



Barracuda Email Security Service



Administrator's Guide

Version 2.x

Copyright Notice

Copyright (c) 2004-2012, Barracuda Networks, Inc., 3175 S. Winchester Blvd, Campbell, CA 95008 USA

www.barracuda.com

v2.x-120202-04-0425pd

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

Trademarks

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

Chapter 1 – Introduction 7

Overview	8
Easy Deployment and Administration	8
Rich Cloud-Based Virus and Spam Protection	8
Inbound Versus Outbound Message Filtering	9
Email Spooling	9
Contacting Technical Support.	9

Chapter 2 – Concepts 11

Multiple Layers of Defense	12
Connection Management Layers	12
Denial of Service Protection.	12
Rate Control.	12
IP Analysis	12
Sender Authentication.	13
Mail Scanning Layers	13
Virus Scanning	13
Barracuda Anti-virus Supercomputing Grid	13
Intent Analysis.	14
Image Analysis	14
Advanced Spam Detection	14
Predictive Sender Profiling	14
Notifications.	15
Monitored Outbound Email Volume.	15

Chapter 3 – Getting Started 17

Initial Setup of the Service	18
Connect to the Barracuda Email Security Service	18
Purchase and Activate Your Subscription	18
Configure Your Domains and Mail Servers	18
Secure your Mail Server.	20
Set Up User Accounts.	20
Configure Scanning of Outgoing Mail	20
Encryption of Outbound Mail	21
Outbound Message Footer	21
Verify That Mail is Flowing	21
Tune and Monitor the Default Spam and Virus Settings	22
Per-Domain Management	22
Basic Spam and Virus Checking	22
Viewing Email Statistics.	22
The Message Log	23
Spam or Not Spam?.	23
Message Details.	23
Setting up Quarantine	23

Chapter 4 – Advanced Inbound Spam Filtering Policy . . . 25

IP Analysis	26
Creating Custom IP Policy	26
Barracuda Reputation	26
Subscribing to External Blocklist Services	26
Content Analysis - Inbound	27
Custom Content Filters	27
Attachment Filtering	27
Intent Analysis	27
Image Analysis	28

Chapter 5 – Outbound Filtering Policy 29

IP Analysis	30
DLP and Encryption of Outbound Mail	30
Sending and Receiving Encrypted Messages	30
Rate Control for Outbound Mail	31
Abuse Monitor for Rate Controlled IP Addresses	31
Content Analysis - Outbound Mail	31
Custom Content Filters - Outbound	31
Attachment Content Filtering - Outbound	31
Image Analysis - Outbound	32

Chapter 6 – Managing Quarantine 33

How Quarantine of Inbound Mail Works	34
Where Do the Quarantined Messages Go?	34
Linking (Aliasing) Domains	34
Quarantine Notifications	35
The Quarantine Digest	35

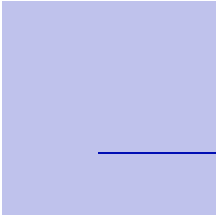
Chapter 7 – Advanced Configuration 37

Sender Authentication	38
Sender Policy Framework (SPF)	38
SPF for Sending Outbound Email	38
Custom policies and Sender Spoof Protection	38
Recipient Verification	39
LDAP Lookup	39
Secured Message Transmission	39
TLS For Secured Inbound and Outbound Messages	40

Chapter 8 – Managing Accounts and Domains 41

Creating and Managing Domains	42
Domain Level Settings	42
Creating and Managing Accounts	42
Local User Accounts	42
Automatic Account Creation	42

	Editing User Accounts	43
	User Account Features	43
	User Authentication With LDAP	44
Appendix 9 – Regular Expressions		45
	Using special characters in expressions	46
	Examples	46
Appendix B – Limited Warranty		47
	Barracuda Online Services License and Warranty	47
Index		71



Chapter 1

Introduction

This chapter provides an overview of the Barracuda Email Security Service and includes the following topics:

<i>Overview</i>	8
<i>Easy Deployment and Administration</i>	8
<i>Rich Cloud-Based Virus and Spam Protection</i>	8
<i>Contacting Technical Support</i>	9

Overview

The Barracuda Email Security Service is a comprehensive and affordable cloud-based email security service that protects both inbound and outbound email against the latest spam, viruses, worms, phishing and denial of service attacks.

Spam and viruses are blocked in the cloud prior to delivery to the your network, saving network bandwidth and providing additional Denial of Service protection. In addition to network bandwidth savings, cloud-based filtering offloads any processing required for spam and virus filtering from the email server. The Barracuda Email Security Service can be scaled to support hundreds of thousands of active email users.

This guide provides concepts and general guidance the administrator needs to understand how to best configure the Barracuda Email Security Service according to the organization's deployment needs, policies and email infrastructure.

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

Easy Deployment and Administration

The powerful Web interface of the Barracuda Email Security Service allows for convenient configuration and management of spam and virus filtering policies and email security settings from one central location. Key email statistics can be viewed at a glance on the **STATUS** page with the ability to drill down for more detail in the **Message Log**. Spam and virus configuration as well as IP and content filtering policies can be set at the global and/or per-domain level.

Without the need to install software or deploy hardware, the Barracuda Email Security Service can start filtering inbound and outbound email in a matter of minutes. Users can access their own message log to deliver quarantined emails to ease the burden of administration.

The standard deployment configuration consists of Barracuda Email Security Service filtering inbound and outbound email in the cloud. Barracuda Email Security Service will attempt delivery to an alternate network if the primary destination is not available. In case the secondary destination is also unavailable, then emails will be stored for up to 96 hours. End users will be able to log in during this time to check emails.

Rich Cloud-Based Virus and Spam Protection

The Barracuda Email Security Service employs multiple protection layers, including:

- Denial of service - insulates your organization's mail server from receiving direct Internet connections and associated threats.
- Rate control - Protects your email infrastructure from flood-based attacks by counting the number of incoming connections from a particular IP address (inbound mail) or sender email

address (outbound mail) during a 30 minute interval and deferring the connections once a particular threshold is exceeded.

- IP Reputation Analysis - real-time blocklists (RBLs) or DNS blocklists (DNSBLs),
- Sender Authentication
- Recipient Verification
- Virus Scanning
- Anti-phishing, using Barracuda Anti-Fraud Intelligence
- Patent-pending Barracuda Anti-virus Supercomputing Grid - a layer to detect polymorphic viruses leveraging the power of cloud computing
- Custom policies
- Intent Analysis
- Image Analysis

Inbound Versus Outbound Message Filtering

Any message sent through the Barracuda Email Security Service addressed to a domain that is configured in the service is treated as an *inbound* message. All others are treated as *outbound* messages. In addition to thorough spam and virus scanning of *inbound* email, the Barracuda Email Security Service includes essential outbound mail filtering techniques, including optional encryption of message content, that help organizations to ensure that all outgoing email is legitimate, secured and virus-free.

Email Spooling

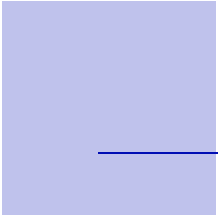
The Barracuda Email Security Service provides email continuity by providing queuing of email for up to four days and backup MX for email rerouting to a separate destination. This feature ensures seamless disaster recovery capabilities in the event of network downtime or system outage. Barracuda Networks recommends enabling spooling of email. See *Configure Your Domains and Mail Servers* on page 18 for details.

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> 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>.



Chapter 2

Concepts

This chapter introduces the general topics that will help you understand what your Barracuda Email Security Service can do and how to approach configuring the features that are important to your organization policies. It is recommended that you understand these concepts before customizing the configuration of your Barracuda Email Security Service.

<i>Multiple Layers of Defense</i>	12
<i>Connection Management Layers</i>	12
<i>Mail Scanning Layers</i>	13
<i>Predictive Sender Profiling</i>	14

Multiple Layers of Defense

Understanding each of the multiple layers of defense prepares you to make decisions about which - if not all- of the connection and mail scanning features to enable for the best combination of performance and accuracy of the Barracuda Email Security Service. More information about features that support each layer, pros and cons, as well as Barracuda Networks' recommendations are addressed in later chapters.

Connection Management Layers

These layers identify and block unwanted email messages before accepting the message body for further processing. 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

The Barracuda Email Security Service 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 Email Security Service counts the number of incoming connections from a particular IP address (inbound and outbound mail) or sender email address (outbound mail only) during a 30 minute interval and defers the connections once a particular threshold is exceeded. Rate control is automatically configured by the Barracuda Email Security Service.

IP Analysis

After applying rate controls based on IP address, the Barracuda Email Security Service performs analysis on the IP address of email 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 list, if enabled, and connections from suspicious senders are dropped.
- **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 used by spammers. The Barracuda Email Security Service **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.

Mail Scanning Layers

Virus Scanning

The most basic level of mail scanning is virus scanning. The Barracuda Email Security Service utilizes three layers of virus scanning and automatically decompresses archives for comprehensive protection. By utilizing virus definitions, Barracuda Email Security Service 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 System (BRTS). 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. The Barracuda Real-Time System 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.

Barracuda Anti-virus Supercomputing Grid

An additional, patent-pending layer of virus protection offered by the Barracuda Email Security Service is the Barracuda Anti-virus Supercomputing Grid, which can protect your network from polymorphic viruses. Not only does it detect new outbreaks similar to known viruses, it also identifies new threats for which signatures have never existed using “premonition” technology.

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 Email Security Service applies various forms of Intent Analysis to both inbound and outbound mail, including real-time and multi-level intent analysis. Enable or disable this feature on the [INBOUND SETTINGS > Anti-spam/Anti-virus](#) page.

Image Analysis

The Barracuda Email Security Service 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 Email Security Service 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 Email Security Service 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 Email Security Service to block messages.
- **Animated GIF analysis** - The Barracuda Email Security Service contains specialized algorithms for analyzing animated GIFs for suspect content.

Advanced Spam Detection

You can configure spam detection for custom categories by setting a ‘score’ for content type on the [INBOUND SETTINGS > Anti-spam/Anti-virus](#) page. This score ranges from 0 (definitely not spam) to 5 (definitely spam). Based on this score, the Barracuda Email Security Service will block messages that appear to be spam and they will appear in the user’s [Message Log](#) with the category responsible for the block.

Predictive Sender Profiling

When spammers try to hide their identities, the Barracuda Email Security Service can use Predictive Sender Profiling to identify behaviors of all senders and 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 Email Security Service 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 Email Security Service limits the number of connections made from any IP address within a 30 minute time period. Violations are logged to

identify spammers. Rate Control is automatically configured by the Barracuda Email Security Service.

- **Attempting to send to too many invalid recipients**

Many spammers attack email infrastructures by harvesting email addresses. **Recipient Verification** on the Barracuda Email Security Service 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. You can exempt email addresses of trusted, verified recipients from Recipient Verification using the [INBOUND SETTINGS > Recipient Policies](#) page.

- **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 Email Security Service 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. Enable Intent Analysis on the [INBOUND SETTINGS > Anti-spam/Anti-virus](#) page.

- **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 Email Security Service inspects the results of Web queries to URIs of well-known free Web sites for redirections to known spammer sites. Enable Intent Analysis on the [INBOUND SETTINGS > Anti-spam/Anti-virus](#) page.

Notifications

The Barracuda Email Security Service sends out two kinds of notifications:

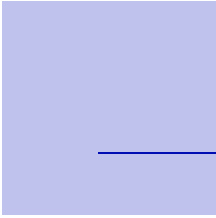
- **Quarantine Digest:** For email recipients which are listed in the Barracuda Email Security Service database (see *Managing Accounts* on page 41), a notification email containing a summary of quarantined email is sent to their email address at an interval you specify for users. See *Quarantine Notifications* on page 35 for information about configuring these types of notifications.
- **Attachment Blocking for Content:** A notification will be sent to the *sender* of a message when it is blocked due to attachment content filtering. Configure content filtering for inbound email from the [INBOUND SETTINGS > Content Policies](#) page.

Monitored Outbound Email Volume

The Barracuda Email Security Service monitors the volume of *outbound* email from the system to the internet. If the volume exceeds normal thresholds during any given 30 minute interval, the Rate Control function will take effect, causing all outbound mail to be deferred until the end of the 30 minute time frame. The outbound mail flow will then continue unless the volume is exceeded again in the next 30 minute interval. If so, Rate Control will again be triggered and outbound mail will be deferred until the end of the time frame.

