smoothwall®

The Web You Want

Unified Threat Management

Anti-Spam Installation and Administration Guide

Smoothwall® Anti-Spam, Installation and Administration Guide, August 2014

Smoothwall publishes this guide in its present form without any guarantees. This guide replaces any other guides delivered with earlier versions of Anti-Spam.

For more information, contact: docs@smoothwall.net

Trademark notice

Acknowledgements

Smoothwall acknowledges the work, effort and talent of the Smoothwall GPL development team: Lawrence Manning and Gordon Allan, William Anderson, Jan Erik Askildt, Daniel Barron, Emma Bickley, Imran Chaudhry, Alex Collins, Dan Cuthbert, Bob Dunlop, Moira Dunne, Nigel Fenton, Mathew Frank, Dan Goscomb, Pete Guyan, Nick Haddock, Alan Hourihane, Martin Houston, Steve Hughes, Eric S. Johansson, Stephen L. Jones, Toni Kuokkanen, Luc Larochelle, Osmar Lioi, Richard Morrell, Piere-Yves Paulus, John Payne, Martin Pot, Stanford T. Prescott, Ralf Quint, Guy Reynolds, Kieran Reynolds, Paul Richards, Chris Ross, Scott Sanders, Emil Schweickerdt, Paul Tansom, Darren Taylor, Hilton Travis, Jez Tucker, Bill Ward, Rebecca Ward, Lucien Wells, Adam Wilkinson, Simon Wood, Nick Woodruffe, Marc Wormgoor.

Anti-Spam contains graphics taken from the Open Icon Library project http://openiconlibrary.sourceforge.net/

Address	Smoothwall Limited 1 John Charles Way Leeds. LS12 6QA United Kingdom	
Email	info@smoothwall.net	
Web	www.smoothwall.net	
Telephone	USA and Canada: United Kingdom: All other countries:	1 800 959 3760 0870 1 999 500 +44 870 1 999 500
Fax	USA and Canada: United Kingdom: All other countries:	1 888 899 9164 0870 1 991 399 +44 870 1 991 399

Contents

About This Guide

Anti-Spam is a licenced feature of your Smoothwall System.

This manual provides guidance for installing and managing Anti-Spam.

Audience and Scope

This guide is aimed at system administrators maintaining and deploying Anti-Spam.

This guide assumes the following prerequisite knowledge:

- An overall understanding of the functionality of the Smoothwall System
- An overall understanding of networking concepts

Note: We strongly recommend that everyone working with Smoothwall products attend Smoothwall training. For information on our current training courses, contact your Smoothwall representative.

Organization and Use

This guide is made up of the following chapters and appendices:

Conventions

The following typographical conventions are used in this guide:

Item	Convention	Example
Key product terms	Initial Capitals	Anti-Spam
Cross-references and references to other guides	Italics	See *Chapter 1, Introducing Anti-Spam* on page 3
Filenames and paths	`Courier`	The `portal.xml` file
Variables that users replace	*`Courier Italics`*	`http://<my_ip>/portal`

This guide is written in such a way as to be printed on both sides of the paper.

Related Documentation

The following guides provide additional information relating to the Anti-Spam feature:

- *Anti-Spam Upgrade Guide* explains how to upgrade a compatible Smoothwall System to the latest version of Anti-Spam
- http://www.smoothwall.net/ contains the Smoothwall support portal, knowledge base and the latest product manuals.

1 Introducing Anti-Spam

This chapter introduces the Anti-Spam feature of Unified Threat Management, including:

Anti-Spam Overview

Welcome to Anti-Spam, Smoothwall's add-on module for protecting email servers and users by blocking malware and spam at the network perimeter.

Anti-Spam provides:

- Mail relaying – relay inbound and outbound SMTP traffic, transparently if required
- Malware scanning – drop, bounce, neutralize or log email which is carrying malware
- Anti-spam and quarantine – reduce and eliminate junk email and SMTP abuse
- Mail archiving – backup mail for specific domains or email addresses
- POP3 proxying – transparently proxy POP3 traffic, scan for viruses and protect against spam
- Queue and log viewing, reports and alerts.

About this Guide

This guide explains how to install and administer Anti-Spam.

Support

- Email: support@smoothwall.net
- Web site: www.smoothwall.net/support

2 Installing Anti-Spam

In this chapter:

- How to install Anti-Spam in your Smoothwall System.

Prerequisites

Before installing, ensure that your Smoothwall System has all the latest updatesinstalled.

You do this as follows:

1. Navigate to the **System > Maintenance > Updates** page.
2. Click **Refresh update list**. The Updates area displays any updates available.
3. Click **Download updates** and then click **Install updates**.

Installing Anti-Spam

You install Anti-Spam by installing it from the System > Maintenance > Modules page.

To install Anti-Spam:

1. Log on to your Smoothwall System, browse to the **System > Maintenance > Modules** page and click **Refresh module list**.
2. In the **Available modules** area, locate **Anti-Spam** and click **Install**. Your Smoothwall System installs Anti-Spam.
3. You must now reboot your system. Browse to the **System > Maintenance > Shutdown** page, select **Immediately** and click **Reboot**.

Once your Smoothwall System has rebooted and you have logged on, Anti-Spam becomes available from the **Email** menu. Your next steps are to configure Anti-Spam. For more information, see the *Anti-Spam Administrator's Guide*.

