



# SmoothZap

## Quick Start Guide

## SmoothWall SmoothZap 2008, Quick Start Guide, Version 1, January 2008

SmoothWall Ltd. publishes this guide in its present form without any guarantees. This guide replaces any other guides delivered with earlier versions of SmoothZap.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of SmoothWall Ltd.

For more information, contact: docs@smoothwall.net

This document was created and published in the United Kingdom.

© 2001 – 2008 SmoothWall® Ltd. All rights reserved.

### Trademark notice

SmoothWall and the SmoothWall logo are registered trademarks of SmoothWall Ltd.

Linux is a registered trademark of Linus Torvalds. Snort is a registered trademark of Sourcefire INC.

DansGuardian is a registered trademark of Daniel Barron. Microsoft, Internet Explorer, Window 95, Windows 98, Windows NT, Windows 2000 and Windows XP are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Netscape is a registered trademark of Netscape Communications Corporation in the United States and other countries. Apple and Mac are registered trademarks of Apple Computer Inc. Intel is a registered trademark of Intel Corporation. Core is a trademark of Intel Corporation.

All other products, services, companies, events and publications mentioned in this document, associated documents and in SmoothWall software may be trademarks, registered trademarks or servicemarks of their respective owners in the UK, US and/or other countries.

### End user notice

During their development, all SmoothWall products are subjected to exhaustive penetration testing. There are no insecurities in a standard SmoothWall system or SmoothWall add-on module.

All files that implement SmoothWall security policies are part of the system configuration and must only be altered using the recommended configuration procedures outlined in this documentation.

SmoothWall Ltd. disclaims all responsibility for any configuration and/or installation changes that may compromise network security.

### 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 Laroche, 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.

**Address** SmoothWall Limited  
1 John Charles Way  
Leeds. LS12 6QA  
United Kingdom

**Email** info@smoothwall.net

**Web** www.smoothwall.net

**Telephone** USA and Canada: 1 800 959 3760  
United Kingdom: 0870 1 999 500  
All other countries: +44 870 1 999 500

**Fax** USA and Canada: 1 888 899 9164  
United Kingdom: 0870 1 991 399  
All other countries: +44 870 1 991 399

# Contents

- SmoothZap Quick Start ..... 1
- Prerequisites ..... 1
- Installing SmoothZap..... 1
- Configuring SmoothZap..... 1
- Configuring Email Relaying..... 1
- Configuring POP3 Proxying ..... 3
- Configuring Anti-spam Settings..... 4



# SmoothZap Quick Start

In this guide:

- How to install and configure SmoothZap in your SmoothWall system.

## Prerequisites

Install and configure a compatible SmoothWall system.

## Installing SmoothZap

You can install SmoothZap by installing it from your SmoothWall system or from a SmoothZap CD.

To install SmoothZap:

- 1 Log on to your SmoothWall system and browse to the `system > maintenance > modules` page.
  - To install SmoothZap from your SmoothWall system, click `Refresh module list`.
  - To install from a CD, click `Advanced` to display all options, click `Browse`, navigate to and select `SmoothZap-X.x-module.tar.gz` where `X.x` is the version number. Click `Upload` to upload SmoothZap to your SmoothWall system. Click `Refresh module list` to update the Available modules area.
- 2 In the Available modules area, locate SmoothZap and click `Install`. Your SmoothWall system installs SmoothZap. The next step is to reboot your system.
- 3 Browse to the `system > maintenance > shutdown` page, select `Immediately` and click `Reboot`. Once the system has rebooted and you have logged on, SmoothZap becomes available. Your next steps are to configure SmoothZap.

## Configuring SmoothZap

Configuring SmoothZap entails:

- Configuring relaying by specifying domains and networks that SmoothZap will relay email for and to, see *Configuring Email Relaying* on page 1 for more information
- Configuring POP3 proxying, see *Configuring POP3 Proxying* on page 3
- Configuring protection against spam, see *Configuring Anti-spam Settings* on page 4

## Configuring Email Relaying

You can configure SmoothZap to relay email and scan it for malware, viruses and unsolicited content.

