuda Spam & Virus Firewall are presented here while detailed, procedural configuration steps are given in the rich online help of the Web interface. To view the online help, click the Help button on the right side of any page of the Web interface.

When referring to specific feature settings, this guide will specify the name of the tab in the Web interface in uppercase letters, followed by a ( > ) and the actual page name. For example, you can view system email and performance statistics and subscription status on the BASIC > Status page.

Easy Administration

The powerful Web interface of the Barracuda Spam & Virus Firewall allows for convenient configuration and management of spam and virus filtering policies and email security settings from one central location.

The administrator can elect to receive alerts and notifications from the Barracuda Spam & Virus Firewall at any email address and has message and system logs available to quickly assess the status of the system. Key email statistics and system performance can be viewed at a glance on the BASIC > Status page of the Web interface.

To minimize ongoing administration associated with security, Barracuda Central, the 24x7 operations center operated by Barracuda Networks to monitor and block the latest Internet threats, automatically delivers Energize Updates to your Barracuda Spam & Virus Firewall (see below). These updates include the latest spam and virus definitions for the most current protection against viruses and other security threats.

IPv6 Network Support

Note that version 5.1 and later of the Barracuda Spam & Virus Firewall supports sending and receiving email over both IPv4 and IPv6 networks. While email sent over IPv6 networks will be scanned for viruses and spam, IP-based analysis and policies are not applied to IPv6 in this version.
12 Layers of Virus and Spam Protection

Inbound Message Filtering

Using the Web interface, you can configure up to twelve defense layers that protect your users from spam and viruses. Every “good” inbound email message passes through these 12 layers, which include five connection management layers and seven mail scanning layers:

- Denial of service
- Rate control
- IP Reputation Analysis
- Sender Authentication
- Recipient Verification
- Virus Scanning
- Custom policies
- Spam Fingerprint Analysis
- Intent Analysis
- Image Analysis
- Bayesian Analysis
- Rule-based spam scoring

The following figure shows each of these defense layers in action and indicates that six of the twelve layers of defense are updated constantly by Barracuda Networks Energize Updates:

Figure 1.1: Twelve Layers of Defense

During the connection management process, inbound emails are filtered through five defense layers to verify authenticity of envelope information and any inappropriate incoming mail connections are dropped even before receiving the message. Any emails that survive the connection verification process must then undergo a thorough mail scanning process that involves seven defense layers of message analysis. The algorithms and techniques used by the Barracuda Spam & Virus Firewall are continuously updated via the Barracuda Energize Updates service to stay ahead of spam and virus trends as they emerge.

Outbound Message Filtering and Encryption

Any message sent through the Barracuda Spam & Virus Firewall addressed to a domain that is configured on the system is treated as an inbound message. All others are treated as outbound messages. All Barracuda Spam & Virus Firewall models include essential outbound mail filtering techniques that help organizations to ensure that all outgoing email is legitimate and virus-free. Outbound messages can optionally be encrypted based on the filtering policy you configure.
If you already have an email encryption service or server in place, you can use the **redirect** action in your filtering policy for outbound mail that you want to redirect to that encryption server.

Quarantine of outbound messages can be managed at the per-domain level as well as at the global level, and every outbound email message passes through the following layers:

- Rate Control
- Virus Scanning
- Custom Policies
- Spam Fingerprint Analysis
- Intent Analysis
- Image Analysis
- Rule-based Spam Scoring

See *Outbound Filtering Policy*, p. 61, for configuring outbound mail filtering.

### Internal Virus Scanning

The easy-to-install Barracuda Exchange Anti-Virus Add-in provides virus scanning for internal mail that may not pass through the Barracuda Spam & Virus Firewall. For details on installation and configuration, see *Internal Virus Scanning For Your Microsoft Exchange Mail Server* on page 40.

---

**Energize Updates Maximize Protection**

**Barracuda Central**

To provide your organization with maximum protection against the latest types of spam and virus attacks, engineers at Barracuda Central monitor the Internet for trends in spam and virus attacks, collecting data from worldwide collection points. These updates are then automatically updated around the clock to your Barracuda Spam & Virus Firewall via the Energize Updates feature.

*Figure 1.2: Constant Updates to Barracuda Central*
By identifying spam and virus trends at an early stage, the team at Barracuda Central can quickly develop new and improved blocking techniques that are automatically made available to your Barracuda Spam & Virus Firewall.

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

- Barracuda Reputation (see *Barracuda Reputation (BRBL)*, p. 53)
- Spam definitions
- Security definitions
- Virus definitions
- Access to the latest firmware
- Ability to use outbound email encryption

*Figure 1.3: Energize Updates from Barracuda Central Delivers New Spam and Virus Definitions*

**How Energize Updates Defeat Spam**

The Barracuda Spam & Virus Firewall scrutinizes all the characteristics of a message and uses a complex system of scores to determine whether or not a message is spam. When an email reaches the spam scoring filter, the Barracuda Spam & Virus Firewall assigns scores to all the properties of the message.

For example, the Barracuda Spam & Virus 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 & Virus Firewall to determine the spam score for a message that you’ll see displayed on the Message Log page of the Web interface.

By default, Energize Updates are set to automatically keep the spam rules and scores up-to-date so that the Barracuda Spam & Virus Firewall can quickly counteract evolving techniques used by spammers.
## Barracuda Spam & Virus Firewall Models

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

**Table 1.1:**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Model 100</th>
<th>Model 200</th>
<th>Model 300</th>
<th>Model 400</th>
<th>Model 600</th>
<th>Model 800</th>
<th>Model 900</th>
<th>Model 1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active email users</td>
<td>1–50</td>
<td>1–500</td>
<td>300–1,000</td>
<td>1,000–5,000</td>
<td>3,000–10,000</td>
<td>8,000–22,000</td>
<td>15,000–30,000</td>
<td>25,000–100,000</td>
</tr>
<tr>
<td>Domains</td>
<td>10</td>
<td>50</td>
<td>250</td>
<td>500</td>
<td>5,000</td>
<td>5,000</td>
<td>5,000</td>
<td>5,000</td>
</tr>
<tr>
<td>Quarantine Storage</td>
<td>10 GB</td>
<td>50 GB</td>
<td>100 GB</td>
<td>200 GB</td>
<td>250 GB</td>
<td>750 GB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compatible with all mail servers</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Hardened and secure OS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Spam blocking</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Virus scanning</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Outbound Email Filtering</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>STARTTLS encryption support</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Per-user settings and quarantine</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MS Exchange/ LDAP Accelerator</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Syslog support</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SNMP/API</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Per Domain Settings</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Clustering</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Redundant Disk Array (RAID)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Hot Swap</td>
</tr>
</tbody>
</table>
### Contacting Technical Support

To contact Barracuda Networks Technical Support:

- By phone: call 1-408-342-5400, or if you are in the United States, (888) Anti-Spam, or (888) 268-4772
- By email: use support@barracuda.com
- Online: visit [http://www.barracuda.com/support](http://www.barracuda.com/support) and click on the **Support Case Creation** link.

There is also a Barracuda Networks Support Forum available where users can post and answer other users’ questions. Register and log in at [http://forum.barracuda.com](http://forum.barracuda.com).

### Table 1.1:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Model 100</th>
<th>Model 200</th>
<th>Model 300</th>
<th>Model 400</th>
<th>Model 600</th>
<th>Model 800</th>
<th>Model 900</th>
<th>Model 1000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per-user score settings</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customizable Branding</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hot Swap</td>
<td>Hot Swap</td>
<td>Hot Swap</td>
<td>Hot Swap</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redundant Power Supply</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

*Introduction 15*
Chapter 2

Barracuda Spam & Virus Firewall Concepts

This chapter introduces the general topics that will help you understand what your Barracuda Spam & Virus Firewall can do and how to approach configuring the features that are important to your particular deployment and organization policies. The Getting Started chapter walks through initial setup and configuration of the system to get you up and running.

- Twelve Layers of Defense .......................................................... 18
- Connection Management Layers ........................................... 19
- Mail Scanning Layers ............................................................. 21
- Predictive Sender Profiling ..................................................... 24
Twelve Layers of Defense

Understanding each of the 12 layers of defense prepares you to make decisions about which - if not all- of the connection and mail scanning features to enable and tune for the best combination of performance and accuracy of the Barracuda Spam & Virus Firewall. More detailed information about features that support each layer, pros and cons, as well as Barracuda Networks’ recommendations are addressed in chapter 5, Advanced Spam Filtering Policy and chapter 6, Advanced Configuration.

The Barracuda Spam & Virus Firewall takes a configured action when it identifies a message as spam or otherwise in violation of configured Block and Accept policies. Inbound messages may be Blocked, Quarantined, Tagged or Allowed, while outbound messages may be Blocked, Quarantined or Sent. Note that using the Quarantine or Tag actions with some layers may use more system resources than Block or Allow actions.

Maximizing Efficiency and Performance of Spam Scanning

Using Rate Control, Barracuda Reputation (realtime RBLs) and Recipient Verification, as described below, can maximize filtering performance of the Barracuda Spam & Virus Firewall for inbound mail. These layers have the greatest impact on filtering speed and performance relative to all the other layers such that any inappropriate incoming mail connections are dropped even before receiving the message.
Connection Management Layers

These layers provide the most value in your Barracuda Spam & Virus Firewall deployment for inbound mail as they identify and block unwanted email messages before accepting the message body for further processing. The Connection Management layers generally require less processing time than the seven content scanning layers that follow. For the average small or medium business, more than half of the total email volume can be blocked using Connection Management techniques. Extremely large Internet Service Providers (ISPs) or even small Web hosts, while under attack, may observe block rates at the Connection Management layers exceeding 99 percent of total email volume.

Denial of Service Protection

Built on a hardened and secure Linux operating system, the Barracuda Spam & Virus Firewall receives inbound email on behalf of the organization, insulating your organization’s mail server from receiving direct Internet connections and associated threats. This layer does not apply to outbound mail.

Rate Control

Automated spam software can be used to send large amounts of email to a single mail server. To protect the email infrastructure from these flood-based attacks, the Barracuda Spam & Virus Firewall counts the number of incoming connections from a particular IP address (inbound mail) or sender email address (outbound mail) during a 30 minute interval and throttles the connections once a particular threshold is exceeded. See Rate Control, page 52, for more on configuring this feature.

IP Analysis

After applying rate controls based on IP address, the Barracuda Spam & Virus Firewall performs analysis on the IP address of inbound mail based on the following:

• **Barracuda Reputation** - this feature leverages data on network addresses and domain names collected from spam traps and throughout other systems on the Internet. The sending histories associated with the IP addresses of all sending mail servers are analyzed to determine the likelihood of legitimate messages arriving from those addresses. IP addresses of incoming connections are compared to the Barracuda Reputation Blocklist and the Barracuda Reputation Whitelist, if enabled, and suspicious incoming messages are either blocked, tagged or quarantined.

• **External blocklists** - Also known as real-time blocklists (RBLs) or DNS blocklists (DNSBLs). Several organizations maintain external blocklists of known spammers.

• **Allowed and blocked IP address lists**: Customer-defined policy for allowed and blocked IP addresses. By listing trusted mail servers by IP address, administrators can avoid spam scanning of good email, both reducing processing requirements and eliminating the chances of false positives. Likewise, administrators can define a list of bad email senders for blocking. In some cases, administrators may choose to utilize the IP blocklists to restrict specific mail servers as a matter of policy rather than as a matter of spam protection.
**Sender Authentication**

Declaring an invalid “from” address is a common practice by spammers. The Barracuda Spam & Virus Firewall Sender Authentication layer uses a number of techniques on inbound mail to both validate the sender of an email message and apply policy, including domain name spoof protection, performing a DNS lookup of domain names and enforcing RFC 821 compliance.

**Sender Policy Framework** (SPF) tracks sender authentication by having domains publish reverse MX records to display which machines are designated as mail sending machines for that domain. The recipient can check those records to make sure mail is coming from a designated sending machine.

**DomainKeys (DKIM)** dictates that a sending domain cryptographically signs outgoing messages, allowing the sending domain to assert responsibility for a message. When receiving a message from a domain, the recipient can check the signature of the message to verify that the message is, indeed, from the sending domain and that the message has not been tampered with.

See the *Advanced Configuration*, page 73 chapter for details on configuring this layer.

**Recipient Verification**

The Barracuda Spam & Virus Firewall verifies the validity of recipient email addresses for inbound messages (not outbound) through multiple techniques to prevent invalid bounce messages. See the *Advanced Configuration*, page 73 chapter to learn about LDAP integration, SMTP recipient verification and using a local database for recipient verification.
Mail Scanning Layers

Virus Scanning

The most basic level of Mail Scanning is virus scanning. The Barracuda Spam & Virus Firewall utilizes three layers of virus scanning and automatically decompresses archives for comprehensive protection. By utilizing virus definitions, Barracuda Spam & Virus Firewall customers receive the best and most comprehensive virus and malware protection available. The three layers of virus scanning of inbound and outbound mail include:

- Powerful open source virus definitions from the open source community help monitor and block the latest virus threats.
- Proprietary virus definitions, gathered and maintained by Barracuda Central, our advanced 24/7 security operations center that works to continuously monitor and block the latest Internet threats.
- Barracuda Real-Time Protection (BRTS), a set of advanced technologies that enables each Barracuda Spam & Virus Firewall to immediately block the latest virus, spyware, and other malware attacks as they emerge. This feature provides fingerprint analysis, virus protection and intent analysis. When BRTS is enabled, any new virus or spam outbreak can be stopped in real-time for industry-leading response times to email-borne threats. BRTS allows customers the ability to report virus and spam propagation activity at an early stage to Barracuda Central.

Virus Scanning takes precedence over all other Mail Scanning techniques and is applied even when mail passes through the Connection Management layers. As such, even email coming from “whitelisted” IP addresses, sender domains, sender email addresses or recipients are still scanned for viruses and blocked if a virus is detected.

The Barracuda Exchange Anti-Virus Add-in for the Microsoft Exchange Server can empower your mail server to do virus scanning of internal mail and of previously stored mail using constantly updated virus signatures detected by Barracuda Central. See Internal Virus Scanning For Your Microsoft Exchange Mail Server on page 40 for details about getting and installing the add-in from the Barracuda Spam & Virus Firewall Web interface.

User-specified rules (custom policy)

Administrators can choose to define their own policies, perhaps for compliance or governance reasons, which take precedence over spam blocking rules delivered to the system automatically through Barracuda Energize Updates. Administrators can set custom content filters for inbound and/or outbound mail based on the subject, message headers, message bodies and attachment file type.

Fingerprint Analysis

A message “fingerprint” is based on commonly used message components (e.g., an image) across many instances of spam. Fingerprint analysis is often a useful mechanism for blocking future instances of spam once an early outbreak is identified. Engineers at Barracuda Central work around the clock to identify new spam fingerprints which are then updated on all Barracuda Spam & Virus Firewalls through hourly Barracuda Energize Updates. Both inbound and outbound email messages are subject to Fingerprint Analysis.
### Intent Analysis

All spam messages have an “intent” — to get a user to reply to an email, to visit a Web site or to call a phone number. Intent analysis involves researching email addresses, Web links and phone numbers embedded in email messages to determine whether they are associated with legitimate entities. Frequently, Intent Analysis is the defense layer that catches phishing attacks. The Barracuda Spam & Virus Firewall applies various forms of Intent Analysis to both inbound and outbound mail, including real-time and multi-level intent analysis.

### Image Analysis

While Fingerprint Analysis captures a significant percentage of images after they have been seen, the Barracuda Spam & Virus Firewall also uses Image Analysis techniques on both inbound and outbound mail which protect against new image variants. These techniques include:

- **Optical character recognition (OCR)** - Enables the Barracuda Spam & Virus Firewall to analyze the text rendered inside embedded images.
- **Image processing** - To mitigate attempts by spammers to foil OCR through speckling, shading or color manipulation, the Barracuda Spam & Virus Firewall also utilizes a number of lightweight image processing technologies to normalize the images prior to the OCR phase. More heavyweight image processing algorithms are utilized at Barracuda Central to quickly generate fingerprints that can be used by the Barracuda Spam & Virus Firewall to block messages.
- **Animated GIF analysis** - The Barracuda Spam & Virus Firewall contains specialized algorithms for analyzing animated GIFs for suspect content.

### Bayesian Analysis

Bayesian Analysis applies only to inbound mail and is a linguistic algorithm that profiles language used in both spam messages and legitimate email for any particular user or organization. To determine the likelihood that a new email message is spam, Bayesian Analysis compares the words and phrases used in the new email against the corpus of previously identified email. The Barracuda Spam & Virus Firewall only uses Bayesian Analysis after administrators or users profile a corpus of at least 200 legitimate (not spam) messages and 200 spam messages. Bayesian Analysis does not apply to outbound mail.

### Spam Scoring

Once an inbound or outbound message has passed the initial Barracuda Spam & Virus Firewall block/accept filters, it receives a score for its spam probability. This score ranges from 0 (definitely not spam) to 9 or greater (definitely spam). Based on this score, the Barracuda Spam & Virus Firewall can take one of the following actions:

- Block
- Quarantine
- Tag (inbound mail only)
- Allow (inbound mail only)
- Send (outbound mail only)
**Domain Level Spam Scoring:** The Barracuda Spam & Virus Firewall 400 and higher allows for setting spam score levels for inbound mail at the domain level. The administrator or the Domain admin role can set the spam scoring levels on the **BASIC > Spam Checking** page.

**Per-User Spam Scoring:** The Barracuda Spam & Virus Firewall 600 and higher allows the administrator to enable users to set their own spam score levels for inbound mail if per-user quarantine is enabled. If per-user spam scoring is enabled, when the user logs into their account, they will see the **PREFERENCES > Spam Settings** page from which they can set tag, quarantine and block scoring levels for that account.
Predictive Sender Profiling

When spammers try to hide their identities, the Barracuda Spam & Virus Firewall can use Predictive Sender Profiling to identify behaviors of all senders and apply the applicable Barracuda Spam & Virus Firewall defense tactic to reject connections and/or messages from spammers. This involves looking beyond the reputation of the apparent sender of a message, just like a bank needs to look beyond the reputation of a valid credit card holder of a card that is lost or stolen and used for fraud.

Some examples of spammer behavior that attempts to hide behind a valid domain, and the Barracuda Spam & Virus Firewall features that address them, include the following:

- **Sending too many emails from a single network address**
  Automated spam software can be used to send large amounts of email from a single mail server. The Rate Control feature on the Barracuda Spam & Virus Firewall can be set to limit the number of connections made from any IP address within a 30 minute time period. Violations are logged to identify spammers. Rate Control is configured from the BLOCK/ACCEPT > Rate Control page.

  The Messages Per SMTP Session setting limits 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 are displayed in the message log as being "Deferred" with "Per-Connection Message Limit Exceeded" as the reason for the postponement. The sender is required to make a new connection to continue sending messages, which may ultimately trigger a Rate Control deferral. For this and other SMTP security settings, see the ADVANCED > Email Protocol page.

- **Attempting to send to too many invalid recipients**
  Many spammers attack email infrastructures by harvesting email addresses. Recipient Verification on the Barracuda Spam & Virus Firewall enables the system to automatically reject SMTP connection attempts from email senders that attempt to send to too many invalid recipients, a behavior indicative of directory harvest or dictionary attacks.

  Using LDAP lookup or a local database to verify valid recipients as well as Sender Spoof Protection, which blocks email with "From" addresses which use an allowed recipient domain on the Barracuda Spam & Virus Firewall, protects against receiving mail targeted to invalid recipients.

- **Registering new domains for spam campaigns**
  Because registering new domain names is fast and inexpensive, many spammers switch domain names used in a campaign and send blast emails on the first day of domain registration. Real-time Intent Analysis on the Barracuda Spam & Virus Firewall is typically used for new domain names and involves performing DNS lookups and comparing DNS configuration of new domains against the DNS configurations of known spammer domains.

- **Using free Internet services to redirect to known spam domains**
  Use of free Web sites to redirect to known spammer Web sites is a growing practice used by spammers to hide or obfuscate their identity from mail scanning techniques such as Intent Analysis. With Multilevel Intent Analysis, the Barracuda Spam & Virus Firewall inspects the results of Web queries to URIs of well-known free Web sites for redirections to known spammer sites.
Chapter 3
Getting Started

This chapter will guide you in installing the Barracuda Spam & Virus Firewall and beginning to scan and monitor email traffic.

Initial Setup ................................................................. 26
Initial Configuration of the System................................. 31
Route Incoming Email to the Barracuda Spam & Virus Firewall.... 34
Administrative Settings and the Web Interface........................ 36
Tune and Monitor the Default Spam and Virus Settings ............ 38
Viewing Performance and Email Statistics.......................... 41
Setting up Quarantine....................................................... 42
Initial Setup

For hardware appliance deployment, skip the following section. Configuration is the same for virtual and hardware appliances.

Virtual Machine Deployment

Barracuda Networks offers a virtual appliance version of the Barracuda Spam & Virus Firewall to provide organizations a way to save money, simplify deployments and reduce their environmental footprint. The Barracuda Spam & Virus Firewall Vx virtual appliance easily integrates with existing virtual environments such as VMware. As the organization grows, virtual appliances can be easily scaled for performance and capacity and also lend themselves to quicker backup and disaster recovery.

Important: When deploying the Barracuda Spam & Virus Firewall Vx, you will need to configure your network firewall to allow ICMP traffic to outside servers as well as opening port 443 to updates.barracudacentral.com. Also make sure your DNS servers can resolve updates.barracudacentral.com.

Once you have installed your Barracuda Spam & Virus Firewall Vx and configured your firewall, you can test the configuration using the ADVANCED > Troubleshooting page in the Web interface to ping updates.barracudacentral.com.

Best Practices for Configuring Your Hypervisor

Barracuda Networks recommends the following for best configuration of your VM client running the Barracuda Spam & Virus Firewall Vx:

• Allocate 1 GB of RAM for the virtual appliance per CPU allocated.
• You will need only a single virtual NIC on your virtual appliance. Most likely you will want to use the 'bridged' networking setup on VMWare.

Checklist for Unpacking

Before installing your Barracuda Spam & Virus Firewall, match the items on this list with the items in the box.

If any item is missing or damaged, please contact your Barracuda Networks Sales representative.

• Barracuda Spam & Virus Firewall (check that you have received the correct model)
• AC power cord
• Mounting rails (Barracuda Spam & Virus Firewall 600, 800, and 900 only)

Also required for installation:

• VGA monitor
• PS2 keyboard
• Ethernet cables
Installation Examples

Barracuda Spam & Virus Firewall Behind Corporate Firewall

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

*Figure 3.1:* The Barracuda Spam & Virus Firewall behind the corporate firewall

In this type of setup, perform the following tasks:

- Forward (port redirection) incoming SMTP traffic on port 25 to the Barracuda Spam & Virus Firewall at 10.10.10.3.
- Configure the Barracuda Spam & Virus 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 & Virus Firewall in the DMZ

The figure below shows the Barracuda Spam & Virus Firewall in front of your corporate firewall in the DMZ. In this example, the Mail Server has an IP address of 64.5.5.6 and the Barracuda Spam & Virus Firewall has an internal IP address of 64.5.5.5.
In this type of setup, perform the following tasks:

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

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

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

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

```
IN MX 10 barracuda.yourdomain.com
```

### Clustering the Barracuda Spam & Virus Firewall

Clustering two or more Barracuda Spam & Virus Firewalls makes sense if your organization requires high availability, scalability, data redundancy and/or fault tolerance. Clustering also provides centralized management of policy because once you configure one of the devices, configuration settings are synchronized across the cluster almost immediately. Clustered systems can be geographically dispersed and do not need to be located on the same network.

For more information about setting up a cluster of Barracuda Spam & Virus Firewalls, see *Clustering the Barracuda Spam & Virus Firewall*, page 77.
**Install the Barracuda Spam & Virus Firewall**

**To physically install the Barracuda Spam & Virus Firewall:**

1. Fasten the Barracuda Spam & Virus 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 & Virus Firewall.

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

**Note**

The Barracuda Spam & Virus Firewall 600 and higher supports 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 & Virus Firewall:
   - Power cord
   - VGA monitor
   - PS2 keyboard

   After you connect the AC power cord the Barracuda Spam & Virus 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 *Front Panel Indicator Lights*, page 115.

**APC UPS Support**

An APC (American Power Conversion) UPS (Uninterruptible Power Supply) device with a USB interface is supported with the Barracuda Spam & Virus Firewall. No configuration changes are needed on the Barracuda Spam & Virus Firewall to use one. When the APC UPS device is on battery power, the Web interface will display an alert, and the Barracuda Spam & Virus Firewall will shut down safely when there is an estimated time of 3 minutes of battery power remaining.
Configure IP Address and Network Settings

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

- Connect directly to the Barracuda Spam & Virus Firewall with a keyboard and monitor and specify a new IP address through the console interface.
- Applies only to the Barracuda Spam & Virus Firewall 200, 300, 400, and 600: Push and hold the Reset button on the front panel. Holding the Reset button for 5 seconds changes the IP address to 192.168.200.200. Holding the Reset button for 8 seconds changes the IP address to 192.168.1.200. Holding the Reset button for 12 seconds changes the IP address to 10.1.1.200.

**To connect directly to the Barracuda Spam & Virus 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 will display 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 & Virus Firewall, and select OK when finished.

4. Select No when prompted if you want to change the IP configuration. Upon exiting the screen, the new IP address and network settings will be applied to the Barracuda Spam & Virus Firewall.