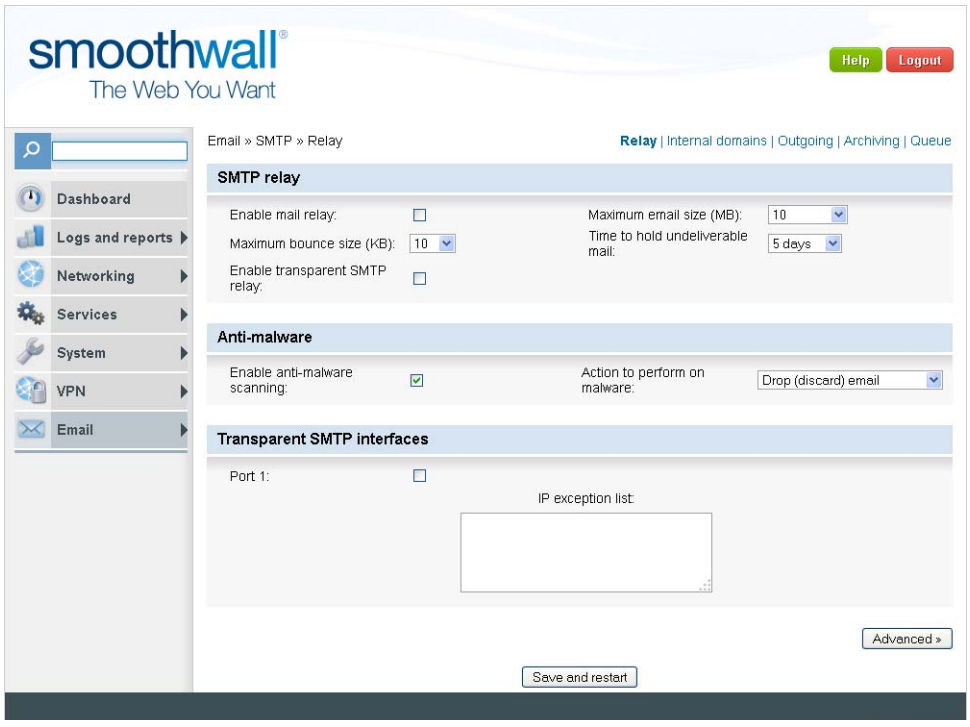
3 Accessing Anti-Spam

This chapter includes:

Accessing Anti-Spam

To access Anti-Spam:

1. Start a web browser, browse to Smoothwall System, authenticate yourself and navigate to **email**.



2. See your Smoothwall System Administrator's Guide if you need more information on accessing your system. The following sections explain Anti-Spam email pages.

Email

The email section contains the following sub-sections and pages:

SMTP

Pages	Description
Relay	This is where you configure and enable email relay settings. For more information, see *Chapter 4, SMTP Relay Settings* on page 11.
Internal domains	This is where you set the domains that Anti-Spam will relay incoming email for. For more information, see *Chapter 4, Internal Domains* on page 14.
Outgoing	This is where you set the IP address or subnets of machines on the local network that are to be allowed to relay mail through Anti-Spam. For more information, see *Chapter 4, Outgoing* on page 14.
Archiving	Here you can specify the criteria used to determine which email messages are to be archived. For more information, see *Chapter 4, Archiving* on page 15.
Queue	Here you can view summary information and statistics about the email relay queue. You can also manually flush the email queue if required. For more information, see *Chapter 4, The Email Queue* on page 15.

POP3

Pages	Description
Proxy	Here you configure and enable transparent POP3 proxying and AV scanning for incoming email. For more information, see *Chapter 4, POP3 Proxy* on page 16.

Content

Pages	Description
Footers	Here you can enter text you want to add to email managed by Anti-Spam. For more information, see *Chapter 4, Footers* on page 17.
Attachments	Here you specify how Anti-Spam should manage email attachments. For more information, see *Chapter 4, Attachments* on page 18.

Anti-spam

Pages	Description
Anti-spam	Here you configure protection against spam. For more information, see *Chapter 4, Anti-spam* on page 18.

Quarantine

Pages	Description
Viewer	On this page, you can preview release and/or delete email messages. For more information, see *Chapter 6, Managing Quarantined Email* on page 29.

Pages	Description
Settings	On this page, you configure quarantine settings. For more information, see *Chapter 6, Configuring Quarantine* on page 28.

4 Email Settings

This chapter describes various aspects of Anti-Spam's user interface, including:

SMTP Settings

Anti-Spam's SMTP settings enable you to configure email relaying using SMTP. For more information on SMTP in general, see *About Email Protocols* on page 33.

The following sections document the settings available.

SMTP Relay Settings

To access SMTP relay settings:

1. Navigate to the **Email > SMTP > Relay** page.
2. Click **Advanced** to view all settings. The following settings control email relaying:

Setting	Description
Enable mail relay	Select to activate relaying after configuring incoming and outgoing relaying.

Setting	Description
Maximum email size	Used to specify the maximum email size, in Mb, that Anti-Spam will accept. Any emails above this limit will be rejected. Min = 1 MB Default = 10 MB Max = Unlimited
Maximum bounce size	Specifies the maximum size of an email which is used in a bounce email. Min = 10 KB Default = 10 KB Max = Unlimited
SMTP name	Enables you to specify a different hostname to be used within Anti-Spam to prevent email being rejected by other mail relays. **Use system hostname** – Select this option to use Anti-Spam's SMTP hostname when relaying email. **User defined hostname** – Select this option and enter a different hostname to use when relaying email.
Time to hold undeliverable mail	Used to specify the amount of time an email will be held in the queue if it cannot be sent. Anti-Spam will periodically attempt to re-send all email that is held in the queue. Min = 5 hours Default = 5 days Max = 5 days
Enable transparent SMTP relay	Capture outgoing email and relay it through Anti-Spam.

Anti-malware Settings

Anti-Spam can scan relayed email for malware and take appropriate action as specified by the anti-malware settings configured here.

Setting	Description
Enable anti-malware scanning	Activates anti-malware scanning for relayed email.
Action to perform on malware	Determines what to do if malware is found in relayed email. **Drop (discard) email** Discard the email, without notifying the sender or intended recipient. **Bounce email (warn sender)** Return the email to the sender, along with a warning message. **Neutralize email** Send a warning email to the recipient, with the original email as an attachment. **Allow email delivery** Allow the email to be delivered, and the malware will be logged.

Transparent SMTP Interfaces Settings

If you select the Enable transparent SMTP relay option, see *SMTP Relay Settings* on page 11, you must select at least one internal interface to proxy the traffic.