To configure email relaying:

- 1 Browse to the system > administration > external access page. Configure the following settings:

Setting	Description
Interface	From the drop-down list, select the external interface that will accept SMTP traffic.
Source IP or network	Leave this field blank to allow SmoothZap to get mail from anywhere
Service	From the drop-down interface, select SMTP (25).
Comment	Optionally, enter information on the configuration.
Enabled	Select to enable the configuration.

- 2 Click Add. The SMTP access rule is added to the list of current rules.

- 3 Go to the email > smtp > internal domainspage and configure the following settings:

Setting	Description
Domain to relay for	Enter the domain name to relay emails for. For example, to accept and relay emails for joe.smooth@smoothwall.net, enter smoothwall.net.
Relay IP	Enter the internal IP address of the mail server responsible for handling mail for this domain.
AV scanning	Select if you want to scan the email for viruses.
Append footer	Select this option to append footers to mails originating from this domain. You can create footer content on the content page.
Comment	Optionally, enter information on the configuration.
Enabled	Select to enable the configuration.

- 4 Click Add. The configuration is listed in the Current domains area.

---

**Note:** SMTP admin access must be enabled on the external interface to allow incoming email.

---

- 5 Go to the email > smtp > outgoing page and configure the following settings:

Setting	Description
IP or subnet to relay from	Enter the IP address or subnets of machines on the local network that are to be allowed to relay mail through SmoothZap.
Comment	Optionally, enter information on the configuration.
Enabled	Select to enable the configuration.

- 6 Click Add. The configuration is listed in the Current allowed addresses area.

- 7 Go to the email > smtp > relay page and configure the following settings:

Setting	Description
Enable mail relay	Select this option to enable email relaying.
Enable transparent SMTP relay	Optionally, select to enable transparent email relaying
Enable AV scanning	Optionally, select to enable anti-virus scanning.

Setting	Description
Action to perform on viruses	<p>If you have selected AV scanning, from the drop-down list, select what to do if SmoothZap detects a virus. The following options are available:</p> <p>Drop (discard) email – Select to discard the email, without notifying the sender or intended recipient.</p> <p>Bounce email (warn sender) – Select to return the email to the sender, along with a warning message.</p> <p><b>Note:</b> Because the sender’s address can be easily forged, bounced mail may not be returned to the real sender.</p> <p>Neutralize email – Select to send a warning email to the recipient, with the original mail as an attachment.</p> <p>Allow email delivery – Select to allow the email to be delivered. The virus will be logged.</p>
Transparent SMTP interfaces	If you have enabled transparent SMTP relaying, see above, select the interfaces on which to enable it.

- 8 Click Save and restart to implement email relaying.

## Configuring POP3 Proxying

You can configure SmoothZap to automatically scan email retrieved via POP3 for malware, viruses and unsolicited content.

To configure POP3 proxying:

- 1 On the email > pop3 > proxy page, configure the following settings:

Setting	Description
Enable transparent POP3 proxy	Select to enable SmoothZap to transparently retrieve email using POP3 proxying.
Enable AV scanning	Select to enable AV scanning of email retrieved by SmoothZap.
Interfaces	Select the interfaces on which to enable POP3 transparent proxying.

- 2 Click Save and restart to implement SmoothZap POP3 proxying.

## Configuring Anti-spam Settings

To configure anti-spam settings:

- 1 Navigate to the email > anti-spam > anti-spam page and configure the following settings:

Area	Setting	Description
SMTP	Enable spam filtering	Select to enable spam filtering for relayed email.
	Action to perform on spam	Select what SmoothZap should do with relayed email deemed to be spam. The options are:  Drop (discard) email – Discard the email – discarded email is not relayed.  Quarantine email – Send the email to the quarantine mailbox as specified in the Quarantine mailbox field.  Mark subject as spam – Add <b>***SPAM***</b> to the subject of the email and relay it.  Allow email delivery – Relay the email and take no action.
	Spam threshold	SmoothZap 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 SmoothZap 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.  <b>Note:</b> When using the Spam check optimization mode: Most accurate option, see below, we recommend that you set the spam threshold to 90.
	Quarantine mailbox	Enter the address of the mailbox you want to use to hold quarantined email.