Configure your Corporate Firewall

If your Barracuda Spam & Virus Firewall is located behind a corporate firewall, you need to open specific ports to allow communication between the Barracuda Spam & Virus 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:**

<table>
<thead>
<tr>
<th>Port</th>
<th>Direction</th>
<th>Protocol</th>
<th>Used for...</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Out</td>
<td>TCP</td>
<td>Remote diagnostics and technical support services (recommended)</td>
</tr>
<tr>
<td>25</td>
<td>In/Out</td>
<td>TCP</td>
<td>SMTP</td>
</tr>
<tr>
<td>53</td>
<td>Out</td>
<td>TCP/UDP</td>
<td>Domain Name Server (DNS)</td>
</tr>
<tr>
<td>80</td>
<td>Out</td>
<td>TCP</td>
<td>Virus, firmware, security and spam rule definitions</td>
</tr>
<tr>
<td>123</td>
<td>Out</td>
<td>UDP</td>
<td>NTP (Network Time Protocol)</td>
</tr>
</tbody>
</table>

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

**Initial Configuration of the System**

After specifying the IP address of the system and opening the necessary ports on your firewall, you need to configure the Barracuda Spam & Virus Firewall from the Web interface. Make sure the computer from which you configure the Barracuda Spam & Virus Firewall is connected to the same network, and the appropriate routing is in place to allow connection to the Barracuda Spam & Virus Firewall’s IP address from a Web browser.

To configure the Barracuda Spam & Virus Firewall:

1. From a Web browser, enter the IP address of the Barracuda Spam & Virus Firewall followed by port 8000.
   

2. Log in to the Web interface by entering **admin** for the username and **admin** for the password.

3. On the **BASIC > IP Configuration** page, enter the required information in the fields as described in the following table:

   **Table 3.2:**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP/IP Configuration</td>
<td>The IP address, subnet mask, and default gateway of your Barracuda Spam &amp; Virus Firewall. The TCP port is the port on which the Barracuda Spam &amp; Virus Firewall receives incoming email. This is usually port 25.</td>
</tr>
</tbody>
</table>
Click **Save Changes**.

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

**Activate Your Subscriptions**

After installation, your Energize Updates subscription must be activated for the Barracuda Spam & Virus Firewall to be fully enabled, and continue to receive the latest updates to all virus, policy, and spam definitions from Barracuda Central. The Energize Updates service is responsible for downloading these updates to your Barracuda Spam & Virus Firewall.

5. At the top of every page, you may see the following warning:

```
Error: Activation has not been completed. Please activate your Barracuda Spam & Virus Firewall to enable functionality. [Click here for activation]
```
6. Click on the designated link to open up the **Product Activation** page in a new browser window.

7. On the **Product Activation** page, fill in the required fields and click **Activate**. A confirmation page opens to display the terms of your subscription.

8. Return to the Barracuda Spam & Virus Firewall Web interface and navigate to the **BASIC > Status** page. In the **Subscription Status** section, verify that the word **Current** appears next to **Energize Updates, Instant Replacement Service** (if purchased) and **Premium Support** (if purchased).

9. There may be a slight delay of a few minutes for the display to reflect your updated subscription status. If the status is still showing as unactivated, click **Refresh** in the **Subscription Status** section.

**Note**

If your subscription status does not change to **Activated** within an hour, or if you have trouble filling out the **Product Activation** page, contact your Barracuda Networks sales representative.

---

### Update the Barracuda Spam & Virus Firewall Firmware

Prior to upgrading the firmware on your Barracuda Spam & Virus Firewall, it is always recommended that you read the release notes.

**To upgrade the firmware on the Barracuda Spam & Virus Firewall:**

1. Go to the **ADVANCED > Firmware Update** page. Verify that the installed version matches the Latest General Release. The **Download Now** button next to the Latest General Release is disabled if the Barracuda Spam & Virus Firewall is already up-to-date with the latest firmware.

**Note**

ALWAYS read the release notes prior to downloading a new firmware version. Release notes provide you with information on the latest features and fixes provided in the updated firmware version. You can access the release notes from the **Advanced > Firmware Update**.

2. **If the installed version does not match the Latest General Release**: read the release notes to learn about the latest features and fixes provided in the new firmware version, and click **Download Now** to begin the download. Updating the firmware may take several minutes. Do not turn off the unit during this process.

   You can view the download status by clicking the **Refresh** button next to the firmware download progress. A “Firmware downloaded” message displays once the download is complete, and the **Refresh** button will turn into **Apply Now**.

**Note**

The “apply” process takes several minutes to complete. It is important to not power-cycle the unit during the download. Inbound and outbound traffic for mail resumes automatically when the update process is complete.

3. Click **Apply Now** to activate the newly-downloaded firmware. This process will automatically reboot your system when completed, which can cause your Web interface to disconnect momentarily. **This is normal and expected behavior**, so there is no need to perform a manual
reboot. A Status page displays the progress of the reboot. Once the reboot is complete, the login page will reappear.

Update Definitions

To apply the newest definitions provided by Energize Updates:

1. Select ADVANCED > Energize Updates.
2. Select On for Automatically Update. The recommended setting is On for all available definitions. If you are using the Barracuda Exchange Anti-Virus Add-in, you must set Automatically Update to On for Virus Update Definitions. See Internal Virus Scanning For Your Microsoft Exchange Mail Server, page 40, for more information about this add-in.
3. Check to see if the current version is the same as the latest general release. If the rules are up-to-date, proceed to the next section. If the rules are not up-to-date, continue to the next step.
4. Click Update to download and install the latest available definitions onto the Barracuda Spam & Virus Firewall.

Routing Email

Route Incoming Email to the Barracuda Spam & Virus Firewall

The next step in setting up your Barracuda Spam & Virus Firewall is to route incoming email 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 & Virus Firewall:

- **Port forwarding** to redirect incoming SMTP traffic (port 25) to the Barracuda Spam & Virus Firewall if it is installed behind a corporate firewall running NAT (Network Address Translation). Configure this option on the ADVANCED > Advanced Networking page. For more information about port forwarding, refer to your firewall documentation or network administrator.

- **MX records** are used when your Barracuda Spam & Virus Firewall is located in a DMZ with a routable public IP address. If your Barracuda Spam & Virus 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 & Virus Firewall.
     The following example shows a DNS entry for a Barracuda Spam & Virus Firewall with a name of barracuda and an IP address of 66.233.233.88:
     \[\text{barracuda.yourdomain.com IN A 66.233.233.88}\]
  2. Change your DNS MX Records.
     The following example shows the associated MX record with a priority number of 10:
     \[\text{IN MX 10 barracuda.yourdomain.com}\]

You can configure specific SMTP settings from the ADVANCED > Email Protocol page. After you route incoming email to the Barracuda Spam & Virus Firewall, it will begin filtering all email it receives and routing good email to your mail server.
Testing Spam and Virus Scanning With a Local User Set

From the ADVANCED > Explicit Users page, you have the option to use the Explicit Users to Scan For feature to test a subset of locally defined users before fully deploying the Barracuda Spam & Virus Firewall.

Configure Scanning of Outgoing Mail

The Barracuda Spam & Virus Firewall may be configured to scan outgoing mail simultaneously with scanning inbound mail. Virus Scanning and Rate Control are applied to outbound mail as well as the following filters, if specifically enabled, which are configurable from the BASIC > Spam Checking and BLOCK/ACCEPT pages:

- Spam Scoring, with Block or Quarantine actions
- IP Address Filtering
- Sender Domain Filtering
- Sender Email Address Filtering
- Recipient Filtering
- Content Filtering (Subject, Header and Body)
- Attachment Filtering
- Fingerprint Analysis
- Image Analysis
- Intent Analysis

The following scanning tools are not applied to outbound mail:

- IP Reputation, a sender authentication mechanism
- SPF (Sender Policy Framework), a sender authentication mechanism
- DKIM (DomainKeys), an email authentication system designed to verify the DNS domain of an email sender
- Regional Settings, the application of special spam analysis rules for particular languages
- Per-user Whitelist/Blocklist
- Per-domain Whitelist/Blocklist

To scan outgoing mail with the Barracuda Spam & Virus Firewall, you must configure outbound operation on the BASIC > Outbound page. There you'll specify your trusted outbound mail server IP address or domain name (either your mail server or another trusted relay), identify a Smart host if you have one, and, optionally, an authentication type. The Barracuda Spam & Virus Firewall supports SMTP/SASL authentication and LDAP.

Note

When configuring outbound mail, ensure that your network firewall blocks all port 25 traffic that doesn't originate from your Barracuda Spam & Virus Firewall.

If you are relaying though a Smart host, you must also configure the Smart host to send to the Internet.

Be aware that configuring the Barracuda Spam & Virus Firewall to scan outbound as well as inbound mail will increase the load on the system. You may find that you need to upgrade your Barracuda Spam & Virus Firewall to another model.
Outbound Message Footer - Global or Domain-level

The Barracuda Spam & Virus Firewall can append a custom text and/or html footer to each outbound message, configurable at either the global level on the **ADVANCED > Outbound Footers** page, or at the per-domain level. You can also opt to exclude certain email senders from having the outbound footer appended to their outgoing messages.

To enable or disable an outbound message footer for a specific domain, effectively overriding the global setting, navigate to the **DOMAINS** page, click **Manage** for the domain and navigate to the **ADVANCED > Outbound Footers** page.

Administrative Settings and the Web Interface

Global Versus Domain Level Administration

The Barracuda Spam & Virus Firewall 400 and higher provides for global-level settings for most features as well as for domain-level, or “per-domain” settings, some of which can optionally override global settings. Some settings, such as user authentication mechanisms, are domain-level specific. The Web interface enables “drilling down” from the global scope, as shown in **Figure 3.4**, to the domain scope. The domain scope provides for reporting and configuring quarantine, spam scoring, content and attachment filtering options and user authentication settings on a per-domain basis.

**Figure 3.4:** Drilling down to domain scope from global scope

Domain Level Configuration

Per-domain settings are useful in cases where different domains protected by the Barracuda Spam & Virus Firewall belong to various organizations, each with their own set of email security requirements or users with different levels of knowledge or permissions.

For example, a medical organization may want to whitelist domains that send pharmaceutical related messages, while another organization would consider such email to be spam. Some organizations will want to configure per-user quarantine, giving their users control of their own whitelist/blocklist settings and spam scoring, while others may not want their users to have to manage a separate mailbox for quarantined messages. Per-domain settings are administered in the “domain scope” level of the Web interface, accessible from the **DOMAINS** tab as shown above in **Figure 3.4**.
For details about configuring domain-level settings, see *Domain Level Settings*, page 92.

User accounts under each domain can be configured with custom whitelist/blocklist, spam scoring levels and quarantine inbox settings. User accounts can be managed either from the global level *USERS > Account view* page or at the domain level from the *DOMAINS > Manage Domain > USERS > Account view* page. Links in the upper right section of the page always indicate the name of the logged in account and, if working at the domain level, the name of the domain currently being managed. See *Role-based Administration*, page 96 for more information and illustrations of scope and Web interface navigation.

**Controlling Access to the Web Interface**

The *BASIC > Administration* page allows you to perform the following tasks for initial setup:

- **Required**: Provide email addresses in the *Email Notifications* section of the page so the Barracuda Spam & Virus Firewall and Barracuda Networks can send out important alerts and informative notifications if needed.
- Change the password of the administration account.
- Change the HTTP port used to access the Web interface. For security, HTTPS access is recommended - see *Securing Network Access*, page 46
- Change the length of time users can be logged into the Web interface after a period of no activity (Session Expiration Length - default is 20 minutes).
- Specify the IP addresses and netmask of the systems that can access the Web interface. All other systems will be denied access. This is configurable in the *Administrator IP/Range* section.

**Customizing the Appearance of the Web interface**

The *ADVANCED > Appearance* page allows you to customize the default images used on the Web interface. This tab is only displayed on the Barracuda Spam & Virus Firewall 600 and higher.

**Changing the Language of the Web Interface**

You can change the language of the Web interface by selecting a language from the drop-down menu in the upper right corner of the page near the *Log Off* link. Supported languages include Chinese, Japanese, Spanish, French, and others. The language you select is only applied to your individual Web interface. No other user’s Web interface is affected.

**Setting the Time Zone of the System**

You can set the time zone of your Barracuda Spam & Virus Firewall from the *BASIC > Administration* page. The current time on the system is automatically updated via Network Time Protocol (NTP). When the Barracuda Spam & Virus Firewall resides behind a firewall, NTP requires port 123 to be opened for outbound UDP traffic. You can specify one or more NTP servers to use on the *ADVANCED > Advanced Networking* page. Each server will be tried in order until one successfully connects. The default server is *ntp.barracudacentral.com*.

It is important that the time zone is set correctly because this information is used in all logs and reports. **Note:** The Barracuda Spam & Virus Firewall automatically reboots when you change the timezone.
Enabling SSL for Administrators and Users

SSL (Secure Socket Layer) ensures that your passwords are encrypted and that all data transmitted to and received from the Web interface is encrypted as well. All Barracuda Spam & Virus Firewalls support SSL access without any additional configuration. However, some sites may wish to enforce using a secured connection to access the Web interface, or prefer to use their own trusted certificates. For more information about and best practices for securing your Barracuda Spam & Virus Firewall on your network, see Securing the Barracuda Spam & Virus Firewall, page 45.

To enforce SSL-only access (recommended):

1. On the ADVANCED > Secure Administration page, select Yes to enable HTTPS/SSL access only to the Web interface. Setting this to No will still allow the Barracuda Spam & Virus Firewall to accept non-SSL connections.
2. Select Yes to Use HTTPS links in emails for per-user quarantine messages sent from the Barracuda Spam & Virus Firewall.
3. Enter your desired Web Interface HTTPS/SSL port for the Web interface. The default is 443.
4. Click Save Changes.

If you wish to change the certificate that is used, you must first create and upload it to the Barracuda Spam & Virus Firewall before changing the Certificate Type in the SSL Certificate Configuration section of the ADVANCED > Secure Administration page. See the online help for instructions. The Barracuda Spam & Virus Firewall supports the following types of certificates:

- **Default (Barracuda Networks)** certificates are signed by Barracuda Networks. On some browsers, these may generate some benign warnings which can be safely ignored. No additional configuration is required to use these certificates, and are provided free of charge 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). These certificates are created by providing the information requested in the Private (self-signed) section of the page. You may also want to download the Private Root Certificate and import it into your browser, to allow it to verify the authenticity of the certificate and prevent any warnings that may come up when accessing the Web interface.

- **Trusted (signed by a trusted CA)** certificates are issued by trusted Certificate Authorities (CA), and must be purchased from them separately with a Certificate Signing Request (CSR). This can be downloaded after providing the information requested in the Trusted (Signed by a trusted CA) section of the page. Once you have received the certificate and key from the CA, you must upload both items to the Barracuda Spam & Virus Firewall from this section of the page. The certificate will be in effect as soon as the upload is complete.

Tune and Monitor the Default Spam and Virus Settings

After you install the Barracuda Spam & Virus Firewall, the system begins filtering incoming email based on the default settings. The system automatically checks incoming email for viruses and uses the Barracuda Reputation service to identify spam.
Spam Scoring - Block, Quarantine and Tag

As a message passes through the last of all of the defense layers, it is scored for spam probability. This score ranges from 0 (definitely not spam) to 10 or higher (definitely spam). Based on this score, the Barracuda Spam & Virus Firewall either tags (inbound messages only), quarantines, blocks or allows (or sends, for outbound) the message.

Initial spam scoring limits for your Barracuda Spam & Virus Firewall are shown on the BASIC > Spam Checking page and are described in Table 3.3. Once you have more experience with the Barracuda Spam & Virus Firewall you can adjust how aggressively the system deals with spam. For example, you may decide to tag (inbound) or quarantine spam instead of blocking it.

The following table describes the spam scoring settings on the BASIC > Spam Checking page. A score setting of 10 for any action disables that action.

**Table 3.3:**

<table>
<thead>
<tr>
<th>Setting (inbound only)</th>
<th>Description</th>
</tr>
</thead>
</table>
| Tag score (inbound only) | Messages with a score above this threshold, but below the quarantine threshold, are delivered to the sender with the word [BULK] (default) added to the subject line.  
You can change the default text added to the subject line by entering new text in the Spam Tag Configuration section of the page.  
Any message with a score below the tag threshold is automatically allowed. The default value is 3.5. |
| Quarantine score | Messages with a score above this threshold, but below the block threshold, are forwarded to the quarantine mailbox you specify. For information on specifying the quarantine mailbox, refer to Chapter 9, Managing Inbound Quarantine, p. 83.  
The default setting is 10 (quarantine disabled). To enable quarantine, this setting must have a value lower than the block threshold. |
| Block score | Messages with a score above this threshold are not delivered to the recipient. By default, the Barracuda Spam & Virus Firewall does NOT send an NDR (non-delivery receipt) bounce message to the sender, but this feature can be enabled, either for inbound or outbound messages, in the Spam Bounce (NDR) Configuration section of the ADVANCED > Bounce/NDR Settings page. The default inbound message block score value is 6. |

Monitor and Classify Incoming Emails

Once email is flowing through the Barracuda Spam & Virus Firewall, the administrator can view the BASIC > Message Log page to get an idea of how many messages are being blocked, quarantined, tagged or allowed, with reasons for each of those actions. Reviewing this log will give an idea of how...
current settings are filtering messages, and the page enables adding or removing message senders to or from the whitelist.

If you enable Bayesian filtering on the BASIC > Spam Checking page, you will then see Spam and Not Spam buttons on the BASIC > Message Log page in the tool bar. Use these actions to train the Bayesian database. Bayesian training works only on messages with 11 words or more. With Bayesian filtering enabled, if a message is not classified as spam by the Barracuda Spam & Virus Firewall, but it appears to be spam, you can elect to submit that message to Barracuda Central from the BASIC > Message Log page. For best Bayesian accuracy, it is recommended that you reset your Bayesian database every 6 months. Note that Bayesian filtering is turned off by default.

See Chapter 5, Advanced Inbound Spam Filtering Policy, p. 51 for more details on using the Message Log with Bayesian filtering, and creating custom whitelists and blocklists to allow or block messages from specific IP addresses, domains or email accounts.

Monitor and Classify Outgoing Emails

If you have configured the Barracuda Spam & Virus Firewall to filter outbound mail, watch the log on the BASIC > Outbound Quarantine page. Based on Outbound Spam Scoring Limits you specify on the BASIC > Spam Checking page, as well as any Block/Accept filters you configure, outbound messages will be quarantined or blocked as needed and listed on the BASIC > Outbound Quarantine page. Look for false positives and adjust spam scoring accordingly. Any message listed in the outbound quarantine can be delivered, whitelisted, deleted, or rejected by an administrator.

Virus Checking and Notifications

Virus scanning is automatically enabled on the Barracuda Spam & Virus Firewall and the system checks for definition updates on a regular basis (hourly by default). Virus Scanning takes precedence over all other mail scanning techniques and is applied even when mail passes through the Connection Management layers. As such, even email coming from “whitelisted” IP addresses, sender domains, sender email addresses or recipients are scanned for viruses and blocked if a virus is detected.

Use the BASIC > Virus Checking page to enable or disable virus checking. If you enable Barracuda Real-Time Protection, the Barracuda Spam & Virus Firewall will check unrecognized spam and virus fingerprints against the latest virus threats logged at Barracuda Central that have not yet been downloaded by the Barracuda Spam & Virus Firewall Energize Updates. See the online help on the BASIC > Virus Checking page for more details about this setting.

Internal Virus Scanning For Your Microsoft Exchange Mail Server

The Barracuda Spam & Virus Firewall offers an add-in you can download from the Web interface and install on your Microsoft Exchange Server to provide internal virus scanning within your network. The Barracuda Exchange Anti-Virus Agent runs as a Windows service on your 2003, 2007 or 2010 MS Exchange server, enabling your MS Exchange Server to receive constant virus signature updates from the Barracuda Spam & Virus Firewall.

Any time a new virus signature is released, the Barracuda Exchange Anti-Virus Agent will scan all internal mail traffic for that virus as well as mail previously stored on the MS Exchange Server, depending on how you configure settings for the add-in. See the ADVANCED > Exchange Anti-Virus page for instructions on downloading and configuring the add-in for your organization’s needs.

The Barracuda Exchange Anti-Virus Agent only provides data to the customer that is made available by the MS Exchange Server. MS Exchange does not provide a quarantine tool for viewing infected
messages, information on false positives or other infected message details. All threat statistics provided to the add-in by MS Exchange are listed in the Exchange Anti-Virus Add-in Statistics section on the ADVANCED > Exchange Anti-Virus page in the web interface. For infected filename information, see the MS Windows Event Log. To view performance of virus scanning on your MS Exchange server, use the MS Windows Performance Monitor or other 3rd party tool.

If you are using the Barracuda Exchange Anti-Virus Agent, you must set Automatically Update to On for Virus Update Definitions on the Advanced > Energize Updates page.

Attachment Block Notifications

You can enable or disable notification emails to senders of messages that are blocked due to file attachment content filters. Configure these notifications for inbound and outbound mail from the ADVANCED > Bounce/NDR Settings page. From this page you can also enter custom message text to insert in the notifications. Attachment content filters are configured in the Attachment Content Filters section of the BLOCK/ACCEPT > Content Filters page.

Spam and Quarantine Notifications

Separate non-delivery notifications (NDR) can be configured to alert the sender when a message is blocked or quarantined due to spam scoring or policy (content filtering). See Non-Delivery Reports (NDRs), page 81, for more information.

Viewing Performance and Email Statistics

The BASIC > Status page provides an overview of the health and performance of your Barracuda Spam & Virus Firewall, including:

- Hourly and daily email statistics that display the number of inbound and outbound messages blocked, tagged (inbound messages only), quarantined, sent (outbound messages only), redirected (outbound messages only), encrypted (outbound only), rate controlled and allowed (inbound only) for the last 24 hours and 28 days.
- The subscription status of Energize Updates.
- Performance statistics, including CPU temperature and system load. Performance statistics displayed in red signify that the value exceeds the normal threshold. These values will fluctuate based on the amount of traffic that is being handled, but if any setting remains consistently in the red for a long period of time, please contact Contacting Technical Support, page 15.

Product Tips

At the top of the BASIC > Status page you’ll see the Product Tips bubble. This space is populated with usage tips, new programs and features from Barracuda Networks specific to your product, and with a link to the release notes for the latest firmware update. These tips are updated frequently from Barracuda Central. You have the following options in managing this feature:
• To hide a particular message permanently, click the Hide link.
• To hide the Product Tips section of the page, set Show Product Tips in the Product Tips section of the BASIC > Administration page to No.

Email Statistics - Inbound

This section of the BASIC > Status page summarizes how inbound mail traffic is handled by the Barracuda Spam & Virus Firewall based on how you have configured the system. Actions reported include Blocked, Blocked:Virus, Rate Controlled, Quarantined, Allowed:Tagged and Allowed. Statistics are tallied by hour, by current calendar day starting at midnight, and total since installation (or since the last reset).

If you have not configured any domains for receiving inbound mail on the DOMAINS page, and you configure the Barracuda Spam & Virus Firewall only for processing outbound mail, it is possible to see some messages logged as inbound mail traffic. For example, if a message is received addressed to the default domain configured under BASIC > IP Configuration page, then the email will be counted as an inbound message.

Email Statistics - Outbound

Outbound mail traffic is summarized in this table on the BASIC > Status page much the same way as inbound traffic, except that a count of outbound message Blocked due to custom policy or spam are reported separately, outbound messages are not tagged, and messages counted as Sent are the counterpart of inbound Allowed messages.

If you have not configured the Barracuda Spam & Virus Firewall for outbound mail and only expect inbound mail, it is still possible to see some messages logged as outbound traffic. If a spammer tries to relay a message through the Barracuda Spam & Virus Firewall by spoofing a valid domain as the sender to an invalid recipient, the Barracuda Spam & Virus Firewall will block the message and it will appear in the outbound mail statistics table as Blocked.

As an example, consider that mydomain.com is configured as a valid domain on the DOMAINS page and badomain.com is not. A spammer sends a message from sender@mydomain.com to the IP address of the Barracuda Spam & Virus Firewall, addressed to recipient@badomain.com. The message will show as Blocked with a reason of ‘invalid domain’ in the Message Log and will be included in the outbound mail Blocked statistics.

Setting up Quarantine

By default, the Barracuda Spam & Virus Firewall does not quarantine incoming or outgoing messages, but you may want to enable quarantine for inbound mail, at least, because it offloads storage of potential spam from the mail server and backups. It also keeps potential spam messages out of the user’s inbox. While some organizations require quarantine behavior, tagging inbound messages that might be spam is recommended over quarantining them for several reasons:

• With tagging of inbound messages, the user doesn’t need an additional inbox for storing quarantined messages because the potential spam message is delivered to their regular inbox with a special word or phrase prepended to the Subject line to indicate that it has been tagged as potential spam. These messages can be filtered to a special mailbox if the user desires, or can be viewed or deleted from their regular inbox.
- Tagging inbound messages on the Barracuda Spam & Virus Firewall saves system resources because the message is not stored on the appliance itself; it’s sent on to the user’s mailbox or to an administrator’s mailbox to manage.

Note that, by enabling quarantine of incoming messages identified as possible spam, either the user or the administrator is required to maintain the quarantine inbox and settings.

Quarantine of inbound mail can be enabled or disabled in the **Spam Scoring Limits** section on the **BASIC > Spam Checking** page as well as on various **BLOCK/ACCEPT** pages. If enabled, you can select either Global quarantine or Per-User quarantine. For more information, refer to *Chapter 9, Managing Inbound Quarantine*, p. 83.

Quarantine of **outbound** mail can be enabled or disabled in the **Outbound Spam Scoring Limits** section on the **BASIC > Spam Checking** page, as well as on various **BLOCK/ACCEPT** pages, and outbound quarantined mail can be logged and managed at the **per-domain** level as well as at the global level. For more information on using outbound quarantine, see *Encryption of Outbound Mail*, page 62.
Chapter 4

Securing the Barracuda Spam & Virus Firewall

This chapter covers best practices to secure your Barracuda Spam & Virus Firewall with respect to deployment on your network, user access and inbound and outbound email. The following topics are covered:

Securing Network Access................................................................. 46
Limiting User Access ........................................................................ 47
Advanced Email Security Policy...................................................... 48
Securing Network Access

To secure your Barracuda Spam & Virus Firewall on your network, begin by locking down the user interface ports. Barracuda Networks recommends using the non-standard port 8000 for internal access to the Web interface, which is configured on the BASIC > Administration page. From that page you can also further limit access to the Web interface by IP address with the Administrator/IP Range setting. If no IP address is specified in this field, then all systems are granted access with the correct administrator password.