Setting	Description
Interface name	Specify which interface(s) SMTP traffic will be transparently captured from.
IP exception list	Enter any IP addresses, subnets or ranges that should not be transparently proxied.

Once SMTP traffic has been captured, Anti-Spam will apply all anti-malware and anti-spam checks that are enabled, and relay the email accordingly. Outgoing SMTP traffic will be queued and relayed as if the client had sent the email directly to Anti-Spam.

External Mail Relay

By default, Anti-Spam will attempt to deliver all outbound email directly to the appropriate server. However, using the settings below you can configure Anti-Spam to relay all outgoing email to another mail relay.

Setting	Description
Enable relay host	Select to enable Anti-Spam to send outgoing email to another relay within an existing email infrastructure.
Relay host	The IP address or hostname of the relay.
Username	The username, if required by the remote relay.
Password	The password, if required by the remote relay.

Non-standard SMTP Checking

Non-standard SMTP checking options enable Anti-Spam to check email which does not adhere to the SMTP message format and contains badly formatted or bogus information about the sender and/or recipient.

Note: In order for the non-standard SMTP checks to work, Anti-Spam must be operating as the MX record for the recipient domain.

To alter your domain's MX record, you will need to access your domain's DNS server settings. Refer to your email server documentation and/or your email provider to find out how to alter the MX record. It should be set to your Smoothwall System's external IP address.

Setting	Description
Use strict HELO checks	Ensure validity of the initial communication between a connecting SMTP client and the Anti-Spam email relay.
Sender domain validity	Check that the sender domain is formatted correctly and has a real IP address.
Recipient domain validity	Check that all recipient domains are formatted correctly and have real IP addresses.

Setting	Description
External sender domain spoofing	Check if the sender of incoming email is falsely using an internally relayed domain in their from address. Emails are rejected if the sender's email address purports to be from a domain listed on the incoming page, but the sender's IP address cannot be found on the outgoing page.

Internal Domains

On the internal domains page, you specify which incoming email messages will be accepted and relayed by Anti-Spam. Only messages to addresses whose domain names are listed here will be accepted by Anti-Spam.

To access settings:

1. Navigate to **Email > SMTP > Internal domains** page.

The following settings are available:

Setting/field	Description
Domain to relay for	The name of the domain that Anti-Spam will accept email for. For example, for Anti-Spam to accept email for people at Smoothwall, enter: `smoothwall.net`
Relay IP	The IP address of the email server that the incoming email is relayed to. In most cases this will be an internal IP, usually the email server behind your Smoothwall System.
Anti-malware scanning	Activates anti-malware scanning for email accepted by Anti-Spam for the specified domain.
Append footers	This option appends the text entered in the Email > Content > Footers page below to all outgoing email except HTML and signed email. **Note:** HTML emails are normally sent in two parts: an HTML part and a text part. The footer will be appended to the text part even if the Append to HTML emails option is selected.
Comment	A useful description for a particular domain, for example, Inbound relay domain for smoothwall.net.
Enabled	Enables incoming email relaying for the specified domain.
Current domains	Lists the domains for which Anti-Spam will accept and relay email.

Outgoing

On the outgoing page, you specify which IP address or subnets of machines on the local network that are allowed to relay mail through Anti-Spam.

To access outgoing relay settings:

1. Navigate to **Email > SMTP > Outgoing** page.

The following outgoing relay email settings are available:

Setting/field	Description
IP or subnet to relay from	The IP address or subnets of machines on the local network that are to be allowed to relay mail through Anti-Spam For example: `192.168.10.10`
Comment	A useful description for a particular IP or subnet, for example, Outbound relaying for smoothwall.net.
Enabled	Select to enable outbound email relaying for the specified IP or subnet.
Current allowed addresses	Lists the addresses from which outgoing email can be sent.

Archiving

On the Archiving page you specify what email you want archived based on domain information, a specific email address, by sender or recipient.

To access archiving settings:

1. Navigate to **Email > SMTP > Archiving** page.

The following archiving settings are available:

Setting/field	Select to/enter:
Match domain or address	Specify either a domain or an email address to match.
Archive address	Specify the email address that matched email is forwarded to.
Match recipient	Specify that matching of the domain or address should be performed against the recipient's email address.
Match sender	Specify that matching of the domain or address should be performed against the sender's email address.
Comment	A useful description for a match rule, for example, 'email archiving for company domain'.
Enabled	Used to enable email archiving for the archive rule.

The Email Queue

On the Email queue page you can view summary information and statistics about the email relay queue. You can also flush the queue.

To access the queue:

1. Navigate to **Email > SMTP > Queue** page.

The Summary area contains the following information/options:

Information/option	Description
Mails in queue	The total number of email messages waiting in the queue.

Information/option	Description
Total size of queue	The amount of data in KB currently held in the queue.
Number of unique senders	The total number of unique senders for all email messages in the queue.
Number of unique recipients	The total number of unique recipients for all email messages in the queue.
Manually flush mail queue	Requests Anti-Spam attempt to re-send all queued email.
Refreshing page	Updates the page and displays the current status of the queue.

The mail queue viewer provides a view of all email currently waiting in the queue.

POP3 Proxy

On the pop3 proxy page, you enable and configure transparent POP3 proxying. Anti-Spam's transparent POP3 proxying captures POP3 traffic without the user's knowledge, and automatically scans it for malware, viruses and unsolicited content. This ensures that email downloaded from POP3 servers is subjected to scanning without requiring every employee to install expensive email anti-malware software on their workstations.

For general information on POP3, see *About POP3* on page 34.

To access POP3 proxy settings:

1. Navigate to the **Email > POP3 > Proxy** page.

POP3 Proxy Configuration

Setting	Description
Enable transparent POP3 proxy	Enables transparent POP3 proxy.

