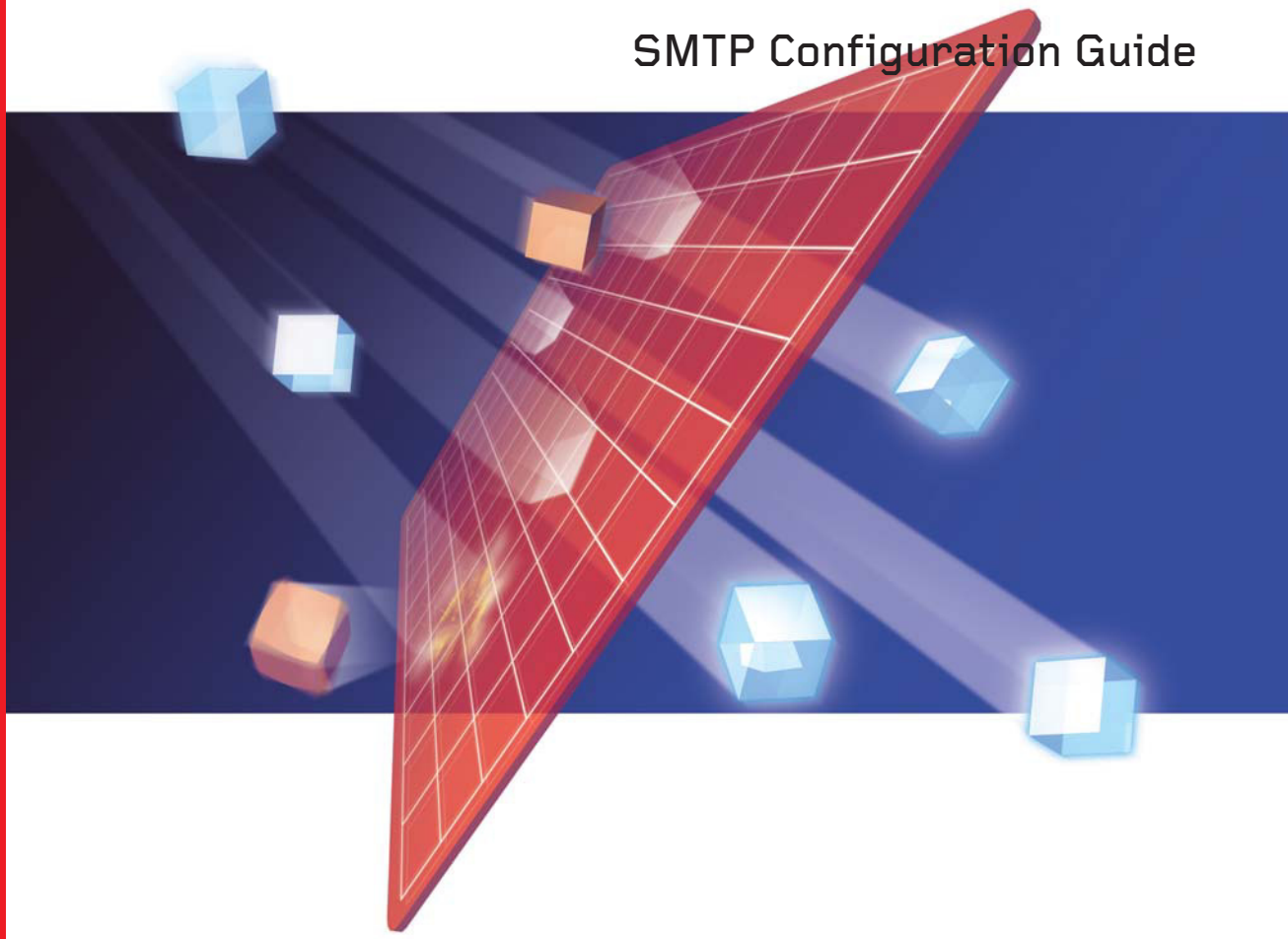
TREND MICRO™
InterScan™ VirusWall™ 6

Integrated virus and spam protection for your Internet gateway

for Linux™

SMTP Configuration Guide



TREND MICRO™

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes (if any), and the latest version of the Getting Started Guide, which are available from Trend Micro's Web site at:

http://www.trendmicro.com/download/documentation/

Trend Micro, the Trend Micro t-ball logo, IntelliTrap, InterScan VirusWall, are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright© 2002-2006 Trend Micro Incorporated. All rights reserved.

Document Part No. IVEM62710/60419

Release Date: July 2006

Protected by U.S. Patent Nos. 5,623,600; 5,889,943; 5,951,698; and 6,119,165

The *SMTP Configuration Guide for Trend Micro InterScan VirusWall 6 for Linux* is intended to provide detailed information about how to use the SMTP-related features of the software. Read it before using the software.

Additional information about how to use specific features within the software is available in the online help file and the online Knowledge Base at the Trend Micro Web site.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any other Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Contents

Chapter 7: SMTP Content Filtering

List of Figures

Chapter 1: Preparing InterScan VirusWall to Protect SMTP Traffic

Chapter 2: Configuring SMTP Virus Scan Settings

Chapter 3: Configuring IntelliTrap

Chapter 4: Configuring Anti-Phishing Settings

Chapter 5: Configuring SMTP Anti-Spam Settings

Chapter 6: Configuring SMTP Anti-Spyware / Grayware Settings

Chapter 7: SMTP Content Filtering

Chapter 1

Preparing InterScan VirusWall to Protect SMTP Traffic

This chapter covers the following topics:

How InterScan VirusWall Scans SMTP Traffic

You can use InterScan VirusWall to monitor incoming and outgoing SMTP mail traffic. You can enable or disable scanning of SMTP traffic during the installation process or at any time thereafter through the Summary page of the InterScan VirusWall Web console. You can enable or disable virus scanning of SMTP traffic on the SMTP Scanning (Incoming) and (Outgoing) pages.

The SMTP scanning function of InterScan VirusWall (SMTP VirusWall) can scan all inbound and outbound messages for viruses. It can be installed and configured to support a variety of network configurations, including scanning traffic sent using a sendmail program on the same or a different machine and traffic sent to other SMTP servers.

The SMTP configuration for InterScan VirusWall 6.0 for Linux is very similar to that in InterScan VirusWall for Unix 3.8x. But it is quite different from what is in the Windows (6.0) version. In the Windows version, InterScan VirusWall acts as an MTA (mail transport agent), that is, it is acting as an SMTP server. In the Linux version, however, InterScan VirusWall acts as an SMTP proxy, forwarding any requests/responses from the upstream/downstream SMTP server to an actual MTA.

However, a user's network may use multiple MTAs, configured differently for different parts of the network. For such a network environment, a user can configure InterScan VirusWall to relay the mail traffic so that messages originating from certain hosts are forwarded to a specific MTA, thus preserving the original sender-to-MTA ("Sender-Recipient") relationships. A user can make this configuration by using the Forward Messages for Final Processing function. (See *Forward Messages for Final Processing* on page 1-11.)

InterScan VirusWall SMTP filtering services can:

- Scan incoming and outgoing email for viruses and other types of malware
- Use IntelliTrap to scan compressed executable files that could contain potentially malicious code
- Detect Phishing email messages
- Detect spam and enable you to configure preset categories and adjust how aggressively to filter for spam
- Detect spyware and other grayware in incoming and outgoing email
- Filter content using keywords (with an exception list), attachment type, attachment size, or *From:*, *To:*, *CC:*, and *Reply To:* fields
- Enable administrator to configure SMTP server port and delivery options for incoming and outgoing mail

The Mail (SMTP) tab on the InterScan VirusWall Summary screen provides statistics concerning the number of viruses, spyware, spam messages, and phishing messages that InterScan VirusWall SMTP scanning detected in incoming and outgoing email communication.

Enabling or Disabling SMTP Services

You can enable or disable scanning services for SMTP mail message traffic in two ways:

1. During installation, in the Preconfiguration screen. (See the *InterScan VirusWall 6 Quick Start Guide* for installation instructions.)
2. On the Summary screen, Mail (SMTP) tab. Select or clear the **Enable SMTP Traffic** check box shown in figure 1-1, “The Mail (SMTP) tab of the Summary screen,” on page 1-4.

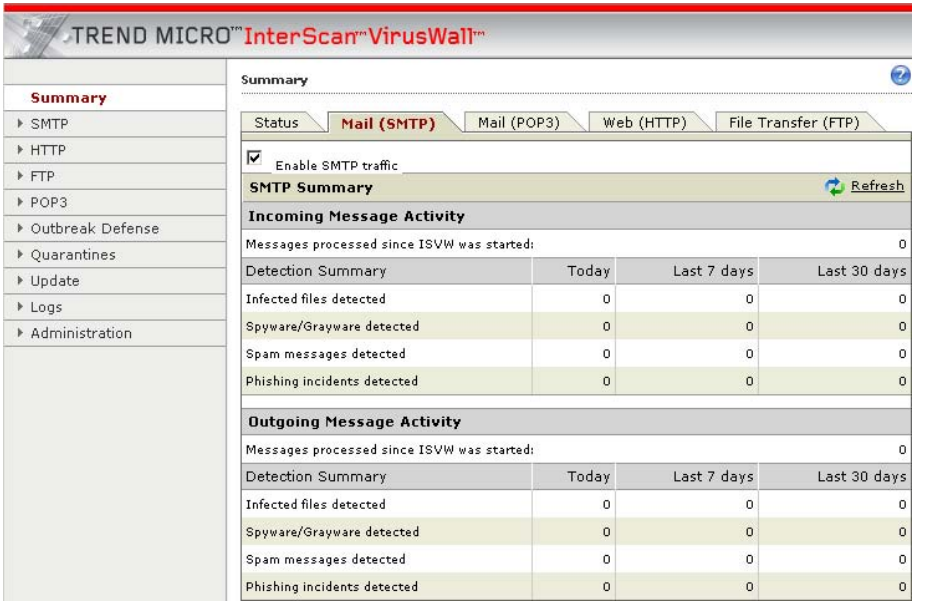


FIGURE 1-1. The Mail (SMTP) tab of the Summary screen

Configuring SMTP Services

The SMTP scanning feature of InterScan VirusWall for Linux (SMTP VirusWall) offers the InterScan VirusWall administrator a great deal of flexibility in configuring how the program will behave.

Note: Before InterScan VirusWall can scan SMTP traffic, it must have information about how to work with the mail servers in your network.