You can secure external access to the Barracuda Spam & Virus Firewall with the Web Interface HTTPS/SSL Port setting on the ADVANCED > Secure Administration page. The recommended port is 443 because it is a standard HTTPS/SSL port that is used for secure Web browser communication, and the identity of the remotely connected server can be verified with significant confidence.

Note

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

SSL Certificates

As described above, limiting user interface access to HTTPS provides further security and can also be configured on the ADVANCED > Secure Administration page along with the use of SSL certificates. There are three types of SSL certificates to choose from: Default (Barracuda Networks), Private (self-signed) or Trusted certificate - a certificate signed by a trusted certificate authority (CA). Configuring SSL certificates is described in this guide in the Enabling SSL for Administrators and Users, page 38 section of the Getting Started chapter as well as in the online help of the ADVANCED > Secure Administration page

Secure Links in Notification Emails

If Per-User quarantine (as opposed to Global) is configured on the BASIC > Quarantine page, you might want to secure hyperlinks in quarantine correspondence emails that are sent from the Barracuda Spam & Virus Firewall to users and administrators. Setting Use HTTPS Links in Emails to Yes on the ADVANCED > Secure Administration page ensures that these emails sent from the Barracuda Spam & Virus Firewall contain only HTTPS links.

Use the Cloud Protection Layer

Using the Cloud Protection Layer feature means that all email going into your organization will be pre-filtered for spam and viruses before it reaches your network. This feature requires using the Barracuda Control Center and validating your domain ownership with the cloud service. To use this feature, please see Chapter 7, Cloud-Based Protection, p. 69 for details on configuration.
Limiting Access to the API

The Barracuda set of APIs provides for remote administration and configuration of the Barracuda Spam & Virus Firewall. More detailed information regarding the API can be found in the Barracuda Spam & Virus Firewall API Guide 4.x located at http://www.barracuda.com/documentation. Common settings, such as IP addresses and spam scoring levels, that you can set by clicking the Save Changes button in the Web interface, can be configured via the API.

To limit access to the API, use the Allowed SNMP and API IP/Range setting on the BASIC > Administration page. The IP addresses you enter in that field can also establish an SNMP connection to the system. To secure use of the API, you must also create an API password which can be entered on this page.

Tracking Changes to the Configuration and User Login Activities

The syslog function of the Barracuda Spam & Virus Firewall provides two kinds of logs, capturing:

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

From the ADVANCED > Troubleshooting page, use the Monitor Web Syslog button view the Web syslog output. You can also configure a syslog server as described in the Using a Syslog Server to Centrally Monitor System Logs, page 114.

Limiting User Access

Securing User Access With Single Sign On

With Single Sign-On (SSO), users can log into their quarantine inbox via the Web interface using their domain passwords instead of a password managed separately by the Barracuda Spam & Virus Firewall. Single Sign-On is not a global setting, and can only be configured by the administrator or a Domain Admin. See Managing Accounts and Domains, page 91 for more detail about role-based administration of the Barracuda Spam & Virus Firewall.

Note that, if you are using LDAP authentication for single sign-on, you can either use the same LDAP server and settings for user authentication as the one you’re using for recipient verification (configured on the USERS > LDAP Configuration page), or you can configure a separate LDAP server for single sign-on from the USERS > Single Sign-On page.

If you select LDAP authentication, you must set Exchange Accelerator/LDAP Verification to Yes on the USERS > LDAP Configuration page.

Warning: If enabling Single Sign On for a domain, you should also configure HTTPS/SSL Access Only at the global level on the ADVANCED > Secure Administration page to protect the transmission of network passwords. See Enabling SSL for Administrators and Users, page 38 to configure SSL on the Barracuda Spam & Virus Firewall.
User Account Authentication

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

To configure authentication, navigate to the USERS > Single Sign On page for the selected domain and select the Authentication Type. For RADIUS and POP, fill in the server settings on the page.

To require users to log in to the Barracuda Spam & Virus Firewall Web interface (as opposed to single sign on) to view and manage their account, select Local for Authentication Type.

LDAP and User Account Authentication

Configure LDAP settings on the USERS > LDAP Configuration page. LDAP server types supported include Active Directory, Open LDAP, Novell eDirectory and Domino Directory. You can configure LDAPS (SSL/TLS) for encryption of LDAP queries between the Barracuda Spam & Virus Firewall and your LDAP server. LDAPS can optionally be required. As stated above, these settings are domain-specific.

Limiting User Access to a Clustered System

You can choose to dedicate a single Barracuda Spam & Virus Firewall in the cluster as the Quarantine Host to serve up the end-user interface through which users will access their quarantine inboxes, even though their actual quarantine inbox (primary or secondary) may be hosted by another Barracuda Spam & Virus Firewall in the cluster. By then not directing email to the Quarantine Host, you can:

- Enhance network security by limiting end-user access (port 8000 by default) and administration to only one Barracuda Spam & Virus Firewall on the Internet
- Insulate the user interface performance from any peaks in email volume

In this configuration, quarantine notifications from all Barracuda Spam & Virus Firewalls in the cluster will direct users to the Quarantine Host. Set the IP address of the Quarantine Host device in the cluster from the BASIC > Quarantine page.

Advanced Email Security Policy

The Barracuda Spam & Virus Firewall offers various levels of secure communications over SMTP for both incoming email and outbound email that is relayed through the Barracuda Spam & Virus Firewall from your network. For health care providers, governmental agencies and other entities who need to protect private, sensitive and valuable information communicated via email, the Barracuda Spam & Virus Firewall provides the option of email encryption (or redirection to your existing encryption service or server) based on policy you set for outbound mail in the BLOCK/ACCEPT pages. See Encryption of Outbound Mail, page 62 for details and usage.

SMTP/TLS (Transport Layer Security) encryption

TLS can provide authentication (identification of the communication partner), privacy/confidentiality (communication is not intercepted or eavesdropped), and integrity (message has not been modified)
over an SMTP connection. TLS uses different algorithms for encryption, signing and message authentication. The Barracuda Spam & Virus Firewall can communicate via SMTP over TLS/SSL over the Internet when both the sender and recipient are using a Barracuda Spam & Virus Firewall or another STARTTLS-capable mail server.

To enable TLS encryption, you need to first configure an SSL certificate from the **ADVANCED > Secure Administration** page following the steps in the online help screen. There are three certificate options, and choosing the Default/Barracuda Networks certificate serves the purpose in most cases. Next, from the **ADVANCED > Email Protocol** page, in the **SMTP over TLS/SSL** section, set **Enable SMTP over TLS/SSL** to **Yes**. Note that SMTP over TLS will be enabled for incoming connections and will be attempted for outgoing connections - the receiving server needs to support it. This configures SMTP over TLS/SSL at the global level.

**Requiring** encrypted TLS connections can be configured at the **domain level** (not as a global setting) for either incoming or outgoing messages (as long as the receiving server supports TLS), from the **DOMAINS** tab. Click **Manage Domain** for the particular domain, and on the **ADVANCED > Email Protocol** page, enter the domain names for which email will be required to be transmitted over a TLS connection. Only the administrator or **Domain Admin** can configure these settings.

### Securing the Outbound Relay of Email

The Barracuda Spam & Virus Firewall may be configured to relay outbound email simultaneously with scanning inbound mail as described in *Configure Scanning of Outgoing Mail*, page 35.

On the **BASIC > Outbound** page, you can configure the IP address and/or domain name of one or more outbound servers that can relay outbound email through the Barracuda Spam & Virus Firewall to the Internet. The most secure practice is to **specify an IP address rather than a domain name** for your trusted mail or relay server(s) to prevent domain name spoofing. Use the **Trusted Relay IP/Range** to do so.

If you do decide to specify a domain name with the **Trusted Relay Host/Domain** field, it is recommended to configure either SASL/SMTP authentication or LDAP Outbound relay authentication using your LDAP directory as well. See the **BASIC > Outbound** page for sender authentication for outbound relayed email.

### Invalid Bounce Suppression

Invalid Bounce Suppression can be used when all outgoing email is relayed through the Barracuda Spam & Virus Firewall and is designed to reduce the number of bounce messages to forged return addresses. Enabling this feature will block any bounce message that did not originate as an outbound message from this Barracuda Spam & Virus Firewall, or others on the same network with the same shared secret.

All email sent out through the Barracuda Spam & Virus Firewall contains a return address tagged with an encrypted password (the **Bounce Suppression Shared Secret**) and expiration time. Any bounce message coming into the Barracuda Spam & Virus Firewall from the Internet that does not include these components is blocked and recorded in the Message Log with the reason "Invalid Bounce". For more details see the online help on the **BLOCK/ACCEPT > Sender Authentication** page.

Note that if you have a cluster of Barracuda Spam & Virus Firewalls, the **Bounce Suppression Shared Secret** will be synchronized across all nodes in the cluster.
Chapter 5

Advanced Inbound Spam Filtering Policy

The goal in configuring a Barracuda Spam & Virus Firewall is to identify spam without blocking valid messages. This chapter addresses using custom spam filtering policy on inbound mail as well as optional, more sophisticated spam identification methods.

Rate Control ....................................................................................... 52
IP Analysis ......................................................................................... 53
Content Analysis - Inbound .............................................................. 55
Rate Control

The Barracuda Spam & Virus Firewall Rate Control feature protects the system from spammers or spam-programs (also known as "spam-bots") that send large amounts of email to the server in a small amount of time. Rate Control is configured on the BLOCK/ACCEPT > Rate Control page.

As part of the Connection Management Layer, the Rate Control mechanism counts the number of connections to the Barracuda Spam & Virus Firewall in a half hour period and compares that number to the Rate Control threshold, which is the maximum number of connections allowed from any one IP address in this half-hour time frame. If the number of connections from a single IP address exceeds the Rate Control threshold within the half hour period, the Barracuda Spam & Virus Firewall will defer any further connection attempts from that particular IP address until the next half hour time frame and log each attempt as deferred in the Message Log with a Reason of ‘Rate Control’.

In this case, for each message deferred, the sender will receive a 4xx level error message instructing the mail server to retry after a predefined time interval. Well-behaving mail servers act upon the defer message and will try sending the message again later, while email from large volume spammers will not retry sending the email again.

When Rate Control Takes Effect

When Rate Control is first enabled on the Barracuda Spam & Virus Firewall, or after a change is made to the Rate Control threshold, five (5) unique IP addresses must connect before Rate Control is invoked. This is to take into account that you may have another appliance receiving email (i.e., a front-end Mail Transfer Agent (MTA) or a trusted forwarder) before the Barracuda Spam & Virus Firewall. Once 5 or more IP addresses have made connections to the Barracuda Spam & Virus Firewall, it indicates that mail is also coming in from other outside sources and rate control should be applied.

Exemptions from Rate Control

You can exempt trusted IP addresses from Rate Control by adding a trusted IP address to the Rate Control Exemption/IP Range list. Also, any IP address that you enter as a trusted forwarder on the BASIC > IP Configuration page will be exempted from Rate Control.

When configuring Rate Control, keep in mind the following

- A rate of 50 is conservative
- Some customers can lower this safely
- Caution – False positives can be hard to diagnose
- Common setting is for 20-30 emails/ half hour
- High volume recipients may need to either set the Rate Control threshold above 50 and/or list IP addresses from which they expect to receive a high volume of email in the Rate Control Exemption/IP Range list.

Note: Organizations that relay email through known servers or communicate frequently with known partners can and should add the IP addresses of those trusted relays and good mail servers to the Rate Control Exemption/IP Range list.
IP Analysis

After applying rate controls, the Barracuda Spam & Virus Firewall then performs analysis on the IP address, applying tag, quarantine or block policies that you configure in the BLOCK/ACCEPT pages.

Once the true sender of an email message is identified, the reputation and intent of that sender should be determined before accepting the message as valid, or “not spam”. The best way to address both issues is to know the IP addresses of trusted senders and forwarders of email and define those on the Barracuda Spam & Virus Firewall as “Allowed” by adding them to a whitelist of known good senders. Various methods for discerning “good” senders of email versus spammers are described in this section to help you to quickly configure your Barracuda Spam & Virus Firewall per the needs of your organization.

Warning  
Barracuda Networks does NOT recommend whitelisting domains because spammers will spoof domain names. When possible, it is recommended to whitelist (Allow) by IP address only.

Trusted Forwarders

On the BASIC > IP Configuration page you can specify the IP addresses of any machines that are set up specifically to forward mail to the Barracuda Spam & Virus Firewall from outside sources. These are called Trusted Forwarders and will bypass SPF, Rate Control and IP Reputation checks. In the IP Analysis layer, the Barracuda Spam & Virus Firewall examines the Received headers and evaluates the first non-trusted IP address when applying the above filters and other block and accept policies.

IP Reputation

The Barracuda Spam & Virus Firewall enables administrators to define a list of trusted mail servers by IP address. By adding IP addresses to this list, administrators can avoid spam scanning of good email, thereby both reducing processing load and eliminating the chances of false positives. Note that virus scanning and blocked attachment checks are still enforced.

Likewise you can define a list of bad email senders. In some cases, you may choose to utilize the IP blocklists (as described in IP Analysis on page 19) to restrict specific mail servers as a matter of policy rather than as a matter of spam.

Barracuda Reputation (BRBL)

Barracuda Reputation is a database maintained by Barracuda Central and includes a list of IP addresses of known, good senders as well as known spammers, or IP addresses with a “poor” reputation. This data is collected from spam traps and other systems throughout the Internet. The sending histories associated with the IP addresses of all sending mail servers are analyzed to determine the likelihood of legitimate messages arriving from those addresses. Updates to Barracuda Reputation are made continuously by the engineers at Barracuda Central and are delivered to all Barracuda Spam & Virus Firewalls via Energize Updates.
On the **BLOCK/ACCEPT > IP Reputation** page, it is strongly recommended that the **Barracuda Reputation Blocklist (BRBL)** option be set to “Block”. Turning the **Barracuda Reputation Whitelist** option to **On** will enable messages from known good IP addresses to bypass all spam filtering, saving resources, while still being scanned for viruses.

**Exempting IP Addresses from the BRBL and Other Blocklists**

The BRBL and other blocklists that you specify on the **BLOCK/ACCEPT > IP Reputation** page can be overridden by listing the IP addresses of trusted forwarders of email or listing email addresses:

- In the **Allowed IP/Range** section of the **BLOCK/ACCEPT > IP Filters** page
- In the **Barracuda Reputation, External RBL IP Exemption Range** on the **BLOCK/ACCEPT > IP Reputation** page. Here, you can exempt particular IP addresses from RBL checks, including from the Barracuda Reputation Blocklist. Messages from these IP addresses will be subject to all other spam and virus checks. You can also enter IP addresses/ranges to this list which are on the Barracuda Reputation Whitelist, but for which you want mail scanned for spam anyway.
- In the **Allowed Email Addresses and Domains** section of the **BLOCK/ACCEPT > Sender Filters** page.

**Subscribing to External blocklist Services**

The **BLOCK/ACCEPT > IP Reputation** page allows you to use various blocklist services. Several organizations maintain external blocklists, such as spamhaus.org. External blocklists, sometimes called DNSBLs or RBLs, are lists of IP addresses from which potential spam originates. In conjunction with Barracuda Reputation, the Barracuda Spam & Virus Firewall uses these lists to verify the authenticity of the messages you receive.

Be aware that blocklists can generate false-positives (legitimate messages that are blocked). However, because the Barracuda Spam & Virus Firewall sends notifications when it rejects such messages, the sender will be notified and legitimate senders will therefore know to try re-sending their message or otherwise notify the recipient that their messages are being blocked.

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

**Sender Whitelisting - Precedence**

The users’ sender whitelists (if the whitelist/blocklist setting is enabled for user accounts) can be overridden by global settings. For example, if the administrator turns on Spoof Protection, which is a global setting, it will supersede any user’s whitelist entry. If a user needs to supersede an global IP address block, that user should communicate to the administrator and request that the email or IP address be added to a global whitelist on the Barracuda Spam & Virus Firewall.

**Reverse DNS Blocking**

The Barracuda Spam & Virus Firewall can do a reverse DNS lookup on inbound and outbound IP connections and finds the hostname associated with the IP address of the sender. By configuring rules on the **BLOCK/ACCEPT > Reverse DNS** page, you can choose to apply **Common Reverse DNS**
Rules by country, Custom Reverse DNS Rules that you define, or both to tag (inbound only), quarantine or block messages from those domains.

The last part of a hostname is known as the top level domain, or TLD. Most TLDs include a country identifier, such as .ca for Canada, .ru for Russia, etc. If most or all of the mail that you receive from a particular country is spam, you can use the Common Reverse DNS Rules to tag (inbound only), block or quarantine any message that has an associated hostname that includes that country’s TLD. Email which is not blocked is subject to all of the usual spam and virus checks. Use the Custom Reverse DNS Rules to tag, quarantine or block messages from hostnames ending with values that you specify. List the sending domains or subdomains you want to whitelist on the BLOCK/ACCEPT > Sender Filters page.

Content Analysis - Inbound

Custom Content Filters

The Barracuda Spam & Virus Firewall enables administrators to set custom content filters based on the subject line, message headers, message body and attachment file content. In general, administrators do not need to set their own filters for the purposes of blocking spam, as these forms of rules are delivered to the Barracuda Spam & Virus Firewall automatically through Barracuda Energize Updates. The online help for the BLOCK/ACCEPT > Content Filtering page includes a link to a Regular Expressions help page that covers expressions you can use for advanced filtering. HTML comments and tags imbedded between characters in the HTML source of a message are also filtered.

You can specify actions to take with messages based on pre-made patterns in the subject line or message body. Credit card, Social Security numbers, privacy information such as driver’s license numbers, phone numbers or expiration dates and HIPAA data can be automatically checked and acted upon by blocking, tagging or quarantining inbound messages. Outbound mail can be blocked, quarantined, encrypted or redirected.

Attachment Filtering

All messages, except those from whitelisted senders, go through attachment filtering. From the BLOCK/ACCEPT > Attachment Filters page you can choose to take certain actions with inbound and/or outbound messages if they contain attachments with certain filename patterns, file types, MIME types, or password protected archives. Actions you can take with inbound messages include block or quarantine. Actions you can take with outbound messages include block, quarantine, encrypt or redirect. You can elect to have a notification sent to the sender when an inbound or outbound message is blocked due to attachment content filtering. See the ADVANCED > Bounce/NDR Settings page to configure notifications.

The BLOCK/ACCEPT > Attachment Filters page provides a table of patterns you can use for specifying the above actions based on attachment filenames, or you can create your own filters.

The Check Archives feature can be selected along with any filter to search the contents of attached archives (zip, tar, etc.) and take one of the above actions with inbound or outbound messages based on filenames or types.

Use the Password Protected Archive Filtering feature to take action with messages with attachments that contain password protected (encrypted) archives.
Messages that are blocked due to attachment filtering will appear in the **Message Log** with the word *Attachment* and the filename in the **Reason** column. For example, if you created a filter on the **BLOCK/ACCEPT > Attachment Filters** page to block messages with attachments whose filenames match a pattern of *word*®, the entry in the **Message Log** for such a blocked message would contain something like this in the **Reason** column:

```
Attachment (word_2010_xml.tgz)
```

where *word_2010_xml.tgz* is the attachment filename that caused the message to be blocked.

**Note**  
The default maximum attachment size allowed by your Barracuda Spam & Virus Firewall is **100 megabytes**. If a message exceeds this size, the Barracuda Spam & Virus 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.

**Blocking Email by Country**

Set tag, quarantine and block policies for specific character sets or regional spam settings using the **BLOCK/ACCEPT > Regional Settings** page. Here you can also choose to specifically allow messages based on valid Chinese or Japanese language content and enable compliance with PRC (People’s Republic of China) requirements if your Barracuda Spam & Virus Firewall resides in the PRC.

**Fingerprint Analysis**

A message “fingerprint” is based on commonly used message components (e.g., an image) across many instances of spam. Fingerprint analysis is often a useful mechanism to block future instances of spam once an early outbreak is identified. Spam fingerprints blocked based on a real-time check will display an ‘*’ before "Fingerprint" in the Message Log. In order to detect real-time spam fingerprints, Barracuda Real-Time Protection must be enabled on the **BASIC > Virus Checking** page.

Engineers at Barracuda Central work around the clock to identify new spam fingerprints which are then updated on all Barracuda Spam & Virus Firewalls through hourly Barracuda Energize Updates. **Fingerprint Analysis** is configured on the **BASIC > Spam Checking** page.

**Intent Analysis**

All spam messages have an “intent” – to get a user to reply to an email, visit a Web site or call a phone number. Intent analysis involves researching email addresses, Web links and phone numbers embedded in email messages to determine whether they are associated with legitimate entities. Frequently, Intent Analysis is the defense layer that catches phishing attacks. The Barracuda Spam & Virus Firewall features multiple forms of Intent Analysis:

- **Intent analysis** - Markers of intent, such as URLs, are extracted and compared against a database maintained by Barracuda Central, and then delivered to the Barracuda Spam & Virus Firewall via hourly Barracuda Energize Updates. Intent can also be associated with general content categories, several of which are provided for Intent filtering.

- **Real-time intent analysis** - For new domain names that may come into use, Real-Time Intent Analysis involves performing DNS lookups against known URL blocklists.
• **Multilevel intent analysis** - Use of free Web sites to redirect to known spammer Web sites is a growing practice used by spammers to hide or obfuscate their identity from mail scanning techniques such as Intent Analysis. Multilevel Intent Analysis involves inspecting the results of Web queries to URLs of well-known free Web sites for redirections to known spammer sites.

**Intent Analysis** is configured on the **BASIC > Spam Checking** page.

---

### Image Analysis

Image spam represents about one third of all traffic on the Internet. While Fingerprint Analysis captures a significant percentage of images after they have been seen, the Barracuda Spam & Virus Firewall also uses Image Analysis techniques which protect against new image variants. These techniques include:

- **Optical character recognition (OCR)** - Embedding text in images is a popular spamming practice to avoid text processing in anti-spam engines. OCR enables the Barracuda Spam & Virus Firewall to analyze the text rendered inside the images.

- **Image processing** - To mitigate attempts by spammers to foil OCR through speckling, shading or color manipulation, the Barracuda Spam & Virus Firewall also utilizes a number of lightweight image processing technologies to normalize the images prior to the OCR phase. More heavyweight image processing algorithms are utilized at Barracuda Central to quickly generate fingerprints that can be used by Barracuda Spam & Virus Firewalls to block messages.

- **Animated GIF analysis** - The Barracuda Spam & Virus Firewall contains specialized algorithms for analyzing animated GIFs for suspect content.

**Image Analysis** is configured on the **BASIC > Spam Checking** page.

---

### Bayesian Analysis

#### How Bayesian Analysis Works

Bayesian Analysis is a linguistic algorithm that profiles language used in both spam messages and legitimate email for any particular user or organization. To determine the likelihood that a new email is spam, Bayesian Analysis compares the words and phrases used in the new email against the corpus of previously identified email. Note that Bayesian training works only on messages with 11 words or more. The Barracuda Spam & Virus Firewall only uses Bayesian Analysis **after** administrators or users classify at least 200 legitimate messages and 200 spam messages.

#### Global Bayesian Filtering Versus Per-User

The administrator can configure a global Bayesian database, per-user Bayesian databases or disable Bayesian altogether. With the global setting, which is configured on the **BASIC > Spam Checking** page, the administrator trains and maintains one Bayesian database for all users. With the per-user configuration, users must train and manage their own Bayesian databases, which they access from their **PREFERENCES > Spam Checking** page. There are pros and cons to each configuration.

A global Bayesian database is typically more effective than per-user databases because the administrator can maintain and reset it for all to use, thereby providing a more reliable source of Bayesian management. If, however, the Barracuda Spam & Virus Firewall is filtering mail for many
domains, the users of which expect to receive different types of email, it could be either difficult or impossible to train the global Bayesian database to identify spam for all users. For example, if one domain for a medical organization typically receives email regarding medical topics, while another domain for a political organization tends to receive political emails and yet another domain is an entertainment site, then what is spam to one domain may be valid email for another on the same Barracuda Spam & Virus Firewall. In this case, per-user Bayesian filtering would make more sense than global.

In most cases, however, it is not practical to enable Bayesian at the user level because maintaining an accurate Bayesian database requires that users understand the concept of how Bayesian analysis works and how to use it as an effective tool. That said, while sophisticated users may be trained and savvy enough to initially train their own Bayesian database, they may not have the time to spend in their regular work schedule to effectively maintain their Bayesian databases.

Note Because spammers frequently change tactics and content, Bayesian data can quickly become “stale” if the database is not reset from time to time and new messages consistently classified as spam or not spam in equal numbers. Without this maintenance the users may see false positives resulting in the blocking of good email.

Getting the Best Accuracy From the Bayesian Database

All Bayesian systems rely on the fact that messages classified are not much different than new messages arriving. Over time however, spam messages change drastically and the Bayesian system – while initially able to compensate for the new format – gradually declines in its effectiveness. When this happens new classifications are needed to update the Bayesian database. To keep a Bayesian database accurate:

- For a global Bayesian database, the administrator should periodically (every 6 months or so) clear it out by resetting it from the BASIC > Spam Checking page, then, from the BASIC > Message Log page, marking at least 200 messages as either Spam or Not spam using the buttons on the page. Bayesian filtering will NOT take effect until 200 or more of each spam and not-spam messages are marked as such.
- For each per-user database, the user should reset their own Bayesian database and follow up with marking 200 or more messages as spam or not spam, either in their quarantine inbox (QUARANTINE > Quarantine Inbox page) or from their regular email client if they have installed either the MS Outlook add-in or Lotus add-in (see below).

When to Use Bayesian Analysis

Barracuda Networks does not recommend using Bayesian filtering in most circumstances. With Energize Updates constantly updating the Barracuda Spam Firewall with protection against the latest spam and virus threats, spam accuracy should not be an issue for most organizations.