The allowable volume of outbound mail for an IP address can potentially be increased if the user clicks the **Request Increased Limit** button on the [OUTBOUND Settings > Abuse Monitor](#) page. The request will be reviewed by Barracuda Networks and the limit on the rate of outbound mail from the Barracuda Email Security Service may be increased.

If this situation occurs frequently for a particular sending IP address, that IP address will be listed in the **OUTBOUND Settings > Abuse Monitor** page in the **IP Addresses With Recent Abuse** table.



Chapter 3

Getting Started

This chapter will guide you in connecting your mail server(s) to the Barracuda Email Security Service and beginning to scan and monitor email traffic.

- Initial Setup of the Service* 18
- Verify That Mail is Flowing*..... 21
- Tune and Monitor the Default Spam and Virus Settings* 22
- Viewing Email Statistics*..... 22
- The Message Log*..... 23
- Setting up Quarantine*..... 23

Initial Setup of the Service

Connect to the Barracuda Email Security Service

Start by logging into Barracuda Networks with your account credentials at www.barracudanetworks.com by clicking the **Customer Login** button, and then skip to the next section. If you don't have an account, you can create one by following these steps:

1. Visit www.barracudanetworks.com and click the **Customer Login** button.
2. From the **Sign In** page, click the [Create an Account](#) link. Enter your name, email address and company name and click the **Create Account** button.
3. You will receive an email momentarily from the service which you'll use to continue your registration. Click on the link in the email message and make a note of your username (email address you entered in step 2).
4. In your browser you'll see a screen in the Barracuda Networks interface prompting you to create a password for your new account. Type in your new password twice and click **Create Password**. Passwords must be at least 6 characters long.
5. After saving your new password, you'll see the **Account** tab in the Barracuda Networks Account interface. Click **Manage Users** to show your account name, associated privileges, username and products you've associated with your Barracuda Networks account. Additional user accounts can be added in the future from here and will be listed on this page. You can add users now if desired by clicking the **Add User** button on this page.
6. Click on the **Email Security Service** product link to the left to connect with the service. On the setup page, click the **Start Email Security Service Setup** button. You will be directed to enter your contact information and number of users. Once the form is complete, click **Create Account**.
7. You will see the Welcome page where you can either:
 - 7a. Click the **Begin Express Setup** button to use the setup wizard, or
 - 7b. Click the **Email Security Service** link on the left side of the page to use the web interface and configure domains and settings manually. See *Configure Your Domains and Mail Servers*, page 18 (below) for manual configuration.

Purchase and Activate Your Subscription

If you have not yet purchased a Barracuda Email Security Service subscription, you will have 30 days to try the service before purchase. Once you have paid for the service, you'll receive a confirmation email with a Serial Number and a Linking Code. To activate your subscription, you must click the [Click here to enter your linking code](#) link on the **STATUS** page and enter both of these values on the **Enter purchased linking code** page.

Configure Your Domains and Mail Servers

First configure your mail server(s), then all domains for which you want the Barracuda Email Security Service to filter email. Your Barracuda Email Security Service will only accept email addressed to domains that it has been configured to recognize.

1. Add each domain and mail server you want the Barracuda Email Security Service to secure on the **DOMAINS > Domain Manager** page:

- 1a. Enter the domain name and Smart host, mail server IP address or hostname (FQDN), then click the **Add** button. You'll be redirected to the **DOMAINS > Domain Settings** page. Entering a Priority for the mail server is optional and only applies if there are multiple mail server hostnames added. To add additional mail servers, click the **Add Mail Server** button.
 - 1b. Once the Barracuda Email Security Service has verified the mail server, you will see *Verified* in the **Status** column in the table.
 - 1c. To test the mail server, click the Test link in the table for that server. To delete the mail server entry, click the Remove link in the table.
2. **Add and verify each of the domains** for which you want to filter email on the **DOMAINS** tab. Domains must be verified by the Barracuda Email Security Service for proof of ownership. Repeat the steps below for each domain for which Barracuda Email Security Service will be processing mail. If you don't verify all of the domains you add, you'll be prompted by an error message at the top of the page to verify them.
- 2a. **Verify the domain** after adding it by clicking the **Verify** link in the **Status** column (mail will not be processed for unverified domains). The **DOMAINS > Domain Verification** page will prompt you to select one of three ways to verify the domain ownership:
 - **MX Records** - To use this method, add one or both of the Barracuda MX (Mail Exchange) records to your domain's DNS server. Give these records a higher priority than your domain's existing MX records. This will ensure that your mail will continue to flow until your Barracuda Email Security Service domain is validated. **Note that it is possible that it could take up to 24 hours** for the Barracuda Email Security Service DNS server to see this change in your MX records. Once your domain has been validated, you can remove the old MX records, leaving just the Barracuda MX records. Your mail will now be sent to the Barracuda Email Security Service for scanning.
 - **Email to the domain's administrative contact** - This method sends a verification email to the administrative contact email address listed on your domain's WHOIS entry. **Note:** This verification option will not be available if the Barracuda Email Security Service can't find your domain's WHOIS entry.
 - **Email to the postmaster** - This method sends a verification email to the postmaster email address for your domain. The confirmation email will include a link that the recipient can click to verify the domain.
 - 2b. **Alias the domain** to another domain you've already added and configured. This is optional. If you make this domain an alias for one you've already configured, this domain will 'inherit' the settings you created for the other domain. To access the **DOMAINS > Domain Details** page, click on the **Settings** link in the **Actions** column for that domain on the **DOMAINS > Domains Manager** page.
 - 2c. Select **SMTP over TLS** if you want to send and receive messages via a secure TLS connection to/from this domain.
 - **Optional:** This setting will cause the Barracuda Email Security Service to attempt a TLS connection to the receiving mail server for outgoing email from this domain. If the receiving mail server supports it, the message will be sent over the secure TLS connection.
 - **Required:** All outbound messages from this domain will be sent over a TLS connection. If the receiving mail server does not support a TLS connection, the message will not be delivered (it will bounce).
 - **Never:** Outbound email will never be sent over a TLS connection from this domain.
 - 2d. **Enable Spooling** of email from the **DOMAINS > Domain Details** page if you want the Barracuda Email Security Service to retain all of your email for a limited time if your mail server goes down. Here's how spooling works:

- If spooling is *enabled* and the Barracuda Email Security Service can't reach the destination mail server, the sender will be notified and the message will be logged as *spooled* with a delivery status as *spooled* in the **Message Log**. The Barracuda Email Security Service will try again at intervals to resend the spooled messages for up to 96 hours.
- If spooling is *disabled* and the Barracuda Email Security Service can't reach the destination mail server, the sender will be notified to try again later, and the message will be logged as *allowed* with a delivery status of *spooled* in the **Message Log**.

To configure spooling, access the **DOMAINS > Domain Details** page by clicking on the **Settings** link in the **Actions** column for that domain on the **DOMAINS > Domain Manager** page. Spooling can be enabled or disabled in the **Other Configuration** section of the page.

2e. Click Save Changes.

To view the MX record configuration or mail statistics for a verified domain, click the **Settings** link in the **Actions** column.

Secure your Mail Server

Important: You will need to block all port 25 traffic except for that originating from the Barracuda Email Security Service IP address:

64.235.144.0/20

Set Up User Accounts

There are two ways to create an account in the Barracuda Email Security Service. You can manually create 'local' user accounts or, if you are using LDAP, you can have the service automatically synchronize with your LDAP server and create accounts for users of each domain you've added to the service. For details on user account creation and configuration, please see *Managing Accounts*, page 41.

Configure Scanning of Outgoing Mail

The Barracuda Email Security Service may be configured to scan outgoing mail simultaneously with scanning inbound mail. To enable spam and virus scanning of outbound mail, you must do the following:

1. Verify domains for outbound mail by following step 9 in *Configure Your Domains and Mail Servers*, page 18.
2. Configure allowed sender IP address ranges on the **OUTBOUND SETTINGS > Sender IP Address Ranges** page. These IP addresses are allowed to send outgoing email from your *verified* domains. To add multiple IP addresses, click the **Bulk Edit** button and follow instructions on the page.



Note

To assure recipients of outbound mail from your Barracuda Email Security Service that Barracuda Networks is the authorized sending mail service, please add the following to the INCLUDE line of the SPF record for each of your domains sending outbound mail:

```
include:spf.ess.barracudanetworks.com
```

Outbound mail scanning includes:

- Spam Scanning with Block or Quarantine actions
- Virus Scanning - if you enable it on the [OUTBOUND SETTINGS > Anti-virus](#) page (recommended)
- IP Address Filtering
- Sender Domain, Username or Email Address Filtering
- Recipient Email Address Filtering
- Content Filtering (Subject, Header and Body)
- Attachment Filtering
- 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
- Whitelist/blocklist

Encryption of Outbound Mail

To prevent data leakage and ensure compliance with financial, health care and other federally-regulated agency information policies, you can require all email sent from any or all domains configured in your Barracuda Email Security Service to be encrypted. Specify domains requiring encryption of outbound mail on the [OUTBOUND SETTINGS > DLP/Encryption](#) page. See *DLP and Encryption of Outbound Mail*, page 30 for more information. Transmission of *inbound* and *outbound* email can be required over a TLS channel as well - see *Secured Message Transmission*, page 39 for details.

Outbound Message Footer

The Barracuda Email Security Service can append a custom text and/or html footer to each outbound message, configurable at the global level on the [OUTBOUND SETTINGS > Tagline/Footer](#) page.

Verify That Mail is Flowing

After you configure the Barracuda Email Security Service, the system begins filtering email based on the default settings and those you've configured. The system automatically checks incoming (and outgoing, if you've configured it) email for spam and viruses.

Check the [STATUS](#) and [Message Log](#) pages to make sure that inbound and outbound messages are being logged for the selected domain. The [Message Log](#) page provides rich searching using a set of keywords with your search words or phrases. See *Advanced Search*, page 44 for more information.

Tune and Monitor the Default Spam and Virus Settings

Once email is flowing through the Barracuda Email Security Service, use the [Message Log](#) page to get an idea of how many messages are being blocked or quarantined and for what reasons. Click on any message in the [Message Log](#) to see the message details, including the action and reason if the message was blocked or quarantined. Reviewing this log will give an idea of how current settings are filtering messages. See *The Message Log*, page 23, for more information on using the log.

Per-Domain Management

Note that you can drill down to a particular domain and view and configure spam and virus scanning, policy filters, inbound or outbound settings, etc. at the domain level. For example, you might want to turn *off* virus scanning for a domain that is internal and already protected by an anti-virus solution. Or you might want to customize content and attachment filtering policies for each domain, depending on the type of email you expect to be flowing to and from the domains.

From the [DOMAINS > Domain Manager](#) page, click on the [Manage](#) link for the domain you want to configure. You'll see the same feature configuration pages available at the global level. You can then return to 'global' management of all of your domains by click the **Return to account management** link above the feature configuration pages.

Basic Spam and Virus Checking

Virus scanning is automatically enabled in the Barracuda Email Security Service and the system checks for definition updates on a regular basis (hourly by default). Virus Scanning takes precedence over all other mail scanning techniques, so 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.

The [INBOUND SETTINGS](#) and the [OUTBOUND SETTINGS](#) tabs have pages for enabling or disabling virus checking. If you enable **Use Barracuda Real-Time System** on the [INBOUND SETTINGS > Anti-spam/Anti-virus](#) page, the Barracuda Email Security Service will check unrecognized spam and virus fingerprints against the latest virus threats logged at Barracuda Central.

Use the [INBOUND SETTINGS > Anti-spam/Anti-virus](#) page to enable/disable spam filtering mechanisms and set scoring for spam categories. See *Advanced Inbound Spam Filtering Policy*, page 25, for information about how spam filtering works and determine what might work best for your organization. After you change the settings, you can use the [STATUS](#) and [Message Log](#) pages to monitor and tune your configuration.

Viewing Email Statistics

The [STATUS](#) page provides an overview of the performance of your Barracuda Email Security Service, including:

- Hourly and daily email statistics that display the number of inbound and outbound messages blocked, allowed and deferred as well as bandwidth for the last 24 hours and 30 days.
- Top domains for which mail has been processed by the system.
- A breakdown by reason (action) for:
 - Inbound messages: Allowed, Blocked and Deferred. For example, 'Anti-Fraud', 'Anti-virus', 'Barracuda Reputation', 'Invalid Sender', etc.