For example, you can choose which email attachment types to scan, whom to notify when SMTP VirusWall discovers a virus, and what action to take—clean, delete, move, or pass it on to the recipient along with a warning message.

SMTP VirusWall features include:

- Real-time scanning of inbound and outbound email traffic
- Automatic, customizable virus notifications to the administrator and to both the sender and the recipient of the infected message
- Option to **Clean**, **Move**, **Delete** or **Pass** on infected files
- Message-size filtering and filtering of attachments
- Compressed file scanning
- Ability to insert customized tag line in all outbound mail
- Customizable thread and spawning rate control

SMTP VirusWall works as an SMTP proxy and not as an independent mail transport agent (MTA). Before InterScan VirusWall can scan SMTP traffic, it must have information about how to work with the mail servers in your network.

You can provide this information on the Configuration tab of the SMTP Configuration page (**SMTP > Configuration > Configuration**). (See figure 1-2, “SMTP Configuration screen, Configuration tab, upper half,” on page 1-6.)

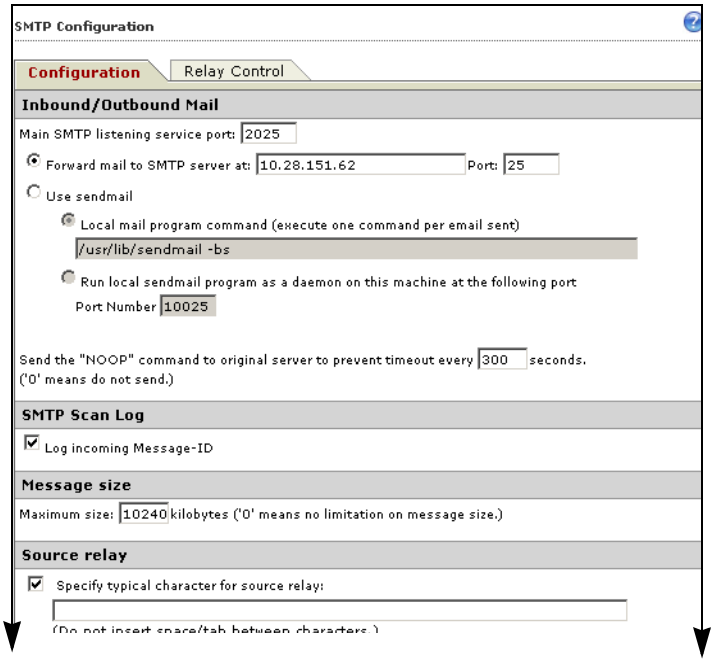


FIGURE 1-2. SMTP Configuration screen, Configuration tab, upper half

Configuring Inbound/Outbound Mail

In the Inbound/Outbound Mail section of the Configuration tab (SMTP Configuration page), you define the email path from gateway to client and the resources used to make the journey. The inbound path goes from the Internet cloud through your firewall through SMTP VirusWall and on to the client. (See figure 1-3,

"Inbound and outbound SMTP mail paths, SMTP VirusWall and SMTP server on different machines (one of several deployment options)," on page 1-7.)

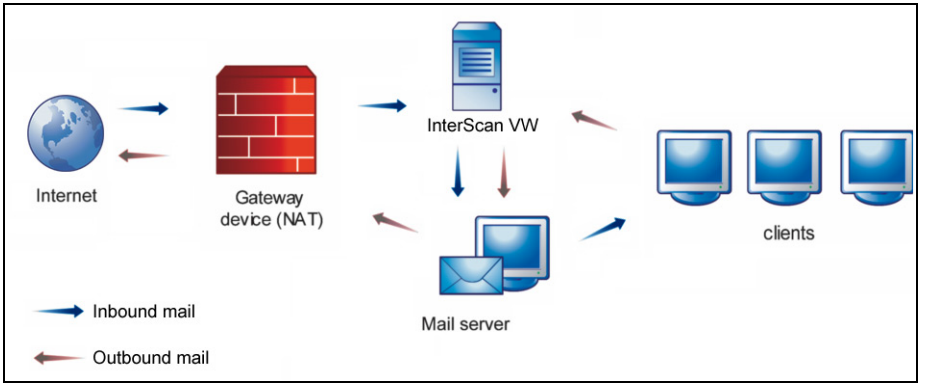


FIGURE 1-3. Inbound and outbound SMTP mail paths, SMTP VirusWall and SMTP server on different machines (one of several deployment options)

The resources are the ports used, email servers, and services that aid the journey. The following parameters need to be set to create the email routing path.

Main SMTP Listening Service Port

The main SMTP listening service port is the port that InterScan VirusWall uses to receive SMTP traffic. The default value is 25, the standard SMTP port specification. This value is configurable, but in most circumstances it should not be changed.

How you configure the **Main SMTP listening service port** option in the Configuration tab depends on the installation topology you have chosen. See the Installation Topologies section of the *Trend Micro InterScan VirusWall for Linux Getting Started Guide* for illustrations of various topologies.

Forward Mail to SMTP Server

The server entered in the Forward Mail to SMTP Server field will deliver the message after it has been scanned for viruses. InterScan VirusWall for Linux is not an MTA (message transfer agent), therefore it needs to send the mail to an SMTP server after scanning. You can think of the server entered in the Forward Mail to SMTP Server field as the *delivery* SMTP server.

Using Your Local Server

If you choose to have a local server deliver the mail, you have two configuration options: Command mode and Daemon mode:

- Command mode (**Local mail program command (execute one command per email sent**)) is used only when the MTA is on the local server. Each time a message is delivered, an instance of *sendmail* is opened to deliver the message. Once the message is delivered, *sendmail* automatically closes. This process is repeated for each message that needs to be delivered.
- Daemon mode (**Run local sendmail program as a daemon on this machine at the following port**) has the SMTP server program running continuously in the background. If you decide to run the SMTP server program in daemon mode, you choose the port that it will run on. After you have configured InterScan VirusWall to work with your SMTP program, the SMTP scanning process will start when InterScan VirusWall starts up.

Using a Remote Server

If you choose to have a remote server deliver the messages after scanning, you must enter the remote host name or IP address of the server and its port number.

Using sendmail

To configure SMTP VirusWall to use *sendmail* when it and sendmail are both on the same machine:

1. Select **SMTP > Configuration** and ensure that the **Configuration** tab is active. In the Inbound/Outbound mail section, specify the port on which SMTP VirusWall will listen for SMTP connections (for example, 25) in the **Main SMTP listening service port** field.
2. Select the **Use sendmail** check box.
3. Select the location of your *sendmail* program. The options are:
   a. **Local mail program command (execute one command per email sent)** (command mode).
   b. **Run local sendmail program as a daemon on this machine at the following port** (daemon mode).

   For example, if you intend to run sendmail in command mode, you would select **Local mail program command (execute one command per email sent)** and type the following in the field provided:

   ```
   # /usr/lib/sendmail -bs
   ```

Tip: The sendmail **`-bs`** flag formats scanned messages for delivery to the SMTP server. Consult your sendmail documentation for more information about sendmail options and flags.

Using Sendmail's Anti-Spam and Anti-Relay Features

InterScan VirusWall has its own anti-relay (and, of course, anti-spam) features. However, if you would like to also use those features that come with Sendmail, you can. If you want to use sendmail's anti-spam and anti-relay features, you will need to use the *sandwich* configurations. The sandwich configurations are used specifically to enable the sendmail anti-spam and anti-relay features.

The term *sandwich* describes a server configuration such as the following:

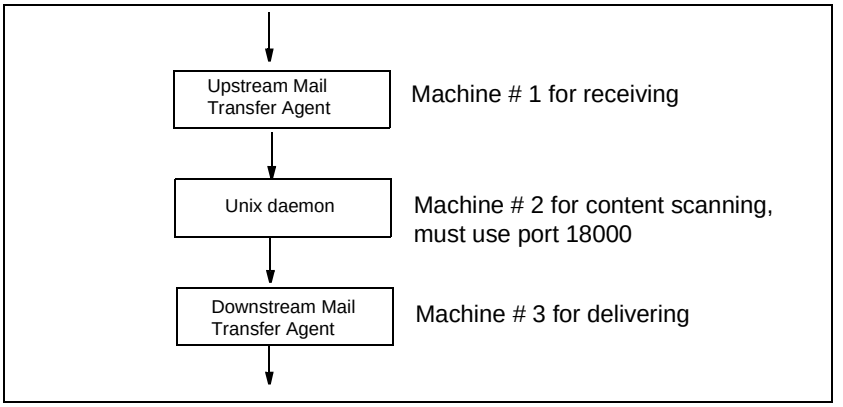


FIGURE 1-4. Sendmail sandwich server configuration

Why Forward Mail to an SMTP Server?

Because SMTP VirusWall can serve only as an SMTP proxy and not as an MTA (mail transport agent), you must tell SMTP VirusWall where to send scanned mail for routing to its ultimate destination. If your SMTP server resides on a different physical machine than SMTP VirusWall, select this option and enter the IP address and port (or FQDN and port) of your SMTP server. If your SMTP VirusWall is deployed on the same machine as your SMTP server, select **Use sendmail** (and see *Using sendmail* on page 1-8 for instructions).

Scan Log, Message Size, and Source Relay

SMTP Scan Log

Some email messages contain Message-IDs. If you would like to keep a record of these messages, select the **Log incoming Message-ID** check box in the SMTP Scan Log section.

Message Size

In the Message Size section, you can set a maximum size for mail messages to scan. Type a value (in kilobytes) in the **Maximum size** field. If you want InterScan VirusWall to scan messages of any size, set the maximum size to zero (0).

Note: This value is the size of the entire message, including the message body and any attachments.

Source Relay

There is also a feature to prevent some obviously spoofed email addresses from being relayed.

To use this feature, do the following:

1. Specify one or more characters for SMTP VirusWall to check for in an email address in order to disallow source relay.
2. Select the **Specify typical character for source relay** check box in the Source Relay section and enter those characters in the accompanying input field.

Note: Do not separate characters by a space or a tab character.

---

3. Click **Save.** SMTP VirusWall will prevent the relaying of any messages whose sender's email address contains any of those characters and will send the sender a 554 error message.

Advanced Configuration

In the Advanced Configuration section, you can choose to:

- Receive greeting when connection is established
- Write connection message to service log file
- Set client, server, and session timeouts (in seconds)

Note: The value for server timeout should be higher than that for client timeout.