Anti-malware

Setting	Description
Enable anti-malware scanning	Enables anti-malware scanning on relayed email. **Note:** For performance reasons, emails larger than 100 MB are not scanned for malware.

Customize Malware Message

Here you specify what information should be displayed in any malware alerts sent by Anti-Spam.

Setting	Description
Show malware name	The malware name in the body of the email alert.
Show sender address	The sender's email address.

Setting	Description
Show recipient address	The recipient's email address.
Show date	The date that the email was sent.
Show subject	The subject of the email.
Show connection data	The IP addresses of both the client connecting to download email and the POP3 server.

Interfaces

Here you set which internal interfaces will transparently proxy POP3 traffic.

Setting	Description
Interface name	Select the interfaces you wish to proxy POP3 traffic. **Note:** You must select at least one internal interface for the POP3 proxy to work.
IP exception list	IP addresses allowed to download email via POP3 without being proxied.

Content

Anti-Spam's content pages manage email footer information and attachments.

Footers

You configure footer content settings, such as standard email disclaimers, on the footers page.

To access the footer settings:

1. Navigate to **Email > Content > Footers** page.

The following settings are available:

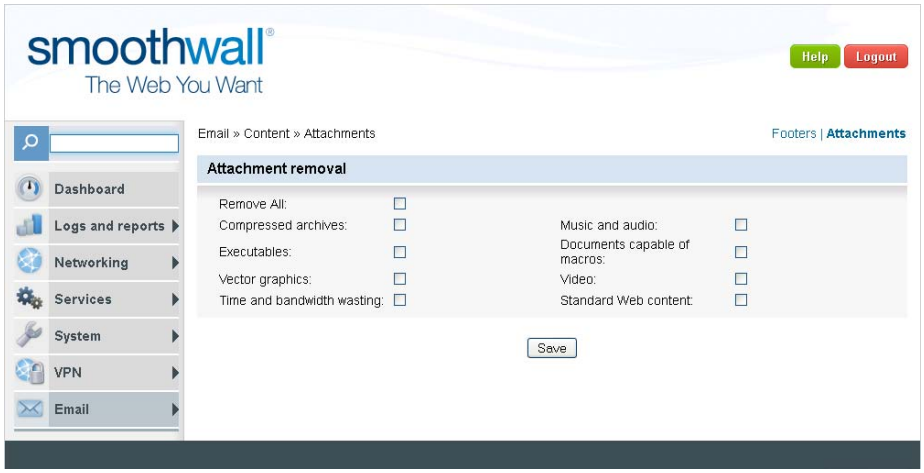
Setting	Description
Append to HTML emails	When enabled, this option appends the text entered in the text box below to outgoing HTML email messages.
Append to signed emails	This option appends the text entered in the text box below to outgoing email messages which have a digital signature attached. When you select this option, the footer is appended to signed emails in a way which maintains the fingerprint.
Per-domain footers	The settings here enable you to specify which footer to use with which domain. **Internal domain** – From the drop-down list, select the domain and click **Select**. If a domain does not have a specific footer, the default domain is used. **Append the following text to outgoing email** – Enter the footer text you want to append.

Attachments

You configure how Anti-Spam handles relayed email attachments on the attachments page.

To access attachment settings:

1. Navigate to **Email > Content > Attachments** page.



The following settings are available:

Setting	Description
Remove All	Removes all attachments from relayed email.
Compressed archives	Removes compressed attachments, such as `tar` and `zip` files, from relayed email.
Executables	Removes files that can be executed, such as `msi` and `exe` files, from relayed email.
Vector graphics	Removes vector graphic files, such as `svg` and `wmf` files, from relayed email.
Time and bandwidth wasting	Removes files deemed to contain time wasting content, such as `iso` and `p2p` files, from relayed email.
Music and audio	Removes files containing music and audio, such as `midi` and `mp3` files, from relayed email.
Documents capable of macros	Removes files that can run macros, such as `doc` and `xls` files, from relayed email.
Video	Removes files containing video, such as `mov` and `mpeg` files, from relayed email.
Standard Web content	Removes files containing Web content, such as `asp` and `php` files, from relayed email.

Anti-spam

Anti-Spam's anti-spam service manages spam filtering.

To access the anti-spam page:

1. Navigate to **Email > Anti-spam > Anti-spam** page.

   The following sections document Anti-Spam's anti-spam settings.

SMTP Anti-spam Settings

The following anti-spam settings are available for relayed email:

Setting	Description
Enable spam filtering	Select to enable spam filtering for relayed email.
Action to perform on spam	Determines what Anti-Spam should do with relayed email deemed to be spam. The options are: **Drop (discard) email** – Discard the email – discarded email is not relayed. **Redirect mailbox** – Send the email to the mailbox as specified in the Redirect mailbox field. **Mark subject as spam** – Add `***SPAM***` to the subject of the email and relay it. **Allow email delivery** – Relay the email and take no action. **Note:** All of the actions above are transparent to the sender; that is, no rejection notices are sent. This is because it is a common spammer tactic to harvest email addresses by sending known bad email and awaiting the rejection notices. Rejection notices not only confirm email addresses as valid, they also inform spammers which anti-spam system you have in place. Therefore, Anti-Spam does not provide options for sender notification for spam.
Apply action above spam score	Anti-Spam calculates a statistical probability that the email it is scanning is spam. The probability of a message being spam varies, and the options here enable you to customize the level at which an email will be treated as spam. Various refinements to the algorithm used by Anti-Spam to optimize for speed or resources will affect the accuracy of this probability. For most configurations, we recommend a spam threshold of 80%; that is, email which is more than 80% likely to be unwanted will be treated as spam. Select the threshold above which email will be considered spam. **90** – The most easily identified spam will be filtered out, but a significant amount of spam may be allowed through. **50-80** – messages likely to be spam will be filtered out, which means some non-spam messages may also be caught. **30-40** – messages that are possibly spam will be filtered out, and non-spam messages are likely to be caught. **10** – spam filtering is very aggressive. Non-spam messages are as likely to be caught as spam messages. **Note:** When using the Spam check optimization mode: Most accurate option, see below, we recommend that you set the spam threshold to 90.
Redirect mailbox	Enter the address of the mailbox you want to redirect email to.