A case for using Bayesian Analysis would depend on the following:

- You are using global Bayesian as opposed to per-user, and the users in the organization tend to be a homogenous population with regard to the kind of content considered to be ‘valid’ email versus spam. This situation would make it easier for an administrator to “train” the global Bayesian database as to what is spam and what is not spam for the organization.
- Your organization requires a very high granularity of accuracy for identifying spam.
- If enabling Bayesian at the per-user level, users are sophisticated and can be trained to properly identify ‘valid’ messages versus spam so as to train the Bayesian database, and
are willing to consistently mark BOTH ‘valid’ messages and spam messages in equal numbers so as to maintain the Bayesian database.

- The administrator and/or users are disciplined about resetting the Bayesian database(s) on a regular basis and re-initializing with 200 each of marked spam and not spam messages to ‘keep current’ with new spam techniques over time.

**Outlook and Lotus Notes Plugins**

If both per-user quarantine and per-user Bayesian are enabled, on the Barracuda Spam & Virus Firewall 300 and higher, the administrator can choose to allow users to download a plugin that allows messages to be classified as Spam or Not Spam directly from their email client. Users must have a quarantine account on the Barracuda Spam & Virus Firewall to use the plugins. For information about automatically or manually creating quarantine accounts for users, see *Creating and Managing Accounts* on page 91.

The Outlook Add-In also provides the user with a button to encrypt the message contents before sending it. Any messages encrypted using the Outlook Add-In will appear in the Barracuda Spam & Virus Firewall with a Reason of **Outlook Add-In**. See *Encryption of Outbound Mail* on page 62 for more information about email encryption.

The Outlook Add-in is compatible with Microsoft Outlook XP, Outlook 2003, Outlook 2007, and Outlook 2010 32-bit and 64-bit.

See the [USERS > User Features](#) page, where you can:

- Enable users to download the Microsoft Outlook Add-In, which they can do from the login page if this feature is enabled
- Download the **Outlook Add-In Deployment Kit**. This Windows zip file includes the installer (MSI) and Administrative Template (ADM) for the add-in, and can be used with a Windows GPO to push the add-in to your users’ PCs.
- Download and install the Lotus Notes Plugin and view an overview document of how it works.

**Note**

If the SMTP option **Remove Barracuda Headers** is turned off in the [ADVANCED > Email Protocol](#) page, any custom X-headers that the Barracuda Spam & Virus Firewall has applied before the message leaves the appliance will be removed. This is not a recommended setting, and if these headers are removed, any Barracuda Outlook add-in or other add-in will not work correctly.

**Bayesian Poisoning**

Some spammers will insert content in messages intended to bypass spam rules, such as excerpts of text from books or other content that may look “legitimate” in order to fool spam filtering algorithms. This tactic is called Bayesian Poisoning and could reduce the effectiveness of a Bayesian database if many of these messages are marked as either spam or not spam. The Barracuda Networks Bayesian engine is, however, very sophisticated and protects against Bayesian Poisoning if administrators or users consistently maintain their databases.
By scanning all outbound messages, you can ensure that all email leaving your organization is legitimate and virus free. This section defines outbound filtering policies that are different from the inbound policies you'd typically apply, including optional encryption for secure transmission based on custom policy. After configuring outbound mail for the Barracuda Spam & Virus Firewall (see Configure Scanning of Outgoing Mail, page 35), choose outbound filtering techniques to best protect the IP reputation of your organization, prevent data leakage and ensure compliance with financial, health care and other federally-regulated agency information policies.

Encryption of Outbound Mail .......................................................... 62
Spam Filtering and Quarantine of Outbound Mail ......................... 64
Rate Control for Outbound Mail ..................................................... 65
IP, Domain and Email Address Filtering of Outbound Mail .......... 65
Content Analysis - Outbound Mail .................................................. 67
Encryption of Outbound Mail

For health care providers, governmental agencies and other entities who need to protect private, sensitive and valuable information communicated via email, the Barracuda Spam & Virus Firewall provides the option of email encryption based on policy you set for outbound mail in the BLOCK/ACCEPT pages. Actual encryption of outbound mail is performed by the Barracuda Email Encryption Service, so system performance is never affected. Encryption is configured at the per-domain level, but actual encryption policy (by sender domain, email address, recipient, etc.) is only configurable at the global level using the BLOCK/ACCEPT pages. These global encryption policies will apply to all domains from which encrypted email messages are sent.

Email encryption can be performed by the Barracuda Spam & Virus Firewall on outbound mail as described in this chapter, OR you can download the Outlook Add-In for your Microsoft Exchange Server to enable users to choose encryption from the New Message window in their MS Outlook client. See Outlook and Lotus Notes Plugins on page 59 or the USERS > User Features page in the Barracuda Spam & Virus Firewall Web interface for information on deploying the Outlook Add-In. For details about sending and retrieving encrypted messages as applies to this add-in, see steps 4-6 of Sending and Receiving Encrypted Messages on page 63 in this chapter.

Secured Message Contents

When the Barracuda Spam & Virus Firewall encrypts the contents of a message, the message body will not be displayed on the BASIC > Message Log, BASIC > Outbound Quarantine, or the ADVANCED > Queue Management pages. For Mail Journaling and the download features in the Message Viewer, the message body will not be sent to the Mail Journaling account and cannot be downloaded to the Desktop.

If you already have an email encryption server or service, you can specify a hostname (FQDN) or IP address and port in the Redirection Mail Server TCP/IP Configuration section of the BASIC > IP Configuration page to which the Barracuda Spam & Virus Firewall should redirect outbound mail for encryption. You can then select the Redirect action for outbound filtering policies in the BLOCK/ACCEPT pages. Redirection of outbound mail per policy is only available at the global (not per-domain) level.

Configuring and Using Encryption

Requirements for Using Encryption

Before applying encryption policy, make sure of the following:

- Your Energize Updates subscription is current. See the Subscription Status section on the BASIC > Status page of the Barracuda Spam & Virus Firewall.
- You must validate sending domains from the DOMAINS > Manage Domain > ADVANCED > Encryption page for each domain that is allowed to send encrypted messages. Several validation methods are available from this page.

Setting Encryption Policy for Outbound Mail

From the BLOCK/ACCEPT pages you can create global custom encryption policy for secure transmission of outbound mail based on:
• Sender email address and/or domain
• Recipient email address and/or domain
• Attachment Filename pattern and/or type as well as attachment content
• Content and content type (such as, for example, secured credit card info.)

These policies will apply for ALL domains from which you send encrypted email.

Branding
You can brand encryption notification emails (see Sending and Receiving Encrypted Messages below) as well as encrypted messages with an image and a domain name to be displayed with the image. Once you have validated a domain through the Barracuda Spam & Virus Firewall, branding is configured at the per-domain level on the ADVANCED > Encryption page where you can upload an image from your local drive or network. You can optionally create custom text or html notification message content and subject from the same page.

Encryption and Quarantine, Blocking and Queuing
• If an encrypted message is quarantined, the administrator will not see the message contents, but can view the message header information and the reason the message was encrypted as well as the reason it was quarantined on the BASIC > Message Log page. From the BASIC > Outbound Quarantine page, the message can be delivered, rejected, deleted or forwarded.
• If an encrypted message is blocked due to policy, the administrator will not see the message contents, but can view the message header information and the reason the message was encrypted as well as the reason it was blocked on the BASIC > Message Log page. The administrator can then deliver the message if desired.
• For encrypted messages in the queue, the administrator will not see the message contents but can view the message header information and why the message was encrypted. From the ADVANCED > Queue Management page, the administrator can deliver, re-queue or delete the message.

Sending and Receiving Encrypted Messages

The Barracuda Message Center provides a Web-based email client for receiving and managing encrypted email sent by the Barracuda Spam & Virus Firewall. The email client looks and behaves much like any Web-based email program. The workflow for email encryption is as follows:

1. The administrator creates a filter from one or more of the BLOCK/ACCEPT pages to encrypt certain types of outbound messages.
2. Outbound messages that meet this filtering criteria are sent over a TLS channel to the Barracuda Message Center for encryption.
3. The outbound message information appears in the Barracuda Spam & Virus Firewall Message Log, but the message body does not, as it is encrypted for security purposes.
4. The Barracuda Message Center sends a notification to the recipient of the email message that includes a link the recipient can click to view and retrieve the message from the Barracuda Message Center. Notifications can be branded as described above.
5. The first time the recipient clicks this link, the Barracuda Message Center will prompt for creation of a password. Thereafter the recipient can re-use that password to pick up subsequent encrypted messages.
6. The recipient logs into the Barracuda Message Center and is presented with a list of email messages, much like any Web-based email program. All encrypted messages received will appear in this list for a finite retention period or until deleted by the recipient.

When the recipient replies to the encrypted email message, the response will also be encrypted and the sender will receive a notification that includes a link to view and retrieve the message from the Barracuda Message Center.

Spam Filtering and Quarantine of Outbound Mail

Outbound mail shares some of the same block / accept mechanisms available for inbound mail, with a few differences, which are described here. Additionally, outbound messages can be encrypted based on filtering criteria you configure on the BLOCK/ACCEPT pages.

Spam Scoring

The last filtering event applied to an outbound email message is assignment of a score based on the probability that it is spam. The administrator can decide how to deal with outbound messages suspected be spam based on the Outbound Spam Scoring Limits as configured on the BASIC > Spam Checking page. Spam scoring limits (from 0 to 9.9) can determine whether to send, quarantine or block outbound messages:

- Quarantining the message means that the message is suspected to be spam or in violation of policy, and will be stored on the Barracuda Spam & Virus Firewall for the administrator to review. The message can then be whitelisted, rejected, deleted or delivered by the administrator.
- Blocking the message means it will not be delivered. If a message is blocked due to its spam score, and if the Send Bounce option for Outbound is set to Yes in the Spam Bounce (NDR) Configuration section of the ADVANCED > Bounce/NDR Settings page, a non-delivery receipt (NDR/bounce message) is also sent to the sender by the Barracuda Spam & Virus Firewall.

Managing Outbound Quarantine

For outbound mail, there is no per-user quarantine mechanism on the Barracuda Spam & Virus Firewall as there is with inbound mail. Messages that meet or exceed the scoring level you set on the BASIC > Spam Checking page for the quarantine of outbound messages, and messages that violate outbound policies you have configured will be placed in outbound quarantine for the system. These messages will be logged and can be viewed on the BASIC > Outbound Quarantine page. At the domain level, messages in outbound quarantine can be viewed and managed by domain under DOMAINS > Manage Domain > BASIC > Outbound Quarantine.

Configure outbound quarantine settings discussed here from the BASIC > Quarantine page.

Immediate notifications can be sent to the administrator via the specified Notification Address whenever an outbound message is placed into quarantine. As with inbound quarantine notifications, a quarantine summary can be sent on a daily or weekly basis, if at all.

A Size Retention Policy can be specified for outbound mail, indicating when “old” quarantined outbound messages should be removed from the Barracuda Spam & Virus Firewall. Use this option together with the Size Limit (KB) to limit the amount of disk space allotted on the Barracuda Spam & Virus Firewall for storing quarantined outbound mail. Regardless of these settings, quarantined outbound messages are always retained for at least 3 days.
Quarantine of outbound messages can also be disabled completely (which is recommended). If it is disabled, no outbound messages are stored on the Barracuda Spam & Virus Firewall.

**Rate Control for Outbound Mail**

Outbound mail is rate controlled based on IP address by the Barracuda Spam & Virus Firewall as described in *Rate Control*, page 52. Rate Control for outbound email, however, can also be applied based on sender email address. If the number of recipients from a sender email address exceeds the specified **Maximum recipients per Sender** over a 30 minute time period, the Barracuda Spam & Virus Firewall will defer any further connection attempts from that particular sender until the next time frame. Deferred outbound messages will be logged as **Rate Controlled** in the Message Log.

**Sender Based Rate Control**, including specifying email addresses you wish to exempt, is configured on the **BLOCK/ACCEPT > Rate Control** page.

**IP, Domain and Email Address Filtering of Outbound Mail**

**IP Address Filtering**

After applying rate controls, the Barracuda Spam & Virus Firewall performs analysis on the IP address, applying quarantine, block, encrypt or redirect policies that you configure in the **BLOCK/ACCEPT** pages.

**Note**

**BLOCK/ACCEPT** policies created at the per-domain level do NOT apply to outbound messages. So, for example, navigating to the **DOMAINS** page, then clicking **Manage Domain** for a particular domain, then configuring policies on the **BLOCK/ACCEPT** pages ONLY applies to inbound messages for that domain.

Once the true sender of an outbound email message is identified, the intent of that sender should be determined before accepting the message as valid, or “not spam”. The best practice is to know the IP addresses of trusted senders and forwarders of email and define those on the Barracuda Spam & Virus Firewall as “Allowed” by adding them to a **whitelist** of known good senders. Various methods for discerning “good” senders of email versus spammers are described in this section to help you to quickly configure your Barracuda Spam & Virus Firewall per the needs of your organization.

**Warning**

Barracuda Networks does NOT recommend whitelisting domains because spammers will spoof domain names. When possible, it is recommended to whitelist (Allow) by IP address only.
Sender and Recipient Filtering

If any of the computers in your organization get infected with a botnet or other malware, it can send out spam emails, thereby possibly landing your domain(s) or IP address(es) on a blocklist, not to mention spreading the malware. Use the BLOCK/ACCEPT > Sender Filters page to control which domains and email addresses can send email out through the Barracuda Spam & Virus Firewall. Note that both inbound and outbound email messages from whitelisted (“allowed”) domains/subdomains bypass spam scoring as well as all other blocklists, but do go through virus checks.

Note

Adding your own domain to the sender whitelist is not allowed because spoofing the domain of the recipient is a frequently used spamming technique. Instead, add the IP address of your mail server(s) to the Allowed IP/Range list using the BLOCK/ACCEPT > IP Filters page.

Email addressed from specified email addresses and domains/subdomains can also be encrypted or redirected from the BLOCK/ACCEPT > Sender Filters page.

Outbound email addressed to specified email addresses (recipients) or domains/subdomains can also be allowed, blocked, encrypted or redirected from the BLOCK/ACCEPT > Recipient Filters page.

For more information about email encryption and redirection, see Encryption of Outbound Mail on page 62.

Reverse DNS Blocking

The Barracuda Spam & Virus Firewall does a reverse DNS lookup on inbound and outbound IP connections and finds the hostname associated with the IP address of the sender. By configuring rules on the BLOCK/ACCEPT > Reverse DNS page, you can choose to apply “common” reverse DNS rules by country or create “custom” rules to quarantine or block outbound messages from those domains.

The last part of a hostname is known as the top level domain, or TLD. Most TLDs include a country identifier, such as .ca for Canada, .ru for Russia, etc. If most or all of the mail that you receive from a particular country is spam, you can use the Common Reverse DNS Rules to tag (inbound only), block or quarantine any message that has an associated hostname that includes that country's TLD. Email which is not blocked is subject to all of the usual spam and virus checks. Use the Custom Reverse DNS Rules to quarantine or block outbound messages from hostnames ending with values that you specify. List the sending domains or subdomains you want to whitelist on the BLOCK/ACCEPT > Sender Filters page.

Attachment Filename and Type Filtering

Attachment filtering based on filename patterns you specify, common text attachment file types and attachment MIME types can be applied to outbound mail just as it can be to inbound mail. See the BLOCK/ACCEPT > Attachment Filters page for details on settings. Note that, in addition to Block and Quarantine, filter actions for outbound mail include Encrypt and Redirect.

The online help for the BLOCK/ACCEPT > Attachment Filters page includes a link to a Regular Expressions help page that covers text patterns you can use for advanced filtering. You can also specify one of the actions listed above to take with outbound messages if attached archive files (zip, tar, etc.) require a password to unpack.
Content Analysis - Outbound Mail

Custom Content Filters - Outbound

Custom content filtering based on the subject line, message headers, message body and attachment file type can be applied to outbound mail just as it can be to inbound mail. See the filtering pages on the BLOCK/ACCEPT tab for details on settings. Note that, in addition to Block and Quarantine, filter actions for outbound mail include Encrypt and Redirect.

The online help for the BLOCK/ACCEPT > Content Filtering page includes a link to a Regular Expressions help page that covers text patterns you can use for advanced filtering.

Note that HTML comments and tags imbedded between characters in the HTML source of a message are filtered out so content filtering applies to the actual words as they appear when viewed in a Web browser.

Attachment Content Filtering - Outbound

All outbound messages, including those from whitelisted senders, go through attachment filtering. You can block, quarantine, encrypt or redirect outbound messages that contain attachments which include text matching the patterns you enter here. Attachment Content Filtering is limited to text type files such as MS Office files, html, pdf files and other document files. A notification will be sent to the sender when an outbound message is blocked due to attachment content filtering.

You can also take actions with outbound messages that contain matches to pre-made patterns in the subject line, message body or attachment. Information types such as credit card patterns, social security numbers (USA only), and combinations of privacy information such as birthday and driver’s license, as well as a diagnosis/prognosis as defined under HIPAA, can be filtered using Barracuda’s predefined regular expressions under the BLOCK/ACCEPT > Content Filters page.

Note that the format of this data varies depending on the country, and these filters are more commonly used in the U.S.; they do not apply to other locales.

See Attachment Filtering on page 55 for details on using these features.

Fingerprint Analysis - Outbound

Outbound messages can undergo Fingerprint Analysis if you enable this feature for both inbound and outbound mail on the BASIC > Spam Checking page. In order to detect real-time spam fingerprints, Barracuda Real-Time Protection must be enabled on the BASIC > Virus Checking page.

Engineers at Barracuda Central work around the clock to identify new spam fingerprints which are then updated on all Barracuda Spam & Virus Firewalls through hourly Barracuda Energize Updates.

Intent Analysis - Outbound

As for inbound mail, this feature is applicable for outbound mail, and block or quarantine actions can be specified accordingly on the BASIC > Spam Checking page.
Image Analysis - Outbound

Fingerprint Analysis captures a significant percentage of images after they have been seen, while Image Analysis techniques protect against new image variants. The techniques detailed in *Image Analysis*, page 57, also apply to outbound messages. *Image Analysis* is configured on the BASIC > Spam Checking page.
The optional **Cloud Protection Layer** (CPL) feature of the Barracuda Spam & Virus Firewall is an additional layer of protection that blocks threats before they reach your network and provides email continuity. Once email passes through the CPL, the Barracuda Spam & Virus Firewall filters email according to the more granular policies, recipient verification, quarantining and other features you configure on the system. You’ll use the **Barracuda Control Center** for central management of both your CPL and your Barracuda Spam & Virus Firewall(s) (see Using the Barracuda Control Center on page 112).

- Advantages of Using Cloud-Based Protection............................ 70
- Setting Up Your Cloud Protection Layer .................................. 70
- Configuring Cloud Protection Layer Spam & Virus Settings........ 71
Advantages of Using Cloud-Based Protection

The CPL (CPL) provides yet another layer of security by pre-filtering *inbound* email for spam and viruses in the cloud before it reaches your actual network. Here are some of the great benefits of enabling this feature:

- **Dual Protection Points** – comprehensive onsite and cloud-based threat protection including the Barracuda Anti-Virus Super Computing Grid and Barracuda Advanced Anti-Fraud Intelligence.
- **Email Burst Handling** – email surge suppression during peak traffic and spam spikes, which offloads a significant volume of spam email to be filtered via the cloud.
- **Immediate Response** – automatic updates in real-time leveraging threat intelligence from Barracuda Labs and Barracuda Central to continuously stay ahead of quickly morphing threats.

Note that the CPL can be configured with many of the same block/accept policies you would apply to the Barracuda Spam & Virus Firewall, but only provides the **Block** and **Allow** actions. The CPL does not support tagging or quarantine of email.

Setting Up Your Cloud Protection Layer

Begin setup of your CPL by either creating an account with Barracuda Networks or logging in with your existing account.

1. Visit http://www.barracudanetworks.com and click the **Customer Login** link in the upper right corner of the page. If you already have an account, log in and skip to step 4.
2. From the **Sign In** page, click the **Create a new account link**. Enter your name and contact information, business name and location. Make a note of your username (email address) and your password.
3. After submitting your new account information, you’ll see the **Account > Users** page which shows your account name, associated privileges, username and products you’ve associated with your Barracuda Networks account. Any additional user accounts you add at a later time will be listed on this page.
4. Click on the **Control Center** link at the top of the page. Click the **Set up your Barracuda Control Center** button. You’ll see the Barracuda Control Center **Status** page and a message indicating that no products have yet been connected.
5. In another browser tab or window, log into your Barracuda Spam & Virus Firewall. From the product **ADVANCED > Firmware Upgrade** page, check to make sure you have the latest firmware installed. If not, download and install it now.
6. From the **ADVANCED > Control Center** page, enter the username and password you created for your Barracuda Networks account. Click **Yes** for **Connect to Barracuda Control Center** to connect your Barracuda Spam & Virus Firewall to the Barracuda Control Center, and then click the **Save Changes** button. Note that your Barracuda Spam & Virus Firewall can connect with only one Barracuda Control Center account at a time.
7. In the Barracuda Control Center window, refresh your browser page. You should see, in the **Products** column in the left side of the page, the **Spam & Virus Firewall** group with two components, or ‘nodes’ listed:
   - The **Cloud Protection Layer** node
   - Each Barracuda Spam & Virus Firewall with its serial number
8. Click on the **Cloud Protection Layer** link and navigate to the **DOMAINS > Domains** page. For each domain for which you want the CPL to filter email, do the following:
8a. Enter one of the domains you have configured on the Barracuda Spam & Virus Firewall using the **New Domain Name** field on this page.

8b. In the **Destination Server** field, enter the *external facing* IP address of your Barracuda Spam & Virus Firewall. This is typically, but not always, the **IP Address** from the **BASIC > IP Configuration** page. **Important**: If your Barracuda Spam & Virus Firewall is behind a firewall, the CPL will not be able to validate your domains.

8c. Add the port of the destination server in the **Dest. Port** field and click **Add Domain**. Repeat this step for each domain.

8d. The CPL will verify domain ownership, and the status of the domain in the table will change from **Verify** to **Re-verify**. If you have not verified ownership of the domain, the CPL will not receive email for that domain.

9. Finally, change the MX Record of each domain you’ve added to that shown in the Manage Domains table.

**Important**: Initially, the configuration on your Barracuda Spam & Virus Firewall will automatically be copied to your CPL so you don’t have to re-configure policy for your existing domains. You can then edit policies in the CPL if needed.

### Configuring Cloud Protection Layer Spam & Virus Settings

You can configure most of the same filtering policies and SMTP settings in the CPL web interface that you can on your Barracuda Spam & Virus Firewall using the **BASIC, BLOCK/ACCEPT** and **ADVANCED > Email Protocol** pages. For greatest security, it is **highly recommended** that you enable virus scanning and Barracuda Real-Time Protection on the **BASIC > Virus Scanning** page in the CPL.

### Viewing Email Statistics

When you click on the top level of the Barracuda Control Center **Products** list, you will see statistics for ALL of your products, including the CPL for your Barracuda Spam & Virus Firewall. However, when you click on the **Email Security** group in the same pane, you’ll see statistics for all *inbound* mail through both the CPL and all *inbound* and *outbound* mail for the Barracuda Spam & Virus Firewall.

To see how many messages were blocked by the CPL, click on that link under the **Email Security** group in the **Products** list and navigate to the **BASIC > Status** page. This page shows you ONLY statistics for *inbound* traffic through the CPL. Use these traffic profiles along with the Message Log to determine how to best tune your spam policies.

To see how many messages were blocked by one or more of your Barracuda Spam & Virus Firewalls, expand the **All Spam & Virus Firewalls** link and click on the system you want to view, then navigate to the **BASIC > Status** page.

### Monitor Incoming Emails

Once email is flowing through the CPL, the administrator can view the **BASIC > Message Log** page of the service to get an idea of how many messages are being blocked by the CPL, with reasons for each of those actions. Reviewing the log will give an idea of how current CPL (as well as Barracuda Spam & Virus Firewall) settings are filtering messages.
Integration With the Barracuda Spam & Virus Firewall

The CPL Message Log fully integrates inbound email activity processed by the CPL with inbound email activity processed by the Barracuda Spam & Virus Firewall. You can look in the Reason column.

The Action and Reason columns in the CPL Message Log are the key to seeing how the CPL blocks spam and virus threats before they reach your network. For blocked messages, the Reason column in the log indicates whether the message was blocked by the CPL or the Barracuda Spam & Virus Firewall. For messages blocked by the CPL, the Reason value will be appended by [Cloud Protection Layer]. For the Barracuda Spam & Virus Firewall, the Reason value will be appended by [BAR-SF-123456], where ‘123456’ represents the serial number.

Remember that only the Barracuda Spam & Virus Firewall tags or quarantine messages. Messages that are Allowed passed through filters in both the CPL and the Barracuda Spam & Virus Firewall.
Chapter 8

Advanced Configuration

This chapter covers advanced administration topics including configuring sender authentication, recipient verification, advanced networking topics, clustering the Barracuda Spam & Virus Firewall and remote administration via the Barracuda API.

Sender Authentication ........................................................................ 74
Recipient Verification ....................................................................... 76
Remote IMAP/POP Accounts ............................................................ 77
Clustering the Barracuda Spam & Virus Firewall ............................. 77
Advanced Networking ...................................................................... 80
Non-Delivery Reports (NDRs) ......................................................... 81
Remote Administration .................................................................... 82
Sender Authentication

This is a key feature of the Barracuda Spam & Virus Firewall for protecting your network and users from spammers who might “spoof” a domain or otherwise hide the identity of the true sender. The following techniques are used to verify the “from” address of a message.

Mail Protocol (SMTP) Checking

The Barracuda Spam & Virus Firewall can perform thorough checks on incoming email for RFC 821 compliance, require mail clients to introduce themselves with an SMTP "HELO" or "EHLO" command before stating a sender, and otherwise manage SMTP protocol to block spammers. See the ADVANCED > Email Protocol page for these and other optional SMTP settings.