Forward Messages for Final Processing

Although SMTP VirusWall works as an SMTP proxy and not as an MTA, some networks may use multiple MTAs, configured differently for different parts of the network.

If yours is such a network environment, you can configure SMTP VirusWall to relay the mail traffic originating from certain hosts to a specific MTA, thus preserving the original sender-to-MTA (sender-recipient) relationships. You can set up this configuration in the Forward Messages for Final Processing section. (See figure 1-5, "SMTP Configuration screen, Configuration tab, lower half," on page 1-13.)

The resulting message redirection is just like a sender-recipient combination.

You can enable or disable each sender-recipient combination according to your current network structure. After you select the check box for a sender-recipient group (Source host / MTA / Port), SMTP VirusWall will relay all mail coming from the sender hosts listed in that **Source host** field to the recipient MTA for delivery. You can map up to five groupings of source hosts to five respective MTAs.

You can enter source hosts either by IP address, domain name, or by any combination of the two, separating each entry with a space.

To forward messages from certain hosts to dedicated MTAs:

1. On the left menu click **SMTP > Configuration** and ensure that you are on the Configuration tab.
2. In the Forward Messages for Final Processing section (in the bottom half of the Configuration tab screen) select the **Enable message redirection** check box. (See figure 1-5, "SMTP Configuration screen, Configuration tab, lower half," on page 1-13.)
3. For each set of originating hosts whose messages you want to forward to a dedicated MTA, select the check box to the left of the **Source host** field and:
   a. Type the source host(s), delimiting multiple hosts with a space.
   b. Type the recipient MTA's IP address (or fully qualified domain name) that you want to use to process messages from the originating hosts that you have configured.
   c. Type the recipient MTA's port (required).
4. Click **Save.**

Note: It is necessary to scroll down in the **SMTP > Configuration > Configuration** tab in order to see the Forward Messages for Final Processing section.

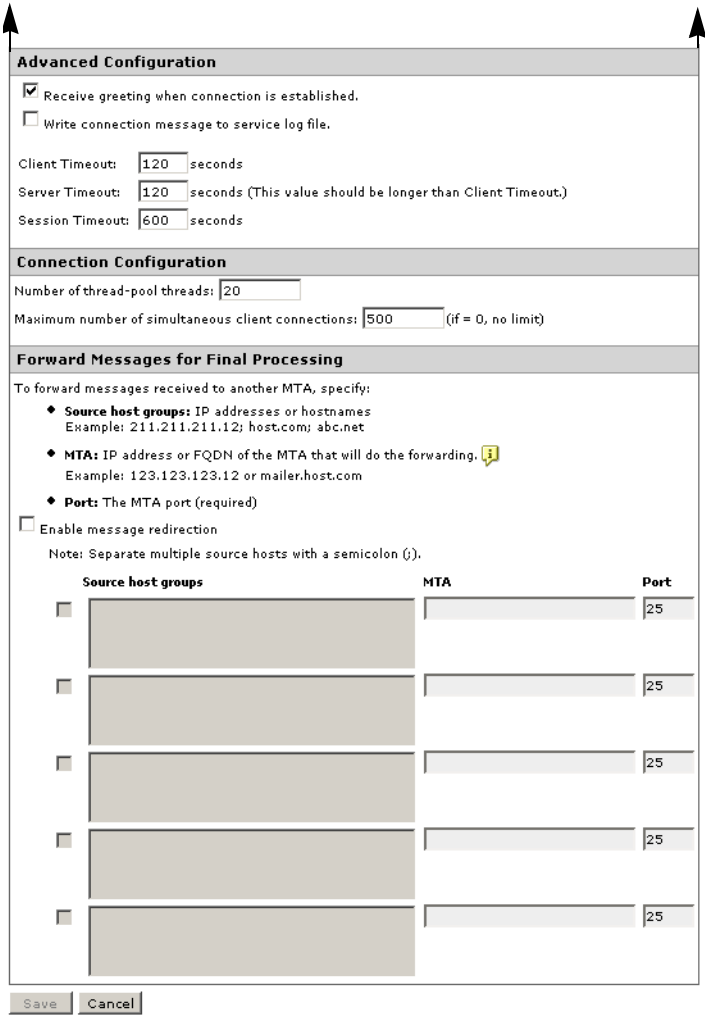


FIGURE 1-5. SMTP Configuration screen, Configuration tab, lower half

Relay Control

The Relay Control tab of the SMTP Configuration screen enables you to:

- Define which messages are legitimate outbound messages from your network
- Add a customized disclaimer to each outbound message
- Block illegitimate relayed messages by accepting only inbound traffic that is addressed to domains in your network

Outbound Processing

In the **To support outbound mail processing, specify your local domains** field, list the IP addresses/host names in your local network, as shown in Figure 1-6.

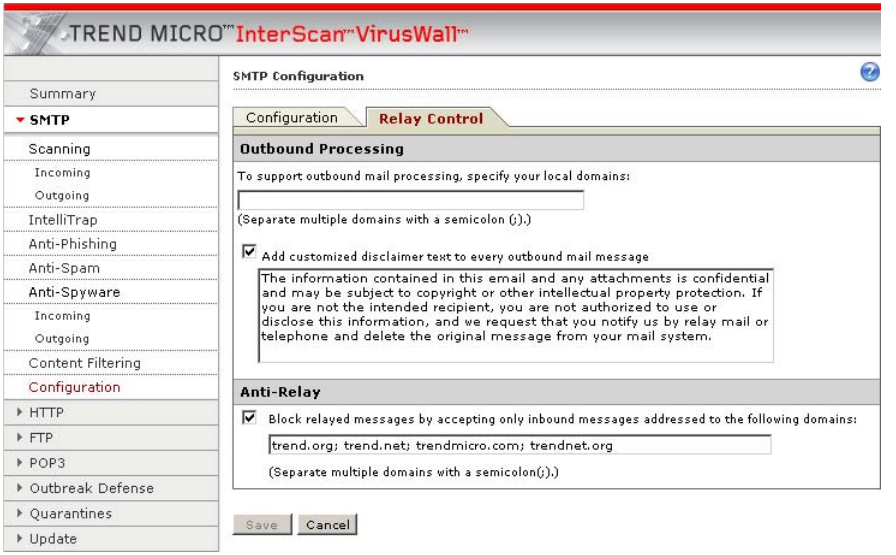


FIGURE 1-6. SMTP Configuration screen, Relay Control tab

SMTP VirusWall will regard any mail sent from machines listed here as outbound mail.

The following formats are supported:

- 192.168.5.226
- 192.168.5.*
- 192.168.*
- 192.*
- *
- 192.168.5.1-226
- 192.168.5-16
- 192.168-180

To add a customized disclaimer to each outgoing message, select the **Add customized disclaimer text to every outbound mail message** check box. You can modify the default by editing or replacing the text in the accompanying text input field.

Anti-Relay

In this section you can identify the domains that inbound messages will be allowed to reach.

To use the anti-relay feature, select the **Block relayed messages by accepting only inbound messages addressed to the following domains** check box in the Relay Control tab/Anti-Rely section (Figure 1-6) and type the legitimate domains for relaying.

Supported formats:

- *.bank.com
- mailserver.*.com
- mailserver.bank.*

Chapter 2

Configuring SMTP Virus Scan Settings

This chapter includes the following topics:

Overview

InterScan VirusWall offers the administrator flexibility in configuring SMTP virus-scanning services. For example, you can specify:

- Attachment types to scan
- Individuals to notify when SMTP VirusWall detects a virus
- Action that SMTP VirusWall takes upon detection—clean, delete, move, or block

---

Note: You can enable SMTP virus scanning only if you have given InterScan VirusWall the location of your SMTP server. Before enabling SMTP scanning, verify that you have supplied this critical information. See *Configuring SMTP Services* on page 1-5, for more information.

SMTP Virus Scanning Features

InterScan VirusWall SMTP virus scanning includes the following features:

- Real-time scanning of incoming and outgoing SMTP email traffic
- Automatic, customizable virus notifications
- Option to clean, delete, move (quarantine), pass, or block infected files
- Size filtering of messages and attachments
- Option to delete infected messages
- Ability to insert customized taglines in messages

Enabling SMTP Virus Scanning

The settings for incoming and outgoing SMTP traffic are separate. Follow the procedures below to enable incoming and/or outgoing scanning.

To enable incoming SMTP virus scanning:

1. On the left side menu, select **SMTP > Scanning > Incoming**.
2. Ensure that you are viewing the Target tab.
3. Select the **Enable SMTP Scanning (incoming)** check box.
4. Click **Save**.

Tip: If the Save button appears greyed out, select one of the available option buttons and then reselect the original. The button will become active.

To enable outgoing SMTP virus scanning:

1. On the left side menu, select **SMTP > Scanning > Outgoing**.
2. Ensure that you are viewing the Target tab.
3. Select the **Enable SMTP Scanning (outgoing)** check box.
4. Click **Save**.

Note: Virus scanning settings apply to all types of SMTP scanning for malicious files, including virus/malware, IntelliTrap, and spyware scanning.

Scan settings for incoming and outgoing SMTP traffic must be set separately.

Specifying the File Types to Scan

InterScan VirusWall can check all or specified attachment types for viruses, including the individual files within compressed volumes. Figure 2-1, “SMTP Incoming SMTP (Virus) Scanning screen, Target Tab,” on page 4 shows the settings that you can specify when scanning inbound file attachments.