- Outbound messages: Allowed, Blocked, Quarantined, Encrypted, and Deferred.
Click either the [Allowed](#), [Blocked](#), or [Deferred](#) links in the **Emails processed, by action** section of the page to see all messages with which that action was taken. You'll be redirected to the [Message Log](#) page, which is described below.

Each time you log into the Barracuda Email Security Service, you'll first be presented with the **STATUS** page. If you have added domains which have not yet been verified by the service, you'll see this message with a warning symbol at the top of the page:

You have one or more unverified domains. [Click here](#) to verify your domains.

To view email statistics for only for inbound mail, click the [Inbound](#) link on the [Email Statistics](#) bar under **Status**. Click the [Outbound](#) link to view email statistics only for outbound mail. Below these links you can select a single domain or *All* domains.

The Message Log

The **Message Log** is a window into how the current spam, virus and policy settings are filtering email coming through the Barracuda Email Security Service. Sorting messages using the powerful [Advanced Search](#) feature can quickly provide a profile of email by allowed, deferred, quarantined, encrypted (outbound) or blocked messages by domain, sender, recipient, time range (last 2- 30 days), envelope to, envelope from, reason, action taken, date or subject. The Message Log reflects ALL email traffic through the Barracuda Email Security Service at the *global* level. If you click on a verified domain on the [DOMAINS > Domain Manager](#) page, you'll see a tab for the Message Log for that domain only.

Spam or Not Spam?

Occasionally the Barracuda Email Security Service may incorrectly identify a piece of mail as *Spam* (false positive) or *Not Spam* relative to the policies you've set. You might want to tune the **Advanced Spam Detection Scoring** levels on the [INBOUND SETTINGS > Anti-spam Anti-virus](#) page by selecting *Custom* and adjusting the score for each category based on what type of mail you consider to be spam.

The **Spam** and **Not Spam** buttons on the [Message Log](#) page (both at the global level and the user account level) allow you to mark a message as such, and those messages will be sent to Barracuda Central for analysis.

Message Details

Message source and the reason for blocking, quarantine or deferral of messages is viewable by clicking on a message and then clicking the [Show Details](#) link in the message header. The administrator (or user, when viewing their own account) can then elect to View the entire message source, deliver, or download the message contents.

Setting up Quarantine

The Barracuda Email Security Service sends the user an email with a login and password the first time an incoming email for that user is quarantined.

Quarantine notifications can be configured to be sent to users daily, weekly, on a 'custom' schedule, or never. See the [USERS > Quarantine Notification](#) page for settings. From this page you can also enable or disable the user's ability to set their own quarantine notification interval from their account.



Advanced Inbound Spam Filtering Policy

The goal in configuring your Barracuda Email Security Service is to identify spam without blocking valid messages. This chapter addresses using custom spam filtering policy on *inbound* mail, configurable on the **INBOUND SETTINGS** pages.

<i>IP Analysis</i>	26
<i>Content Analysis - Inbound</i>	27

IP Analysis

Creating Custom IP Policy

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 as “Exempt” from scanning by adding them to a *whitelist* of known good senders.

You can create your whitelist of known good/trusted sender IP addresses and block those you know are not trusted, using the [INBOUND SETTINGS > IP Address Policies](#) page

Warning



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

Barracuda Reputation

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.

On the [INBOUND SETTINGS > Anti-spam/Anti-virus](#) page, it is strongly recommended that the **Use Barracuda Reputation BlockList (BRBL)** option be checked.

Subscribing to External Blocklist Services

The [INBOUND SETTINGS > Custom RBLs](#) 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 Email Security Service 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). Messages blocked due to external blocklists or the BRBL are the only blocked messages that are not sent to the user’s [Message Log](#).

Content Analysis - Inbound

The Barracuda Email Security Service enables administrators to set custom content filters for *inbound* messages based on message content and attachment file name or MIME type. See the **INBOUND SETTINGS > Content Policies** page for settings.

Custom Content Filters

Message content filtering can be based on any combination of subject, headers, body, attachments, sender or recipient filters, and you can specify actions to take with messages based on pre-made patterns (regular expressions) in the subject line, headers, message body, sender or recipient lines. See *Regular Expressions*, page 45 for 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 that content filtering applies to the actual words as they appear when viewed in a Web browser.

For information about content filtering for *outbound* messages, see *Content Analysis - Outbound Mail on page 31*.

Attachment Filtering

All messages, except those from whitelisted (allowed) senders, go through attachment filtering. From the **INBOUND SETTINGS > Content Policies** page you can choose to take certain actions with *inbound* messages if they contain attachments with certain file name patterns or MIME types. For *outbound* attachment filtering, see *Attachment Content Filtering - Outbound* on page 31.

The **Scan Archives** feature can be selected along with any filter to search the contents of attached archives (zip, tar, etc.). 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* for the **Reason** if you click [Show Details](#) for the message. For example, if you created a filter 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 [Show Details](#) area:

```
Action:Blocked Reason:Attachment (word_2010_xml.tgz)
```

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

Intent Analysis

The Barracuda Email Security Service features the following forms of Intent Analysis:

- **Intent analysis** - Markers of intent, such as URLs, are extracted and compared against a database maintained by Barracuda Central.
- **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 can be enabled or disabled on the [INBOUND SETTINGS > Anti-spam/Anti-virus](#) page.

Domains can also be blocked based on or exempt from Intent Analysis on the [INBOUND SETTINGS > Content Policies](#) page.

Image Analysis

Image spam represents about one third of all traffic on the Internet. The Barracuda Email Security Service 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 Email Security Service 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 Email Security Service 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 Email Security Services to block messages.
- **Animated GIF analysis** - The Barracuda Email Security Service contains specialized algorithms for analyzing animated GIFs for suspect content.

Outbound Filtering Policy

By scanning all outbound messages, you can ensure that all email leaving your organization is legitimate and virus free. Outbound filtering options are configured on the **OUTBOUND SETTINGS** pages and different from those for inbound filtering, including optional encryption for secure transmission. Virus scanning is enabled by default on the **OUTBOUND SETTINGS > Anti-virus** page and is recommended.

<i>IP Analysis</i>	30
<i>DLP and Encryption of Outbound Mail</i>	30
<i>Rate Control for Outbound Mail</i>	31
<i>Content Analysis - Outbound Mail</i>	31

IP Analysis

After applying rate controls, the Barracuda Email Security Service performs analysis on the IP address, applying block or quarantine policies that you configure in the [INBOUND SETTINGS > IP Address Policies](#) pages.

To best protect the IP reputation of your organization, start by listing IP addresses that are allowed to send mail from your organization through the Barracuda Email Security Service. Add these IP addresses on the [OUTBOUND SETTINGS > Sender IP Address Ranges](#) page and include all trusted forwarders of email. Note that all outbound mail from these IP addresses will go through virus checking if the **Enable virus scanning of outgoing emails** option is checked on the [OUTBOUND SETTINGS > Anti-virus](#) page.

DLP and 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 Email Security Service provides optional DLP (Data Leak Prevention) features. These features include advanced content scanning for keywords inside commonly used attachments, as well as email encryption. You can configure email encryption per domain on the [OUTBOUND SETTINGS > DLP/Encryption](#) page. Encryption is performed by the Barracuda Message Center, which also provides a Web interface for recipients to retrieve encrypted messages.

Note



DLP/Encryption is available by subscription. See the **Subscription STATUS** box on the [STATUS](#) page to see if your DLP/Encryption subscription is up to date.

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 Email Security Service. 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 the [OUTBOUND SETTINGS > DLP/Encryption](#) page to encrypt outbound messages by domain.
2. Outbound messages that meet this filtering criteria are encrypted and appear in the Barracuda Email Security Service **Message Log**, but the message body does not appear in the log for security purposes.
3. 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.
4. 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.
5. 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.

Rate Control for Outbound Mail

Outbound mail is rate controlled based on IP address by the Barracuda Email Security Service as described in *Rate Control*, page 12. Rate Control for outbound email, however, can also be applied based on sender email address. If the number of outbound connections from a sender email address exceeds the specified maximum connections per sender over a 30 minute time period, the Barracuda Email Security Service 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. Rate Control is automatically configured by the Barracuda Email Security Service.

Abuse Monitor for Rate Controlled IP Addresses

IP addresses of senders of outbound mail who consistently trigger Rate Control will be logged in the **IP Addresses With Recent Abuse** table on the **OUTBOUND SETTINGS > Abuse Monitor** page. For organizations that need to send a higher volume of outbound mail, the owner of an IP address that appears in this table for consistently exceeding Rate Controls may use this page to request Barracuda Networks to allow a higher volume of outbound mail so that Rate Control does not take effect.

Important: IP addresses that send very high volumes of email, consistently triggering Rate Controls, may be suspended from sending outbound mail through the Barracuda Email Security Service. Please contact Barracuda Networks Technical Support if your IP address appears in this list.

Content Analysis - Outbound Mail

Custom Content Filters - Outbound

Custom content filtering can be based on any combination of subject, headers, body, attachments, sender or recipient and can be applied to outbound mail just as it can be to inbound mail. See the **OUTBOUND SETTINGS > Content Policies** page for settings. Note that filter actions for outbound mail include *Encrypt*.

See *Regular Expressions*, page 45 for 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 that content filtering applies to the actual words as they appear when viewed in a Web browser.

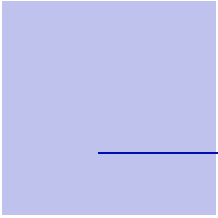
Attachment Content Filtering - Outbound

All outbound messages, including those from whitelisted senders, go through attachment filtering. You can allow, block, quarantine or encrypt 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. See the [OUTBOUND SETTINGS > Content Policies](#) page for settings.

Image Analysis - Outbound

Image Analysis techniques protect against new image variants. The techniques detailed in *Image Analysis*, page 28, for inbound email also apply to outbound messages. **Image Analysis** is automatically configured in the Barracuda Email Security Service.



Chapter 6

Managing Quarantine

The Barracuda Email Security Service provides a robust, per-user quarantine function configurable at the domain level and, if enabled, the user level. This chapter covers how quarantine works and configuration at both domain and user level.

<i>How Quarantine of Inbound Mail Works</i>	34
<i>Where Do the Quarantined Messages Go?</i>	34
<i>Linking (Aliasing) Domains</i>	34
<i>Quarantine Notifications</i>	35

How Quarantine of Inbound Mail Works

Any inbound or outbound message that meets custom filtering criteria for blocking, or is otherwise determined by the Barracuda Email Security Service to be spam, goes into quarantine. The only exception is messages that are blocked due to custom RBLs or the Barracuda Reputation Blocklist (BRBL), because you know that you want to block these messages from your mail server. The administrator can view all messages processed in the [Message Log](#), and, if you enable user quarantine, users can view their quarantined message in their accounts. See *Managing Accounts* on page 41 for details on user account creating and settings.

You can indicate how aggressively you want the Barracuda Email Security Service to block messages that seem to be spam by using the **Advanced Spam Detection Scoring** feature on the **INBOUND SETTINGS > Spam Checking** page. Select *Custom* to see a list of custom categories for which you can assign scores indicating how likely those messages are to be spam for your users and organization.

For example, if your company is a financial institution, you'll want to set a low score for the *Finance* category.

Messages can also be blocked based on custom policies you set based on domain name, IP address, sender, recipient, message or attachment content and other criteria for both inbound and outbound messages.

Where Do the Quarantined Messages Go?

Quarantined messages go to a user's account and are viewable in their [Message Log](#). The user can choose to deliver, delete or download the message and can filter the log by *Allowed*, *Quarantined*, *Blocked* or *All* messages. If the administrator has enabled the user to set their own quarantine notification interval, the user can decide how often to receive a notification report to their regular mailbox with a summary of their quarantined messages.

Linking (Aliasing) Domains

In some cases it may be practical to direct all quarantined email to one user account in the Barracuda Email Security Service. You may employ one or more "power users" to manage it, or allow all users to log in to the same account.