POP3 Anti-spam Settings

The following anti-spam settings are available for POP3 email:

Setting	Description
Enable spam filtering	Select to enable spam filtering for POP3 email.

Setting	Description
Action to perform on spam	Determines what to do with POP3 email deemed to be spam. The options are: **Replace spam with warning** – Send an automatic warning to the recipient and do not send the email. **Mark subject as spam** – Add `***SPAM***` to the subject of the email and deliver it. **Allow email delivery** – Deliver the email and take no action. **Note:** All of the actions above are transparent to the sender; that is, no rejection notices are sent. This is because it is a common spammer tactic to harvest email addresses by sending known bad email and awaiting the rejection notices. Rejection notices not only confirm email addresses as valid, they also inform spammers which anti-spam system you have in place. Therefore, Anti-Spam does not provide options for sender notification for spam.
Spam threshold	Anti-Spam calculates a statistical probability that the email it is scanning is spam. The probability of a message being spam varies, and the options here enable you to customize the level at which an email will be treated as spam. Various refinements to the algorithm used by Anti-Spam to optimize for speed or resources will affect the accuracy of this probability. For most configurations, we recommend a spam threshold of 80%; that is, email which is more than 80% likely to be unwanted will be treated as spam. Select the threshold above which email will be considered spam. **90** – The most easily identified spam will be filtered out, but a significant amount of spam may be allowed through. **50-80** – messages likely to be spam will be filtered out, which means some non-spam messages may also be caught. **30-40** – messages that are possibly spam will be filtered out, and non-spam messages are likely to be caught. **10** – spam filtering is very aggressive. Non-spam messages are as likely to be caught as spam messages. **Note:** When using the Spam check optimization mode: Most accurate option, see below, we recommend that you set the spam threshold to 90.

Tuning

The following tuning settings are available for spam filtering:

Setting	Description
Spam check optimization mode	Fine-tune how Anti-Spam's anti-spam service uses system resources. **Note:** Due to the transient nature of email, the time taken to scan an individual email is often considered immaterial. We strongly recommend that accuracy options only be decreased in favour of speed in order to alleviate specific bursts of traffic or increase throughput on loaded networks. The following options are available: **Most Accurate** – This option filters spam very accurately. Anti-Spam will bypass the global fingerprint cache and check each email against the latest spam filter information. This can introduce network latency and decrease performance, however it is the most resilient to bursts of spam traffic across the Internet. **More Accurate** – This option filters spam accurately. This option has the same advanced parsing options as the most accurate option but uses a global fingerprint cache to allow for a local comparison to alleviate the network latency of the most accurate option. **Note:** This option offers high levels of accuracy at increased speed, but requires more memory and system resources. **Less Resources** – This option provides moderate levels of spam filtering by using a wide range of spam processing options but omitting the more memory intensive scanning options. **Least Resources** – This option provides reasonable levels of spam filtering by using a range of options which tend to provide the most accurate determination of spam while using the smallest amount of system resources. **Note:** This option is only recommended for machines which have limited system resources or memory, or are heavily loaded. **Fastest** – This option provides moderate levels of spam filtering by omitting the more time intensive scanning methods. Each email is scanned briefly against a set of rules which provide a more immediate appraisal of an email. This option omits any network checking to avoid latency and any labor or processing intensive scanning. **Faster** – This option provides limited spam checking abilities as emails are subjected to only a limited subset of spam recognition techniques. Scanning techniques which are either time-intensive, or prone to network latency are omitted in order to provide the highest possible throughput . **Note:** This option is only recommended for systems which are heavily loaded and should therefore avoid any intensive activity.
Rule update frequency	Determines how often Anti-Spam checks for spam rule updates.
Scan attachments	Select if Anti-Spam should scan email attachments for spam. **Note:** Email is one of the Internet's oldest protocols and has been adapted many times to allow for attachments and HTML emails. In order for these emails to be properly scanned, we recommend that Anti-Spam be configured to scan attachments.

Home Regions

Option	Description
Home region	Here you can specify regions from which Anti-Spam scores email less aggressively for spam. You can select from the following regions: **Australia and Oceania** **European Union** **South America** **Asia** **Europe** **North America**

SMTP Graylisting

Graylisting is an anti-spam feature designed to detect messages that have not been sent by a genuine email server.

Note: In order for graylisting to work, Anti-Spam must be operating as the MX record for the recipient domain.
To alter your domain's MX record you will need to access your domain's DNS server settings. Refer to your email server documentation and/or your email provider to find out how to alter the MX record. It should be set to your Smoothwall System's external IP address.
Only incoming email will be graylisted, outgoing email will be allowed automatically.

To understand how graylisting works, it is necessary to understand how email sent by a spammer differs from that sent by a genuine email server. Most email servers employ a re-send mechanism to try and deliver any failed messages. This approach ensures that the email server pro-actively manages email delivery, and does not annoy users simply because of an intermediary network failure or temporary email server outage.

Most spammers will not go to the trouble of re-sending mails that have been rejected – they are mostly concerned with the volume of spam that they can send to easy targets. Graylisting uses this to its advantage by initially rejecting all incoming email. If the remote SMTP client retries after a short while, the email is allowed because it most likely originates from a genuine sender.

All senders deemed genuine are added to the graylist, and are not subjected to initial blocking for subsequent mails.

Setting	Description
Enable graylisting	Provides spam protection by detecting messages that have not been sent by a genuine email server.
Graylist delay (minutes)	From the drop-down list, select the time in minutes that must pass before re-sent incoming email will be relayed.
Maximum age (weeks)	From the drop-down list, select the time in weeks that a graylisted sender will remain on the graylist. After this time has elapsed, the sender will again be subjected to an initial block. In most cases, senders will be re-added to the graylist because their email server will employ its re-send mechanism again.