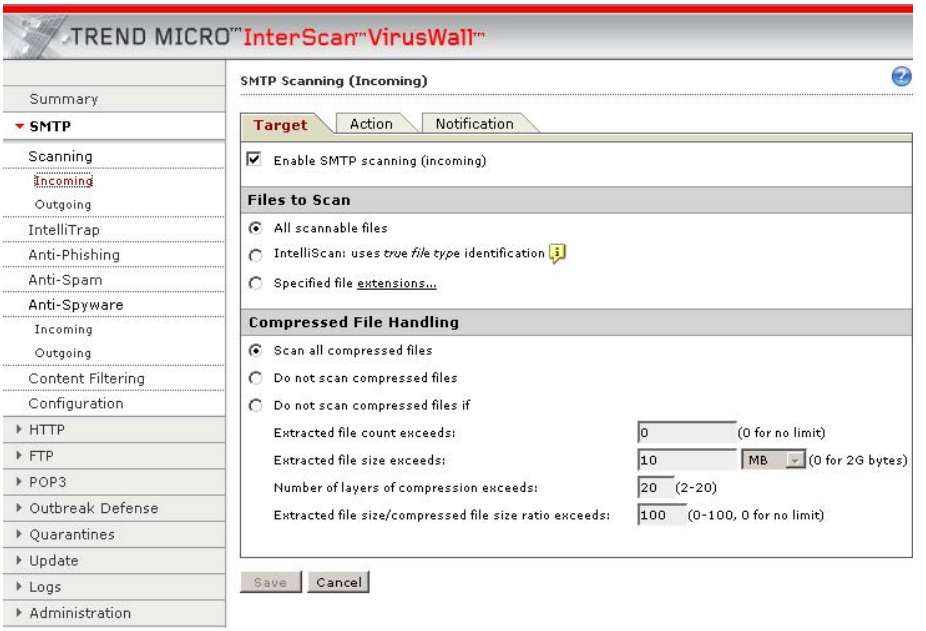


FIGURE 2-1. SMTP Incoming SMTP (Virus) Scanning screen, Target Tab

The options for file types to scan are:

- **All scannable files**. Scans all attachments, regardless of file type. This is the most secure setting, and it is the default.
- **IntelliScan: uses *true file type* identification**. Product intelligently identifies the attachments to scan. This option allows some file types through, resulting in higher performance, but is less secure than scanning all attachments.

Note: IntelliScan optimizes performance by examining file headers using true file type recognition and scanning only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can by disguised by a harmless extension name.

- **Specified file extensions**. Scan only selected attachment types by file name extension. InterScan VirusWall scans only those file types that are explicitly specified in the associated popup window:

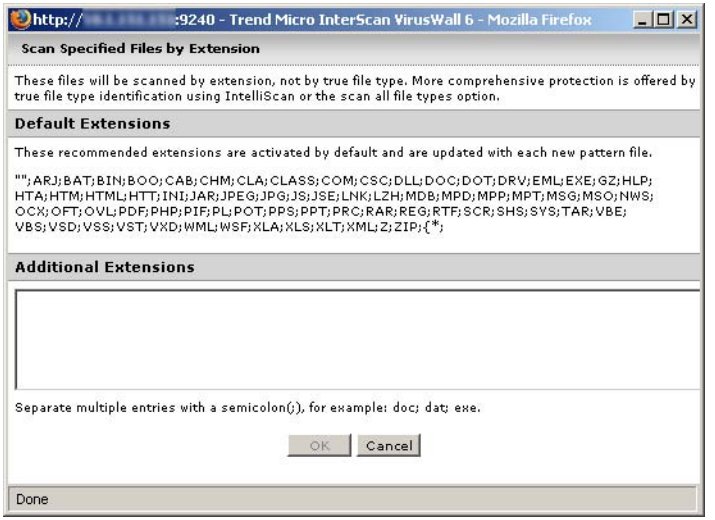


FIGURE 2-2. The Specified Files by Extension popup window

Selecting either of the first two options is straightforward. However, the third option involves a few more steps, as outlined below.

To select specified file extensions for scanning (incoming traffic):

1. From the left menu, select **SMTP > Scanning > Incoming** and ensure that the **Target** tab is active.
2. Under Files to Scan, select **Specified file extensions.**
3. Click the hyperlinked word extensions in **Specified file extensions.** The Specified Files by Extension popup window appears. The window lists the default extensions and displays an input field for additional extensions.
4. To add extensions to the default list, type them in the **Additional Extensions** field, separating multiple entries with a semicolon (;).

5. Click **OK** to save and click **OK** in the confirmation window to close the popup box.

   By default, InterScan VirusWall scans files with the following file name extensions:

```
"";ARJ;BAT;BIN;BOO;CAB;CHM;CLA;CLASS;COM;CSC;DLL;DOC;
DOT;DRV;EML;EXE;GZ;HLP;HTA;HTM;HTML;HTT;INI;JAR;JPEG;
JPG;JS;JSE;LNK;LZH;MDB;MPD;MPP;MPT;MSG;MSO;NWS;OCX;
OFT;OVL;PDF;PHP;PIF;PL;POT;PPS;PPT;PRC;RAR;REG;RTF;SCR;
SHS;SYS;TAR;VBE;VBS;VSD;VSS;VST;VXD;WML;WSF;XLA;XLS;
XLT;XML;Z;ZIP;{*;
```

FIGURE 2-3. The file extensions of those files scanned by default when *Specified file extensions* is selected

Tip: Use the **Specified file extensions** option to modify the default scan list. Certain file types, such as graphics, are unlikely to carry viruses.

Configuring Processing of Compressed Files

Settings for handling compressed files are set in different places based on whether the traffic is incoming or outgoing.

To specify how to handle compressed files during SMTP scanning:

1. On the left side menu, select **SMTP > Scanning** > **Incoming** (or **Outgoing**). The Target tab displays.
2. Under **Compressed File Handling**, select your preferred option:
   - To scan all compressed attachments, select **Scan all compressed files**. This is the most secure setting, and it is the default.
   - To skip all compressed attachments, select **Do not scan compressed files**. SMTP VirusWall will not scan any compressed attachments.
   - To scan compressed attachments based on the number of files, the file size after decompression, the number of compression layers, and the

compression ratio, select **Do not scan compressed files if** and then specify the conditions under which compressed attachments should not be scanned.

- **Extracted file count exceeds**—the maximum number of files within the compressed attachment; (0 means no limit).
- **Extracted file size exceeds**—the maximum file size after decompression. InterScan VirusWall scans only individual files within the limit.
- **Number of layers of compression exceeds**—the maximum number of compression layers.
- **Extracted file size/compressed file size ratio exceeds**—the maximum size ratio before and after compression. InterScan VirusWall scans only individual files within the limit.

3. Click **Save**.

Specifying Action to Take upon Detection of a Virus

InterScan VirusWall can take one of five actions when it detects a virus. Access possible actions on the SMTP Scanning **Action** tab shown in figure 2-4, “SMTP Scanning (Incoming) Action Tab,” on page 2-8.

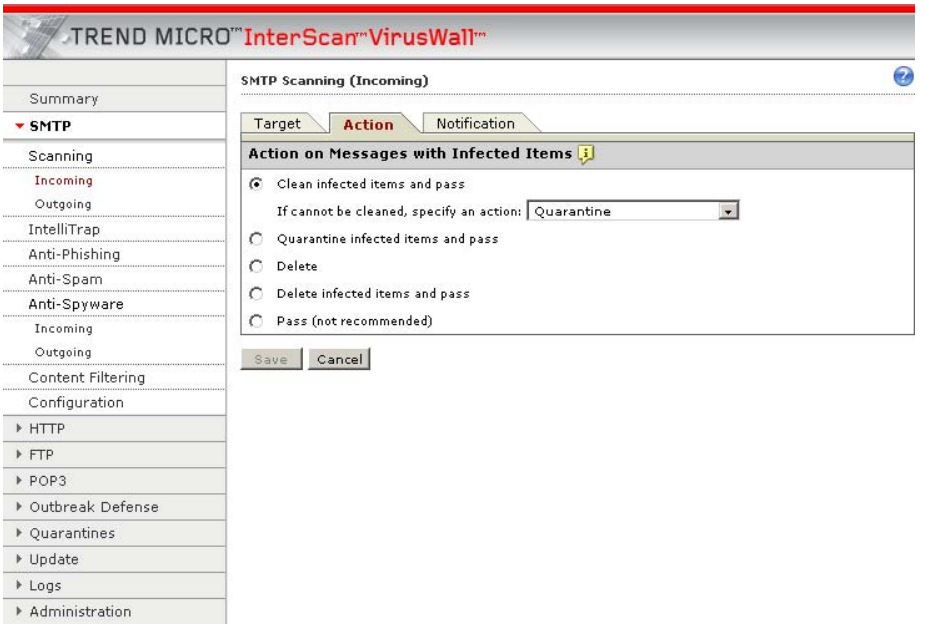


FIGURE 2-4. SMTP Scanning (Incoming) Action Tab

Tip: Specified action to take upon detection of infected attachments must be set separately for incoming and outgoing SMTP traffic. However, the options are identical.

To specify the action to take on incoming or outgoing SMTP traffic when InterScan VirusWall detects infected attachments:

1. On the left side menu, select **SMTP > Scanning** > **Incoming** (or **Outgoing**) and click the **Action** tab.
2. Under **Action on Messages with Infected Items**, select your preferred option:
   - To clean infected attachments and deliver the message, select **Clean infected items and pass**. Then, select the action to take when infected attachments cannot be cleaned:

     Quarantine—removes and quarantines attachments.

     Delete—removes attachments without quarantining them.

     Pass (not recommended)—delivers attachments with the message.
   - To quarantine attachments without cleaning them and deliver the message, select **Quarantine infected items and pass**.
   - To delete the message, select **Delete**.
   - To permanently delete attachments and deliver the message, select **Delete infected items and pass**.
   - To deliver the message with infected attachments, select **Pass (not recommended)**.
3. Click **Save**.

Note: The default quarantine folder for SMTP scanning is ***<installation_directory>/quarantine/smtp***.

Setting Notifications to Send upon Detection of a Virus

When SMTP VirusWall finds a virus, it can notify the administrator, the message recipient, the message sender, or any combination of the above. You can configure the settings, include inline notifications on all scanned messages, and specify separate notification settings for incoming and outgoing messages.

Specifying Notification Settings for Virus Detection

Tip: Specified notifications to send upon detection of infected attachments must be set separately for incoming and outgoing SMTP traffic. However, the options are identical.

To specify notification settings when InterScan VirusWall detects a virus in an incoming or outgoing message attachment:

1. On the left side menu, select **SMTP > Scanning** > **Incoming** (or **Outgoing**) and click the **Notification** tab, shown in figure 2-5.