The **Domain Alias** feature, configurable on the **DOMAINS > Domain Details** page for a particular domain, allows the option for all domains protected by this Barracuda Email Security Service be treated as if they were alternate names for one domain name you configure for the system. All aliased domains will then inherit the same spam and virus filtering policies you set for the 'main domain'. From the **DOMAINS > Domain Manager** page, click on the **Settings** link in the **Actions** column for the domain you want to alias. You'll see the **Domain Details** page, where you can configure domain aliasing, LDAP settings and other options.

Another case for using the **Domain Alias** feature is to configure one domain one time with the scanning policies you want to use for the entire organization, and simply apply those settings to all of your domains.

Quarantine Notifications

The Barracuda Email Security Service can send notifications (quarantine digest) that a user has quarantined messages at predefined intervals. The notification interval can be set by the administrator for all users from the [USERS > Quarantine Notification](#) page, but you can also enable the user to override this setting and configure their own notification interval.

To enable users to manage quarantine notifications for their own accounts, make sure the **Allow users to specify interval** box is checked on the [USERS > Quarantine Notification](#) page. On that page you can also select a **Default interval for quarantine notifications**. Users can then access notification settings from their [Settings > Quarantine Notification](#) page, overriding the global setting.

The Quarantine Digest

The quarantine digest (summary) only goes out if new quarantined mail is saved in the user's account (inbox) 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, *no quarantine digest will be generated and sent* to that user for that same 24 hour period.

Advanced Configuration

Sender authentication and recipient verification are a critical part of maintaining security of email flowing into and out of your organization. By identifying known trusted senders and recipients of email, you can block a large percentage of spam, viruses and malware from your network.

<i>Sender Authentication</i>	38
<i>Recipient Verification</i>	39
<i>Secured Message Transmission</i>	39

Sender Authentication

This is a key feature of the Barracuda Email Security Service to protect 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.

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 are designated as 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 SFP check, it is assumed to be spam. For more information on SPF, please visit <http://www.openspf.org>.

Messages that fail SPF check can be blocked and will be logged as such. Enable or disable the Sender Policy Framework feature **for checking inbound mail** from the **INBOUND SETTINGS > Anti-Spam/Anti-Virus** page. Note that if you enable SPF, you might also want to enable the Sender Redirect Service (SRS) This option is configurable from the **Advanced Configuration** section of the **DOMAINS > Domain Details** page and, if enabled, the Barracuda Email Security Service will make the IP address of your sending mail server visible to the agent doing Sender Policy Framework (SPF) verification on the recipient's end.

SPF for Sending Outbound Email

To assure recipients of outbound mail from your Barracuda Email Security Service that Barracuda Networks is the authorized sending mail service, please add the following to the INCLUDE line of the SPF record for each of your domains sending **outbound** mail:

```
include:spf.ess.barracudanetworks.com
```

Custom policies and Sender Spoof Protection

For inbound email, organizations can define their own allowed sender domains, users or email addresses for sender authentication using the **INBOUND SETTINGS > Sender Policies** page. However, the safest way to indicate valid senders on the Barracuda Email Security Service is to whitelist (exempt) the IP addresses of trusted email servers from being scanned on the **INBOUND SETTINGS > IP Address Policies** page, then blacklist (block) their domain names on the **INBOUND SETTINGS > Sender Policies** page to prevent domain name spoofing. See *Content Analysis - Outbound Mail*, page 31 to configure sender policies for *outbound* email.

Recipient Verification

LDAP Lookup

You can ‘synchronize’ the Barracuda Email Security Service with your existing LDAP server to automatically create accounts for all users in the domain. For more information about user accounts, see *Managing Accounts*, page 41.

Configuration of LDAP lookup as well as LDAP authentication of user logins is done by domain from the **DOMAINS > Domain Details** page. From the **DOMAINS > Domain Manager** page, click the configuration button in the **Actions** column to the right of the domain name.

The following variables will need to be configured:

- **LDAP Host:** The server that is utilized for LDAP lookups. If this setting is a hostname, and is contained in multiple A records, or multiple space-separated hosts are provided, then fail-over capabilities will be available if the Barracuda Email Security Service is unable to connect to one of the machines listed here.
- **Bind DN/Username:** Username used to connect to the LDAP service on the specified LDAP Server. If of the form accountname@domain.com, the username is transformed into a proper LDAP bind DN like CN=accountname, CN=users, DC=domain, DC=com when accessing the LDAP server. Sometimes the default transformation does not generate a proper bind DN. In such cases, a fully formed and valid bind DN must be entered.
- **Password:** Password used to connect to the LDAP service on the specified LDAP Server.
- **Base DN:** The starting search point in the LDAP tree. The default value will look up the 'defaultNamingContext' top-level attribute and use it as the search base.
- **Authentication Filter:** Filter used to look up an email address and determine if it is valid for this domain. The filter consists of a series of attributes that might contain the email address. If the email address is found in any of those attributes, then the account is valid and is allowed into the Barracuda Email Security Service.
- **Mail Attributes:** The LDAP attributes you want to use (ex: mail, proxyAddress, etc.).
- **Synchronize Automatically:** Select *Yes* if you want The Barracuda Email Security Service to automatically synchronize your user list with your LDAP server on a regular basis. Synchronization means accounts will be created in the Barracuda Email Security Service for each user in your LDAP directory for the domain. Select *No* if you want to synchronize manually in case your LDAP server is not always available. To synchronize manually, click the **Synchronize Now** button.
- **Use LDAP for Authentication:** Setting to *Yes* enable authentication of user logins against your existing LDAP server.

Once you have entered information about your LDAP server, click the **Test Settings** button to ensure that the Barracuda Email Security Service can communicate with the server. LDAP server types supported include Active Directory, Novell eDirectory, Domino Directory and OpenLDAP.

Secured Message Transmission

To prevent data leakage and ensure compliance with financial, health care and other federally-regulated agency information policies, you can configure *inbound* and *outbound* message traffic to be transmitted over an encrypted TLS channel. However, if the peer SMTP server does not support TLS,

the message will not be sent over an encrypted channel. If you require a TLS connection, an *outbound* message will bounce if the receiving SMTP server does not support TLS.

For complete message encryption and ensured delivery of *outbound* messages, use the Barracuda Message Center to encrypt the *contents* of every outbound message. You can enable encryption for each domain from the [OUTBOUND SETTINGS > DLP/Encryption](#) page. For details about using encryption with the Barracuda Message Center, see *DLP and Encryption of Outbound Mail*, page 30.

TLS For Secured Inbound and Outbound Messages

TLS provides secure transmission of email content, both *inbound* and *outbound*, using the Secure Sockets Layer (SSL) - also known as TLS. From the [DOMAINS > Domain Details](#) page you can select:

- *Required*: All messages between the Barracuda Email Encryption Service and the destination server MUST be delivered via a TLS channel. If the destination server does not support a TLS connection, the message will not be delivered (it will ‘bounce’).
- *Optional*: All messages between the Barracuda Email Encryption Service and the destination server will be delivered via TLS if the destination server supports TLS connections. If not, the message will be delivered unencrypted.
- *Never*: TLS transmission is disabled.

Managing Accounts and Domains

If your Barracuda Email Security Service is responsible for filtering messages for more than one mail server or domain, you can configure spam and virus settings, filtering policy, authentication and quarantine settings on a per-domain basis.

Use this chapter to understand managing user accounts and domains in the Barracuda Email Security Service and configuring per-domain settings.

<i>Creating and Managing Domains</i>	42
<i>Creating and Managing Accounts</i>	42
<i>Editing User Accounts</i>	43
<i>User Account Features</i>	43

Creating and Managing Domains

Your Barracuda Email Security Service will only accept emails addressed to domains that it has been configured to recognize. After adding and verifying all domains you want the service to manage per instructions in *Configure Your Domains and Mail Servers* on page 18, you can manage each domain individually if you want to configure different policies and settings for each one. Settings for individual domains can be configured from the **DOMAINS** tab by clicking **Manage Domain** next to the domain for which you want to view the Message Log, view Statistics and manage all per-domain settings.

Domain Level Settings

Domains you add and verify will be initially configured with whatever you have specified your default global settings to be. Once you are managing an individual domain, you'll see the same Message Log, Inbound Settings and other tabs you see for managing all domains, but you won't see a **DOMAINS** tab. At the top of the **STATUS** page, you'll see the message:

You are now managing settings for <domain name>. [Return to account management.](#)

Click [Return to account management](#) when you want to go back to managing global settings for all domains.

If the administrator deletes a domain, a confirmation dialog box will prompt for confirmation of whether or not to delete a domain.

Creating and Managing Accounts

Local User Accounts

From the **USERS > User List** page you can manually add, update or delete local user accounts in the Barracuda Email Security Service if you are not using LDAP, or if you just want to create a few test accounts.

The first time the Barracuda Email Security Service receives an email for that user and the message is quarantined, a quarantine inbox will be created for the user automatically. Depending on how you have configured the quarantine notification interval on the **USERS > Quarantine Notification** page, the user will receive a quarantine digest at a specified time. From the **USERS > Quarantine Notification** page you can also enable the user to set their own quarantine notification interval.

Automatic Account Creation

There are two ways to have the Barracuda Email Security Service create user accounts:

- 1. LDAP Synchronization:** For increased security you can configure the Barracuda Email Security Service to validate the receiving email address of a message against your LDAP server before creating an account. This helps prevent creating accounts for invalid users. Configuration of LDAP parameters is detailed under *LDAP Lookup* on page 39.

With LDAP synchronization, the Barracuda Email Security Service can create user accounts for all users in the domain automatically based on your LDAP directory. The user list will then be synchronized with your LDAP server on a regular basis. The first time the Barracuda Email Security Service receives a *Not Allowed* email for a valid user:

- 1a. The Barracuda Email Security Service uses the email address of the recipient as the username of the account and auto-generates a password.
 - 1b. The user will receive an email with the login information so they can access their quarantine account.
 - 1c. The Barracuda Email Security Service places the quarantined message in the account holders's quarantine inbox.
 - 1d. Sends a quarantine summary report to the account holder at the specified notification interval.
2. **Auto Creation:** The first time the Barracuda Email Security Service receives an *Allowed* email for a nonexistent user at a domain configured for the service, a new user account is created. This method of new account creation does not use LDAP lookup.

Editing User Accounts

From the **Users** tab, the administrator can manage accounts for all domains configured in the Barracuda Email Security Service, deleting invalid accounts as needed and changing account passwords or settings, including Default Time Zone and quarantine notification interval.

Using the **USERS > Default Policy** page, you can configure default scan/block/allow policies for both *Managed Users* and *Unmanaged Users*. *Managed Users* are all of those users you have configured either manually or by synchronizing with your LDAP server and which appear in the **USERS > Users List** page. *Unmanaged Users* include all senders and recipients of email for the domains you've configured, but who are not in your users list for some reason.

If you don't edit these settings, all email will be scanned, by default, as opposed to blocked or allowed. From this page you can also set the Default Time Zone for all users.

From the **USERS > Add/Update Users** page, you can:

- Manually create or update user accounts with specific settings. If the Barracuda Email Security Service receives an email for a new user, the user will be sent a welcome email at that time IF you set **Notify New Users** on the page to *Yes*. Note that the link for the user to click in the welcome email to access their quarantine inbox will expire in 7 days.
- **Enable User Quarantine:** set to *On* or *Off*. For information on configuring user quarantine settings, see *Quarantine Notifications* on page 35.

To view or change a particular user's settings and view their **Message Log**, navigate to the **USERS > Users List** page and click the 'Log in' icon to the right of the account name to log in as that user.

User Account Features

Users can view their quarantine inbox (**Message Log**) and set some account preferences, depending on what has been enabled for their account by the administrator. Permissions may include:

- Modify individual settings for quarantine notification reports.
- Management of quarantine inbox - deliver or delete quarantined messages.
- Change password.

- Link Accounts - use the current account as an 'alias'. From the **SETTINGS > Linked Accounts** page, the user can add additional email addresses they may have in the same domain for which quarantined email should be forwarded to this account.
- Create whitelists (exempt) and blocklists (blocked) for email addresses, users and domains.

User Authentication With LDAP

To use LDAP for user login authentication, make sure to set **Use LDAP for Authentication** to *Yes* on the **DOMAINS > Domain Details** page for each domain you have configured in the Barracuda Email Security Service. The service can use your LDAP server both for creating new accounts, recipient verification and for authenticating users.