Sender Spoof Protection

The Barracuda Spam & Virus Firewall has the option to prevent “spoofing” of an organization’s own domain by blocking emails with that domain name in the “From” field that are sent from outside the organization. Note that sender spoof protection should not be enabled if the organization sends messages from outside their internal email infrastructure (e.g., in the case of marketing bulk-mail services).

The Sender Spoof Protection feature can be configured at the global level from the ADVANCED > Email Protocol page or at the per-domain level on the DOMAINS > Manage Domain > ADVANCED > Email Protocol page. At the domain level, however, this feature is labeled as Reject messages from my domain.

Note that if the administrator enables Sender Spoof Protection at the global level it will supersede any whitelist entry created at the per-user level by a User, Helpdesk or Domain Admin account holder.

Invalid Bounce Suppression

The Invalid Bounce Suppression feature is used to determine whether or not the bounce address specified in a message is valid. It is designed to reduce the number of bounce messages to forged return addresses; i.e., you don’t want to get bounced messages from spammers who spoof your domain or email address. Every email sent from the Barracuda Spam & Virus Firewall is tagged with an encrypted password and expiration time. With Invalid Bounce Suppression enabled, any bounced email received by the Barracuda Spam & Virus Firewall that does not include that tag is blocked. Each blocked message is recorded in the Message Log with the reason "Invalid Bounce".

To use the Invalid Bounce Suppression feature, the Barracuda Spam & Virus Firewall must have Outbound Relay configured on the BASIC > Outbound page. For more details about Outbound Relay, refer to Configure Scanning of Outgoing Mail, page 35.

To configure Invalid Bounce Suppression on the BLOCK/ACCEPT > Sender Authentication page and enter a Bounce Suppression Shared Secret as a non-null password which will be included in the headers of valid emails sent from and bounced back to the Barracuda Spam & Virus Firewall. Email bounces that don’t include the password will be blocked if this feature is enabled.
In a clustered environment, the Bounce Suppression Shared Secret will be synchronized across all Barracuda Spam & Virus Firewalls in the cluster.

**Sender Policy Framework (SPF)**

Sender Policy Framework (SPF) is an open standard specifying a method to prevent sender address forgery. The current version of SPF protects the envelope sender address, which is used for the delivery of messages.

SPF works by having domains publish reverse MX records to display which machines (IP addresses) are designated as valid mail sending machines for that domain. When receiving a message from a domain, the recipient can check those records to make sure mail is coming from a designated sending machine. If the message fails the SPF check, it may be spam. Enabling this feature does create more performance overhead for the system due to the multiple DNS queries needed to retrieve a domain's SPF record; for this reason, the default setting for the Enable SPF feature on the BLOCK/ACCEPT > Sender Authentication page is No (off). For more information on SPF, please visit http://www.openspf.org.

Messages that fail SPF check can be tagged or blocked and will be logged as such. The recommended setting is to Tag messages identified by SPF as spam so that if there is any possibility that a message is legitimate, it will be allowed to go on to the next stage of processing.

**Exemptions from SPF Checking - Trusted Forwarders**

You may specify a list of Trusted Forwarder IP addresses, on the BASIC > IP Configuration page, which will be ignored when performing SPF checks, as well as rate control and IP Reputation checks. Trusted Forwarders are mail servers that are set up specifically to forward email to the Barracuda Spam & Virus Firewall from outside sources. The Barracuda Spam & Virus Firewall scans the IP addresses in the Received From headers list of each email and performs an SPF check on the first IP address that is not in the list of Trusted Forwarders.

**Domain Keys (DKIM) Inspection**

DomainKeys is a method of email authentication that enables a sending domain to cryptographically sign outgoing messages, allowing the sending domain to assert responsibility for a message. When receiving a message from a domain, the Barracuda Spam & Virus Firewall can check the signature of the message to verify that the message is, indeed, from the sending domain and that the message has not been tampered with. Because most spam messages contain spoofed addresses, DomainKeys can help greatly in the reduction of spam.

DomainKeys uses a public and private key-pairs system. An encrypted public key is published to the sending server’s DNS records and then each outgoing message is signed by the server using the corresponding encrypted private key. For incoming messages, when the Barracuda Spam & Virus Firewall sees that a message has been signed, it will retrieve the public key from the sending server's DNS records and then compare that key with the message's DomainKeys signature to determine its validity. If the incoming message cannot be verified, the Barracuda Spam & Virus Firewall knows it contains a spoofed address or has been tampered with or changed.

The benefits of enabling this feature include:

- Email sender is validated
- Email body is validated
• Validation through DNS is difficult to foil
• DomainKeys works well with email forwarding because it doesn’t deal with the relay server IP address

You can choose to tag, block or quarantine both DKIM signed messages that fail the DKIM database check as well as unsigned messages, depending on how you configure DomainKeys Inspection on the BLOCK/ACCEPT > Sender Authentication page. You can also exempt domains from being tagged, quarantined or blocked if they fail this check. As stated elsewhere in this guide, it is safest to NOT exempt domain names from any kind of spam filtering due to the possibility of domain name spoofing by spammers.

DomainKeys inspection does require more CPU resources to encrypt & decrypt the key and is turned off by default.

**Custom policies**

Organizations can define their own allowed sender domains or email addresses for sender authentication using the BLOCK/ACCEPT > Sender Filters page, but the safest way to indicate valid senders on the Barracuda Spam & Virus Firewall is to whitelist (allow) the IP addresses of trusted email servers on the BLOCK/ACCEPT > IP Filters page, then blocklist (block, quarantine or tag) their domain names on the BLOCK/ACCEPT > Sender Filters page to prevent domain name spoofing.

**Recipient Verification**

**LDAP lookup**

On the Barracuda Spam & Virus Firewall 300 and higher, email recipients can be validated with your existing LDAP server. Configuration of LDAP lookup is done by domain from the DOMAINS > Domain Manager page. After clicking Manage Domain for the selected domain, you’ll configure LDAP on the USERS > LDAP Configuration page. See the online help on that page for details about entering your server details. If LDAP is not configured, the Barracuda Spam & Virus Firewall will do SMTP recipient verification through RCPT TO commands.

LDAP server types supported include Active Directory, Novell eDirectory, Domino Directory and OpenLDAP.

**Explicit Users to Accept For (Valid Recipients)**

If LDAP lookup is not being used for recipient verification, the Barracuda Spam & Virus Firewall provides a local database with which email recipients can be compared for validation. Valid Recipients (Explicitly Accepted Users) can be specified either at the global level from the ADVANCED > Explicit Users page or at the per-domain level from the DOMAINS > Domain Manager > USERS > Valid Recipients page. Note that the number of entries in the text box for Explicitly Accepted Users and Alias Linking is limited by model: on the Barracuda Spam & Virus Firewall 600 and lower, the maximum is 1000 per domain, and on the Barracuda Spam & Virus Firewall 800 and above, the limit is 5000 per domain.
To administer the local database, either at the global or domain level, fill in the text box in the Explicit Users to Accept For section of the page, entering each email address for which the Barracuda Spam & Virus Firewall should accept email. If you select Yes for the Only accept email for these recipients feature, email will REJECTED for any email recipients not in the list. Note that domain-specific lists override the global list.

**Alias Linking**

Alias linking allows quarantined email from multiple accounts to be directed to one account when using per-user quarantine. In the Advanced > Explicit Users page you can specify the email addresses to be linked together in the Explicit Users to Accept For and Alias Linking text box. See the online help on that page for more details. The quarantine account for all of the linked email addresses will be associated with the first email address. Make sure to also enter the first email address on a separate line as well. In this way, a "catchall" account can be created to receive all quarantined emails from a particular domain.

**Remote IMAP/POP Accounts**

The Barracuda Spam & Virus Firewall provides an email-retrieval and forwarding utility which fetches email from remote mail servers and forwards it to your local machine's delivery system. You can repeatedly poll each account at a specified interval. This utility can gather mail from servers supporting POP3 and IMAP and is configured from the Advanced > Remote IMAP/POP page.

Note that all email will be DELETED from the remote mail server after retrieval by the Barracuda Spam & Virus Firewall.

There are two types of operations for each account from which the Remote Accounts utility retrieves mail: Global and User. With the User type, it is assumed that all messages in the user's account are intended for a single recipient. The Global type is used when multiple recipients under the same domain are specified for a particular server account.

From the Advanced > Remote IMAP/POP page you can specify polling interval, SSL (yes/no), user account passwords and email addresses.

**Clustering the Barracuda Spam & Virus Firewall**

Deploying clustered Barracuda Spam & Virus Firewalls is easy - once you configure one of the devices, configuration settings are synchronized across the cluster almost immediately. Clustered systems can be geographically dispersed and do not need to be located on the same network. Every Barracuda Spam & Virus Firewall in a cluster must be the same model (400 and above) and have the same version of firmware installed.

Instructions to set up and configure a Barracuda Spam & Virus Firewall cluster, including removing a system from the cluster, are detailed on the Advanced > Clustering page.

**IMPORTANT:** When replacing a failed system in a cluster, be sure to follow step #3 as described below under Removing a Barracuda Spam & Virus Firewall From a Cluster, page 79.
Setting Up Clustered Systems

To cluster two Barracuda Spam & Virus Firewalls together, where one system is designated as “Barracuda1” and the other is designated “Barracuda2”, do the following:

1. Complete the installation process for each system as described in Install the Barracuda Spam & Virus Firewall, page 29.

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 a 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.

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 8.1: Two Barracuda Spam & Virus Firewall systems in a cluster

6. Distribute the incoming mail traffic to each Barracuda Spam & Virus Firewall using a Barracuda Load Balancer (preferred) or another load balancing device, or use multiple DNS MX records of equal priority.

7. Each Barracuda Spam & Virus Firewall in a cluster must be on exactly the same firmware version. See the online help on the ADVANCED > Clustering page for instructions in updating the firmware on all systems in the cluster at the same time.
Removing a Barracuda Spam & Virus Firewall From a Cluster

1. Log into the system to be removed and change or clear the Cluster Shared Secret on the ADVANCED > Clustering page. Click Save Changes. Changing the cluster shared secret prevents the systems in the cluster from communicating with one another.

2. On the same system, delete all other systems from the Clustered Systems list.

3. On any system that remains in the cluster, go to the ADVANCED > Clustering page. In the Clustered Systems list, delete the system to be removed from the cluster. This step is very important when removing a failed Barracuda Spam & Virus Firewall from a cluster.

Centralized Policy Management With a Quarantine Host

You can optionally designate one Barracuda Spam & Virus Firewall as the “host” of the cluster such that all administration of configuration settings and access to per-user quarantine for the cluster can only be accessed and set from that node. This option has two advantages: it provides for additional security by limiting access to administration of the cluster, and it protects the user interface from mail processing load since, with this configuration, you do not direct any email traffic to the host node.

If you want to set up one Barracuda Spam & Virus Firewall as the host of the cluster, enter the hostname of that device in the Quarantine Host field on the BASIC > Quarantine page and do not direct any email to that device.

Redundancy of user quarantine data on the cluster

Each user account has a primary and backup server in the cluster. Regardless of how many Barracuda Spam & Virus Firewalls there are in the cluster, there are always two appliances that have the same quarantine information (configuration and quarantine messages).

Data Not Synchronized Across the Cluster

Clustering not only makes managing multiple Barracuda Spam & Virus Firewalls more manageable, it also provides 100% redundant coverage of the propagated data. However, for practical reasons, some data is not propagated to the other clustered systems when a new system joins.

Energize updates do not synchronize across systems in a cluster. The following Barracuda Spam & Virus Firewall configurations are considered unique and will not sync to match other Barracuda Spam & Virus Firewalls in a cluster:

- IP Address, Subnet Mask, and Default Gateway (on the BASIC > IP Configuration page)
- Primary DNS Server and Secondary DNS Server (on the BASIC > IP Configuration page)
- Serial number (this will never change)
- hostname (on the BASIC > IP Configuration page)
- Any advanced IP configuration (Barracuda Spam & Virus Firewall 600 and above, on the ADVANCED > Advanced Networking page)
- Administrator password
- Guest password
- Time Zone (on the BASIC > Administration page)
• Cluster hostname (on the ADVANCED > Clustering page)
• Cluster Shared Secret, though this must be the same for the cluster to work properly (on the ADVANCED > Clustering page)
• Local Host Map (on the ADVANCED > Clustering page)
• SMTP Welcome Banner (on the ADVANCED > Email Protocol page)
• Web Interface HTTP Port (on the BASIC > Administration page)
• Web Interface HTTPS/SSL port (on the ADVANCED > Secure Administration page)
• Any other secure administration configuration, including saved certificates (on the ADVANCED > Secure Administration page)
• Quarantine Host (on the BASIC > Quarantine page)
• All SSL/TLS information, including saved certificates (on the ADVANCED > SMTP/TLS page)
• Whether to only display local messages in the message log (Only view local messages on the BASIC > Message Log > Preferences page)
• Whether the latest release notes have been read
• All customized branding (Barracuda Spam & Virus Firewall 600 and above, on the ADVANCED > Advanced Appearance page)
• The Explicit Users To Accept For list, if enabled and used, on the ADVANCED > Explicit Users page. This is a global setting.
• The Valid Recipients list on the DOMAINS > Manage Domain > USERS > Valid Recipients page. This is a per-domain setting.

Advanced Networking

Port Forwarding

If your organization has a single public IP address, when you install the Barracuda Spam & Virus Firewall between the Internet and your mail server, you can forward incoming SMTP traffic (port 25) from port 80 on the Barracuda to your mail server using the Port Forwarding feature from the ADVANCED > Advanced Networking page.

Configuring the Network Interfaces

With the Barracuda Spam & Virus Firewall 600 and higher, you can configure each of the two Ethernet (NICS) interfaces directly from the ADVANCED > Advanced Networking page to accept email on both interfaces or to route ingress email to one NIC and egress through the other NIC. Benefits of this feature include redundancy, filtering email for domains on separate networks and improving throughput. Up to 250 IP addresses can be configured per NIC.

Static Routes

You can specify a default gateway between the Barracuda Spam & Virus Firewall and a mail server on another subnet in your organization using the Static Routes feature on the ADVANCED >
Advanced Networking page. This will guarantee that return traffic is routed back to the Barracuda Spam & Virus Firewall from the unassociated network.

**Loopback Adapter**

If you want to use this Barracuda Spam & Virus Firewall with a Barracuda Load Balancer in Direct Server Return mode, you must enable a non-ARPing loopback adapter. If you are using any other mode you do not need to make any changes to the Barracuda Spam & Virus Firewall configuration.

Each Virtual IP address supported by the Real Server (the Barracuda Spam & Virus Firewall in this case) requires its own loopback adapter. For each loopback adapter, enter a Virtual IP address in the Loopback Adapter Configuration field on the ADVANCED > Advanced Networking page.

**Non-Delivery Reports (NDRs)**

**Spam Bounce Non-Delivery Reports (NDRs)**

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

The ADVANCED > Bounce/NDR Messages page allows for customizing the information in an NDR and for selecting the default language to use in the message.

**Reducing Backscatter**

By default, your Barracuda Spam & Virus Firewall is configured to NOT send an NDR to a sender when the Barracuda Spam & Virus Firewall blocks their email. You may want to enable NDRs to alert legitimate senders that their message has not been delivered to the recipient.

However, if the email came from an illegitimate source such as a spammer, then sending a bounce notification is not necessary. Additionally, many spammers spoof valid domains, and you don’t want to send bounce messages to your domain if it is being spoofed. Sending bounce messages to illegitimate senders, or to senders who were spoofed and did *not* actually send the offending message, is known as “backscatter”.

Backscatter can increase the load on your Barracuda Spam & Virus Firewall and may generate a lot of email to fake addresses or to senders whose email addresses were spoofed by a spammer. Additionally, your domain could end up on a real-time blocklist as a consequence. If your Barracuda Spam & Virus Firewall rarely blocks a legitimate email, consider turning off bounce notifications to reduce backscatter by setting the Send Bounce feature on the ADVANCED > Bounce/NDR Settings page to No.
Remote Administration

Barracuda Networks provides a set of APIs for remote administration and configuration of the Barracuda Spam & Virus Firewall, firmware version 4.x. The APIs work through manipulation of variables inside of the system configuration database, and anything that can be declared in that database can be set or checked with the APIs. This includes most things that you can set by clicking the Save Changes button in the Barracuda Spam & Virus Firewall Web interface. For example, from the BASIC > Spam Checking page, you can set global Spam Scoring Limit values for the actions Block, Tag or Quarantine, then click the Save Changes button. These values can be set remotely using the APIs.

The framework of the API provides for the programmer to get or set variables inside an XML-RPC request that correspond to field values in the configuration database in the Barracuda Spam & Virus Firewall. Some languages such as Perl, for example, provide wrappers for XML-RPC requests, providing an interface to form the request. To view the variables and current settings of the Barracuda Spam & Firewall configuration database, on the ADVANCED > Backup page, select System Configuration for Backup Type and click the Backup button.

To prepare the Barracuda Spam & Virus Firewall for use with the APIs, you must first enter the IP addresses that are allowed to communicate with the APIs in the Allowed SNMP and API IP/Range field on the BASIC > Administration page, and you must create an API Password that will be included with all calls to the APIs.

For more information on using the APIs, see the Barracuda Spam & Virus Firewall API Guide 4.x on the Barracuda Web site: http://www.barracuda.com/support.
Managing Inbound Quarantine

The Barracuda Spam & Virus Firewall provides a fully featured, robust quarantine function to apply at either a global level or at a per-user level, configurable for each domain managed by the appliance. This chapter covers some pros and cons of enabling quarantine and how and why to use global or per-user quarantine.

How Quarantine of Inbound Mail Works .................................................. 84
Quarantine Options .................................................................................. 84
Using Global Quarantine ......................................................................... 85
Using Per-user Quarantine ........................................................................ 86
How Quarantine of Inbound Mail Works

After a message travels through the initial filtering layers of the Barracuda Spam & Virus Firewall, it is assigned a score based on the probability that it is spam. The administrator can decide how to deal with messages based on the Spam Scoring levels (from 0 to 10): allow, tag, quarantine or block, as set on the BASIC > Spam Checking page.

- Tagging the message means the user will receive the message in their regular mailbox with the subject text modified to indicate that the message might be spam.
- Quarantining the message means that the message will either be delivered, with the subject text modified to indicate that the message might be spam, to a special “quarantine inbox” assigned to a user or to a “global” quarantine mailbox designated by the administrator.
- Blocking the message means it will not be delivered.

Messages can also be determined to be quarantined (as opposed to allowed, blocked or tagged) by custom policies you set based on domain name, IP address, region, content filters and other filtering tools in the BLOCK/ACCEPT pages. Spam Scoring and some block/accept policy settings can be further refined at the domain level and/or per-user level, depending on what the administrator enables on the USERS > User Features page at the global level and what the Domain Admin role enables on the USERS > User Features page at the domain level. For more information on the Domain Admin and other account roles, please see Role-based Administration, page 96.

Quarantine can be enabled or disabled completely. If it is enabled at the Global level, no messages are stored on the Barracuda Spam & Virus Firewall; rather, all quarantined mail is sent to the Quarantine Delivery Address you specify on the BASIC > Quarantine page. If it is enabled at the Per-User level, user accounts are created on the Barracuda Spam & Virus Firewall for users listed either in the authentication server (see Automatic Account Creation, page 94) or in the local database on the Barracuda Spam & Virus Firewall. Quarantined messages need to be received and determined to either be delivered to the user’s regular email inbox or deleted.

As the administrator, you can configure a Retention Policy to limit the amount of disk space used for storing each user's quarantined messages, thereby conserving system resources on the Barracuda Spam & Virus Firewall. Alternatively, messages can be scheduled for regular purging based on age and/or size (see Retention Policy and Purging Old Messages 89).

Quarantine Options

By default, the Barracuda Spam & Virus Firewall does not quarantine incoming messages, but you may want to enable quarantine if, for example, your organization requires it, or if you want to reduce load on the mail server while giving users a chance to determine what they consider to be “spam” or “not spam”.

The three options available for configuring quarantine with the Barracuda Spam & Virus Firewall and the pros and cons of each are described below.

Turning Quarantine Off

Barracuda Networks recommends disabling quarantine unless, for example, your organization has a business requirement to provide quarantine of messages suspected to be spam or you don’t want those messages stored on the mail server. Disabling quarantine means less management either by the administrator or by the user and, in the case of per-user quarantine, saves system resources that would otherwise be used to store the messages until the user delivers or deletes them.
An alternative to using quarantine is *tagging* email that may be spam based on scoring or are otherwise identified as possible spam. Benefits include:

- No messages are stored on the Barracuda Spam & Virus Firewall, thus saving system resources
- The user doesn’t have an extra quarantine inbox to manage
- Tagged messages, with a keyword such as “[BULK]” prepended to the subject line, can be filtered by the subject line to a separate folder for later examination by the user (see the BASIC > Spam Checking page and the BLOCK/ACCEPT pages to configure spam scoring and criteria for tagging messages).

To disable Quarantine completely, check the **Disable** check box next to “Quarantine” in the Spam Scoring Limits section of the BASIC > Spam Checking page.

### Using Global Quarantine

With global quarantine there is almost no difference in use of system resources versus having quarantine turned off because messages aren’t stored on the Barracuda Spam & Virus Firewall; they are forwarded to a mailbox as designated by the administrator. Global quarantine identifies email to quarantine, rewrites the “From” address of the message and sends it to the Quarantine Delivery Address specified on the BASIC > Quarantine page. The subject line of each message is prepended with the Quarantine Subject Text (for example, [QUAR], as specified on the same page). Global quarantine does require some time and effort by the administrator to manage quarantined messages. Global Quarantine can be enabled at the system level or at the domain level.

Enabling global quarantine on the Barracuda Spam & Virus Firewall provides the administrator with complete control over how quarantined messages are handled, and it saves system resources because messages are not stored on the appliance.

To set up global quarantine, from the BASIC > Spam Checking page, make sure that the **Disable** check box next to Quarantine in the Spam Scoring Limits section is NOT checked. From the BASIC > Quarantine page, select the **Quarantine Type** to **Global** and configure settings as described below for Global Quarantine.

You’ll need to enter a Quarantine Delivery Address: on the BASIC > Quarantine page. This mailbox can either be on the mail server that the Barracuda Spam & Virus Firewall protects or a remote mail server. Note: If you have a Barracuda Spam & Virus 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 Manage Domains link, then using the BASIC > Quarantine page for that domain to configure the address.

Messages determined to be quarantined by the Barracuda Spam & Virus Firewall will have the subject line prepended by the Quarantine Subject Text: as entered on the BASIC > Quarantine page. The default text is [QUAR]. This allows you to identify quarantined messages when you have them delivered to a mailbox that also receives non-quarantine messages.

Note that with global quarantine, users will have no control over whitelisting or blocklisting of email addresses, which they do have with per-user quarantine. Allowing them this control by using per-user quarantine can help reduce the number of messages processed by the Barracuda Spam & Virus Firewall. However, if using global quarantine, users can communicate domains, IP addresses or email addresses that should be white or blocklisted to the administrator to configure at the global level.
Using Per-user Quarantine

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 inbox on the Barracuda Spam & Virus Firewall. Since per-user quarantine entails storing quarantined messages on the Barracuda Spam & Virus Firewall until the user delivers or deletes them, you may want to only provide a quarantine inbox to a subset of power users.

When enabling per-user quarantine on the Barracuda Spam & Virus Firewall, keep in mind that quarantined email stored on the Barracuda Spam & Virus Firewall requires storage capacity, so system load will vary with the average size of emails.

If the email patterns of your organization are such that many emails include large attachments (as with architecture firms, marketing firms, etc.), the system may push the edge of performance more quickly than if emails tend to be small in size. See the Mail/Log Storage indicator in the Performance Statistics pane of the BASIC > Status page to monitor disk storage on the Barracuda Spam & Virus Firewall.

To set up per-user quarantine, the first thing to do is to enable quarantine using the Spam Scoring Limits on the BASIC > Spam Checking page. On the BASIC > Quarantine page, select the Quarantine Type to be Per-User and configure settings as described below for Global Quarantine. If Per-User quarantine is set by the administrator or the Domain Admin can either enable or disable Per-User quarantine at the domain level.

You can choose to allow the user to decide whether to deliver quarantined messages to their regular email address associated with their account or to their quarantine inbox. You can alternatively decide this for the user and prevent them from accessing this setting. You can also allow the user to control their whitelist (allowed) and blocklist (blocked) of email addresses.

Where Do the Quarantined Messages Go?

If the administrator sets Quarantine Type to Per-User on the BASIC > Quarantine page and the New User Quarantine State feature is set to On, the Barracuda Spam & Virus Firewall will automatically create quarantine accounts for all users listed in the authentication server or local database as configured at the domain level. Account holders can the log into the Barracuda Spam & Virus Firewall and view their Quarantine Inbox to view and take actions with quarantined messages.

If a user's quarantine inbox is disabled (by an administrator or a Domain Admin or Helpdesk account, or by the user), emails sent to that user that would normally have been placed in quarantine will simply be delivered to the user's regular mailbox with the subject line prepended with a quarantine tag.

Linking Domains for One Quarantine Inbox

In some cases it may be practical to direct all quarantined email to one quarantine inbox on the Barracuda Spam & Virus Firewall. You may employ one or more “power users” to manage it, or allow all users to log in to the same inbox.

Using only one quarantine inbox for all users greatly simplifies management of per-user quarantine because you only have to configure user features (from the BASIC > User Features page) for ONE inbox. The Linking Domains feature, configurable on the BASIC > Quarantine page, allows the...

Note

For the Barracuda Spam & Virus Firewall 300 and higher, be sure to set a Retention Policy before enabling per-user quarantine in order to prevent running out of quarantine space.
option for all domains protected by this Barracuda Spam & Virus Firewall be treated as if they were alternate names for the default domain name for the system. So, for example, if the Default Domain for the system as specified on the BASIC > IP Configuration page is mybarracuda.com, then user@domain1.com will be treated as user@mybarracuda.com when determining user validity and preferences, and will have a quarantine inbox under the name user@mybarracuda.com.