Area	Setting	Description
POP3	Enable spam filtering	Select to enable spam filtering for POP3 email.
	Action to perform on spam	<p>Select what to do with POP3 email deemed to be spam. The options are:</p> <p>Replace spam with warning – Send an automatic warning to the recipient and do not send the email.</p> <p>Mark subject as spam – Add <b>***SPAM***</b> to the subject of the email and deliver it.</p> <p>Allow email delivery – Deliver the email and take no action.</p>
	Spam threshold	<p>SmoothZap 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.</p> <p>Various refinements to the algorithm used by SmoothZap to optimize for speed or resources will affect the accuracy of this probability.</p> <p>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.</p> <p>Select the threshold above which email will be considered spam.</p> <p>90 – The most easily identified spam will be filtered out, but a significant amount of spam may be allowed through.</p> <p>50-80 – messages likely to be spam will be filtered out, which means some non-spam messages may also be caught.</p> <p>30-40 – messages that are possibly spam will be filtered out, and non-spam messages are likely to be caught.</p> <p>10 – spam filtering is very aggressive. Non-spam messages are as likely to be caught as spam messages.</p> <p><b>Note:</b> When using the Spam check optimization mode: Most accurate option, see below, we recommend that you set the spam threshold to 90.</p>

Area	Setting	Description
Tuning	Spam check optimization mode	<p>Fine-tune how SmoothZap’s anti-spam service uses system resources.</p> <p><b>Note:</b> 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.</p> <p>The following options are available:</p> <p><b>Most Accurate</b> – This option filters spam very accurately. SmoothZap 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.</p> <p><b>More Accurate</b> – 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.</p> <p><b>Note:</b> This option offers high levels of accuracy at increased speed, but requires more memory and system resources.</p> <p><b>Less Resources</b> – 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.</p> <p><b>Least Resources</b> – This option provides reasonable levels of spam filtering by using a range of options which tend to provide the most accurate determination of spam whilst using the smallest amount of system resources.</p> <p><b>Note:</b> This option is only recommended for machines which have limited system resources or memory, or are heavily loaded.</p> <p><b>Fastest</b> – 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 ommits any network checking to avoid latency and any labor or processing intensive scanning.</p> <p><b>Faster</b> – 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 .</p> <p><b>Note:</b> This option is only recommended for systems which are heavily loaded and should therefore avoid any intensive activity.</p>

Area	Setting	Description
Home region	Australia and Oceania European Union South America Asia Europe North America	Specify regions from which SmoothZap scores email less aggressively for spam.
Automatic Whitelisting	Enabled	Select to add any email sent through SmoothZap automatically to the white list.
White-list spam addresses	Sender addresses and domains	Enter the email addresses and domains of email senders whose messages SmoothZap should always accept.
	Recipient addresses and domains	Enter the email addresses and domains of recipients of messages SmoothZap should always accept.
Black-list spam addresses	Sender addresses and domains	Enter the email addresses and domains of email senders whose messages SmoothZap should always treat as spam.
	Recipient addresses and domains	Enter the email addresses and domains of recipients of messages SmoothZap should always treat as spam.

- 2 Click **Save** to save your anti-spam settings.
- 3 Navigate to the **system > maintenance > licenses** page. In the Anti-spam subscription area, click **Refresh subscription information**. This ensures you have the latest anti-spam information and subscription settings.

SmoothZap is now configured to stop spam. For full information on SmoothZap and all of its options, see the *SmoothZap Administrator's Guide*.