Regular Expressions

You can use regular expressions in some of the Barracuda Email Security Service features. Regular Expressions allow you to flexibly describe text so that a wide range of possibilities can be matched.

The following caveats apply when using regular expressions:

- Be careful when using special characters such as |, *, '!' in your text. For more information, refer to *Using special characters in expressions* on page 46.
- All matches are NOT case sensitive.

Table 9.1 describes the most common regular expressions supported by the Barracuda Email Security Service.

Table 9.1: Common Regular Expressions

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

Table 9.1: Common Regular Expressions

Expression	Matches...
Miscellaneous	
^	Beginning of line
\$	End of line
\b	Word boundary
\t	Tab character

Using special characters in expressions

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

Table 9.2: Special Characters

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

Examples

Table 9.3 provides some examples to help you understand how regular expressions can be used.

Table 9.3: Regular Expressions

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



Appendix B

Limited Warranty

Barracuda Online Services License and Warranty

READ THIS AGREEMENT CAREFULLY. Barracuda Networks, Inc. will provide Barracuda Networks Products or Services to you only if you accept all of these terms and conditions, the Barracuda Networks Privacy Policy, as well as any operating rules, policies, price schedules, and other supplemental documents published by Barracuda Networks from time to time, all of which are incorporated herein by reference (collectively, “License and Warranty” or “this Agreement”). BY DOWNLOADING OR USING THE BARRACUDA NETWORKS PRODUCTS AND SERVICES, YOU ARE AGREEING ON BEHALF OF THE ENTITY USING THE BARRACUDA NETWORKS PRODUCTS AND SERVICES THAT YOU WILL BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT AND THAT YOU HAVE THE AUTHORITY TO BIND THE ENTITY.

1. Definition of Terms

1.1 “Barracuda Networks,” “we,” “us,” or “our” mean Barracuda Networks, Inc. and its subsidiaries.

1.2 “You,” “yourself,” “user,” “subscriber,” “client,” and “you” refer to the individual or legal entity registering for or using the Barracuda Networks Products or Services.

1.3 “Barracuda Networks Products or Services” means data backup services, web filtering and security services, websites (including without limitation, www.barracuda.com, backup.barracuda.com, and control.barracuda.com), hardware, all other documentation, features, tools, Barracuda Networks Software or Hardware, and any other products or services provided by Barracuda Networks or its authorized agents, distributors, and licensees.

1.4 “Barracuda Networks Software or Hardware” means software or hardware provided or sold to you or for your use by Barracuda Networks. “Barracuda Networks Software” means the software licensed for your use located on Barracuda Networks Hardware or for installation on your network or computers. “Barracuda Networks Hardware” means hardware purchased or provided for your use by Barracuda Networks.

1.5 “Computer” means a desktop or laptop computer, network device, and any storage device attached to them in any fashion.

1.6 “Personal Information” means information that you may provide at the time of registration or otherwise, such as name, physical location or address, IP address, e-mail address, gender, year of birth, billing information, payment information, and postal code.

1.7 “Backup Data” includes any data you back up through Use of the Barracuda Networks Products or Services and any related data that are in the possession of Barracuda Networks or affiliates.

1.8 To “Publish” documents or information means to provide to or make them accessible to you by mailing, emailing, desktop messaging, faxing, or delivering them to you and/or by posting them to www.barracuda.com or any other website you visit to register for, subscribe to, license, buy, or Use Barracuda Networks Products or Services.

1.9 To “Use” Barracuda Networks Products or Services means each time you visit a Barracuda Networks website, register with Barracuda Networks, download Barracuda Networks Software or receive Barracuda Networks Hardware, use Barracuda Networks Software or Hardware, view the status of a Barracuda product, control a Barracuda Networks Product or Service, view the status of your Backup Data, store or restore Backup Data, or request support.

1.10 “Barracuda Networks Affiliate” means persons or entities who have provided products, licenses, or services to Barracuda Networks and persons or entities with which Barracuda Networks has entered into an agreement to sublicense or to provide Barracuda Networks Products or Services to users.

1.11 “Activation Date” means the earlier of: (i) the date Barracuda Networks grants you access to the services and (ii) the date on which you complete the online activation process.

1.12 “Authorized User” means an employee or a contractor of Customer who is authorized to use the Barracuda networks services provided hereunder.

1.13 Maximum Data Traffic Limit. An average of 950MB of data traffic per user per month.

2. Barracuda Backup Services

If you are using Barracuda Networks Backup Services and have paid for such services, the terms of this section apply; otherwise, they do not.

2.1 Guarantee of Data Backup. Barracuda Networks is responsible for backing up your data in accordance with the selections you make through the web-based control panel. Barracuda Networks does not make any further guarantee, expressed or implied, to backup any other data on or off of the client’s premises beyond the particular files and directories indicated by you in the control panel.

2.2 Data Backup STATUS Reporting. Barracuda Networks will provide you with the ability to view the condition of the overall backup status, as well as, backup status of individual files via the web-based control panel. It is your responsibility to verify that the data you intend to backup is accurately setup in the web-based control panel and is being backed-up and reporting no errors. Barracuda Networks will, in addition, monitor backup status and alert you by e-mail or telephone to potential problems, however, Barracuda Networks cannot be held responsible in any way if data is not backed up. It is your responsibility to verify that Barracuda Networks has the correct contact information for providing any alerts regarding backup issues.

2.3 Data Restoration. Barracuda Networks will provide various tools for you to restore data that has been backed-up. These tools include the secure web-based control panel and local network access using FTP protocol.

2.4 Failed Data Backups. Barracuda Networks is committed to maintaining reliable and redundant infrastructure to store your data. Barracuda Networks will normally complete your selected backup transfers within 72 hours. If the data backups are not completed within this time frame, Barracuda Networks will provide you notice via the control panel interface. This provision is restricted by the condition of your data network and all physical and Internet connectivity requirements being suitable for Barracuda Networks to perform its function properly. If Barracuda Networks indicates your data is properly backed up and it is determined that the data can not be restored as a direct result of a defect or error with a Barracuda Networks Product or Service, you shall be eligible for a refund. Properly backed up data is limited to data that the control panel shows as successfully backed up and for which there are no backup process warnings or errors reported in the control panel. You are solely responsible for verifying that the necessary files to restore specialized software systems, such as

databases and other data environments, are being created and are included in the data Barracuda Networks is backing up for you. The maximum amount of the refund shall be the total amount of money you have paid to Barracuda Networks directly related to the impacted product or service.

2.5 Barracuda Networks Products and Services save your data to a server operated by Barracuda Networks or a Barracuda Networks Affiliate. A copy of each file you designate is saved. Barracuda Networks Products and Services scans for changes or additions to these files and then periodically creates a copy of modified or newly designated file. You will not be able to restore files that Barracuda Networks has not completed copying or files that have been changed but not yet been backed up or not eligible for back up.

2.6 All your data, backed up by Barracuda Networks or otherwise stored via a Barracuda Networks Product or Service, is considered confidential and private, and will be secured using standard and proprietary encryption methods, and stored in facilities secured electronically and physically. In order to ensure integrity of data, Barracuda Networks computer software conducts bit level comparisons on some files and stores the data in an unidentifiable format on Barracuda Networks' storage servers. Barracuda Networks personnel require no express permission from the you to view this unidentifiable version of the raw data being stored on Barracuda Networks' storage servers. Barracuda Networks will also review information pertaining to file names, sizes, and revision dates for the purpose of confirming that your data is stored correctly. From time to time, you may request that Barracuda Networks personnel assist in setup process, the data restoration process, or review information in the web-based control panel. This action may expose information and the contents of your data to Barracuda Networks personnel. Your provide permission for Barracuda Personnel to view this data.

3. Barracuda Networks Web Filtering and Security Services

If you are using Barracuda Networks Web Filtering and Security Services and have paid for such services the terms of this section apply, otherwise they do not.

3.1 Subject to the terms and conditions of this Agreement, as of the Activation Date, Barracuda Networks will provide to you access to Barracuda Networks service, and bug fixes or other minor enhancements or improvements to such service. You acknowledges and agrees that the service will redirect your Internet web traffic to Barracuda Networks servers and such traffic will be checked against rules regarding malware uploaded by you to the service and then the traffic will be transmitted back to you.

3.2 Subject to the terms and conditions of this Agreement, if you order or download one or more Barracuda Networks Hardware or Software products. Barracuda Networks hereby grants to you a non-exclusive, non-transferable, limited license (without the right to sublicense) to use the Barracuda Networks Hardware or Software products solely as necessary to access and use the services as described herein.

3.3 Subject to the terms and conditions of this Agreement, Barracuda Networks hereby grants to you (and to each Authorized User for whom you have paid the applicable fee a non-exclusive, non-transferable, limited license (without the right to sublicense) to access and use the services via the Internet, solely for your internal business purposes and only in accordance with any applicable documentation. Your use of the services is subject to the Maximum Data Traffic Limit.

3.4 If usage of the service by Customer's Authorized Users exceeds the Maximum Data Traffic Limit in any given month during the term of the Agreement, Barracuda Networks will charge you the then-current overage fees and/or terminate this Agreement immediately.

4. Acceptance of License and Warranty; Modification; Cancellation

By registering to use Barracuda Networks Products or Services, and each time you use a Barracuda Networks Product or Service, you affirm your acceptance of these License and Warranty and agree to comply with them now and throughout the period of your use of the Barracuda Networks Products

or Services and thereafter, as noted in Section 6 (Barracuda Networks License to You) below. If you do not agree to these License and Warranty in their entirety, do not Use Barracuda Networks Products or Services.

Barracuda Networks may change the License and Warranty at any time, without prior notice to you, and in its sole discretion. The new or modified License and Warranty will be effective immediately upon posting on our website at www.barracuda.com, control.barracuda.com, or backup.barracuda.com.

If you do not agree to be bound by Barracuda Networks' License and Warranty as Published by Barracuda Networks from time to time, your sole and exclusive remedy is to discontinue using Barracuda Networks Products or Services and return any Barracuda Products.

If you wish to cancel your Barracuda Networks license after a change in the License and Warranty, you must do so in writing or by email within thirty (30) calendar days after your next Use of a Barracuda Networks Product or Service following the change in the License and Warranty. For this type of cancellation you will receive a pro-rata refund for the unused portion of your Barracuda Networks license as of your date of notice. You acknowledge and agree that if you do elect to cancel your license within this specified period after a change in the License and Warranty, or if you cancel your license or fail to renew an expired or terminated license for any reason, Barracuda Networks may delete any information that Barracuda Networks has obtained through your Use of Barracuda Networks Products or Services, including without limitation, your Backup Data, Configuration data, and account data. Barracuda Networks will not have any Backup Data available for your use.

4.1 Requirements for Registration or Use of Barracuda Networks Products: Barracuda Networks Products or Services are intended and offered only for lawful Use by individuals or organizations with the legal capacity and authority under applicable law to enter into a contract. Barracuda Networks does not offer Barracuda Networks Products or Services to minors or where prohibited by law. By registering for and/or by Using Barracuda Networks Products or Services, you represent and warrant that you have the legal capacity and authority to enter into a binding agreement to adhere to the Barracuda Networks License and Warranty and that you will Use Barracuda Networks Products or Services only in accordance with these License and Warranty and with all applicable laws. If you are Using Barracuda Networks Products or Services on behalf of an entity or organization, you warrant, represent, and covenant to Barracuda Networks that you are duly authorized to agree to these License and Warranty on behalf of the organization and to bind the organization to them.

You agree to provide accurate and complete information when you register for a Barracuda Networks Product or Service and you agree to keep such information accurate and complete during the entire time that you Use Barracuda Networks Products or Services.

We may ask you from time to time to establish a user name or password to access or Use the Barracuda Networks Products or Services. You are solely responsible for any consequences arising in whole or in part out of your failure to maintain the confidentiality of your username and/or password.

You acknowledges that the use of or connection to the Internet provides the opportunity for unauthorized third parties to circumvent security precautions and illegally gain access to Barracuda Networks Products and Services. Accordingly, Barracuda Networks cannot and does not guaranty the privacy, security or authenticity of any information so transmitted over or stored in any system connected to the Internet.