The Quarantine Inbox

When an account holder with the User role logs in to the Barracuda Spam & Virus Firewall they’ll see the QUARANTINE INBOX and PREFERENCES tabs. They can view and choose to whitelist, deliver or delete quarantined emails from the QUARANTINE INBOX page and configure their account settings from the PREFERENCES page to the extent that their account permissions allow as described below under Controlling Access to Account Features, page 87.

Domain Admin and Helpdesk account holders will see the QUARANTINE INBOX and PREFERENCES tabs when they click the Manage Account link in the upper-right corner of the Web interface.

For details on how all account holders manage their quarantine inbox, please see the Barracuda Spam & Virus Firewall User’s Guide at http://www.barracudanetworks.com/documentation.

Alias Linking

This feature allows one quarantine account to receive quarantined email for multiple accounts, using the Explicit Users to Accept For section of the USERS > Valid Recipients page. Note that this account, if entered on one line only with associated accounts for which it should receive email, is not considered a Valid Recipient. This account needs to be added on a separate line to also be considered a Valid Recipient. The quarantine account that receives quarantined email for other accounts does not need to belong to the same domain as the others.

Controlling Access to Account Features

When accounts are created by the Barracuda Spam & Virus Firewall, permissions are automatically assigned for users to manage their account features based on what is configured on the USERS > User Features page in the Default User Features section. Domain Admin roles can further limit user access to these features based on what the administrator has enabled at the global level.

For example, if the Whitelist/blocklist feature is set to No (disabled) at the global level in the Default User Features section of the USERS > User Features page, the Domain Admin role will not see or be able to control that setting for accounts in domains that they manage.

Configurable user account features include:

- Quarantine Inbox - allow the account holder to enable their quarantine inbox on the Barracuda Spam & Virus Firewall, or disable it such that quarantined message go to their regular email inbox.
- Spam scanning - allow the account holder to enable or disable
- Edit frequency at which quarantine notifications are sent to the account holder
- Add addresses and domains to a whitelist or blocklist
- Use Bayesian filtering
- Allow account holder to set their own tag, quarantine and block levels according to spam scoring
If allowed permissions by the administrator, the Domain Admin can edit the Default User Features settings (i.e. disabling certain features that were enabled at the global level by the administrator) at the domain level for account holders in the domain. The Helpdesk role does not have this permission.

**Overriding Default Account Features Settings**

The User Features Override section of the USERS > User Features page allows you to make exceptions to the rules specified above for particular account holders. Domain Admin and Helpdesk roles can view and set override of user feature defaults ONLY for features that are enabled in the Default User Features section by the administrator. Consequently, nothing will appear on the USERS > User Features page for Domain Admin and Helpdesk roles if all Default User Features options have been set to No by the administrator.

User overrides only apply when the domain level setting in Default User Features matches the global setting.

**Assigning Quarantine Inbox Permissions to Selected Users**

One of the most common scenarios for overriding quarantine settings is when you want to provide a few “power users” with a quarantine inbox on the Barracuda Spam & Virus Firewall and have the rest of your users receive quarantine messages in their standard email 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 sophisticated users. In this example, you would do the following:

- Set the quarantine type to Per-user on the BASIC > Quarantine page.
- Set the New User Quarantine State: to Off so that accounts are not automatically created by the Barracuda Spam & Virus Firewall when needed (for conditions under which new accounts can be automatically created, see Automatic Account Creation, page 94).
- In the User Account text box in the User Account Create/Update section of the USERS > User Add/Update page, enter the email addresses of the users you whom you want to create a quarantine inbox and set Enable User(s) Quarantine to Yes in the same section.
- Enable the features you want those account holders to be able to manage for their accounts on the USERS > User Features page.
- Set the Email New User(s):option to Yes to email login information to the new users.

**Quarantine Notifications**

The Barracuda Spam & Virus Firewall can send notifications that a user has quarantined messages at predefined intervals and in selected languages. The notification interval and email address can be set at the global level on the BASIC > Quarantine page and overridden at the domain level if allowed by the administrator. Because creating a quarantine digest for each user requires lots of system I/O, it is recommended to set the Notification Start Time on the BASIC > Quarantine page to outside of peak traffic time frames during the weekday. The default start time is 3:35pm (15:35). Users can override the Notification Interval of daily, weekly or never from their PREFERENCES tab if enabled by the administrator.

---

**Note**

If you enable user quarantine, you should remove any mailing lists you may have added on the ADVANCED > Explicit Users page and public folders so no per-user accounts are created based on those email addresses.
Multiple quarantine notifications can be sent out in a 24 hour period to users that they have quarantined mail by entering multiple times for Notification Start Time. Note that sending multiple notifications could affect system performance.

It is a recommended to set the Quarantine Host value, which appears as the sending hostname in all quarantine and welcome emails from the system. Using this hostname as opposed to the system IP address (default) ensures that users are able to reach the Barracuda Spam & Virus Firewall from their old notifications even after any possible changes in IP addresses.

At the domain level, to enable users (including Domain Admin, Helpdesk and User roles) to manage quarantine notifications for their own accounts, make sure the Enable User Features setting on the BASIC > Quarantine page is turned On. Account holders can then access notification settings from their PREFERENCES > Quarantine page, overriding the global setting. The Default Language used in notification emails can also be set from this page.

How the Quarantine Digest Works

The quarantine digest only goes out if new quarantined mail is saved in the user’s folder since the last notification cycle. Each day the quarantine notification service runs for all users. If there is no new quarantined mail for a user since the last notification interval, or if a user has logged into their account since the last notification interval, no quarantine digest will be generated and sent to that user for that same 24 hour period.

Retention Policy and Purging Old Messages

As the administrator, you can configure retention policy to limit the amount of disk space used for storing each user’s quarantined messages, thereby conserving system resources on the Barracuda Spam & Virus Firewall.

From the USERS > Retention Policies page, you can enable the user to easily schedule quarantined messages for regular purging based on age (in number of days), disk space used (specified in kilobytes), or both. Setting the Age Limit to a 7-14 day range is recommended assuming that older quarantined emails may lose importance with time.

Note that regardless of these settings, no messages younger than 3 days will be removed. For example, if the maximum size limit on email size is 10MB and a quarantined email has a 19MB attachment, the email will be retained for 3 days, giving the user time to examine and process that email before it is automatically deleted by the Barracuda Spam & Virus Firewall.

Minimizing Excessive Storage of Email

It is recommended that users be trained to manage their own quarantine areas, since constant reliance on the Barracuda Spam & Virus Firewall to automatically remove quarantined messages based on either age or disk usage may impact system performance.

The level at which performance is affected depends on the number of user quarantine areas that are kept on the Barracuda, the amount of email that is quarantined each day, and the number of tasks the system performs (e.g., reporting, or body filtering).
Use the filters on the USERS > Account View page to quickly determine which users have the largest quarantine areas. Each account entry shows Yes/No in the Quarantine column (“Yes” indicates per-user quarantine is in effect for that user) and number of Kbytes of email stored in their quarantine inbox in the Size column. Individual user quarantine areas can be disabled from the USERS > Add/Update page so that any repeat offenders can be prevented from utilizing the Barracuda Spam & Virus Firewall quarantine areas. When a user's quarantine is disabled, emails sent to that user that would normally have been placed in quarantine will simply be delivered to the user's actual mailbox with the subject line prepended with a quarantine tag.

Note When you enable retention policies, keep in mind that if your system has been accumulating email without retention policies for a period of time, the first day retention policies are enabled results in 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 daily starting at approximately 02:30 AM.
Chapter 10
Managing Accounts and Domains

If your Barracuda Spam & Virus Firewall is responsible for filtering messages for more than one mail server or domain, the domains associated with each mail server will need to be added to the system. With the Barracuda Spam & Virus Firewall 400 and higher, you can configure various spam settings, filtering policy, authentication and quarantine settings on a per-domain basis. With the Barracuda Spam & Virus Firewall 300 and higher, you can enable per-user quarantine and the system will create user accounts to enable access to quarantine settings and messages. The Barracuda Spam & Virus Firewall 600 and higher supports per-user account spam score settings.

Use this chapter to understand managing user accounts and domains on the Barracuda Spam & Virus Firewall and configuring per-domain and per-user settings.

Creating and Managing Domains...................................................... 92
Creating and Managing Accounts ..................................................... 93
Role-based Administration............................................................... 96
Creating and Managing Domains

Your Barracuda Spam & Virus Firewall will only accept emails addressed to domains that it has been configured to recognize. Settings for individual domains can be configured by the administrator and, with some restrictions, by the Domain Admin and Helpdesk account roles as described below under Role-based Administration, page 96. All three roles will see a DOMAINS tab from which they can click Manage Domain next to the domain for which to edit the domain-level settings.

Only an administrator can add or delete domains using the controls available in the DOMAINS page. The administrator can also add domains from the BASIC > IP Configuration page. Domains added from either page will be initially configured with whatever you have specified your default global settings to be.

If the administrator deletes a domain, all user accounts associated with that domain will also be deleted from the Barracuda Spam & Virus Firewall. A confirmation dialog box will prompt you to confirm whether or not you want to delete a domain.

Clicking the Manage Domain link for a particular domain will show some or all of the BASIC, USERS, BLOCK/ACCEPT, OUTBOUND QUARANTINE and ADVANCED tabs, depending on the permissions level of the logged in account role.

Figure 10.1: The administrator can add domains on which to filter email.

Domain Level Settings

Some settings are only configurable at the domain level, while others are configurable at both the global and domain levels, with the domain level setting taking precedence. The Domain Admin role or the administrator can override some global settings for spam and virus checking and quarantine at the domain level.

Setting values on a per-domain basis overrides the values configured at the global in the web interface. However, if you have never changed a particular setting for a domain, any global level changes to that feature will be applied for that domain. This also means that any changes you make to the global values of the Barracuda Spam & Virus Firewall will NOT be inherited by the domains that you edit and for which you have changed configuration values.

Basic configuration of a domain consists of identifying the name of the domain (and/or a specific sub-domain) and specifying a destination mail server. Additional settings available for a domain are
dependent on the model of your Barracuda Spam & Virus Firewall, and can include any or all of the following:

- Destination Mail Server
- Enabling of spam scanning and setting spam score limits for the domain
- Enabling or disabling virus scanning
- Per-user quarantine enable/disable
- Control over which features users can see and configure for their accounts (see *Controlling Access to Account Features*, page 87)
- A defined global quarantine email address (for the domain only)
- IP address/range, Sender domain, Sender email and Recipient filtering. **Note:** BLOCK/ACCEPT policies created at the per-domain level do NOT apply to outbound messages - they only apply to inbound messages for that domain.
- LDAP configuration
- Option to specify local database of valid recipients (if not using LDAP) and alias linking
- Single Sign On with various authentication mechanisms
- Emailreg.org: option to require header, body or subject content filtering on mail from registered email addresses
- Ability to validate the domain and specify an image for branding encrypted email messages and notifications sent to the recipient. Note that encryption policy can only be set at the global level by the administrator.

**Note**  
The Barracuda Spam & Virus Firewall 400 and higher contain support for APIs that can be used to automate the steps for creating and configuring multiple domains on the Barracuda Spam & Virus Firewall.

### Creating and Managing Accounts

There are two ways of creating user accounts on the Barracuda Spam & Virus Firewall - automatically and manually. Depending on how the administrator configures the Barracuda Spam & Virus Firewall, accounts can include a quarantine inbox for individuals or may only provide users with the ability to manage their own whitelist and blacklist of email addresses and domains or spam scoring levels.

In addition to the administrator account role, which includes permissions to configure all settings on the Barracuda Spam & Virus Firewall, four other account roles with associated levels of permissions are available:

- **User**, the default account role whose permissions are limited to managing their own quarantine account to the degree enabled by the administrator.
- **Auditor**, a unique account (you can only create one instance) whose role it is to monitor the **Outbound Quarantine** - deleting, rejecting or allowing delivery of messages based on policy. This account already exists on the Barracuda Spam & Virus Firewall and must be enabled on the **BASIC > Administration** page.
- **Helpdesk** (available on the Barracuda Spam & Virus Firewall 300 and higher), with increased permissions.
• *Domain Admin* (available on the Barracuda Spam & Virus Firewall 600 and higher), the role with the most permissions other than the administrator. This role can configure certain types of policy for the domains assigned to their account.

Thus you can delegate various levels of authority to members of your organization for administering quarantine accounts, monitoring outbound quarantined mail and managing per-domain level settings on the Barracuda Spam & Virus Firewall.

Once accounts are created, each account (with the exception of *Auditor*) can be assigned a role other than the default *User* role from the **USERS > Account View** page at the global level or at the per-domain level. This feature is especially useful for ISPs/Web hosting providers to give helpdesk and more sophisticated technical support personnel access to domain and per-user account configuration for groups of users. See *Role-based Administration*, page 96, for details on role-based permissions and web interface navigation.

### Automatic Account Creation

The Barracuda Spam & Virus Firewall automatically creates accounts when all of the following conditions are met:

- The *New User Quarantine State* features is set to **On** on the **BASIC > Quarantine** page:
- The administrator enables quarantine and sets quarantine type to **per-user** on the **BASIC > Quarantine** page. For more information on enabling quarantine, refer to *Managing Inbound Quarantine*, page 83.
- The Barracuda Spam & Virus Firewall receives an email that needs to be quarantined, which triggers creation of the account.

The Barracuda Spam & Virus Firewall automatic account creation process is as follows:

1. Checks the recipient email address against the **Local** database or the **LDAP** server as specified at the per-domain level on the **USERS > Single Sign-On** page (Barracuda Spam & Virus Firewall 400 and higher), as well as the **Explicit Users to Accept For** text box on the **USERS > Valid Recipients** page. To increase security, you can configure the Barracuda Spam & Virus Firewall to validate the receiving email address (using LDAP or the SMTP command RCPT TO) before it creates an account. This helps prevent the Barracuda Spam & Virus Firewall from creating accounts for invalid users.

2. Creates a new account with *User* level permissions (See *Role-based Administration*, page 96 for more information about account roles and permissions) for the recipient if the address does not exist. The Barracuda Spam & Virus Firewall uses the email address of the recipient as the username of the account and auto-generates a password.

3. If **Single Sign-On** is **not** enabled, the Barracuda Spam & Virus Firewall sends the account holder an email with the login information so they can access their quarantine inbox. With **Single Sign-On** enabled, the account holder will be able to log into the Barracuda Spam & Virus Firewall with their regular network credentials.

4. Places the quarantined message in the account holders’s quarantine inbox.

5. Sends a quarantine summary report to the account holder.

---

**Note**

The settings chosen in the **Default User Features** section of the **USERS > User Features** page are applied to all new accounts that are created.
When to Disable Automatic Creation of Accounts

If your LDAP server is running slowly, email will still be processed by the Barracuda Spam & Virus Firewall but unavailability of your LDAP server could result in creation of invalid quarantine accounts for unverified users on the Barracuda Spam & Virus Firewall. In this case it may be preferable to disable automatic account creation by setting the New User Quarantine State to Off from the BASIC > Quarantine page. User accounts can be manually created in bulk as described below.

Another reason to disable automatic creation of accounts is that you may not want all of your users to have quarantine inboxes to manage, access to whitelist/blocklist capabilities, etc. In that case, you can manually create user accounts for those individuals for whom it is appropriate, as described in the next section.

Manually Creating User Accounts

In addition to the two cases mentioned above, you will want to manually create user accounts with the USERS > User Add/Update page when you want to override the default quarantine, virus and spam checking settings for specific account holders. Creating the account before the Barracuda Spam & Virus Firewall automatically creates it enables you to initially configure the account settings if they are different from the default settings for other users.

The Barracuda Spam & Virus Firewall allows for account holders to manage various aspects of spam and virus checking and whitelist/blocklist behavior for their email without having to have a quarantine inbox on the appliance. By doing this you can enable global quarantine, but create per-user settings for user control of spam and virus checking features.

For example, if you want your users to be able to maintain their own whitelists and blocklists of email addresses and domains, but you don’t want to use resources on the Barracuda Spam & Virus Firewall to store quarantine messages, or you don’t want to have to train or depend on users to manage their quarantine inboxes, you can easily create accounts from the USERS > User Add/Update page for one or more users and disable their quarantine inbox(es). Then, on the USERS > User Features page, enable the features over which you want those users to have control by entering the same list of new account names (email addresses) in the User Account(s): text box in the User Features Override section of the page.

Account Creation by Users

Another way to manually create accounts on the Barracuda Spam & Virus Firewall is to use the Create New Password button on the login page which new users can click to create an account with their email address as their username. Their password will be emailed to the email address they enter in the username field.

Single Sign-On and User Authentication

Single Sign-On is a per-domain setting on the Barracuda Spam & Firewall, and if Single Sign-On is enabled for a particular domain, account holders associated with that domain can log into the Web interface of the Barracuda Spam & Virus Firewall with their regular network credentials to manage their accounts.

If enabling Single Sign-On for a domain, you should also configure HTTPS/SSL Access Only at the global level on the ADVANCED > Secure Administration page to protect the transmission of network passwords. See Enabling SSL for Administrators and Users, page 38 to configure SSL on the Barracuda Spam & Virus Firewall 400 and higher.
Assigning Features to User Accounts

The **USERS > User Features** page enables the administrator to enable or disable user control over their account settings:

- For newly created accounts, in the **Default User Features** section of the page
- For existing accounts, in the **User Features Override** section of the page

These features provide the user’s ability to enable or disable the following:

- Whitelist/blocklist of email addresses and domains
- Quarantine inbox
- Notification settings - email address for receiving a quarantine summary report, and notification intervals
- Use of a personal Bayesian database
- Spam scanning (on/off)
- Setting spam tag, quarantine and block score levels (Barracuda Spam & Virus Firewall 600 and higher)

For all of the user features enabled by the administrator, the **Domain Admin** account role can override the global setting and disable any **Default User Features** for newly created accounts. **BOTH** the **Domain Admin** and **Helpdesk** account roles can override the global settings for existing accounts in the **User Features Override** section of the **USERS > User Features** page on a per-domain basis.

To enable account holders (including **Domain Admin**, **Helpdesk** and **User** roles) to edit preferences/user features for their accounts, make sure that the **Enable User Features** setting on the **BASIC > Quarantine** page is turned **On**.

One of the most common scenarios for overriding quarantine settings is when you want to provide a few “power”users with a quarantine inbox on the Barracuda Spam & Virus Firewall, with the rest of your users receiving quarantined messages in their standard email inbox. Those quarantined messages will have a tag prepended to the subject line indicating that the Barracuda Spam & Virus Firewall suspects the message to be spam. See **How Quarantine of Inbound Mail Works**, page 84 for more information.

Role-based Administration

Roles and Navigating the Web Interface

Depending on the login role, the links in the upper right corner of the web interface will indicate the login name and, if in the domain level scope, the domain being managed, or the name of the user account. The administrator can step into the domain level scope of the web interface, which is what the **Domain Admin** and **Helpdesk** roles will see, from the **DOMAINS** page, by selecting a domain to manage. The **DOMAINS** page represents the “top level” of navigation of the Web interface for **Domain Admin** and **Helpdesk** roles, as shown in **Figure 10.2**.

The **Auditor** role is different than the others in that there are only two pages in the web interface that are visible: the **Outbound Quarantine** page and the **Password** page.
Clicking on **Manage Domain** enables managing domain-level settings and user accounts for that domain. The **Domain Admin** or **Helpdesk** role can “drill down” another level by selecting an account associated with that domain to edit from the **USERS > Account View** page (see Figure 10.3). Editing an account displays the quarantine inbox and preferences for the account, which is what the **User** role sees. **Domain Admin** and **Helpdesk** roles can also edit their own personal account settings and quarantine inboxes.

**Figure 10.3:** Drilling down from the **DOMAINS** page to account level
Editing Accounts and Assigning Roles

From the **USERS > Account View** page in the global scope, the administrator can manage accounts (other than the **Auditor** account) for all domains on the Barracuda Spam & Virus Firewall, editing account roles, deleting invalid accounts as needed and changing account passwords. The **USERS > Account View** page displays role types and whether or not each account has quarantine enabled. Role permissions are described in the next section. The **Auditor** account is managed from the **BASIC > Administration** page.

**Figure 10.5: Account View from global scope as seen by the administrator.**

Note that links in the upper right of the page always indicate the login name of the current account holder, the **Log Off** link and, if applicable, links to manage the system, domains or user accounts.

Clicking **Edit Role** brings up the **Edit Role** page, as shown in **Figure 10.6** for changing the account role from **User** (the default) to **Helpdesk** or **Domain Admin** and assigning domains for **Helpdesk** and **Domain Admin** account holders to manage.

To grant a **Helpdesk** or **Domain Admin** role permissions to manage **ALL** domains configured on the Barracuda Spam & Virus Firewall, put the phrase "all_domains" in the **Managed domains for:** text box on the **Edit Role** page for that account as shown in **Figure 10.7** instead of listing individual domains to manage.
User Role

This is the default role assigned to newly created accounts and only provides the account holder with a view of their quarantine inbox and some account preference settings, depending on what has been enabled for their account. Permissions may include:

- Modify individual settings for quarantine, spam tag, quarantine and block levels.
- Management of quarantine inbox - deliver, whitelist, delete quarantined messages.
- Change password (if Single Sign-On authentication is not configured).
- Create whitelists and blocklists for email addresses and domains.
- Manage a personal Bayesian database.

If granted the permission, the User role can disable quarantine for their account such that all messages quarantined for that account holder’s email address(es) by the Barracuda Spam & Virus Firewall will be delivered to their regular email inbox. The User account holder will see the following page upon..
login, with option to set preferences (see Assigning Features to User Accounts, page 96) and manage their quarantine inbox of messages. See also Using Per-user Quarantine, page 86.

Figure 10.8: User role view of web interface, displaying the Quarantine inbox

Helpdesk Role

This role is available for the Barracuda Spam & Virus Firewall 300 and higher and can manage basic account settings for accounts associated with one or more domains and assist users with managing their quarantine inboxes. This role has the User level permissions plus the ability to:

- Override account settings for existing accounts for the domain(s) the Helpdesk account holder has permissions to manage. The administrator can enable the Helpdesk role to expand or limit user control over their spam scoring, whitelist/blocklist, quarantine enable/disable, notification and Bayesian filtering settings.
- View the Message Log for the domain(s) managed and deliver quarantined messages. The Helpdesk role cannot, however, view the body of messages in the Message Log.
- Log into an account with lesser permissions and manage the associated quarantine inbox - deliver, whitelist or delete messages.
- View domain-level status and reports (with the exception of the daily Traffic Summary, which can only be generated at the global level by the administrator).
- Edit account roles for account holders with lesser permissions.

Helpdesk Role - All_Domains Permissions

The Helpdesk role has the above permissions for ALL domains configured on the Barracuda Spam & Virus Firewall if the Managed domains for: text box on the USERS > Account View > Edit Role page for this account holder includes the phrase "all_domains" (see Figure 10.7).

A Helpdesk account holder with all_domains permission can also do the following:

- Change the role of a Helpdesk account holder (to the User role) who does not have all_domains permissions.
- Log into and manage the quarantine inbox of a Helpdesk or a Domain Admin who does not have all_domains permissions

If the Helpdesk account holder only administers a subset of all domains configured on the Barracuda Spam & Virus Firewall, only those domains will appear in the DOMAINS page. Here, the Helpdesk account only administers two domains:
Clicking on the **Manage Domain** link will show a subset of the web interface. The **Helpdesk** role sees basic email statistics, can view reports and the Message Log for the selected domain and manage the quarantine inbox and settings for other account holders, depending on their permissions level.

**Figure 10.10:** A Helpdesk account holder has a limited view of per-domain data and accounts

From the **USERS > Account View** page, the **Helpdesk** account holder can view and edit accounts and quarantine inboxes for the domain or manage their own account.

**Figure 10.11:** On the **USERS > Account View** page, the Helpdesk role sees a list of the accounts associated with the domain

For any account holders listed for the domain, the **Helpdesk** account holder can manage the quarantine inbox and some account settings, as described above.
Example Helpdesk Use Cases

- Disabling quarantine on the USERS > Add/Edit page for one or more users for reasons such as the following:
  - You don’t want to use Barracuda Spam & Virus Firewall resources to store quarantined email, but you want your users to maintain their own whitelists and blocklists of email addresses and domains.
  - Users don’t want to maintain two inboxes, but want to control spam scoring and quarantine notification intervals for their incoming email.
- A User account holder needs help changing their password.
- A user needs to know why email from a particular address is getting blocked by the Barracuda Spam & Virus Firewall and the Helpdesk role can:
  - View the reason for blocking on the BASIC > Message Log page.
  - Deliver the message if necessary

Domain Admin Role

The Domain Admin role is available on the Barracuda Spam & Firewall 600 and higher and can configure all domain settings for designated domains as well as account settings for account holders who have lesser permissions. This role includes Helpdesk level permissions and use cases as described above plus the ability to:

- View message contents (if privacy settings allow) for designated domains.
- Enable or disable per-user quarantine at the domain level and, if per-user quarantine is disabled, specify a global quarantine email address for designated domains.
- Enable or disable various Default User Features for new accounts (see Controlling Access to Account Features, page 87) for designated domains.

Domain Admin Role - All_Domains Permissions

The Domain Admin role has the above permissions for ALL domains configured on the Barracuda Spam & Virus Firewall if the Managed domains for: text box on the USERS > Account View > Edit Role page for this account holder includes the phrase "all_domains". In this case, all domains for which the Barracuda Spam & Virus Firewall filters email will appear in the DOMAINS page.

A Domain Admin account holder with all_domains permission can also do the following:

- Create or change the role of a Domain Admin account holder who does not have all_domains permissions.
- Log into and manage the quarantine inbox of a Domain Admin who does not have all_domains permissions.
- Create or edit a Helpdesk account with all_domains permissions.

Navigation of the web interface for the Domain Admin role follows the examples illustrated above for the Helpdesk role, plus the following.
Use Case Scenarios For Role Assignments

#1. Role Requirements: An account that will be able to:

- Monitor all configured domains
- Give others the ability to configure individual domain settings
- Will *not* be able to view message content
- Configure domain settings

Solution: Create a Helpdesk account with **all_domains** permissions.