SMTP RBL Checks

Remote Blackhole Listing (RBL) checking blocks email originating from well-known spammers. RBL blocklists are compiled by various organizations on the Internet.

Setting	Description
User defined RBL (comma separated)	Enter the hostnames, separated by commas, of RBL blocklists that you wish Anti-Spam to use.

SMTP Automatic Whitelisting

Option	Description
Enabled	With automatic whitelisting enabled, any email sent through Anti-Spam will be added to the white list. **Note:** Anti-Spam matches partial domains, If a domain like `nhs.gov.uk` is added to a whitelist, then all emails such as: `user@southampton.nhs.gov.uk` and `bob@leeds.nhs.gov.uk` will be matched. This extends all the way up to a single domain, like `uk`.
Number of current entries	Displays the number of entries on the automatic white list.
Clear automatic whitelisted address list	Click to clear the automatic whitelisted address list.

SMTP White-list Spam Addresses

Here you can define senders and recipients that Anti-Spam should accept as not being associated with spam.

Note: Anti-Spam matches partial domains, If a domain like `nhs.gov.uk` is added to a whitelist, then all emails such as: `user@southampton.nhs.gov.uk` and `bob@leeds.nhs.gov.uk` will be matched. This extends all the way up to a single domain, like `uk`.

Setting	Description
Sender addresses and domains	Enter the email addresses and domains of email senders whose messages Anti-Spam should always accept.
Recipient addresses and domains	Enter the email addresses and domains of recipients of messages Anti-Spam should always accept.

SMTP Black-list Spam Addresses

Here you can define sender and recipient information that Anti-Spam should treat as spam.

Note: Anti-Spam matches partial domains, If a domain like `nhs.gov.uk` is added to a blacklist, then all emails such as: `user@southampton.nhs.gov.uk` and `bob@leeds.nhs.gov.uk` will be matched. This extends all the way up to a single domain, like `uk`.

Setting	Description
Sender addresses and domains	Enter the email addresses and domains of email senders whose messages Anti-Spam should always treat as spam.
Recipient addresses and domains	Enter the email addresses and domains of recipients of messages Anti-Spam should always treat as spam.

5 Configuring Spam Management

This chapter describes how to configure Anti-Spam, including:

Configuring Email Relaying

Configuring and enabling email relaying entails allowing SMTP traffic access and configuring relay settings for incoming and outgoing email.

For information on email relay settings, see *Chapter 4, Email Settings* on page 11.

To configure email relaying:

1. Browse to the **System > Administration > External access** page.
2. Configure the following settings:

Setting	Description
Interface	From the drop-down list, select the external interface that will accept SMTP traffic.
Service	From the drop-down list, select **SMTP (25)**.
Comment	Optionally, enter information on the configuration.
Enabled	Select to enable the configuration

3. Click **Add**. The SMTP access rule is added to the list of current rules.
4. Go to the **Email > SMTP > Internal domains** page.

5. Configure the relay settings for incoming email. See *Chapter 4, Internal Domains* on page 14 for information on the settings available.
6. Click **Add**. The configuration is listed in the Current domains area.
7. Go to the **Email > SMTP > Outgoing** page.
8. Configure the relay settings for outgoing email. See *Chapter 4, Outgoing* on page 14 for information on the settings available.
9. Click **Add**. The configuration is listed in the Current allowed addresses area.
10. Go to the **Email > SMTP > Relay** page.
11. Configure the settings for email relaying. See *Chapter 4, SMTP Settings* on page 11 for information on the settings available.
12. Click **Save and restart** to implement email relaying.

Configuring POP3 Proxying

You can configure Anti-Spam to retrieve POP3 email traffic and automatically scan it for malware.

To configure POP3 proxying:

1. Go to the **Email > POP3 > Proxy** page.
2. Configure the POP3 settings you require for your environment, see *Chapter 4, POP3 Proxy* on page 16 for more information on the settings available.
3. Click **Save and restart** to implement Anti-Spam POP3 proxying.

Configuring Footers

Anti-Spam's Footers page manage email footer information.

To configure footers:

1. Browse to the **Email > Content > Footers** page.
2. Select the footer options you want to use, see *Chapter 4, Footers* on page 17 for information on the options available.
3. Click **Save** to implement the footer content.

Managing Attachments

To manage attachments:

1. Browse to the **Email > Content > Attachments** page.
2. Select the attachment options you want to use, see *Chapter 4, Attachments* on page 18 for information on the options available.
3. Click **Save** to implement the attachment options.

6 Administering Email

This chapter describes how to manage Anti-Spam email, including:

About Subscription Information

The License page displays information on your anti-spam and anti-malware subscriptions.

To review subscription information:

1. Navigate to **System > Maintenance > Licenses** page.
2. Click **Refresh subscription information** to get the latest information.

Manually Managing Malware Protection

Anti-Spam automatically updates anti-malware signatures every hour and this is usually sufficient. However, if required, you can update anti-malware signatures manually or restart the anti-malware service with the latest anti-malware signatures.

Manually Updating Signatures

Anti-Spam automatically updates anti-malware signatures every hour. Anti-Spam also enables you to update to the latest anti-malware signatures at any time by manually downloading them.

To manually update signatures:

1. On the **System > Maintenance > Licenses** page, in the Licenses area, click **Update signatures now**. Anti-Spam gets the latest information available and updates the signatures.

Restarting the Anti-malware Service with the Latest Signatures

Anti-Spam automatically updates anti-malware signatures every hour. Anti-Spam also enables you to manually restart the anti-malware service with the latest signatures.

Note: Services such as FTP proxy, POP3 proxy and SMTP relay which use the anti-malware service will be interrupted while Anti-Spam downloads the latest signatures and restarts the malware service.