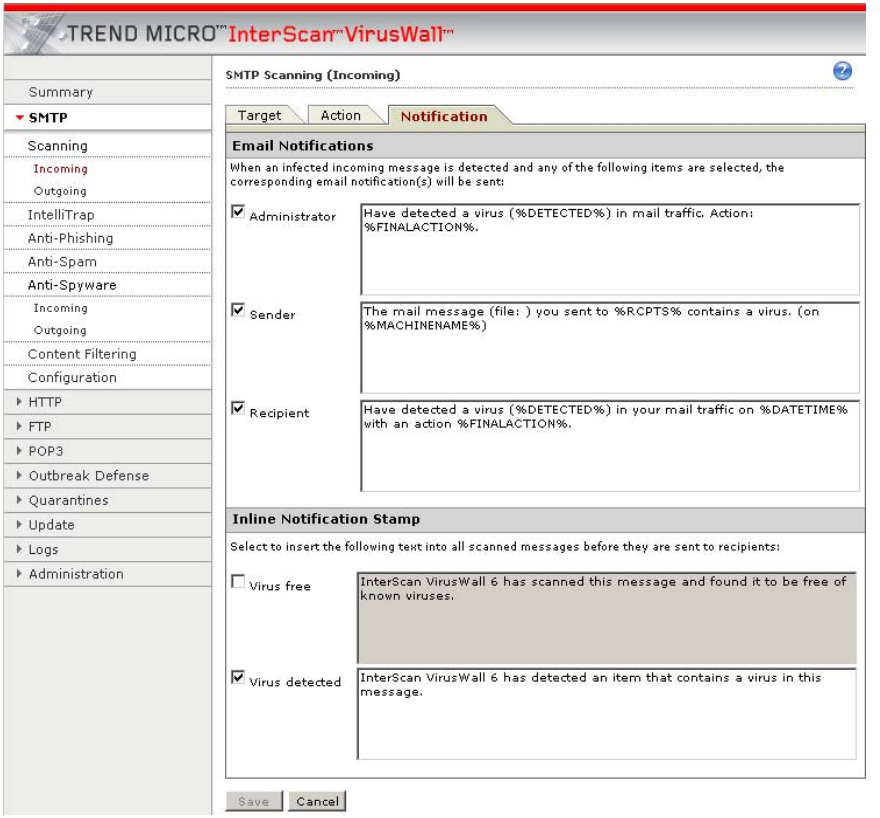


FIGURE 2-5. SMTP Scan (Incoming) screen, Notification Tab

2. Under **Email Notifications**, select the recipients of the notification sent when a virus is found.

3. Modify the message to send to each recipient (or accept the defaults). Use any of the following tokens or tags on the message:

Token	Description
%DETECTED%	name of detected virus/malware
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%DATETIME%	scan date and time
%HEADERS%	mail message header
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the InterScan VirusWall machine

4. Click **Save**.

To specify notification settings when InterScan VirusWall detects a virus in an incoming or outgoing message attachment:

1. On the left side menu, select **SMTP > Scanning** > **Outgoing** (or **Incoming**) and click the **Notification** tab, shown in figure 2-6.

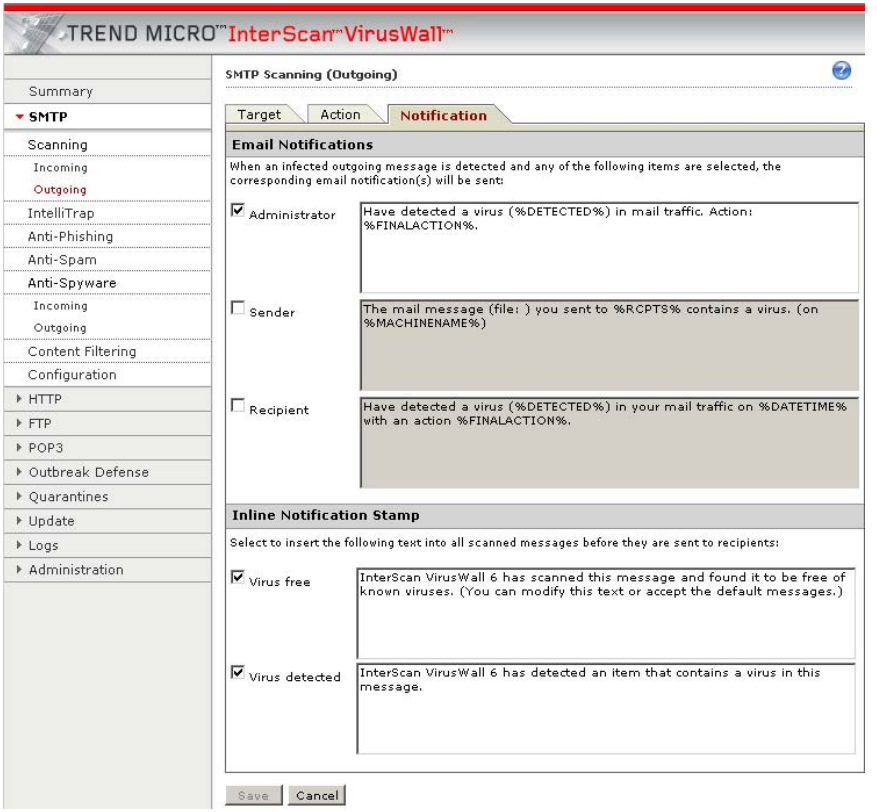


FIGURE 2-6. SMTP Scan (Outgoing) screen, Notification Tab

2. Under **Email Notifications**, select the recipients to notify when SMTP VirusWall finds a virus.

3. Modify the message to send to each recipient or accept the defaults. Use any of the following tokens or tags on the message:

Token	Description
%DETECTED%	name of detected virus/malware
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%DATETIME%	scan date and time
%HEADERS%	mail message header
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the InterScan VirusWall machine

4. Click **Save**.

Specifying Inline Notification Settings

InterScan VirusWall can insert text (an inline notification) into the message body of an incoming or outgoing message. When you select the message types **Virus free** and **Virus detected**, the inline notification will appear in all messages that InterScan VirusWall scans.

Tip: These settings must be set separately for incoming and outgoing SMTP traffic, although the options are identical.

To specify inline notification settings for incoming or outgoing messages:

1. On the left side menu, select **SMTP > Scanning** > **Incoming** (or **Outgoing**) and click the **Notification** tab.
2. Under Inline Notification Stamp (see figure 2-7), select the check box next to the kind of messages (**Virus free** and **Virus detected**) to put the inline notification in.
3. Modify the message to send to each recipient or accept the defaults. Use any of the following tokens or tags on the message:

Token	Description
%VIRUSNAME%	name of the virus found
%FILENAME%	name of the infected file
%CONTAINERNAME%	name of the archive or other files that contain compressed files
%ACTION%	action taken on the infected attachment

4. Click **Save**.

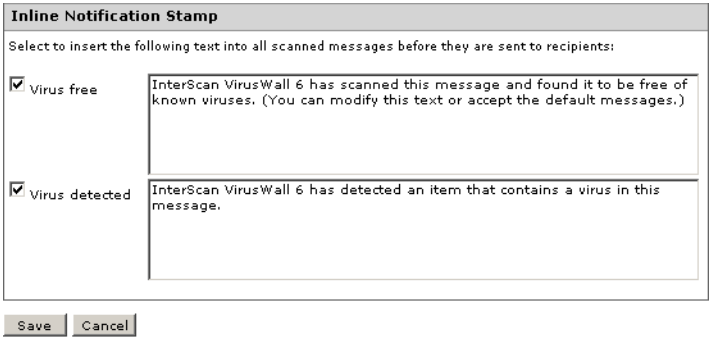


FIGURE 2-7. Inline Notification Stamp

Chapter 3

Configuring IntelliTrap

This chapter includes the following topics:

Overview

IntelliTrap detects potentially malicious code in real-time compressed executable files that arrive as email attachments. Enabling IntelliTrap allows InterScan VirusWall to take user-defined actions on infected attachments and to notify the sender of the infected message, the recipients, an administrator, or any combination of the above.

Enabling or Disabling IntelliTrap Scanning

To enable or disable SMTP IntelliTrap scanning:

1. On the left side menu, select **SMTP** > **IntelliTrap** and click the **Target** tab, shown in figure 3-1.

FIGURE 3-1. SMTP IntelliTrap screen, Target tab

2. Select or clear the **Enable SMTP IntelliTrap** check box to enable or disable IntelliTrap scanning.
3. Click **Save**.

Specifying the Action to Take When IntelliTrap Detects Potentially Malicious Code

You can select one of three actions for SMTP VirusWall to take when IntelliTrap detects potentially malicious code.

To specify the action to take when IntelliTrap detects potentially malicious code:

1. On the left side menu, select **SMTP > IntelliTrap** and click the **Action** tab, shown in figure 3-2.

FIGURE 3-2. SMTP IntelliTrap screen, Action tab

2. Under **Action on Messages With Infected Attachments**, select your preferred option:
   - Select **Quarantine infected attachments and pass** to quarantine attachments and deliver the message. Users will receive the message without the attachment(s) and the attachment(s) will be stored in the quarantine folder.

Note: The default quarantine folder for SMTP scanning is ***<installation_directory>/quarantine/smtp***.

- Select **Delete infected attachments and pass** to permanently delete attachments but deliver the message. Users will receive the message without the attachment.
- Select **Pass (not recommended)** to deliver the message with the infected attachments. Users will receive the message with the attachment(s) and an inline warning.

3. Click **Save**.

Configuring IntelliTrap Notification Settings

SMTP VirusWall can automatically notify selected recipients whenever IntelliTrap detects potentially malicious code in compressed executable files.