#2. Role Requirements: An account that will be able to:

- Monitor all configured domains
- Create (only) end user accounts
- Will *not* be able to view message content or configure domain settings

Solution: Create a Helpdesk account that does *not* have **all_domains** permissions (this prevents the ability to create other Domain Admin or Helpdesk accounts). Then manually associate all domains with this account by listing each domain on a separate line in the **Domains Managed** text box. This will allow monitoring of all domain traffic.

#3. Role Requirements: An account that can configure settings on all domains configured on your Barracuda Spam & Virus Firewall, but cannot create or edit other accounts with the Domain Admin role.

Solution: Create a Domain Admin account that does *not* have **all_domains** permissions (this prevents the ability to create other Domain Admin accounts). Then manually associate all of the domains on the Barracuda Spam & Virus Firewall with this account by listing each domain on a separate line in the **Domains Managed** text box. This will allow configuration of all domain settings.

### Auditor Account

The *Auditor* account is a unique account to be given to a trusted individual in the organization. This account can monitor and manage outgoing messages that have been quarantined due to policy. For example, if company policy requires the banning of certain keywords in outgoing messages, the *Auditor* can scan outgoing messages quarantined for content to determine if they are valid or not. If
so, the *Auditor* can decide to deliver the message. If not, the *Auditor* can either reject the message, with a notification being sent to the sender, or just delete the message with no notification sent.

This account is always ‘available’ for use on the Barracuda Spam & Virus Firewall, but must be enabled from the **BASIC > Administration** page. Once it is enabled, the person assuming this role logs in with the default login and password for the account, both of which are *auditor*. When the *Auditor* logs in, the password can be changed from the **Password** page. Thus, there is always only one login and password pair for this account. If the password is lost, please contact Barracuda Networks Technical Support.

The account can be disabled from the **BASIC > Administration** page. If so, the next time the account is enabled, the password will be reset to the default value.
Chapter 11

Monitoring the System

This chapter describes the monitoring and diagnostic tools provided on the Barracuda Spam & Virus Firewall Web interface for the administrator to track system performance and troubleshoot issues.

Viewing Performance Statistics .............................................................. 106
The Message Log .............................................................................. 108
Setting up Alerts .............................................................................. 109
Reporting .......................................................................................... 111
Using the Barracuda Control Center .................................................. 112
Diagnostic Tools .............................................................................. 114
Using a Syslog Server to Centrally Monitor System Logs ................. 114
Front Panel Indicator Lights ............................................................. 115
Viewing Performance Statistics

The **BASIC > Status** page provides an overview of the health and performance of your Barracuda Spam & Virus Firewall, including:

- Hourly and daily email statistics that display the number of viruses blocked and messages rate controlled (deferred), blocked, quarantined, tagged (inbound only), sent (outbound only) and allowed (inbound only) for the last 24 hours and 28 days.
- The subscription status of Energize Updates.
- Performance statistics, including CPU temperature and system load. Performance statistics displayed in red signify that the value exceeds the normal threshold. These values will fluctuate based on the amount of traffic that is being handled, but if any setting remains consistently in the red for a long period of time, please contact Barracuda Networks Technical Support.

If the **Mail/Log Storage** rises above 75%, this indicates that more disk space has been taken up by the message and log storage than is allocated for that purpose and you should contact Barracuda Networks Technical Support.

If per-user quarantine is enabled and system performance has decreased, check the **Quarantined** number of messages shown in the Email Statistics [inbound] pane on the **BASIC > Status** page. If this number is high, changing the Retention Policies for per-user quarantine on the **USERS > Retention Policies** page may solve the problem. See **Retention Policy and Purging Old Messages** on page 89 for details and warnings about deleting large amounts of messages.

On the Barracuda Spam & Virus Firewall 600 and higher, if a disk drive in the RAID array exhibits a problem, the **Redundancy (RAID)** indicator will highlight in red and show one of the drives as **degraded** with a link **Click To Repair**. Clicking this link will display a pop-up indicating the drive to replace and an **Ok** button and a **Cancel** button. You must first replace the disk drive that indicates a problem before proceeding with the repair operation. Please contact Barracuda Networks Technical Support if you need assistance.

Inbound and Outbound Message Queues

You can view the mail queues from the **BASIC > Status** page with the **In/Out Queue Size** link.

![Performance Statistics](image)

The number of current inbound messages (In) plus accepted messages waiting for virus and spam scanning is shown, separated by a “/”, from the number of messages in the outbound queue (Out) waiting for the outbound server. Click either number to view a summary of the messages currently in the queues.

**To view the queues in a Message Log format**, with the ability to filter, requeue, delete and view details of selected queued messages, use the **ADVANCED > Queue Management** page.

**Retrying All Outbound Messages**

If the outbound queue number is high, the mail server could be down or there could be another network issue. Messages in the outbound queue will automatically expire if not successfully delivered within 48 hours (default). This may happen normally if the destination mail server rejects email based on mail server policy and the message is bounced back to the sender.
To requeue, or retry delivering ALL email messages in the out queue, click the **Retry** button at the bottom of the **BASIC > Administration page** to retry sending the messages immediately. The button will then be disabled until the requeue process has completed. To requeue, or retry delivering selected email messages in the out queue, use the **ADVANCED > Queue Management** page.

**Note that alerts and notifications are queued separately from email** so that the administrator can be alerted if the out message queue is high.
The Message Log

The BASIC > Message Log page displays details about all email traffic that passes through the Barracuda Spam & Virus Firewall. Message source and analysis is viewable by clicking on a message, and includes spam scoring and Bayesian analysis, if enabled.

This data is captured initially in the Mail Syslog and appears on the mail facility at the debug priority level on the specified syslog server.

The Message Log is a window into how the current spam and virus settings are filtering email coming through the Barracuda Spam & Virus Firewall, and sorting data using the wide variety of filters can quickly provide a profile of email by allowed, tagged, quarantined or blocked messages by domain, sender, recipient, time, subject, size, reason for action taken or score.

Watch the Message Log after making changes to the spam and virus settings to determine if the Barracuda Spam & Virus Firewall spam checking and quarantine behavior is tuned per the needs of your organization. See Monitor and Classify Incoming Emails on page 39 for more information about using the Message Log.
Setting up Alerts

Setting up Emailed System Alerts

The **BASIC > Administration** page allows you to configure the Barracuda Spam & Virus Firewall to automatically email *system* notifications and alerts to the email address(es) you specify. To enter multiple addresses, separate each address with a comma. Note that notifications are queued separately from outbound messages.

System alerts are sent from the Barracuda Spam & Virus Firewall to the **System Alerts Email Address(es)** you specify when a system issue triggers an automated alert, including:

- LDAP lookup or server errors. This alert email is sent once per day reporting LDAP errors logged over the past 24 hours. A few errors may not be indicative of a problem, but more than a few may mean that there is mail that is being blocked for one or more invalid recipients.
- Failure of an automated backup. The email will indicate the cause of failure, such as, for example, the backup server is not available, invalid username or invalid password. Check the settings on the **ADVANCED > Backup** page in the **Automated Backups** section.

Notifications are sent from Barracuda Central to the **System Contact Email Address** when:

- Your Energize Update subscription is about to expire
- Problems arise with RAID disk storage
- New security bulletins are available

Setting up SNMP Query and Alerts

While the Barracuda Spam & Virus Firewall will send email alerts to the **System Alerts Email Address** specified on the **BASIC > Administration** page, these alerts are limited and do not include latency, inqueue sizes, and other similar information. To monitor more specific information on a Barracuda Spam & Virus Firewall, Barracuda Networks recommends using SNMP monitoring with an SNMP server.

The Barracuda Spam & Virus Firewall 400 and higher offers the ability to monitor various settings via SNMP, including:

- System statistics, such as:
  - inbound/outbound queue size
  - average email latency
  - encrypted, blocked, quarantined and tagged messages based on spam, custom policy, virus, etc. (outbound mail included)
  - appliance uptime
- Performance statistics, including mail/log storage, CPU temperature and system load.

To query the Barracuda Spam & Virus Firewall for these statistics via SNMP, you must first enable the SNMP agent, specify the SNMP version you’re using, the community string, and enter the IP address of the server(s) that will be making the SNMP connection in the **SNMP Manager** section of the **BASIC > Administration** page.

For details about configuring SNMP with the Barracuda Spam & Virus Firewall, see the technical paper *SNMP Monitoring for the Barracuda Spam & Virus Firewall 5.x* at...
**Generating System Reports**

The Barracuda Spam & Virus 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.

Reports can be created for data collected at the global level as well as at the per-domain level. You can run reports and configure report settings from the `BASIC > Reporting` page, and online help for that page includes a table listing all reports, the kind of data each report includes for inbound and/or outbound mail, and types of graphs available. You can either generate a system report on demand or schedule reports for regular delivery to specific users.

On demand reports can cover data for a specified date range, but generating a report to view instead of to send as an email can potentially consume excessive system resources on the Barracuda Spam & Virus Firewall. For this reason, discretion should be used when deciding on the date range a given report is to cover. To minimize impact of report generation on the Barracuda Spam & Virus Firewall performance, reports of over 7 days in length can only be generated through email.

**Automating the Delivery of Scheduled System Reports**

The **Reporting Email Options** section of the `BASIC > Reporting` page lets you configure the Barracuda Spam & Virus Firewall to automatically deliver system reports daily, weekly or monthly to specific users by entering their email addresses in the field next to each report type.

You can enter as many email 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 email address next to that report type.

Each scheduled report covers traffic for one day only. The **Daily Traffic** report is a good status reporting tool and is only available to administrators. Having it emailed to your mail box every day is helpful for monitoring the system.
Using the Barracuda Control Center

The Barracuda Control Center enables administrators to manage, monitor and configure multiple Barracuda Spam & Virus Firewalls (firmware version 5.0 and higher) at one time from one console. If you are using the Cloud Protection Layer feature of the Barracuda Spam & Virus Firewall, you will manage it using the Barracuda Control Center (see Cloud-Based Protection on page 69 for details).

The same tabbed pages are available on the Barracuda Control Center for managing all aspects of your Barracuda Spam & Virus Firewall configuration that you see in each individual Web interface, and you can create aggregated reports for multiple Barracuda Spam & Virus Firewalls from the Barracuda Control Center console. You can connect one or more Barracuda Spam & Virus Firewalls to the Barracuda Control Center by doing the following:

1. If you don't already have an account with Barracuda Networks, visit http://www.barracudanetworks.com and click the Customer Login button to create one.

2. On the Sign In page, click the Create a new account link. Enter your name and contact information. Make a note of the username (email address) and password you chose.

3. Log into your Barracuda Spam & Virus Firewall as the administrator. From the ADVANCED > Firmware Upgrade page, check to make sure you have the latest firmware installed. If not, download and install it now.

4. From the ADVANCED > Control Center page, enter the Barracuda Networks username and password you created and click Yes to connect to the Barracuda Control Center. Note that your Barracuda Spam & Virus Firewall can connect with only one Barracuda Control Center account at a time.

5. Log into the Barracuda Control Center with your username and password and you will see your Barracuda Spam & Virus Firewall statistics displayed on the BASIC > Status page. To access the Web interface of your Barracuda Spam & Virus Firewall, click on the link in the Products column in the Control Center pane on the left side of the page. Or you can click on the product name in the Product column of the Unit Health pane on the right side of the page.

6. Follow steps 3 and 4 to connect every subsequent Barracuda Spam & Virus Firewall to the Barracuda Control Center.

7. To stop the synchronization between your Barracuda Spam & Virus Firewall and the Barracuda Control Center, from the ADVANCED > Control Center page on the Barracuda Spam & Virus Firewall, enter the Barracuda Control Center username and password for the particular account associated with that device and click No for Connect to Barracuda Control Center. Do this when you know that there will be a loss of connectivity between the Barracuda Spam & Virus Firewall and the Barracuda Control Center due to the appliance being physically moved or other network connectivity issues.

Note that reports cannot be emailed using the Barracuda Control Center.

For more information about using the Barracuda Control Center, see the Barracuda Control Center Administrator’s Guide at http://www.barracuda.com/documentation.
Using the Task Manager to Monitor System Tasks

The **ADVANCED > Task Manager** page provides a list of tasks that are in the process of being performed and displays any errors encountered when performing these tasks. Some of the tasks that the Barracuda Spam & Virus Firewall tracks include:

- Clustered environment setup
- Configuration and Bayesian data restoration
- Removal of invalid users

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 automatically phased out over time.
Troubleshooting

Diagnostic Tools

Testing Network Connectivity

The Barracuda Spam & Virus Firewall Web interface provides a suite of tools to help diagnose potential network problems, including ping, telnet, dig/NS-lookup, TCP dump and traceroute. See the online help on the Network Connectivity Tests section of the ADVANCED > Troubleshooting page for details about using these tools.

Connect to Barracuda Support Servers

In the Support Diagnostics section of the ADVANCED > Troubleshooting page, you can initiate a connection between your Barracuda Spam & Virus Firewall and the Barracuda Networks Technical Support Center which will allow technical support engineers to troubleshoot any issues you may be experiencing.

Using a Syslog Server to Centrally Monitor System Logs

Use the ADVANCED > Networking page to specify a server to which the Barracuda Spam & Virus Firewall sends syslog data. 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.

The Web Syslog data contains information about user login activities and any configuration changes made on the machine. This syslog data appears on the local facility with login information at the info priority level, and configuration changes appear at the debug priority level on the specified syslog server.

The Mail Syslog captures data related to mail flow and is the same information as that used to build the Message Log in the Barracuda Spam & Virus Firewall. The Mail Syslog includes data such as the connecting IP, envelope 'From' address, envelope 'To' address, and the spam score for the messages transmitted. This syslog data appears on the mail facility at the debug priority level on the specified syslog server.

See the Syslog Configuration section of the ADVANCED > Troubleshooting page for the facility to open a window and view the Mail Syslog or Web Syslog output. For details about using the Barracuda syslog with the Barracuda Spam & Virus Firewall, see the technical paper Syslog and the Barracuda Spam & Virus Firewall 4.x at http://www.barracudanetworks.com/documentation
Front Panel Indicator Lights

The Barracuda Spam & Virus Firewall has five indicator lights on the front panel that blink when the system processes any message. Figure 11.1 displays the location of each of the lights.

Figure 11.1: Barracuda Spam & Virus Firewall front panel indicator lights
This chapter provides instructions for general maintenance of the Barracuda Spam & Virus Firewall using the Web interface, and covers the following topics:

- Updating the Firmware and Definitions ........................................... 118
- Backing up and Restoring Your System ........................................... 119
- Reloading, Restarting, and Shutting Down the System ..................... 121
- Using the Built-in Troubleshooting Tools ........................................ 122
- Rebooting the System in Recovery Mode ........................................ 123
Updating the Firmware and Definitions

Updating the Firmware on your Barracuda Spam & Virus Firewall

This should be one of the steps the administrator performs in the initial installation of the Barracuda Spam & Virus Firewall. The ADVANCED > Firmware Update page 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.

Updating the Firmware of Clustered Systems

If a system is part of a cluster, we recommend changing the system’s Mode in the Clustered Systems section of the ADVANCED > Clustering page to Standby before you upgrade its firmware, and then repeat this process on each system in the cluster. Once the firmware on each system has been upgraded, you can then change the mode on each system back to Active.

Changing a clustered system to Standby mode before upgrading prevents a system on a more recent firmware version from trying to synchronize its configuration with a system on an earlier firmware version. If you have the latest firmware version already installed, the Download Now button on the ADVANCED > Firmware Update page is disabled.

The current firmware version shows in the top section of the page, with the latest General Release version of the firmware shown below in the Firmware Download section. To download the latest firmware version, click the Download Now button. The Web interface will display download progress. When the firmware download is complete, click the Apply Now button. The Barracuda Spam & Virus Firewall will reboot and you will need to log in again to the Web interface.

Updating the Definitions from Energize Updates

This should be one of the steps the administrator performs in the initial installation of the Barracuda Spam & Virus Firewall. The ADVANCED > Energize Updates page allows you to manually update the Virus, Policy, and Security Definitions used on your Barracuda Spam & Virus Firewall or to have them updated automatically. Barracuda Networks recommends that the Automatic Updates option be set to On for all three types of definitions so that your Barracuda Spam & Virus Firewall receives the latest rules as soon as they are made available by Barracuda Networks.

Important: If you are using the Barracuda Exchange Anti-Virus Add-in with your MS Exchange mail server, make SURE to set the Automatic Updates option to On in the Virus Definition Updates section of the ADVANCED > Energize Updates page. This is necessary to ensure that the add-in receives constant updates of virus signatures from the Barracuda Spam & Virus Firewall.

Note

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours. Before upgrading, BE SURE TO TAKE THE Barracuda Spam & Virus Firewall OFFLINE. This will ensure that the inbound mail queue is emptied and all messages are scanned before the upgrade process begins. DO NOT MANUALLY REBOOT YOUR SYSTEM at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support.

The current firmware version shows in the top section of the page, with the latest General Release version of the firmware shown below in the Firmware Download section. To download the latest firmware version, click the Download Now button. The Web interface will display download progress. When the firmware download is complete, click the Apply Now button. The Barracuda Spam & Virus Firewall will reboot and you will need to log in again to the Web interface.

Note

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours. Before upgrading, BE SURE TO TAKE THE Barracuda Spam & Virus Firewall OFFLINE. This will ensure that the inbound mail queue is emptied and all messages are scanned before the upgrade process begins. DO NOT MANUALLY REBOOT YOUR SYSTEM at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support.

The current firmware version shows in the top section of the page, with the latest General Release version of the firmware shown below in the Firmware Download section. To download the latest firmware version, click the Download Now button. The Web interface will display download progress. When the firmware download is complete, click the Apply Now button. The Barracuda Spam & Virus Firewall will reboot and you will need to log in again to the Web interface.

Note

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours. Before upgrading, BE SURE TO TAKE THE Barracuda Spam & Virus Firewall OFFLINE. This will ensure that the inbound mail queue is emptied and all messages are scanned before the upgrade process begins. DO NOT MANUALLY REBOOT YOUR SYSTEM at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support.

The current firmware version shows in the top section of the page, with the latest General Release version of the firmware shown below in the Firmware Download section. To download the latest firmware version, click the Download Now button. The Web interface will display download progress. When the firmware download is complete, click the Apply Now button. The Barracuda Spam & Virus Firewall will reboot and you will need to log in again to the Web interface.

Note

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours. Before upgrading, BE SURE TO TAKE THE Barracuda Spam & Virus Firewall OFFLINE. This will ensure that the inbound mail queue is emptied and all messages are scanned before the upgrade process begins. DO NOT MANUALLY REBOOT YOUR SYSTEM at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support.

The current firmware version shows in the top section of the page, with the latest General Release version of the firmware shown below in the Firmware Download section. To download the latest firmware version, click the Download Now button. The Web interface will display download progress. When the firmware download is complete, click the Apply Now button. The Barracuda Spam & Virus Firewall will reboot and you will need to log in again to the Web interface.

Note

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours. Before upgrading, BE SURE TO TAKE THE Barracuda Spam & Virus Firewall OFFLINE. This will ensure that the inbound mail queue is emptied and all messages are scanned before the upgrade process begins. DO NOT MANUALLY REBOOT YOUR SYSTEM at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support.

The current firmware version shows in the top section of the page, with the latest General Release version of the firmware shown below in the Firmware Download section. To download the latest firmware version, click the Download Now button. The Web interface will display download progress. When the firmware download is complete, click the Apply Now button. The Barracuda Spam & Virus Firewall will reboot and you will need to log in again to the Web interface.

Note

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours. Before upgrading, BE SURE TO TAKE THE Barracuda Spam & Virus Firewall OFFLINE. This will ensure that the inbound mail queue is emptied and all messages are scanned before the upgrade process begins. DO NOT MANUALLY REBOOT YOUR SYSTEM at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support.

The current firmware version shows in the top section of the page, with the latest General Release version of the firmware shown below in the Firmware Download section. To download the latest firmware version, click the Download Now button. The Web interface will display download progress. When the firmware download is complete, click the Apply Now button. The Barracuda Spam & Virus Firewall will reboot and you will need to log in again to the Web interface.

Note

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours. Before upgrading, BE SURE TO TAKE THE Barracuda Spam & Virus Firewall OFFLINE. This will ensure that the inbound mail queue is emptied and all messages are scanned before the upgrade process begins. DO NOT MANUALLY REBOOT YOUR SYSTEM at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support.

The current firmware version shows in the top section of the page, with the latest General Release version of the firmware shown below in the Firmware Download section. To download the latest firmware version, click the Download Now button. The Web interface will display download progress. When the firmware download is complete, click the Apply Now button. The Barracuda Spam & Virus Firewall will reboot and you will need to log in again to the Web interface.

Note

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours. Before upgrading, BE SURE TO TAKE THE Barracuda Spam & Virus Firewall OFFLINE. This will ensure that the inbound mail queue is emptied and all messages are scanned before the upgrade process begins. DO NOT MANUALLY REBOOT YOUR SYSTEM at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support.

The current firmware version shows in the top section of the page, with the latest General Release version of the firmware shown below in the Firmware Download section. To download the latest firmware version, click the Download Now button. The Web interface will display download progress. When the firmware download is complete, click the Apply Now button. The Barracuda Spam & Virus Firewall will reboot and you will need to log in again to the Web interface.

Note

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours. Before upgrading, BE SURE TO TAKE THE Barracuda Spam & Virus Firewall OFFLINE. This will ensure that the inbound mail queue is emptied and all messages are scanned before the upgrade process begins. DO NOT MANUALLY REBOOT YOUR SYSTEM at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support.

The current firmware version shows in the top section of the page, with the latest General Release version of the firmware shown below in the Firmware Download section. To download the latest firmware version, click the Download Now button. The Web interface will display download progress. When the firmware download is complete, click the Apply Now button. The Barracuda Spam & Virus Firewall will reboot and you will need to log in again to the Web interface.

Note

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours. Before upgrading, BE SURE TO TAKE THE Barracuda Spam & Virus Firewall OFFLINE. This will ensure that the inbound mail queue is emptied and all messages are scanned before the upgrade process begins. DO NOT MANUALLY REBOOT YOUR SYSTEM at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support.

The current firmware version shows in the top section of the page, with the latest General Release version of the firmware shown below in the Firmware Download section. To download the latest firmware version, click the Download Now button. The Web interface will display download progress. When the firmware download is complete, click the Apply Now button. The Barracuda Spam & Virus Firewall will reboot and you will need to log in again to the Web interface.

Note

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours. Before upgrading, BE SURE TO TAKE THE Barracuda Spam & Virus Firewall OFFLINE. This will ensure that the inbound mail queue is emptied and all messages are scanned before the upgrade process begins. DO NOT MANUALLY REBOOT YOUR SYSTEM at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support.

The current firmware version shows in the top section of the page, with the latest General Release version of the firmware shown below in the Firmware Download section. To download the latest firmware version, click the Download Now button. The Web interface will display download progress. When the firmware download is complete, click the Apply Now button. The Barracuda Spam & Virus Firewall will reboot and you will need to log in again to the Web interface.

Note

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours. Before upgrading, BE SURE TO TAKE THE Barracuda Spam & Virus Firewall OFFLINE. This will ensure that the inbound mail queue is emptied and all messages are scanned before the upgrade process begins. DO NOT MANUALLY REBOOT YOUR SYSTEM at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support.

The current firmware version shows in the top section of the page, with the latest General Release version of the firmware shown below in the Firmware Download section. To download the latest firmware version, click the Download Now button. The Web interface will display download progress. When the firmware download is complete, click the Apply Now button. The Barracuda Spam & Virus Firewall will reboot and you will need to log in again to the Web interface.
Backing up and Restoring Your System

Backup Up

Three Types of Backups Available

The ADVANCED > Backup page lets you back up and restore three kinds of backup files for your Barracuda Spam & Virus Firewall:

- System configuration
- Bayesian databases - global and per-user (if your model supports per-user)
- Explicit Users to Accept For and Alias Linking data

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

To prepare the system for backing up, first configure your backup server information, then select which, if not all, backups you want to create, and, if desired, a schedule of automated backups on the ADVANCED > Backup page. If you are restoring a backup file on a new Barracuda Spam & Virus Firewall that is not configured, you first need to assign your new system an IP address and DNS information on the BASIC > IP Configuration page of the new system.

Important notes about backups:

- **Do not edit backup files.** Any configuration changes you want to make need to be done through the Web interface. The configuration backup file contains a checksum that prevents the file from being uploaded to the system if any changes are made.
- You can safely view a backup file in Windows WordPad or TextPad. You should avoid viewing backup files in Windows Notepad because the file can become corrupted if you save the file from this application.
- **Information not backed up with the system configuration file** includes system password, system IP information, DNS information and clustering settings. For a complete list of settings that are not backed up, please see the online help of the ADVANCED > Backup page.
- For Automated Backups, you must select a server type. If you select FTP, note the following. The Barracuda Spam & Virus Firewall, by default, initiates ftp in passive mode. If your backup times out, and your ftp server is running in passive mode, and you have a firewall between your Barracuda Spam & Virus Firewall and your ftp server, you may need to open ports on your firewall to allow passive-mode ftp connections. The port range depends on your ftp server configuration. Ideally, the firewall should be configured so that only that range of ports is accessible to the ftp server machine. Make sure that there aren't any other TCP services with port numbers in the port range listening on the ftp server machine.
Restoring a Backup

Restoring a backup simply requires browsing your local system with the click of a button on the **ADVANCED > Backup** page and selecting a backup file. Please see the online help on that page for details about restoring backups.

**Warning**

Do not restore a configuration file onto a machine that is currently part of a cluster. All cluster information will be lost and the units will need to be re-clustered if this happens.
Reloading, Restarting, and Shutting Down the System

The System Management/Shutdown section on the BASIC > Administration page allows you to shut down, restart, and reload system configuration on the Barracuda Spam & Virus Firewall. You can also take the system offline if necessary, which is recommended whenever you do a Firmware Update. A unit in Offline (Maintenance) mode will stop accepting incoming mail until it is put back online.