To download the signatures and restart the service:

1. On the **System > Maintenance > Licenses** page, in the Licenses area, click **Restart anti-malware engine with new signatures**. Anti-Spam removes the currently installed signatures, downloads the latest signatures and restarts the anti-malware service.

Managing Spam Protection

To configure anti-spam options:

1. Browse to the **Email > Anti-spam > Anti-spam** page.
2. Configure the anti-spam options, see *Chapter 4, Anti-spam* on page 18 for more information on the options available.
3. Click **Save** to implement the options.

Placing Email in Quarantine

Anti-Spam enables you to manage email which is probably spam by placing it in quarantine where you can review, release or delete it.

Note: You must have administrator or SMTP quarantine permissions to access the SMTP quarantine pages. Permissions are set on the System > Administration > Administrative users page.

The following sections explain how to configure and manage email quarantine,

Configuring Quarantine

Each email message received by Anti-Spam is given a spam score which indicates the probability that the message is spam. The higher the score, the higher the probability. You can use this score to determine whether to quarantine or drop the message.

To configure quarantine:

1. Browse to the **Email > Quarantine > Settings** page.
2. Configure the following settings:

Setting	Description
Enable quarantine	Select this option to quarantine email messages which have a higher spam score than specified in the Quarantine above spam score option.
Quarantine above spam score	From the drop-down list, select the spam score above which messages will be quarantined.

Setting	Description
Enable spam drop	Select this option to drop email messages which have a higher spam score than specified in the Drop above spam score option.
Drop above spam score	From the drop-down list select the spam score above which messages will be dropped.
Send quarantine email	From the drop-down list, select when to send subscribed users a summary of email to them that has been quarantined. Users who receive a summary can review it and release any incorrectly categorized email. **Always** – Select to always send a daily summary of the user's quarantined email. **If mail in quarantine** – Select to send a daily summary of the user's quarantined email if email has been quarantined. **Never** – Select to never send a daily summary of the user's quarantined email.
Subscribed quarantine users' email addresses	Enter the email addresses of the users you want to subscribe to the quarantine service. Enter one email address per line.
Max disk usage	From the drop-down list, select the maximum amount of disk space to be used to hold quarantined email. **Note:** If the size limit is reached, Anti-Spam deletes messages newer than the configured maximum age.
Max age of quarantined mail	From the drop-down list, select how long to keep quarantined email before dropping it. Anti-Spam prunes quarantined email every hour and deletes messages which are older than the age specified.

3. Click **Save** to save the settings and enable quarantine.

Managing Quarantined Email

Managing quarantined email entails previewing messages and releasing and/or deleting them.

Previewing Quarantined Messages

To preview a message:

1. Browse to the **Email > Quarantine > Viewer** page.
2. In the Quarantined emails area, locate the message and click **Preview**. Anti-Spam displays the message.
3. By default, Anti-Spam displays main header information and the message in plain text. Click on All headers and text/html to view or hide their contents.

Releasing Messages

To release a message:

1. Browse to the **Email > Quarantine > Viewer** page. Select the message and click **Release**. Anti-Spam sends the message to the recipient.

Tip: You can also release a message when previewing it.

Deleting Messages

To delete a message:

1. Browse to the **Email > Quarantine > Viewer** page. Select the message and click **Delete**. Anti-Spam deletes the message.

Quarantine and Users

Any users subscribed to Anti-Spam's spam quarantine service will receive a summary email listing email messages addressed to them which have been placed in quarantine.

The summary email contains links to the quarantined message(s). Users can use the links to preview and/or release the messages.

Users can also use a link in the summary email to request an updated report. This lists all the spam from the last 24 hours.

Archiving Email

Anti-Spam enables you to archive email based on domain information, a specific email address, by sender or recipient. When a match is found, Anti-Spam archives the email by Blind Carbon Copying (BCC-ing) it to the specified email address. The archive email address can be different for each match.

Creating Archive Rules

To create an archive rule:

1. Browse to **Email > SMTP > Archiving** page.
2. Enter the criteria to use to identify email to be archived. See *Chapter 4, Archiving* on page 15 for information on the settings available.
3. Click **Add**. The archive rule is added to the Current archives list.

Editing Archive Rules

To edit an archive rule:

1. Browse to **Email > SMTP > Archiving** page.
2. In the Current archives list, select the rule and click **Edit**. The rule's settings are displayed in the Add domain or address to archive area.
3. Make the changes you require and click **Edit**. The rule is updated in the Current archives list.

Deleting Archive Rules

To delete an archive rule:

1. Browse to **Email > SMTP > Archiving** page.
2. In the Current archives list, select the rule and click **Remove**. Anti-Spam deletes the rule.

Managing the Email Queue

The email queue contains all incoming and outgoing emails that have not yet been relayed.

To manage the queue:

1. Navigate to the **Email > SMTP > Queue** page.

   For information on queue details, see *Chapter 4, The Email Queue* on page 15.

2. Click **Refresh page** to ensure you have the current contents to review.
3. Click **Manually flush mail queue** to flush the queue. Anti-Spam flushes the queue.

Appendix A: About Email Protocols

This appendix describes the email protocols relevant to Anti-Spam, including:

About SMTP

Simple Mail Transfer Protocol (SMTP) is a protocol used to send and receive email between mail servers. The protocol specifies the control messages and means of interaction that allow email to be transferred between two mail servers.

When a user sends an email, their mail client software uses SMTP to connect and transfer the email to the SMTP server listed in their account settings. Once an email has been transferred in this manner, it will continue to be transferred by successive SMTP servers until it arrives at its final destination. Each successive transfer is initiated by the SMTP server that currently holds the email.

Because every email transferred using SMTP is initiated by an SMTP client process, it is easiest to describe an email's journey to its destination from the point of view of successive SMTP clients. In this sense, the term “SMTP client” can be used to refer to the user's mail client software, or any intermediary SMTP server that serves to transfer the mail to another SMTP server en route.