To specify notification settings when IntelliTrap detects a security threat in a message attachment:

1. On the left side menu, select **SMTP > IntelliTrap** and click the **Notification** tab, shown in figure 3-3.

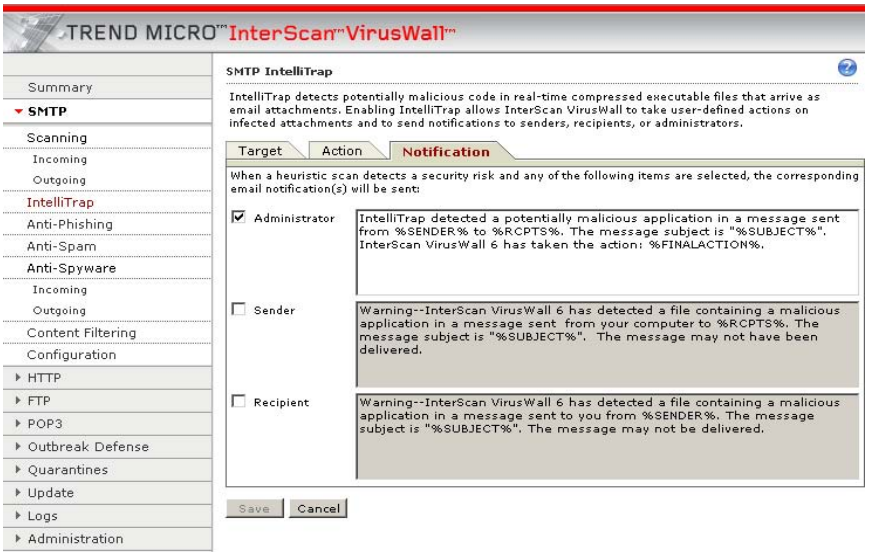


FIGURE 3-3. SMTP IntelliTrap screen, Notification tab

2. Select the recipients of the notification that SMTP VirusWall will send when IntelliTrap detects a security risk. The options are:
   - **Administrator**.—You or your network administrator
   - **Sender**.—The person who sent the message with an attachment that contains potentially malicious code
   - **Recipient**.—The person who received the message with an attachment that contains potentially malicious code

3. Modify the message to send to each recipient or accept the default notification messages. Use any of the following tokens or tags to customize the notification message:

Token	Description
%DETECTED%	name of detected virus/malware
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%DATETIME%	scan date and time
%HEADERS%	mail message header
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	host name of the InterScan VirusWall machine

4. Click **Save.**

Chapter 4

Configuring Anti-Phishing Settings

This chapter includes the following topics:

Overview

Phish, or *phishing*, is a rapidly growing form of fraud that mimics a legitimate Web site and seeks to fool Web users into divulging private information. Phishing attacks involve email messages that falsely claim to be from an established, legitimate organization. The messages typically encourage recipients to click on a link that will redirect their browsers to a fraudulent Web site, where they are asked to update personal information. Victims usually give up passwords, social security numbers, and credit card numbers.

In a typical scenario, unsuspecting users receive an urgent-sounding (and authentic-looking) email telling them that there is a problem with their account that they must immediately fix or else the account will be closed. Such email messages include the URL of a Web site that looks exactly like the real thing (it is simple to clone a legitimate email message and a legitimate Web site but then change the back end—by which the collected data is actually sent).

Tip: This manual includes guidance on scanning SMTP traffic for phishing email messages. For information on blocking known phishing sites, see the *Trend Micro InterScan VirusWall 6 HTTP Configuration Guide*, a separate manual.

Enabling SMTP Anti-Phishing

To enable the SMTP anti-phishing feature:

1. On the left side menu, select **SMTP > Anti-phishing** and click the **Target** tab, shown in figure 4-1.
2. Select the **Enable SMTP Anti-phishing** check box.
3. Click **Save**.

FIGURE 4-1. SMTP Anti-phishing Target Tab

Specifying the Action to Take upon Detection of a Phishing Message

To specify the action on phishing messages:

1. On the left side menu, select **SMTP > Anti-Phishing** and click the **Action** tab, shown in figure 4-2.
2. Select the action for phishing messages:
   - Select **Quarantine** to move the message to the quarantine folder.
   - Select **Delete** to delete the message without delivering it.
   - Select **Pass (not recommended)** to deliver the phishing message normally.
3. Click **Save**.

FIGURE 4-2. SMTP Anti-Phishing screen, Action tab

Specifying Notifications to Send upon Detection of a Phishing Message

When InterScan VirusWall detects a phishing message, it can send an email notification to the administrator, the recipient(s), or both. You can report suspected or known phishing sites to TrendLabs. Figure 4-3, “SMTP Anti-Phishing screen, Notification tab,” on page 5 shows the SMTP Anti-phishing Notification tab that allows you to specify whether to send email notifications when InterScan VirusWall detects a phishing site.

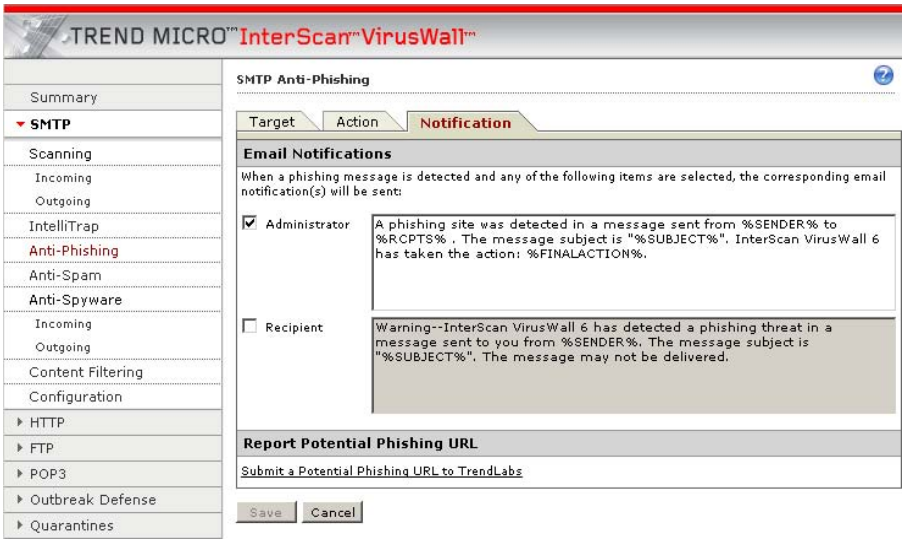


FIGURE 4-3. SMTP Anti-Phishing screen, Notification tab

To specify notification settings when a phishing URL is detected:

1. On the left side menu, select **SMTP** > **Anti-phishing** and click the **Notification** tab.
2. Select the recipients of the notification sent when InterScan VirusWall detects a phishing URL.
3. Modify the message to send to each recipient or accept the message defaults. Use any of the following tokens or tags to modify the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers
%DATETIME%	scan date and time
%HEADERS%	mail message header
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%DETECTED%	name of the security risk found
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	host name of the InterScan VirusWall machine

4. Click **Save**.

Reporting a Potential Phishing URL

To report suspected or known phishing sites to TrendLabs, click **Submit a Potential Phishing URL to TrendLabs** and email the URL to:

`antifraud@support.trendmicro.com`

The Trend Micro Internet security threat analysis center, TrendLabs, monitors sites that obtain information for fraudulent purposes. TrendLabs distributes known phishing site information as part of the automatic updates that Trend Micro makes available to InterScan VirusWall customers.

Note: To view the Trend Micro Phishing Encyclopedia, a list of known phishing email messages, visit http://www.trendmicro.com/en/security/phishing/overview.htm.

Chapter 5

Configuring SMTP Anti-Spam Settings

This chapter includes the following topics:

SMTP Anti-Spam Features

SMTP VirusWall uses the following basic features to filter spam in SMTP email communication:

Filter Tuning (by detection level)

Administrators set a spam detection level to filter out spam. The higher the detection level, the more messages that SMTP VirusWall classifies as spam. You can set a global detection level for all messages or set one detection level for each spam category.

The detection level determines how tolerant SMTP VirusWall will be toward suspect email messages.

A high detection level quarantines the most email as spam, but it might also falsely identify and quarantine legitimate email messages as spam, creating “false positive” spam mail.

A low detection level does not rigorously screen email messages for spam but does not create many false positive spam messages.

Keyword Exceptions

List keywords to identify messages as not spam. If a message contains one of the keywords listed, SMTP VirusWall will consider it a legitimate email message and will allow it to be delivered.

Approved and Blocked Senders Lists

These lists filter on the sender’s email address rather than on content. InterScan VirusWall always delivers approved sender messages and always classifies blocked sender messages as spam.

Note: The Exchange administrator maintains a separate Approved and Blocked Senders list for the Exchange server. If an end user adds a sender to the Approved Senders list, but that sender is already on the administrator's Blocked Senders list, then messages from that sender will be blocked.

Categories of Spam

SMTP VirusWall screens spam according to seven categories and allows administrators to specify a detection level for each category:

- Commercial
- Health
- Make money fast
- Racist
- Religion
- Sexual content
- Others

For example, if an administrator's clients work in a medical field, the administrator might decide to set a high sensitivity level for the make money fast category, but may decide that it would be risky to filter messages in the health category. The administrator can set a low sensitivity level for email messages in the health category.

Enabling SMTP Anti-Spam

On the SMTP Anti-Spam screen, Target tab, shown in figure 5-1, you can enable spam filtering and specify detection levels for various predefined categories of spam.

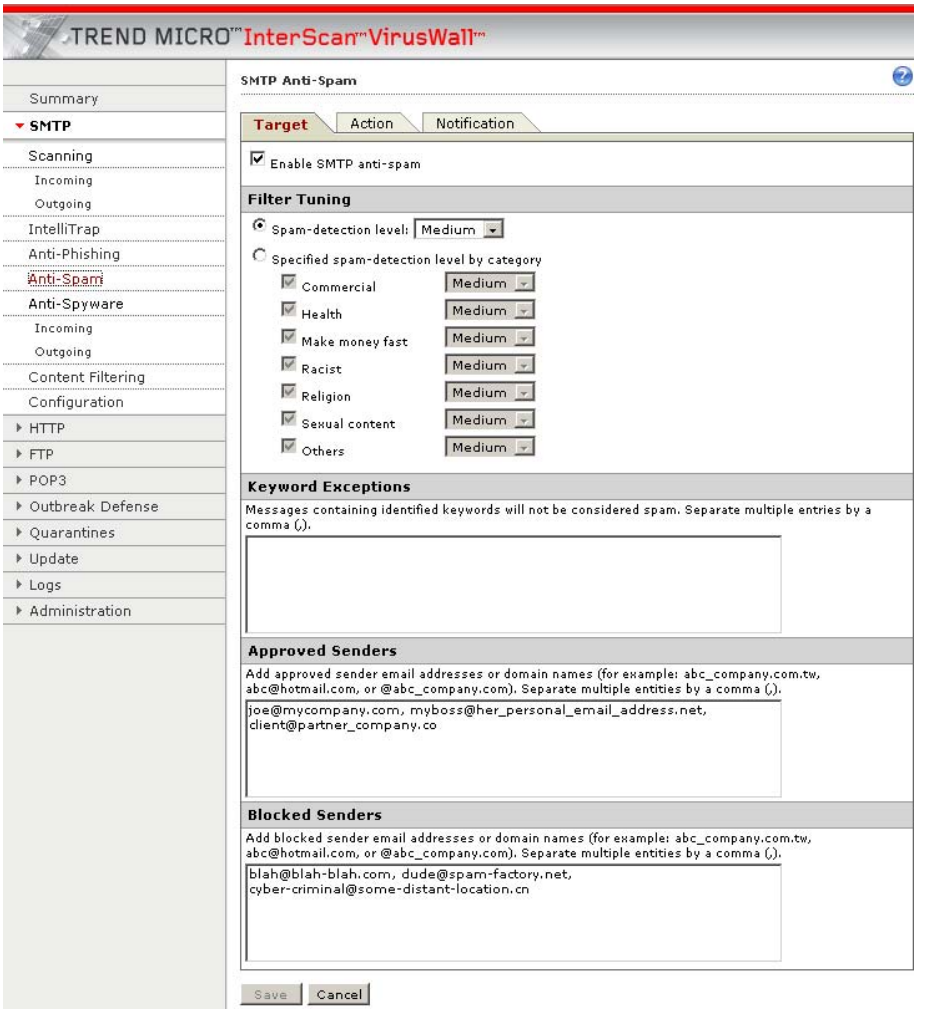


FIGURE 5-1. SMTP Anti-Spam screen, Target tab

To enable SMTP anti-spam filtering:

1. On the left-side menu, select **SMTP** > **Anti-spam**.
2. Click the **Target** tab.
3. Select the **Enable SMTP anti-spam** check box.
4. Click **Save**.