Shutting down the system powers off the unit. Restarting the system reboots the unit. Reloading the system re-applies the system configuration.

You can also perform a hard reset of the Barracuda Spam & Virus Firewall by pressing the RESET button on the front panel of the system. Caution should be used when pressing the reset button, however, since doing so while the Barracuda Spam & Virus Firewall is in the midst of a configuration update or other task can result in inadvertent corruption of the system.
Using the Built-in Troubleshooting Tools

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

For example, you can test your Barracuda Spam & Virus Firewall’s connection to the Barracuda Networks update servers to make sure that it can successfully download the latest Energize Update definitions. You can also ping other devices from the Barracuda Spam & Virus Firewall, perform a trace route from the Barracuda Spam & Virus Firewall to any another system, and execute various other troubleshooting commands.
Rebooting the System in Recovery Mode

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

Before you use the diagnostic and recovery tools, do the following:

• Use the built-in troubleshooting tools on the ADVANCED > Troubleshooting page to help diagnose the problem.
• 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 & Virus Firewall and run a memory test or perform a complete system recovery, as described below.

To perform a system recovery or hardware test:

1. Connect a monitor and keyboard directly to your Barracuda Spam & Virus Firewall.
2. Reboot the system by doing one of the following:
   • Click the Restart button on the BASIC > Administration page.
   • Press the Power button on the front panel to turn off the system, and then press the Power button again to turn the system back on.

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 three seconds, the Barracuda Spam & Virus Firewall defaults to starting up in the normal mode (first option).

   For a description of each boot option, refer to Reboot Options on page 123 below.

Note

To stop a hardware test, reboot your Barracuda Spam & Virus Firewall by pressing Ctrl-Alt-Del on the keyboard you’ve connected to the appliance.

Reboot Options

Table 12.1 describes the options available at the reboot menu.

Table 12.1: Reboot Options

<table>
<thead>
<tr>
<th>Reboot Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barracuda</td>
<td>Starts the Barracuda Spam &amp; Virus Firewall in the normal (default) mode. This option is automatically selected if no other option is specified within the first three (3) seconds of the splash screen appearing.</td>
</tr>
</tbody>
</table>
Replacing a Failed System

Before you replace your Barracuda Spam & Virus Firewall, use the tools provided on the ADVANCED > Troubleshooting page to try to resolve the problem, or call Barracuda Networks Technical Support.

Barracuda Instant Replacement Service

In the event that a Barracuda Spam & Virus Firewall fails and you cannot resolve the issue, customers that have purchased the Instant Replacement service can call Barracuda Networks Technical Support and arrange for a new unit to be shipped out within 24 hours.

After receiving the new system, ship the old Barracuda Spam & Virus Firewall back to Barracuda Networks at the address below with an RMA number marked clearly on the package. Barracuda Networks Technical Support can provide details on the best way to return the unit.

Barracuda Networks
3175 S. Winchester Blvd
Campbell, CA 95008

attn: RMA # <your RMA number>

Recovery Displays the Recovery Console where you can select the following options:

- Perform file system repair: Repairs the file system on the Barracuda Spam & Virus Firewall.
- Perform full system re-image: Restores the factory settings on your Barracuda Spam & Virus Firewall and clears out all configuration information.
- Enable remote administration: Initiates a connection to that allows Barracuda Networks Technical Support to access the system. Another method for enabling this troubleshooting connection is to click Establish Connection to Barracuda Networks 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 first.

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. Reboot your Barracuda Spam & Virus Firewall to stop the hardware test.

<table>
<thead>
<tr>
<th>Reboot Options</th>
<th>Description</th>
</tr>
</thead>
</table>
| Recovery       | Displays the Recovery Console where you can select the following options:
|                | - Perform file system repair: Repairs the file system on the Barracuda Spam & Virus Firewall.
|                | - Perform full system re-image: Restores the factory settings on your Barracuda Spam & Virus Firewall and clears out all configuration information.
|                | - Enable remote administration: Initiates a connection to that allows Barracuda Networks Technical Support to access the system. Another method for enabling this troubleshooting connection is to click Establish Connection to Barracuda Networks 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 first. |
| 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. Reboot your Barracuda Spam & Virus Firewall to stop the hardware test. |

Note To set up the new Barracuda Spam & Virus Firewall so it has the same configuration as your old failed system, first manually configure the new system’s IP information on the BASIC > IP Configuration page, and then restore the backup file from the old system onto the new system. For information on restoring data, refer to Backing up and Restoring Your System on page 119 in this chapter.
About the Hardware

Appendix A

Hardware Compliance

This section contains compliance information for the Barracuda Spam & Virus Firewall hardware.

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 in 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)

Power Requirements

AC input voltage 100-240 volts; frequency 50/60 Hz.
Limited Warranty

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 one (1) year: (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 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 ERROR-FREE, 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.

Software License

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("AGREEMENT") CAREFULLY BEFORE USING THE BARRACUDA SOFTWARE. BY USING THE BARRACUDA SOFTWARE YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE DO NOT USE THE SOFTWARE. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE YOU MAY RETURN THE SOFTWARE OR HARDWARE CONTAINING THE SOFTWARE FOR A FULL REFUND TO YOUR PLACE OF PURCHASE.

1. The software, documentation, whether on disk, in read only memory, or on any other media or in any other form (collectively "Barracuda Software") is licensed, not sold, to you by Barracuda Networks, Inc. ("Barracuda") for use only under the terms of this License and Barracuda reserves all rights not expressly granted to you. The rights granted are limited to Barracuda's intellectual property rights in the Barracuda Software and do not include any other patent or intellectual property rights. You own the media on which the Barracuda Software is recorded but Barracuda retains ownership of the Barracuda Software itself.

2. Permitted License Uses and Restrictions. This License allows you to use the Software only on the single Barracuda labeled hardware device on which the software was delivered. You may not make copies of the Software and you may not make the Software available over a network where it could be utilized by multiple devices or copied. You may not make a backup copy of the Software. You may not modify or create derivative works of the Software except as provided by the Open Source Licenses included below. The BARRACUDA SOFTWARE IS NOT INTENDED FOR USE IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, LIFE SUPPORT MACHINES, OR OTHER EQUIPMENT IN WHICH FAILURE COULD LEAD TO DEATH, PERSONAL INJURY, OR ENVIRONMENTAL DAMAGE.

3. You may not transfer, rent, lease, lend, or sublicense the Barracuda Software.
4. This License is effective until terminated. This License is automatically terminated without notice if you fail to comply with any term of the License. Upon termination you must destroy or return all copies of the Barracuda Software.

5. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT THE USE OF THE BARRACUDA SOFTWARE IS AT YOUR OWN RISK AND THAT THE ENTIRE RISK AS TO SATISFACTION, QUALITY, PERFORMANCE, AND ACCURACY IS WITH YOU. THE BARRACUDA SOFTWARE IS PROVIDED "AS IS" WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND BARRACUDA HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE BARRACUDA SOFTWARE, EITHER EXPRESSED OR IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR ANY APPLICATION, OF ACCURACY, AND OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS. BARRACUDA DOES NOT WARRANT THE CONTINUED OPERATION OF THE SOFTWARE, THAT THE PERFORMANCE WILL MEET YOUR EXPECTATIONS, THAT THE FUNCTIONS WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION WILL BE ERROR FREE OR CONTINUOUS, OR THAT DEFECTS WILL BE CORRECTED. NO ORAL OR WRITTEN INFORMATION GIVEN BY BARRACUDA OR AUTHORIZED BARRACUDA REPRESENTATIVE SHALL CREATE A WARRANTY. SHOULD THE BARRACUDA SOFTWARE PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION.

6. License. YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT YOU WILL PROVIDE AN UNLIMITED ZERO COST LICENSE TO BARRACUDA FOR ANY PATENTS OR OTHER INTELLECTUAL PROPERTY RIGHTS UTILIZED IN THE BARRACUDA SOFTWARE WHICH YOU EITHER OWN OR CONTROL.

7. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT SHALL BARRACUDA BE LIABLE FOR PERSONAL INJURY OR ANY INCIDENTAL SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION, OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR ABILITY TO USE OR INABILITY TO USE THE BARRACUDA SOFTWARE HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY AND EVEN IF BARRACUDA HAS BEEN ADVISED OF THE POSSIBILITY OF DAMAGES. In no event shall Barracuda's total liability to you for all damages exceed the amount of one hundred dollars.

8. Export Control. You may not use or otherwise export or re-export Barracuda Software except as authorized by the United States law and the laws of the jurisdiction where the Barracuda Software was obtained.

Energize Update Software License

PLEASE READ THIS ENERGIZE UPDATE SOFTWARE LICENSE CAREFULLY BEFORE DOWNLOADING, INSTALLING OR USING BARRACUDA NETWORKS OR BARRACUDA NETWORKS-SUPPLIED ENERGIZE UPDATE SOFTWARE.

BY DOWNLOADING OR INSTALLING THE ENERGIZE UPDATE SOFTWARE, OR USING THE EQUIPMENT THAT CONTAINS THIS SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS LICENSE. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS LICENSE, THEN (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE FOR A FULL REFUND, OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE
PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM BARRACUDA NETWORKS OR AN AUTHORIZED BARRACUDA NETWORKS RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL PURCHASER.

The following terms govern your use of the Energize Update Software except to the extent a particular program (a) is the subject of a separate written agreement with Barracuda Networks or (b) includes a separate "click-on" license agreement as part of the installation and/or download process. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be (1) the written agreement, (2) the click-on agreement, and (3) this Energize Update Software License.

License. Subject to the terms and conditions of and except as otherwise provided in this Agreement, Barracuda Networks, Inc., or a Barracuda Networks, Inc. subsidiary (collectively "Barracuda Networks"), grants to the end-user ("Customer") a nonexclusive and nontransferable license to use the Barracuda Networks Energize Update program modules and data files for which Customer has paid the required license fees (the "Energize Update Software"). In addition, the foregoing license shall also be subject to the following limitations, as applicable:

Unless otherwise expressly provided in the documentation, Customer shall use the Energize Update Software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non-Barracuda Networks equipment) for communication with Barracuda Networks equipment owned or leased by Customer; Customer's use of the Energize Update Software shall be limited to use on a single hardware chassis, on a single central processing unit, as applicable, or use on such greater number of chassis or central processing units as Customer may have paid Barracuda Networks the required license fee; and Customer's use of the Energize Update Software shall also be limited, as applicable and set forth in Customer's purchase order or in Barracuda Networks' product catalog, user documentation, or web site, to a maximum number of (a) seats (i.e. users with access to the installed Energize Update Software), (b) concurrent users, sessions, ports, and/or issued and outstanding IP addresses, and/or (c) central processing unit cycles or instructions per second. Customer's use of the Energize Update Software shall also be limited by any other restrictions set forth in Customer's purchase order or in Barracuda Networks' product catalog, user documentation or web site for the Energize Update Software.

General Limitations. Except as otherwise expressly provided under this Agreement, Customer shall have no right, and Customer specifically agrees not to:

i. transfer, assign or sublicense its license rights to any other person, or use the Energize Update Software on unauthorized or secondhand Barracuda Networks equipment, and any such attempted transfer, assignment or sublicense shall be void;

ii. make error corrections to or otherwise modify or adapt the Energize Update Software or create derivative works based upon the Energize Update Software, or to permit third parties to do the same; or

iii. decompile, decrypt, reverse engineer, disassemble or otherwise reduce the Energize Update Software to human-readable form to gain access to trade secrets or confidential information in the Energize Update Software.

Upgrades and Additional Copies. For purposes of this Agreement, "Energize Update Software" shall include (and the terms and conditions of this Agreement shall apply to) any Energize Update upgrades, updates, bug fixes or modified versions (collectively, "Upgrades") or backup copies of the Energize Update Software licensed or provided to Customer by Barracuda Networks or an authorized distributor/reseller for which Customer has paid the applicable license fees. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO USE ANY SUCH ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL ENERGIZE UPDATE SOFTWARE AND HAS PAID THE
APPLICABLE FEE FOR THE UPGRADE; (2) USE OF UPGRADES IS LIMITED TO BARRACUDA NETWORKS EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR WHO OTHERWISE HOLDS A VALID LICENSE TO USE THE ENERGIZE UPDATE SOFTWARE WHICH IS BEING UPGRADED; AND (3) USE OF ADDITIONAL COPIES IS LIMITED TO BACKUP PURPOSES ONLY.

Energize Update Changes. Barracuda Networks reserves the right at any time not to release or to discontinue release of any Energize Update Software and to alter prices, features, specifications, capabilities, functions, licensing terms, release dates, general availability or other characteristics of any future releases of the Energize Update Software.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Energize Update Software in the same form and manner that such copyright and other proprietary notices are included on the Energize Update Software. Except as expressly authorized in this Agreement, Customer shall not make any copies or duplicates of any Energize Update Software without the prior written permission of Barracuda Networks. Customer may make such backup copies of the Energize Update Software as may be necessary for Customer's lawful use, provided Customer affixes to such copies all copyright, confidentiality, and proprietary notices that appear on the original.

Protection of Information. Customer agrees that aspects of the Energize Update Software and associated documentation, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Barracuda Networks. Customer shall not disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of Barracuda Networks. Customer shall implement reasonable security measures to protect and maintain the confidentiality of such trade secrets and copyrighted material. Title to Energize Update Software and documentation shall remain solely with Barracuda Networks.

Indemnity. Customer agrees to indemnify, hold harmless and defend Barracuda Networks and its affiliates, subsidiaries, officers, directors, employees and agents at Customers expense, against any and all third-party claims, actions, proceedings, and suits and all related liabilities, damages, settlements, penalties, fines, costs and expenses (including, without limitation, reasonable attorneys fees and other dispute resolution expenses) incurred by Barracuda Networks arising out of or relating to Customers (a) violation or breach of any term of this Agreement or any policy or guidelines referenced herein, or (b) use or misuse of the Barracuda Networks Energize Update Software.

Term and Termination. This License is effective upon date of delivery to Customer of the initial Energize Update Software (but in case of resale by a Barracuda Networks distributor or reseller, commencing not more than sixty (60) days after original Energize Update Software purchase from Barracuda Networks) and continues for the period for which Customer has paid the required license fees. Customer may terminate this License at any time by notifying Barracuda Networks and ceasing all use of the Energize Update Software. By terminating this License, Customer forfeits any refund of license fees paid and is responsible for paying any and all outstanding invoices. Customer's rights under this License will terminate immediately without notice from Barracuda Networks if Customer fails to comply with any provision of this License. Upon termination, Customer must cease use of all copies of Energize Update Software in its possession or control.

Export. Software, including technical data, may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Energize Update Software.
Restricted Rights. Barracuda Networks' commercial software and commercial computer software documentation is provided to United States Government agencies in accordance with the terms of this Agreement, and per subparagraph "(c)" of the "Commercial Computer Software - Restricted Rights" clause at FAR 52.227-19 (June 1987). For DOD agencies, the restrictions set forth in the "Technical Data-Commercial Items" clause at DFARS 252.227-7015 (Nov 1995) shall also apply.

No Warranty. The Energize Update Software is provided AS IS. Customer's sole and exclusive remedy and the entire liability of Barracuda Networks under this Energize Update Software License Agreement will be, at Barracuda Networks option, repair, replacement, or refund of the Energize Update Software.

Renewal. At the end of the Energize Update Service Period, Customer may have the option to renew the Energize Update Service at the current list price, provided such Energize Update Service is available. All initial subscriptions commence at the time of sale of the unit and all renewals commence at the expiration of the previous valid subscription.

In no event does Barracuda Networks warrant that the Energize Update Software is error free or that Customer will be able to operate the Energize Update 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 Energize Update Software or any equipment, system or network on which the Energize Update Software is used will be free of vulnerability to intrusion or attack.

DISCLAIMER OF WARRANTY. ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION.

General Terms Applicable to the Energize Update Software License Disclaimer of Liabilities. IN NO EVENT WILL BARRACUDA NETWORKS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE ENERGIZE UPDATE SOFTWARE EVEN IF BARRACUDA NETWORKS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL BARRACUDA NETWORKS' LIABILITY TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EXCEED THE PRICE PAID BY CUSTOMER. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

This Energize Update Software License shall be governed by and construed in accordance with the laws of the State of California, without reference to principles of conflict of laws, provided that for Customers located in a member state of the European Union, Norway or Switzerland, English law shall apply. The United Nations Convention on the International Sale of Goods shall not apply. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Energize Update Software License shall remain in full force and effect. Except as expressly provided herein, the Energize Update Software License constitutes the entire agreement between the parties with respect to the license of the Energize Update Software and supersedes any conflicting or additional terms contained in the purchase order.
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, (GPL) 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 program 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. Also, 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 of particular patents limiting applications of a free program. Patents add restrictions that are not part of the public domain and are therefore incompatible with the spirit and purpose of the General Public License. Therefore we have made patents available to the same extent as is needed for our protection on this free program.

Activities other than copying, distribution and modification are not covered by this License. Those activities 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.

We have designed this License to be self-contained. It includes every clause that grants or restricts rights. 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.

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.

Limited Warranty and License 135
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 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
desires 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 simultaneuously 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.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice
This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Barracuda Products may contain programs that are copyright (c)1995-2005 International Business Machines Corporation and others. All rights reserved. These programs are covered by the following License:

"Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation." Barracuda Products may include programs that are covered by the BSD License: "Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE."

Barracuda Products may include the libgps library which is Copyright (c) 2004 James Couzens & Sean Comeau All rights reserved. It is covered by the following agreement: Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS MAKE ANY WARRANTY WHETHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OF NONINFRINGEMENT, OR THE IMPLIED WARRANTIES ARISING UNDER STATUTE, OR FROM A COURSE OF DEALING OR USAGE OF TRADE, OR ARISING FROM THE USE OF THIS SOFTWARE.

Barracuda Products may contain programs that are copyright (c) 1998-2003 Carnegie Mellon University. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without specific prior written permission. For permission or any other legal details, please contact Office of Technology Transfer Carnegie Mellon University 5000 Forbes Avenue Pittsburgh, PA 15213-3890 (412) 268-4387, fax: (412) 268-7395 tech-transfer@andrew.cmu.edu. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Barracuda products may include programs that are covered by the Apache License or other Open Source license agreements. The Apache license is reprinted 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 copyrighted by Barracuda Networks. Apache License

Version 2.0, January 2004 http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to source software code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).
"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity on behalf of whom a Contribution is submitted to Licensor and subsequently incorporated within the Work.

A "Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute, at least one of the following: within a NOTICE text file distributed as part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, and for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement You may have executed with the Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages (including damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any
other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

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.
Index

A
Account creation
  automatic 94
  disabling 95
  manually, by administrators 95
  manually, by users 95
Advanced networking topics 80
alerts
  backup failures 109
  emailed 109
  LDAP errors 109
  SNMP 109
  system 109
Alias Linking 77, 87
All_domains permissions
  assigning 99
  Domain Admin 102
  Helpdesk 100
allowed email recipient domains 32
and password-protected archives 66
Anti-Virus, Barracuda Exchange Anti-Virus Agent for MS Exchange Server 40
API for remote configuration of the Barracuda Spam & Virus Firewall 93
Attachment blocking, notifications of 41
attachment filtering 66
  inbound 55
  outbound 66, 67
Auditor account role 93, 96, 98
  defined 103
Authentication
  LDAP, POP, RADIUS 48
  single sign-on 47
Barracuda Real-Time protection (BRTS) 21
Barracuda Reputation 19, 53
Bayesian learning
  classifying messages 39, 40
  getting the best accuracy 58
  how it works 57
  when to use it 58
block score 39
Bounce messages, sending or not 81
Bounce suppression 49, 74
Branding of encrypted message notifications 63
C
Certificate generation 38
Classify incoming emails 39, 40
Cloud Protection Layer 69
  Advantages 70
clustering the Barracuda Spam & Virus Firewall
  data not synchronized across the cluster 79
  limiting user access to a clustered system 48
  removing a failed system from a cluster 79
  setting up clustered systems 77
configuration
  reloading 121
Configure 30
content filtering
  inbound mail 55
  outbound mail 67
  pre-made patterns 55
Control Center
  and Hybrid Mode 70
  using 112
D
daily mail statistics 106
definitions, updating 34, 118
diagnostic memory test 124
Disk space, managing 89
domain configuration, default for the Barracuda Spam & Virus Firewall 32
domain level settings
   accessing 92
   and quarantine 92
   list of 36

E
   email
      routing incoming 34
   Email Statistics
      inbound 42
      outbound 42
   Encryption of outbound email
      by redirection to existing encryption service 62
      Requirements for using 62
      using built-in encryption as outbound mail policy 48, 62
      with the Microsoft Outlook Add-In 59
   Energize Updates 118
   Ethernet interfaces 80
   Exchange Mail Server, Barracuda Exchange Anti-virus Agent 40
   Explicit Users to Scan For 35

F
   failed system, replacing 124
   Firewall, locating the Barracuda Spam & Virus Firewall in your network 27
   Firmware update 118
   Front panel indicator lights 115

H
   hardware compliance 125
   hardware test 124
   Helpdesk account role 100
   Hostname, default used in reply address 32
   hourly mail statistics 106

I
   indicator lights 115
   Initial 31
   Instant Replacement Service 124
   Internal virus scanning 40
   Invalid Bounce Suppression 74
   IP address, initial setting 30
   IP Reputation 53
   IPv6 networks 10

L
   Language
      blocking email by country 56
      Non-delivery reports (NDRs) 81
      notifications 89
      Web Interface, selecting 37
   LDAP and User Account Authentication 48
   LDAP errors
      alerts email 109
   LDAPS (SSL/TLS) for user authentication 48
   LEDs (on front panel) 115
   Load Balancer in Direct Server Return Mode, configuring for 81
   Logging in
      administrator login 31
      new account credentials 95
   Loopback Adaptor 81

M
   mail statistics 41, 106
   Mail syslog 108
   memory test 124
   Message Log 39, 71, 108
      CPL, how filtering messages 71
      CPL, integration with Barracuda Spam & Virus Firewall 72
   Microsoft Exchange Server
      Barracuda Exchange Anti-virus Agent 40
   Models of the Barracuda Spam & Virus Firewall 14
   monitoring tasks 105
   MX records 34

N
   network interfaces, configuring 82
   network settings, initial configuration 30
   Non-Delivery Reports (NDRs) 81
   Notifications
      default language 89
      for blocked attachments 41
      for outbound quarantined messages 64
      for recipients of encrypted messages 63
      of quarantined messages 88
      System Alerts Email Address 109
      System Contact Email Address 109

O
   Online Help 10
   Outbound relay
      configuring 35, 49
   Outlook and Lotus Notes plugins
      for classifying messages as Spam or Not Spam 59
      sender-side option to encrypt 59

P
   Password-protected attachment archives, filtering 66
   Performance statistics 41
   Permissions, user-level 88
Plugins
   for classifying messages as Spam or Not Spam 59
   for encrypting messages from Microsoft Outlook 59
POP 48
POP user account authentication 48
Port Forwarding 80
post-installation tasks 38
Preferences, enabling users to edit 96
Private (self-signed) certificates 38

Q
Quarantine
   disabling 85
   domain level settings 92
   global 85
   inbox 87, 88
   notifications 88
   outbound mail 64
   setting up 42
   where quarantined messages go 86
Queue
   inbound and outbound messages 106

R
RADIUS user account authentication 48
RAID 14
RAID disk storage
   alerts when problems arise 109
   and Barracuda Spam & Virus Firewall models 14
   status indicator on BASIC > Status page 106
rate control
   inbound mail 52
   outbound mail 65
reboot options 123
Recipient Verification 76
recovery mode 123
Redirection of outbound mail 62
re-imaging the system 124
reloading the system 121
remote administration 124
Removing a Barracuda Spam & Virus Firewall From a Cluster 79
Replacement Service (Instant) 124
replacing a failed system 124
Reporting 111
Reputation, IP addresses 53
Requeuing outbound messages 107
RESET button 121
restarting the system 121
Restoring a backup 120
Retention Policy
   inbound messages 84
   outbound messages 64
Retry button
   retrying delivery of outbound messages 106
Role-based Administration 92
Roles
   Domain Admin 102
   Helpdesk 100
   User 99
Roles, Auditor account (unique) 93
Routing Email 34
routing incoming email 34

S
Securing user access with single sign-on 47
Sender Policy Framework (SPF) 75
shutting down the system 121
Single Sign-On
   newly created accounts 95
   user authentication 47
SMTP Encryption 48
SNMP query and alerts 109
spam scoring
   configuring via the API 47
   domain level settings 37, 93
   initial settings 39
   outbound mail 62
   overview 13
   per-user settings 36
SSL certificates, generating 38
Static Routes 80
Statistics
   email 41
   performance 41
Storage of email, minimizing 89
Syslog
   mail syslog 108
   tracking changes to the configuration 47
   using a syslog server for monitoring 114
system
   alerts 109
   reboot 121
   shutdown 121
System Alerts Email Address 109
System Contact Email Address 109

T
tag score 39
Task Manager, using to monitor system tasks 113
TCP ports 30
technical support, contacting 15
Testing spam and virus scanning with a local user set 35
time zone 37
TLS encryption 48
Troubleshooting tools 122
Trusted (signed by a trusted CA) certificates 38
Trusted Forwarder 52, 75

U
UDP ports 30
Updating
  definitions 118
  firmware 118
updating firmware and definitions 118
UPS Support 29
User Access, Limiting 47
User Account Authentication
  LDAP, RADIUS, POP 48
User account role 99
User accounts
  enabling features 96
User Features, Default 87
User Login Activities
  tracking with syslog 47

V
valid recipients
  and Predictive Sender Profiling 24
  recipient verification 24
  using the local database 76
Virtual Machine Deployment 26
virus scanning
  Hybrid mode 71
  internal with Barracuda Exchange Anti-Virus Agent 40
  when and where it is applied 40

W
Warranty, limited 129
Web interface
  for configuration 10
  logging in 31
  setting the default language 37
  SSL-only access 38