To summarize, successive SMTP clients will act independently to transfer an email to its destination, by following these steps:

- SMTP client finds the next SMTP server for onward mail transfer.
- SMTP client connects to the next SMTP server.
- SMTP client authenticates itself to the SMTP server.
- SMTP client informs SMTP server of recipient address.
- SMTP client transfers email to SMTP server.

- SMTP client disconnects from SMTP server.

This process is repeated until the email arrives at its final destination. Note that step 1 (where the SMTP client “finds” the next SMTP server) is the only area where the behavior of a user's mail client differs from that of an SMTP server:

User's mail client – This SMTP client looks at the user's mail account settings to find the next SMTP server for onward mail transfer.

SMTP server – This SMTP client looks at the MX (Mail eXchange) record in the DNS record of the recipient domain to find the next SMTP server for onward mail transfer.

When email is transferred between one server and another, it is said to have been “relayed”. Mail servers usually provide additional services such as POP3 or IMAP so that mail can be downloaded or viewed by end-users.

About Mail Relay

In contrast to a fully featured mail server, a mail relay can be considered as a cut-down mail server that provides mail transfer capabilities only – it does not store mail, and hence does not provide end-users with the facility to download their mail from it. Mail relays are typically used by larger organizations to distribute a high volume of mail to a number of internal mail servers. Anti-Spam’s SMTP relay can be used exactly for this purpose.

About POP3

Post Office Protocol 3 (POP3) is a standard protocol designed for retrieving email from mail servers. All popular mail client applications support the POP3 protocol, including Eudora, Microsoft Outlook Express and Mozilla Thunderbird.

Such applications use POP3 to connect to a user's mail server and download email from their personal mailbox to their local system. Most mail clients can be configured to periodically check for email, as well as allowing users to manually request their mailbox to be checked.

Appendix B: Email Infrastructures

This appendix describes the email infrastructures relevant to Anti-Spam, including:

Internal Self-Managed SMTP Server

In many networks, the email server, running via SMTP, exists internally to the protected network, usually on a demilitarized zone (DMZ). In these cases, it is common to place Anti-Spam between the outside world and the email server, usually on or as close to the firewall or gateway as is possible.

In such situations, it is common practice for the domain name servers (DNS) to have their mail exchange (MX) records for the appropriate domain to contain the IP address of the firewall. The firewall then uses a system of network translations to direct incoming email to the local SMTP server.

In these scenarios, it is usually not necessary to make any changes to the existing DNS records to direct mail through Anti-Spam. Anti-Spam would be configured to relay mail from the firewall to the internal SMTP server.

For assistance in setting up the external DNS servers, see *External Self-Managed SMTP Email Server* on page 35.

External Self-Managed SMTP Email Server

In many company infrastructures, the company email server will exist on an external network, being either at a remote geographical location or a server in some form of network data centre. In these cases, it is often necessary to deliver email to Anti-Spam and then back out to the existing network

server. Since this requires a level of redirection which is not already established, it frequently mandates the alteration of the DNS MX records for a domain.

A comprehensive introduction and explanation to DNS and in particular MX records is outside of the scope of this document, however a few simple concepts will be explained in order to make this guide easier to understand.

In SMTP email delivery, the sending email process will attempt to register where to deliver the email to. Since the email address is of the form `name@domain.tld`, the server will perform a specialized DNS request to find the address of the server which handles email for the appropriate domain. This is known as an MX record.

Since mail servers are prone to being unavailable for periods of time, a domain may have several MX records, each given a numeral value. By default, MX records will be processed lowest numbered first. That is to say, an email will be delivered to whichever server responds correctly, starting with the one with the lowest number.

Assuming that the DNS MX record for `example.com` currently points at `123.123.123.123`, it is necessary to break this arrangement and insert Anti-Spam before it reaches the server `123.123.123.123`.

Assuming that Anti-Spam is located at address `200.200.200.200`, the primary MX record would be changed to point to `200.200.200.200`. Anti-Spam would then be configured on the **Email > SMTP > Incoming** page to direct traffic to `example.com` to `123.123.123.123`.

Tip: Since Anti-Spam may be temporarily unavailable for one reason or another – be it as the result of a minor network glitch or something more serious – it is considered good practice to place the final destination, in this case `123.123.123.123`, as a secondary or higher numbered MX record for the domain.
Where this is done, should Anti-Spam be unavailable, email will be delivered immediately, albeit unchecked for spam and malware, to the original email server.

Note: The technique described in the tip above can be very effective, however caution should be paid to dealing with secondary MX records.
Increasingly, spam is being directed deliberately at the secondary MX record as opposed to the primary. This is because, in many situations, the secondary MX record has less aggressive anti-spam and anti-malware measures applied to its email. Of course, to combat such mechanisms the secondary and tertiary MX records could all be routed through a Anti-Spam-enabled system.

External Mail Server using POP3 Collection

Many external mail servers are connected to and managed via a POP3 or Post Office Protocol system. This traditionally includes most Internet Service Providers (ISPs) although it is a service increasingly offered by the web-mail based services.

Anti-Spam supports POP3 services via a system known as a transparent pop3 proxy, that is to say, any traffic originating on a local network and accessing the Internet via an enabled Anti-Spam will have any traffic on the POP3 port, port 110, intercepted and analyzed by Anti-Spam.

In these cases, little more is required than to install Anti-Spam somewhere in the traffic path between the client machine and the POP3 server and enable the transparent POP3 proxy.

Note that due to the manner of the POP3 protocol, Anti-Spam is only able to offer a limited array of options for unsolicited or malware infected email. It is not possible to completely discard any such messages when processing POP3 communications in-line. Therefore, the options are limited to those that will either amend the content of the email, or, in the case of malware, strip any offending attachments or content.

Note: In some situations, a mail server, such as Microsoft Exchange, may be using POP3 for mail retrieval since the POP3 protocol is not strictly limited to client delivery. In these scenarios, Anti-Spam's transparent pop3 proxy would allow for email to be processed on route to the mail server.


smoothwall®
The Web You Want