4.2. Lawful Use of Barracuda Networks Products or Services: You may not Use Barracuda Networks Products or Services for any unlawful purpose. Without limiting the foregoing:

Barracuda Networks Products or Services may not be Used to store, backup, or distribute child pornography and may not be Used in violation of U.S. export control laws or the export or import regulations of other countries. You agree to comply strictly with all such laws and regulations and acknowledge that you have the responsibility to obtain licenses to export, re-export, or import as may be required.

You may not Use Barracuda Networks Products or Services if you are a citizen, national, or resident of, or are under control of, the government of Cuba, Iran, Sudan, Libya, North Korea, Syria, or any other country to which the United States has prohibited export. Each time you Use Barracuda Networks Products or Services you represent, warrant, and covenant that: (i) You are not a citizen, national, or resident of, nor under the control of, any such country to which the United States has prohibited export; (ii) You will not download or otherwise export or re-export the Barracuda Networks Software or Hardware, directly or indirectly, to the above mentioned countries nor to citizens, nationals or residents of those countries; (iii) You are not listed on the U.S. Department of Treasury's Lists of Specially Designated Nationals, Specially Designated Terrorists, and Specially Designated Narcotic Traffickers, the U.S. Department of State's List of Statutorily Debarred Parties, or the U.S. Department of Commerce's Denied Persons List, Entity List, or Unverified List Table of Denial Orders; (iv) You will not download or otherwise export or re-export the Barracuda Networks Software or Hardware, directly or indirectly, to persons on the above mentioned lists; (v) You will neither Use nor allow the Barracuda Networks Software or Hardware to be Used for, any purposes prohibited by United States federal or state law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical, or biological weapons of mass destruction; (vi) The Barracuda Networks Software or Hardware will not be exported, directly, or indirectly, in violation of these laws, nor will the Barracuda Networks Products or Services be Used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation; and (vii) You are not using or permitting others to Use Barracuda Networks Products or Services to create, store, backup, distribute, or provide access to child pornography.

5. Changes to the Barracuda Networks Products or Services

Barracuda Networks has the right at any time to change, modify, add to, discontinue, or retire any Barracuda Networks Product or Service and any aspect or feature of the Barracuda Networks Products or Services including, but not limited to, the software, hours of availability, equipment needed for access or Use, the types of files that are backed-up (not every file on your computer is backed-up), the maximum disk space that will be allotted on Barracuda Networks servers on your behalf either cumulatively or for any particular service, or the availability of Barracuda Networks Products or Services on any particular device or communications service.

Barracuda Networks will provide notice of material changes to the Barracuda Networks Products or Services or changes to this Agreement by posting them to www.barracuda.com, control.barracuda.com, or backup.barracuda.com. Barracuda Networks shall have no obligation to provide you with notice of any such changes in any other manner. It shall be your responsibility to check our website periodically to inform yourself of any such changes.

From time to time, Barracuda Networks may issue new releases, revisions, or enhancements to the Barracuda Networks Products or Services available to you free of charge or for a fee. New releases, revisions or enhancements may be licensed, downloaded, and installed only to the extent that you hold a valid license to Use the Barracuda Networks Products or Services being updated or upgraded, and you may Use them only in accordance with the then-current License and Warranty and any additional license terms that may accompany them.

Barracuda Networks may automatically update Barracuda Networks Products or Services you have installed on your computer without your prior consent. If any automatic updates involve the payment of additional fees, we will provide you with the opportunity to approve such fees prior to the new functionality being enabled. If you fail or refuse to approve such fees, Barracuda Networks may, in its sole discretion, terminate your current license, continue to support your current Barracuda Networks Products or Services without the automatic update, or replace your Barracuda Networks

Products or Services with other Barracuda Networks Products or Services. If Barracuda Networks terminates your current license on account of your failure or refusal to approve such fees, then Barracuda Networks will refund, on a pro-rata basis based on the remaining term of the current license, any fees related to the period during which you will not have access to your Barracuda Networks Products or Services. If Barracuda Networks updates the Barracuda Networks Products or Services without requiring an additional fee and you object to such change, your sole remedy shall be to terminate your use of the Barracuda Networks Products and Services.

Barracuda Networks reserves the right at any time to charge or modify fees for the Barracuda Networks Products or Services. However, such fees shall not be charged unless your prior agreement to pay such charges is obtained. Thus, if at any time Barracuda Networks requires a fee for the Service, you will be given reasonable advance notice of such fees and the opportunity to cancel before such charges are imposed. If you elect not to pay any fees charged by Barracuda Networks, Barracuda Networks shall have the right to cease providing Barracuda Networks Products or Services to you.

6. Barracuda Networks License to You; Renewals, Modifications, Limits

6.1 Scope of License. Barracuda Networks grants you a non-exclusive, non-transferable limited and revocable license to use the Barracuda Networks Software or Hardware only on the hardware provided by Barracuda Networks for which you have paid the applicable fees and taxes and from which you are licensed to access the Barracuda Networks Products or Services, and to Use the Barracuda Networks Products or Services for the sole and exclusive purposes of connecting to and using the Barracuda Networks Products or Services for your personal or internal business purposes in accordance with these License and Warranty, provided you comply and remain in compliance with this Agreement. We reserve all other rights to the Barracuda Networks Products or Services.

You may not sub-license, or charge others to Use or access, the Barracuda Networks Products or Services and you may not redistribute the Barracuda Networks Products or Services or provide others with access to or Use of them, unless you have entered into a Reseller, Affiliate or similar Agreement with Barracuda Networks to engage in this activity. Without limiting the forgoing, you will not permit others to Use the Barracuda Networks Products or Services to access or decrypt data stored on servers provided by Barracuda Networks or Barracuda Networks Affiliates; you will not Use or permit others to Use the Barracuda Networks Products or Services to decrypt data encrypted by others; and you will not Use or permit others to Use the Barracuda Networks Products or Services to provide encryption or decryption services to others, whether or not such services are compensated.

6.2 Renewals and Payments. You agree that Barracuda Networks shall have the right to automatically and without notice renew your license to continue to Use the Barracuda Networks Products or Services upon expiration of your then-current license, and that as part of such renewal Barracuda Networks shall have the right to charge the applicable renewal fees and any applicable taxes to any credit card you used to purchase your then-current license. You agree that if you elect to not permit Barracuda Networks the right to automatically renew your license to Use Barracuda Networks Products or Services or your credit card information on file with Barracuda Networks does not permit automatic renewal, then Barracuda Networks may terminate your license.

You agree that if you have licensed Barracuda Networks Products or Services for a period of greater than ninety (90) calendar days you have thirty (30) calendar days from the date that your license was renewed to elect to discontinue your Use of Barracuda Networks Products or Services. If you have licensed Barracuda Networks Products or Services for a period of less than or equal to ninety (90) calendar days you have seven (7) calendar days from the date that your license was renewed to elect to discontinue your Use of Barracuda Networks Products or Services. If you elect to discontinue your Use of Barracuda Networks Products or Services within this period, you will be issued a full refund for the amount of your license renewal. You are responsible for ensuring that Barracuda Networks has current and accurate records necessary, to renew your license, including without limitation, credit card data.

Any payment not received from you by the due date shall accrue (except with respect to charges then under reasonable and good faith dispute), at the lower of one and a half percent (1.5%) of the outstanding balance per month (being 18% per annum), or the maximum rate permitted by law, from the date such payment is due until the date paid. You also agree to pay all sums expended (including reasonable legal fees) in collecting overdue payments.

6.3 Barracuda Networks does not offer any refunds for purchases of Barracuda Networks Products or Services, except as expressly provided in this Agreement.

6.4 Permitted License Uses and Restrictions. This License allows you to use the Barracuda Networks Software provided on the Barracuda Networks Hardware only on the single Barracuda labeled hardware device on which the software was delivered. You may not make copies of the Barracuda Networks Software provided on the Barracuda Networks Hardware 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. You may not transfer, rent, lease, lend, or sublicense the Barracuda Networks Software.

7. Assignment and Delegation by Barracuda Networks

Barracuda Networks may, in its sole discretion, transfer or assign all or any part of its rights in the Barracuda Networks Software or Hardware, the Barracuda Networks Products or Services, and any license or contract related thereto, and may delegate all or any portion of its duties, if any, under any such Barracuda Networks Products or Services, licenses, or other contracts.

8. No Transfers or Modifications by You

You may not sell, assign, grant a security interest in or otherwise transfer any right in the Barracuda Networks Products or Services, nor incorporate them (or any portion of them) into another product or service. You may not copy the Barracuda Networks Products or Services. You may not translate, reverse-engineer or reverse-compile or decompile, disassemble, make derivative works from, or otherwise attempt to discover any source code in the Barracuda Networks Software or Hardware or decrypt any files that are not associated with your computer. You agree not to create Internet links to any database portion or frame or mirror any data contained in any Barracuda Networks Product or Service. You agree not to make any data accessible from or use Barracuda Networks Product or Service in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, or any other data or code for detecting malicious code or data. You agree to delete any Barracuda Networks Software from any device on which it is installed prior to selling or transferring the device.

You may not modify the Barracuda Networks Software or Hardware or use it in any way not expressly authorized by these License and Warranty. You may not obtain the communications protocol for accessing the Barracuda Networks Products. You may not authorize or assist any third party to do any of the foregoing.

9. Protection of Data

You are solely responsible for protecting the information on your computer such as by installing anti-virus software, updating your applications, password protecting your files, and not permitting third party access to your computer. You understand that the Barracuda Networks Products or Services may back-up files that are no longer usable due to corruption from viruses, software malfunctions or other causes. This might result in you restoring files that are no longer usable.

9.1 For the purposes of maintaining hardware systems responsible for providing Barracuda Networks' services to you, you grant to Barracuda Networks permission to obtain remote access to such Barracuda Networks Products and Services in order to perform routine software maintenance and system health evaluations. Some of these functions include, but are not limited to, the maintenance of operating systems & Barracuda Networks software, installation and setup of new software versions, installation of security patch updates, hardware health monitoring, processor load monitoring, and bandwidth usage monitoring.

9.2 From time to time, you may request that Barracuda Networks personnel assist in setup process, the data restoration process, or review information in the web-based control panel for a Barracuda Networks Product or Service. This action may expose information and the contents of your data to Barracuda Networks personnel. You provide permission for Barracuda Personnel to view this data.

10. Deletion of Backup and other data

If your license to Use Barracuda Networks Products or Services expires, is terminated, is not renewed, or is otherwise discontinued for any reason, Barracuda Networks and the Barracuda Networks Affiliates may, without notice, delete or deny you access to any of your data that may be in their possession or control.

You agree that if your license has been terminated, expired, or otherwise lapsed for any reason, that your files may not be available should you wish to restore them, your data may not be viewable, and that network traffic may be blocked.

You agree that Barracuda Networks and Barracuda Networks Affiliates may retain (but shall have no obligation to retain) your data for a period after your license has been terminated, expired, or otherwise lapsed, as part of Barracuda Networks' marketing to you the opportunity to purchase, renew, or extend a license.

11. Customer Support

Subject to payment by you of the applicable fees, and provided that you are in compliance with the terms and conditions of this Agreement, Barracuda Networks will provide you standard support services for the specific product purchased by you. Support may be available only on selected days and during a limited number of hours. Support may also be available through only certain delivery vehicles such as email or telephone and some support may only be available for the payment of an additional fee or charge. As part of the delivery of support Barracuda Networks may employ a variety of tools or services to aid in the process of resolving your issues. You grant Barracuda Networks the right to use these tools and hold Barracuda Networks harmless for the use of these tools as well as the guidance provided by the support staff who in no way can be fully aware of all of the complexities associated with the Barracuda Networks Product and Services, your computer, and your infrastructure.

12. Restrictions on Access to Barracuda Networks Products or Services

You may access Barracuda Networks Products or Services only through the interfaces and protocols provided or authorized by Barracuda Networks. You agree that you will not access Barracuda Networks Products through unauthorized means, such as unlicensed software clients or tampering. Certain Barracuda Networks Products backup only certain types of files. You agree not to circumvent these limitations in any way, including but not limited to, changing file extensions or header information.

13. Communications

You are responsible for obtaining and maintaining all of the hardware, software, and services that you may need to access and Use Barracuda Networks Products or Services. Without limiting the foregoing, you must pay all charges, taxes, and other costs and fees related to obtaining your own Internet access, telephone, computer, and other equipment. and any communications or other charges incurred by you to access Barracuda Networks Products or Services.