Setting the Spam Detection Level

You can select which categories of spam to scan for and the intensity of the scan for each category. Use this feature to calibrate SMTP VirusWall to precisely enforce the anti-spam policy of your organization.

To specify the spam detection level:

1. On the left side menu, select **SMTP** > **Anti-Spam**. The SMTP Anti-Spam screen opens, displaying the Target tab.
2. In the **Filter Tuning** section, select one of the following:
   - **Spam detection level** to use the same detection level for all categories
   - **Specified spam detection level by category** to specify detection levels for each category independently

Spam Detection Levels

SMTP VirusWall uses the following detection levels:

Detection Level	Filtering Criteria
Low	SMTP VirusWall filters only the most obvious and common spam messages, but there is a very low chance that it will filter false positives. This is the most lenient level of spam detection.
Medium	SMTP VirusWall monitors at a high level of spam detection with a moderate chance of filtering false positives. This setting is the default.
High	SMTP VirusWall monitors all email messages for suspicious files or text, but there is a greater chance of false positives. This is the most rigorous level of spam detection.

Determining Spam Detection Levels

The InterScan VirusWall anti-spam engine uses heuristics and algorithms to calculate the spam detection level. The engine scans the message or file and assigns the scanned item a spam score. Based on this spam score and the spam detection and confidence levels that you specify, SMTP VirusWall determines whether the item is spam.

The predefined threshold settings are:

Detection Level	Low Confidence	Medium Confidence	High Confidence
Low	6	7	10
Medium	4.5	6	10
High	4	5	7

- If you specify a low detection level and the spam score is 6.5, then SMTP VirusWall will perform the action specified for the low confidence level.
- If the spam score is 8, SMTP VirusWall will perform the action specified for the medium confidence level.
- If the spam score is 11, SMTP VirusWall will perform the action specified for the high confidence level.

To see a spam score, see the spam log. A sample entry might be:

```
2006/02/04 20:10:32, SMTP, , Stamp, Success, "LastName\, FirstName"
 <FirstName.LastName@Level3.com>,"SPAM@TrendMicro.com"
 <SPAM@TrendMicro.com>, FW:How are you doing?
 <D7626E4452B0F745B4C7C15BC97EA052D66887@idclexc0005.corp.global.
 level3.com>, 3.51.0.1033, 13974000, Spam, ,14.594000
```

In the above log entry, the very last number, 14.594000, is the spam score.

Tuning the Spam Filter

If you are getting too many false positives, set the spam detection level to a lower setting. Conversely, if users report that they are getting too much spam, adjust the detection level to a higher setting.

To submit samples of false positives to Trend Micro, visit:

http://subwiz.trendmicro.com/SubWiz/spam_mail-Form.asp

Specifying Keyword Exceptions

Keyword exceptions exclude from spam filtering any messages that contain certain text. Separate keywords in the exception lists with a comma (,). Type keywords that should ***not*** be considered spam in the Keyword Exceptions text box shown in figure 5-2, *SMTP Anti-Spam screen, Target tab, showing Keyword Exceptions section*.

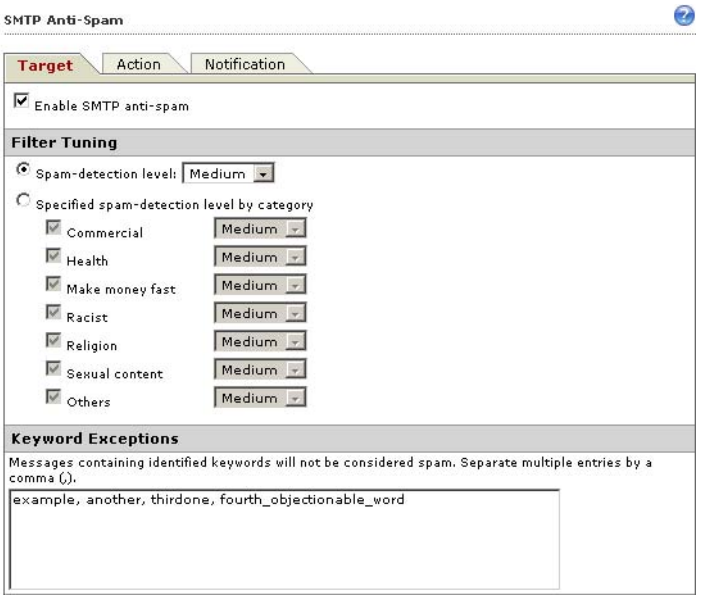


FIGURE 5-2. SMTP Anti-Spam screen, Target tab, showing Keyword Exceptions section

Maintaining Approved and Blocked Senders Lists

The Approved Senders list contains trusted email addresses. SMTP VirusWall does not filter messages arriving from these addresses for spam unless you enable **Detect Phishing incidents**.

The Blocked Senders list contains email addresses that cannot be trusted. SMTP VirusWall automatically considers messages arriving from these addresses as spam

and deletes such messages. InterScan VirusWall does not notify anyone that it deleted the messages.

When an email address is in both the Approved Senders and Blocked Senders lists, messages arriving from this address are considered spam and are deleted.

When adding email addresses to the lists, separate multiple entries with a comma. Type all email addresses in the appropriate list, shown in figure 5-4.

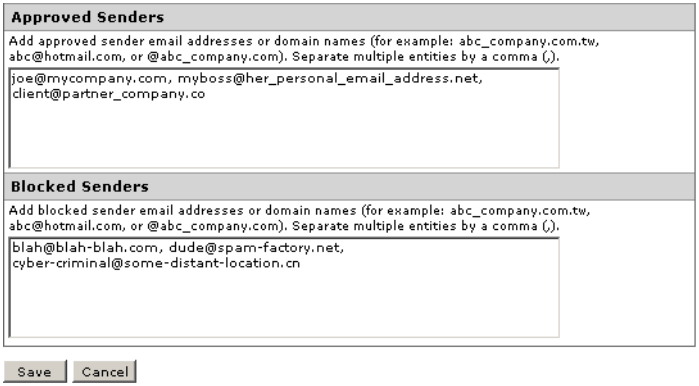


FIGURE 5-3. SMTP Anti-Spam screen, Target tab, Approved Senders and Blocked Senders sections

InterScan VirusWall supports wildcard (*) matching for the Approved Senders and Blocked Senders lists. Sample patterns are shown in Table 5-1, “Using Wildcards (*) in the Senders Lists,” on page 5-10.

TABLE 5-1. Using Wildcards (*) in the Senders Lists

PATTERN	MATCHED SAMPLES	UNMATCHED SAMPLES
john@trend.com	john@trend.com john@trend.com.	Any address different from the pattern.
@trend.com *@trend.com	john@trend.com mary@trend.com.	john@ms1.trend.com john@trend.com.tw mary@trend.comon
trend.com	john@trend.com john@ms1.trend.com mary@ms1.rd.trend.com mary@trend.com	john@trend.com mary@mytrend.com joe@trend.comon
*.trend.com	john@ms1.trend.com mary@ms1.rd.trend.com joe@ms1.trend.com	john@trend.com john@trend.com.tw mary@ms1.trend.com
trend.com.*	john@trend.com.tw john@ms1.trend.com.tw john@ms1.rd.trend.com.tw mary@trend.com.tw.	john@trend.com john@ms1.trend.com. john@mytrend.com.tw
.trend.com.	john@ms1.trend.com.tw john@ms1.rd.trend.com.tw mary@ms1.trend.com.tw.	john@trend.com john@ms1.trend.com john@trend.com.tw john@ms1.trend.com.
..*.trend.com *****.trend.com	The same as *.trend,com	
trend.com trend.com trend.*.com @*.trend.com	They are all invalid.	

Specifying Actions to Take on Messages Identified as Spam

SMTP VirusWall can take one of several actions when it identifies a message as spam. The detection level(s) that you set on the Anti-Spam screen Target tab determine the action. See figure 5-4, “SMTP Anti-Spam screen, Action tab,” on page 5-11.