14. Termination and Fair Use Policy

BARRACUDA NETWORKS SHALL HAVE THE ABSOLUTE AND UNILATERAL RIGHT IN ITS SOLE DISCRETION TO DENY USE OF AND ACCESS TO ALL OR ANY PORTION OF BARRACUDA NETWORKS PRODUCTS OR SERVICES TO USERS WHO ARE DEEMED BY BARRACUDA NETWORKS TO BE USING THE BARRACUDA NETWORKS PRODUCTS OR SERVICES IN A MANNER NOT REASONABLY INTENDED BY BARRACUDA NETWORKS OR IN VIOLATION OF LAW, INCLUDING BUT NOT LIMITED TO SUSPENDING OR TERMINATING A USER'S ACCOUNT WITH BARRACUDA NETWORKS AND THE LICENSE TO USE THE BARRACUDA NETWORKS PRODUCTS OR SERVICES.

You agree that Barracuda Networks may terminate your Account and access to the Barracuda Networks Products or Services for reasons including, but not be limited to, breaches or violations of these Terms of Service, a request by you to terminate your Account, discontinuance or material modification to the Barracuda Networks Products or Services, unexpected technical issues or problems, extended periods of inactivity and requests by law enforcement or other government agencies. Termination of your Barracuda Networks Account includes termination of access to the Barracuda Networks Products or Services, deletion of your Account information such as your e-mail ID and Password and deletion of data in your Account as permitted or required by law. Upon Termination, you agree to uninstall and destroy software components provided to you as part of the Barracuda Networks Products or Services.

You agree that we may, in our sole discretion and from time to time, establish or amend general operating practices to maximize the operation and availability of Barracuda Networks Products or Services and to prevent abuses. As part of these practices, we reserve the right to monitor our system to identify excessive consumption of network resources and to take such technical and other remedies as we deem appropriate. Your consumption of Barracuda Networks Products or Services may be deemed excessive if, within any month, your usage greatly exceeds the average level of monthly usage of Barracuda Networks' users, generally. In the event you are deemed to have violated this policy, we reserve the right to offer an alternative pricing plan that will permit you to continue to use Barracuda Networks Products or Services. Although violations of this policy have been infrequent, we nevertheless reserve the right to terminate or suspend your license and any license to use the Barracuda Networks Software or Hardware, without prior notice in the event of a violation of this policy.

15. Data Collection, Encryption, Privacy, and Disclosure

Barracuda Networks will collect and use Personal Information in accord with the terms of our Barracuda Networks Privacy Policy, which is incorporated into and made a part of these License and Warranty. You hereby consent to Barracuda Networks' use of your Personal Information under the terms of the Barracuda Networks Privacy Policy, as it may be amended from time to time.

To provide its services, Barracuda Networks Software or Hardware routinely scans your computer network in order to detect new, modified, or deleted data files that require further action to complete backup and restore operations. Barracuda Networks Software or Hardware also catalogs the number and total storage size of various file types on your computer network.

Data is transmitted to and stored at Barracuda Networks storage facilities in an encrypted format. You hereby give authorization for Barracuda Networks to access the data during the process of assisting you with any support request or data restoration process.

16. Warranties

16.1 SOFTWARE WARRANTY. Barracuda Networks warrants that the Barracuda Networks Products or Services will for a period of thirty (30) days from the date of registration and payment perform substantially as specified in the applicable Barracuda Networks documentation. If you satisfactorily demonstrate to Barracuda Networks within such thirty (30) day period that a Barracuda Networks Product or Service contains errors, then as Barracuda Networks' sole and exclusive liability

and as your sole and exclusive remedy, Barracuda Networks shall at its sole option either use commercially reasonable efforts to correct the errors reported by you, replace the Barracuda Networks Product or Services affected with a substantially conforming product or service, or refund the fee you paid for the Barracuda Networks Product or Service and terminate your license under the License and Warranty. Barracuda Networks does not warrant the results of its correction or replacement Barracuda Networks Products or Services. Correction or replacement under this Section 16 (Warranties), and the issuance of any corrections, patches, bug fixes, workarounds, upgrades, enhancements, or updates by Barracuda Networks to you, shall not be deemed to begin a new, extended, or additional license, license period, or warranty period. 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.

16.2 LIMITED HARDWARE WARRANTY. Barracuda Networks or authorized Distributor selling the Barracuda Networks Product or Service, if sale is not directly by Barracuda Networks, warrants that commencing from the date of delivery to you (but in case of resale by a Barracuda Networks reseller, commencing not more than sixty (60) days after original shipment by Barracuda Networks), and continuing for a period of one (1) year: (a) its hardware 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 hardware, 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 you 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. 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 hardware 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.** 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 OR SERVICES, 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 SERVICES AND THE SOFTWARE IS PROVIDED "AS-IS" AND BARRACUDA NETWORKS DOES NOT WARRANT THAT ITS PRODUCTS OR SERVICES 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 OR SERVICES, 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.

16.3 DISCLAIMER OF OTHER WARRANTIES. THE LIMITED WARRANTY IN THE PRECEDING PARAGRAPH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, WRITTEN OR ORAL, INCLUDING BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT, AND ANY WARRANTY ARISING BY STATUTE OR OTHERWISE IN LAW, OR FROM A COURSE OF DEALING OR USAGE OF TRADE. Barracuda Networks and the Barracuda Networks Affiliates do not warrant that the functions contained in the Barracuda Networks Products or Services will meet your requirements, that the operation of the Barracuda Networks Products or Services will be uninterrupted or error-free, or that defects in the Barracuda Networks Products or Services will be corrected. Barracuda Networks and Barracuda Networks Affiliates do not warrant or make any representations regarding the use or the results of the use of the Barracuda Networks Products or Services in terms of their correctness, accuracy, reliability or otherwise. Barracuda Networks and Barracuda Networks Affiliates do not represent or warrant that users will be able to access or use the Barracuda Networks Products or Services at times or locations of their choosing, or that Barracuda Networks and Barracuda Networks Affiliates will have adequate capacity for any user's requirements. No oral or written statement, information or advice given by Barracuda Networks, Barracuda Networks Affiliates, or their respective employees, distributors, dealers, or agents shall create any warranties in addition to those express warranties set forth in this Section 16 (Warranties). You may have other statutory rights. However, to the full extent permitted by law, the duration of statutorily required warranties, if any, shall be limited to the warranty period.

17. Limitation of Liability

With respect to defects or deficiencies in the Barracuda Networks Products or Services, the liability of Barracuda Networks and Barracuda Networks Affiliates will be limited to performance of its responsibilities under Section 16 (Warranties) above. With respect to other breaches of contract, the liability of Barracuda Networks and Barracuda Networks Affiliates shall be limited to your actual damages, and in no event will such liability exceed the total amount received by Barracuda Networks from you under these License and Warranty for your current license period, and only such amounts as relate to the computer affected by the breach. IN NO EVENT WILL Barracuda Networks, THE Barracuda Networks CONTRACTS, Barracuda Networks DISTRIBUTORS OR Barracuda Networks SUPPLIERS BE LIABLE TO YOU OR TO ANY THIRD PARTY FOR ANY LOST PROFITS, LOST DATA, INTERRUPTION OF BUSINESS, OR OTHER SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING OUT OF THE USE OR INABILITY TO USE THE Barracuda Networks PRODUCTS OR SERVICES OR TO USE OR RETRIEVE ANY BACKUP DATA, WHETHER FOR BREACH OF WARRANTY OR OTHER CONTRACT BREACH, NEGLIGENCE OR OTHER TORT, OR ON ANY STRICT LIABILITY THEORY, EVEN IF Barracuda Networks HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES OR A REMEDY SET FORTH IN THESE TERMS OF USE IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE, AND WHETHER OR NOT SUCH LOSS OR DAMAGES ARE FORESEEABLE.

Neither Barracuda Networks nor any Barracuda Networks Affiliate assumes any liability to any party other than you arising out of your Use or inability to Use the Barracuda Networks Products or Services. The limitations of damages set forth above are fundamental elements of the bargain between Barracuda Networks and you. Barracuda Networks would not be able to provide the Barracuda Networks Products or Services to you without such limitations.

18. Indemnification

YOU AGREE TO DEFEND, INDEMNIFY AND HOLD HARMLESS Barracuda Networks, Barracuda Networks AFFILIATES, AND THEIR RESPECTIVE DIRECTORS, OFFICERS, EMPLOYEES AND AGENTS FROM AND AGAINST ALL CLAIMS, DAMAGES, LOSSES, LIABILITIES, AND EXPENSES, INCLUDING WITHOUT LIMITATION ATTORNEYS' FEES, ARISING OUT OF YOUR USE OF THE Barracuda Networks PRODUCTS OR SERVICES AND/OR YOUR VIOLATION OF ANY TERM OF THESE License and Warranty.

Barracuda Networks RESERVES THE RIGHT, AT ITS OWN EXPENSE AND IN ITS SOLE DISCRETION, TO ASSUME THE EXCLUSIVE DEFENSE AND CONTROL OF ANY MATTER OTHERWISE SUBJECT TO INDEMNIFICATION BY YOU. IN THAT EVENT, AND ONLY IN SUCH EVENT, SHALL YOU HAVE NO FURTHER OBLIGATION TO PROVIDE A DEFENSE FOR Barracuda Networks IN THAT MATTER. If Barracuda Networks chooses to provide its own defense in connection with any matter subject to indemnification under these License and Warranty, you shall participate and cooperate in the defense of Barracuda Networks and Barracuda Networks Affiliates, at your own expense, to the full extent requested by Barracuda Networks.

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

19. Trademarks, Service Marks, and Other Intellectual Property

All trademarks, service marks or other similar items appearing on the Barracuda Networks Products or Service are the property of their respective owners, including, without limitation, Barracuda Networks, Inc.

The Barracuda Networks Products or Services are protected by copyright and other intellectual property laws, title, ownership rights, and intellectual property rights in the Barracuda Networks Products or Services shall remain with Barracuda Networks and its licensors. You agree not to take any action to jeopardize, limit, or interfere in any manner with Barracuda Networks' or its licensor's ownership of or rights with respect to the Barracuda Networks Products or Services.

20. U.S. Government Restricted Right

The Barracuda Networks Software or Hardware is a "commercial item" as that term is defined at 48 C.F.R. 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in 48 C.F.R. 12.212. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4, all U.S. Government end users acquire the Barracuda Networks Software or Hardware with only those rights set forth therein.

21. High Risk Activity

You acknowledge and agree that the Barracuda Networks Products or Services are not intended for use with any high risk or strict liability activity, including, without limitation, air or space travel, technical building or structural design, power plant design or operation, life support or emergency medical operations or uses, and that Barracuda Networks makes no warranty and shall have no liability arising from any Use of the Barracuda Networks Products or Services in any high risk or strict liability activities.

22. Dispute Resolution, Arbitration, Governing Law, and Venue

(a) Arbitration of Domestic (U.S.) Disputes. All disputes arising under or relating to this Agreement shall be resolved by final and binding arbitration conducted before a single arbitrator pursuant to the commercial arbitration rules of Resolute Systems, Inc. that were in force as of April 30, 2008. Evidentiary hearings and any other proceedings requiring personal attendance of parties or their representatives or witnesses shall be conducted in San Jose, CA or such other place within the United States as the arbitrator may direct in the case of all other Licensees.

(b) Arbitration of International Disputes. Notwithstanding the provisions of Subsection 22(a) (Arbitration of Domestic Disputes), any dispute arising under this Agreement that involves a dispute between Barracuda Networks and a person who is neither a citizen nor a resident of the United States, shall, at either party's request, be finally settled under the Rules of Arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with the said Rules, with such arbitration to be conducted in USA or such other place as the parties to such arbitration may agree.

(c) Exceptions to Agreement to Arbitrate. Notwithstanding the provisions of Subsections 22(a) (Arbitration of Domestic Disputes) and 22(b) (Arbitration of International Disputes), disputes pertaining to i) export controls, ii) unlawful Use of the Barracuda Networks Products or Services, or iii) the scope, applicability, or compliance with governmental or court-ordered access to or limits on use of Backup Data, shall not be resolved by arbitration, but shall instead be resolved by reference to a judicial or administrative body with jurisdiction over the dispute.

(d) Costs of Arbitration. The administrative expenses, arbitrator fees, and facility charges associated with the arbitration, whether domestic or international, shall be split equally between the parties. Each party shall be solely responsible for its attorney fees, expert witness fees, and other costs, fees, and expenses, except as may otherwise be provided in Section 18 (Indemnification).

(e) Discovery Procedures in Arbitration. The parties shall be entitled to such discovery as in the judgment of the arbitrator is appropriate, in light of the nature and objectives of arbitration, to ensure that each party has an adequate opportunity to determine the factual bases for its claims and defenses.

(f) Form and Effects of Award. The arbitrator shall render a naked award. Judgment on any arbitral award under this Agreement may be entered in any court of competent jurisdiction. It is the intent of the parties that neither the award nor any resulting judgment have res judicata (claim preclusion) or collateral estoppel (issue preclusion) effects except as between the parties themselves.

(g) Governing Law. The arbitration undertaking in this Agreement shall be governed by, construed, and interpreted in accordance with the Federal Arbitration Act, 9 U.S.C. §§ 1 et seq. and, in the case of arbitrations involving one or more non-U.S. parties, by the Convention on the Recognition and Enforcement of Foreign Arbitral Awards and the U.S. legislation implementing the same, 9 U.S.C. §§ 201 et seq. To the extent that the Arbitration provisions of this Agreement do not apply, the federal and state courts sitting in Santa Clara County, California, USA shall have exclusive jurisdiction and venue to adjudicate any dispute arising out of this Agreement. Each party hereto expressly consents to the personal jurisdiction of the courts of California and service of process being effected by registered U.S. mail or by private delivery service providing proof of delivery, sent to the party being served.

All other provisions of this Agreement shall be governed by and construed and interpreted in accordance with the internal laws of the State of California Santa Clara County, USA, without regard to conflict of laws provisions. The United Nations Convention on Contracts for the International Sale of Goods as well as any other similar law, regulation or statute in effect in any other jurisdiction shall not apply.

23. Termination, Expiration, Cancellation

(a) Limited Term. Your license will end upon the expiration of its stated term, upon your non-renewal of the licenses, upon your cancellation of the license, when Barracuda Networks elects to discontinue the product, upon your breach of these License and Warranty (if such breach is not cured within the

time indicated below in this Section 23 (Termination, Expiration, Cancellation), or when Barracuda Networks cancels or terminates your license, whichever occurs first (any such expiration, cancellation, discontinuation, or termination are referred to hereafter as “termination.”)

(b) Termination for Unlawful or Abusive Use, Other Breach. Barracuda Networks may block your access to your Backup Data and/or terminate your Use of the Barracuda Networks Products or Services if Barracuda Networks reasonably believes that the Backup Data may contain child pornography or are being used to support other types of illegal activities, if providing Barracuda Networks Products or Services to a person located in a particular country would violate U.S. or other applicable law, or if your continued Use of Barracuda Networks Products or Services may damage, disable, overburden, or impair our servers or networks.

(c) Right to use termination. If you breach these License and Warranty, your right to Use the Barracuda Networks Products or Services shall automatically terminate if you fail to cure the breach after seven (7) calendar days after notice from Barracuda Networks or any of the Barracuda Networks Affiliates, unless your breach is due to violations of Section 4 (Lawful Use), Section 8 (No Transfers or Modifications by You), Section 18 (Indemnification), Section 19 (Trademarks), Section 20 (U.S. Government Restrictions), in which case termination will be without notice and without any right to cure.

(d) Upon termination: i) you shall immediately cease any and all Use of the Barracuda Networks Products or Services and delete all copies of them; ii) the Barracuda Networks Software or Hardware may be disabled by Barracuda Networks without notice to you; and iii) you will no longer have the right to access or retrieve your Backup Data; you hereby grant Barracuda Networks the unrestricted right to delete all such Personal Information and Backup Data at any time after termination, without notice.

24. Survival

In the event of any termination, expiration, or cancellation, the restrictions on your Use of the Software and the other applicable restrictions as set forth in Section 4 (Lawful Use), Section 6 (Barracuda Networks License), Section 8 (No Transfers or Modifications by You), Section 16 (Warranties), Section 17 (Limitation of Liability), Section 18 (Indemnification), Section 19 (Trademarks, Service Marks, and Other Intellectual Property), Section 20 (U.S. Government Restricted Right), Section 21 (High Risk Activity), Section 22 (Dispute Resolution, Governing Law, Venue), Section 24 (Survival), Section 25 (Notice), Section 28 (Limitation on Actions), and Section 30 (Miscellaneous) shall survive such termination, expiration, or cancellation, and you agree to remain bound by those terms.

25. Notice

Any notice that may or must be given by Barracuda Networks in connection with this Agreement or in connection with the Use of the Barracuda Networks Products or Services, may be given by sending it to the email address provided by you upon registering for the Barracuda Networks Products or Services or as you may provide from time to time thereafter by modifying your user profile at www.barracuda.com. You are responsible for ensuring that your accurate email address is available to Barracuda Networks and provide any needed updates. Barracuda Networks may, in its sole discretion, use other means of providing notice, such as: desktop notification; regular, certified, or registered mail; fax; commercial delivery service; or messenger. All such notices shall be deemed given when dispatched with payment of delivery charges made or arranged. You hereby consent to receiving notice by any such means. Notwithstanding the foregoing, Barracuda Networks has no obligation to provide notice or attempt to locate a you other than through the email address provided.

26. English Language

These License and Warranty were negotiated and written in English. Any inconsistency between the License and Warranty as expressed in English and any other language shall, to the full extent permitted by applicable law, be resolved by reference to the English version. Les parties ont convenu de rediger cette entente en anglais.

27. Entire Agreement; Applicability of Terms; Construction; Limit to Modifications; Conflicts in Terms

These License and Warranty (including the items incorporated by reference and modifications that may be made from time to time), constitute the entire agreement between Barracuda Networks and you regarding Barracuda Networks Products or Services, and supersedes all prior agreements between you and Barracuda Networks regarding the subject matters hereof.

Any item or service furnished by Barracuda Networks in furtherance of these License and Warranty, although not specifically identified in them, shall nevertheless be covered by these License and Warranty unless specifically covered by some other agreement entered into in written or electronic form between you and us.

Any modification or change in these License and Warranty proposed or offered by you shall not become a part of these License and Warranty unless accepted in a writing dated after the effective date of the applicable License and Warranty and signed by an authorized officer of Barracuda Networks.

Should there be any conflict in terms between this Agreement and any other document, the terms and conditions set forth in this Agreement shall govern.

Any references that are singular or plural and any references that are masculine, feminine, or neuter in gender, are meant to be used interchangeably as the context of the sentence might imply.

28. Limitation on Actions

Unless otherwise required by law, an action or proceeding by you to enforce an obligation, duty, or right arising under this Agreement or by law must be commenced within one year after the cause of action accrues.

29. Copyright Infringement Notification

As provided in the Digital Millennium Copyright Act of 1998, we have designated the following individual for notification of potential copyright infringement regarding Web sites hosted by Barracuda Networks: info@barracuda.com

If you believe content hosted by Barracuda Networks infringes a copyright, please provide the following information to the person identified above (17 U.S.C. § 512): (i) A physical or electronic signature of the copyright owner or authorized agent; (ii) Identification of the copyrighted work(s) claimed to have been infringed; (iii) Identification of the material that is claimed to be infringing or to be the subject of the infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit us to locate the material; (iv) Information regarding how we may contact you (e.g., mailing address, telephone number, e-mail address); (v) A statement that the copyright owner or its authorized agent has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and (vi) A statement that the information in the notification is accurate, and made under penalty of perjury, and, if an agent is providing the notification, a statement that the agent is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

30. Miscellaneous

You agree to reimburse Barracuda Networks for any costs or fees related to its enforcement of this Agreement, including without limitation the expert fees and attorney fees regularly charged by the experts and legal counsel chosen by Barracuda Networks.

Barracuda Networks is not responsible for misprints, errors or omissions in its advertising and promotional materials.

If you have designated a person (whether by email, orally, by registering such person with Barracuda Networks, or by granting such person access to your username and password) to have access to your Backup Data, in the possession or control of Barracuda Networks, you hereby grant Barracuda Networks the right to give that person access to your Backup Data, including without limitation in the event of your death or incapacity

31. Severability

This Agreement will be enforced to the fullest extent permitted by applicable law. If for any reason any provision of this Agreement is held to be invalid or unenforceable under applicable law to any extent, then (i) such provision will be interpreted, construed, or reformed to the extent reasonably required to render it valid, enforceable, and consistent with the original intent underlying such provision and ii) such invalidity or unenforceability will not affect the validity or enforceability of any other provision of this Agreement and all such provisions shall remain in full force and effect.

32. Billing Issues

You must notify us about any billing problems or discrepancies within sixty (60) days after they first appear on the statement you receive from your bank or credit card company or other billing company. Send such notification to us at the Barracuda Networks Contact Information indicated in Section 33 (Barracuda Networks Contact Information) below. If you do not bring such problems or discrepancies to our attention within that sixty (60) day period, you agree that you waive the right to dispute such problems or discrepancies.

33. Barracuda Networks Contact Information

If you have any questions or comments, please contact us at info@barracuda.com. Although we strongly prefer email communication, you may also send regular postal mail to the address on our web site at www.barracuda.com.

34. Open Source Licensing

Barracuda Networks Products and Services may include programs that are covered by the GNU General Public License (GPL) or other Open Source license agreements. The GNU 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 copyright by Barracuda Networks.

The GNU General Public License (GPL) Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

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

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

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.

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.

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

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

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

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

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

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

- a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

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

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

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

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.

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.

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

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

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

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that

system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

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

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.

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.

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

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.

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 GNU TERMS AND CONDITIONS

Barracuda Networks Products and Services 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 Networks Products and Services 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 Networks Products and Services may include the libspf 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 MAKING USE OF THIS LICENSE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Barracuda Networks Products and Services 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 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 Networks Products and Services may include programs that are covered by the Apache License or other Open Source license agreements. The Apache 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.

Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

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 software source 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 authorized to submit on behalf of the copyright owner. For the purposes of this definition, “submitted” means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as “Not a Contribution.”

“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.

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, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

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.

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 must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within 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, or 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.

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 Licensor regarding such Contributions.

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.

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.

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 of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to 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.

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 APACHE TERMS AND CONDITIONS

Index

A

- Accounts
 - Adding users 20, 39
- Activating your subscription 18
- Administrative contact, method for domain verification 19
- Aliasing/linking domains 19
- Attachment filtering
 - inbound 27
 - notifications of blocked messages 15
 - outbound 31

C

- content filtering
 - inbound mail 27
 - outbound mail 31
 - pre-made patterns 27, 45

D

- Data Leakage Prevention (DLP) 30
- Default time zone 43
- domain level settings
 - and quarantine 42
- Domains
 - configuring 18
 - linking (aliasing) 24

E

- Email Spooling 9, 20
- Email Statistics
 - outbound 23
- Enable User Quarantine 43
- Encryption of Outbound Mail 30

L

- LDAP
 - for user login authentication 44
 - Recipient verification 39
 - Synchronization for account creation 42
- Linking (aliasing) domains 34
- Linking code, for subscription 18

M

- Mail Servers
 - configuring 18
 - securing 20
- mail statistics 22
- MX Records, method for domain verification 19

N

- Not Spam, marking messages 23
- Notifications 15
 - of quarantined messages 35

P

- Per-Domain Management 22

Q

- Quarantine
 - domain level settings 42
 - notifications 35
 - where quarantined messages go 34

R

- Rate Control 12
 - outbound mail 31
- regular expressions, about 45
- Role-based Administration 42
- routing email 19

S

- Sender authentication 13
- Sender Policy Framework (SPF)
 - for inbound mail 38
 - for outbound mail from your sending domains 38
- SMTP over TLS 19
- Spam and Not Spam, marking messages 23
- Spooling of email 9, 20
- Statistics
 - email 22
- Subscription, purchase and activation of 18

T

technical support, contacting 9
TLS encryption 19, 40

U

User Accounts 42, 43

V

virus checking, enabling and disabling 22