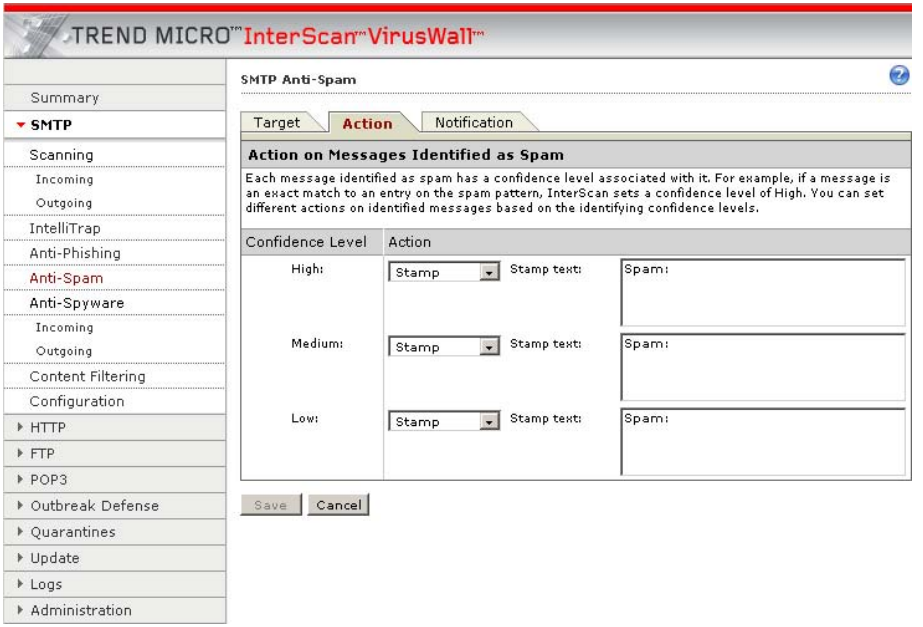


FIGURE 5-4. SMTP Anti-Spam screen, Action tab

To specify the action on spam messages:

1. On the left side menu, select **SMTP > Anti-Spam.** The SMTP Anti-Spam screen opens, displaying the Action tab.
2. Specify the action to take based on the detection confidence level:
   - **High**—SMTP VirusWall is very confident that the mail message is spam.
   - **Medium**—SMTP VirusWall is fairly confident that the mail message is spam.
   - **Low**—SMTP VirusWall is fairly confident that the mail message is not spam.

   For each confidence level, you can select one of four actions:
   - **Delete**—The whole message is deleted.
   - **Quarantine**—The message is quarantined.
   - **Stamp**—A notification content stamp is inserted into the subject line of the message.
   - **Pass**—SMTP VirusWall does nothing to the message and sends it on to the mail server for normal processing.

Specifying Notifications to Send upon Detection of Spam

InterScan VirusWall can notify the administrator or the recipient when it detects spam email messages. You can specify recipients for the email notification and create messages to send to the administrator and mail recipients. Figure 5-5, “SMTP Anti-Spam screen, Notification Settings tab,” on page 13 shows the SMTP Anti-Spam Notification Settings tab.

FIGURE 5-5. SMTP Anti-Spam screen, Notification Settings tab

To specify notification settings when SMTP VirusWall detects spam:

1. On the left side menu, select **SMTP > Anti-Spam.** The SMTP Anti-Spam screen appears, displaying the Notification tab.
2. Select the recipients whom InterScan VirusWall will notify when SMTP VirusWall detects spam.

3. Modify the message to send to each recipient or accept the default messages. You can use several tokens or tags to modify the message, as shown in Table 5-2, “Tokens available for customizing anti-spam notification messages,” on page 5-14.

TABLE 5-2. Tokens available for customizing anti-spam notification messages

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%DETECTED%	name of the security risk found
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	host name of the InterScan VirusWall machine

4. Click **Save**.

Chapter 6

Configuring SMTP Anti-Spyware / Grayware Settings

This chapter includes the following topics:

Types of Grayware

Spyware/grayware comes in many forms and often appears to be a legitimate software program. Trend Micro tracks spyware/grayware and provides regular pattern file updates.

See Table 6-1, “Types of spyware and grayware and their typical functions,” on page 6-2 for some common types of grayware.

TABLE 6-1. Types of spyware and grayware and their typical functions

TYPE OF GRAYWARE	TYPICAL FUNCTION
Spyware	Gathers data, such as account user names and passwords, and transmits them to third parties
Adware	Displays advertisements and gathers data, such as user Web surfing preferences, to target advertisements at the user through a Web browser
Dialers	Changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem
Joke Program	Causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes
Hacking Tools	Helps hackers enter computers
Remote Access Tools	Help hackers remotely access and control computers
Password Cracking Applications	Helps hackers decipher account user names and passwords
Others	Other types not covered above

Enabling SMTP Spyware Scanning

As with SMTP scanning for viruses, the settings for incoming and outgoing SMTP traffic are separate. Follow the procedures below to enable incoming and/or outgoing scanning.

To enable spyware scanning of incoming or outgoing SMTP traffic:

1. On the left side menu, select **SMTP > Anti-Spyware > Incoming (**or **Outgoing)**. The SMTP Anti-Spyware (Incoming) [or Outgoing] screen appears, displaying the Target tab.
2. Select the **Enable SMTP Anti-spyware (incoming)** [or (**outgoing**)] check box.
3. Click **Save**.

Figure 6-1 shows the SMTP Anti-Spyware screen Target tab, from which you can enable SMTP spyware scanning types and exclusions.

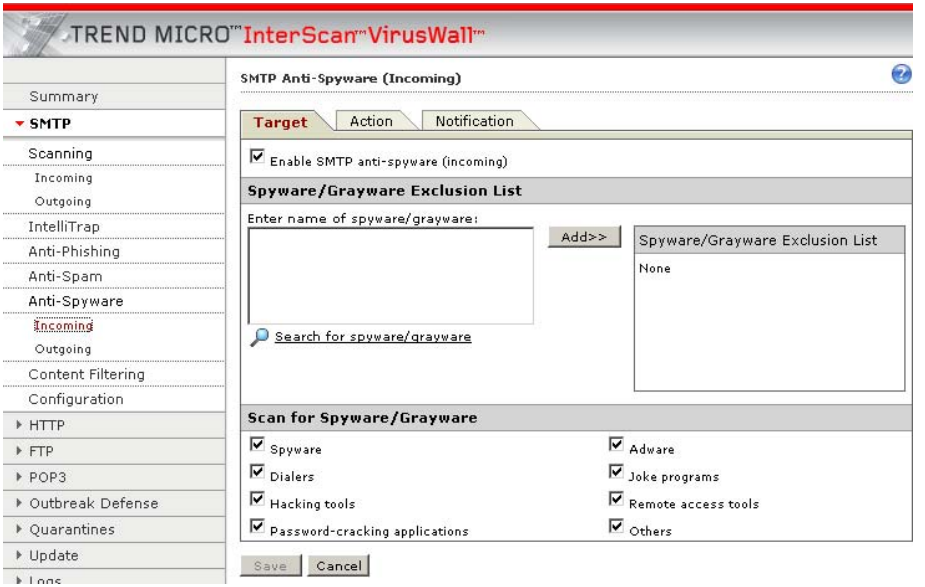


FIGURE 6-1. SMTP Anti-Spyware screen, Target tab

Excluding Specific Spyware/Grayware from SMTP Scanning

There are two spyware/grayware exclusion lists for SMTP scanning; one for incoming traffic and one for outgoing traffic. The interfaces are the same. Follow the procedure below to add spyware/grayware file names to the exclusion list.

To list specific file names or file name extensions to exclude from spyware/grayware scanning of incoming or outgoing SMTP traffic:

1. On the left-side menu, select **SMTP > Anti-Spyware** > **Incoming** (or **Outgoing**). The SMTP Anti-Spyware (Incoming) [or (Outgoing)] screen appears, displaying the Target tab.
2. Under the Spyware/Grayware Exclusion List section, in the **Enter name of spyware/grayware** text box, type the file names or the file extensions to exclude from spyware/grayware scanning (one per line). Use the asterisk (*) as a wildcard character to specify extension names. For example, to exclude .bmp files, type *.bmp.
3. Click **Add** (

). The spyware/grayware name(s) that you just typed are moved to the Spyware Grayware Exclusion List box.
4. Click **Save**.

Note: To delete entries on the exclusion list, click the trash bin () icon. Click **Save** to finalize changes.

If you are unsure of the official name of the spyware/grayware program that you would like to exclude from scanning, click the Search for spyware/grayware hyperlink (below the **Enter name of spyware/grayware** text box) to access the Trend Micro online Spyware/Grayware search form.

Specifying Spyware and Grayware Types to Scan

In this section you can select any combination from eight pre-existing spyware/grayware types. The options are identical for outgoing and incoming SMTP traffic, although you must set these options separately for each.

To specify the types of spyware and grayware in incoming and outgoing SMTP traffic that you want SMTP VirusWall to scan for:

1. On the left-side menu, select **SMTP > Anti-Spyware > Incoming** (or **Outgoing**). The SMTP Anti-Spyware (Incoming) [or (Outgoing)] screen appears, displaying the Target tab.
2. Under **Scan for Spyware/Grayware**, select the types of spyware and grayware for which SMTP VirusWall will scan.
3. Click **Save**.

Specifying the Action to Take upon Detection of Spyware/Grayware

SMTP VirusWall can take one of three actions when it detects spyware or other grayware (see Figure 6-2).

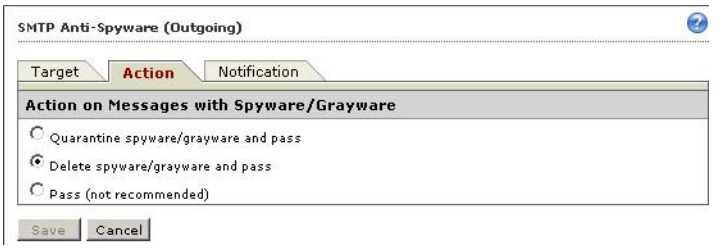


FIGURE 6-2. SMTP Anti-Spyware (Outgoing) screen, Action tab

The options for action to take upon detection of spyware/grayware in SMTP traffic are identical for outgoing and incoming traffic. However, you must set this action separately for each direction of traffic. Follow the procedure below to set action for SMTP VirusWall to perform when it detects spyware/grayware in incoming or outgoing traffic.

To specify the action to take when SMTP VirusWall detects spyware/grayware in incoming or outgoing SMTP traffic:

1. On the left-side menu, select **SMTP > Anti-Spyware > Incoming** (or **Outgoing**) and click the **Action** tab. The Action tab screen appears.
2. Under **Action on Messages with Spyware/Grayware**, select your preferred option:
   a. **Quarantine spyware/grayware and pass**.—To quarantine attachments and deliver the message, select this option. Users will receive the message without the attachment and the attachment will be stored in the quarantine directory.

b. **Delete spyware/grayware and pass**.—To permanently delete detected attachments and deliver the message, select this option. Users will receive the message without the attachment.

c. **Pass (not recommended)**.—To deliver the message with the detected attachments, select this option.

3. Click **Save**.

Specifying Notifications to Send upon Detection of Spyware/Grayware

When SMTP VirusWall detects spyware or other grayware in an incoming or outgoing message, you can choose to send notifications to the administrator, the sender of the message, the recipient(s) of the message, or any combination of the above. (See figure 6-3, *SMTP Anti-Spyware (Incoming) screen, Notification tab* for the default appearance of this screen.)

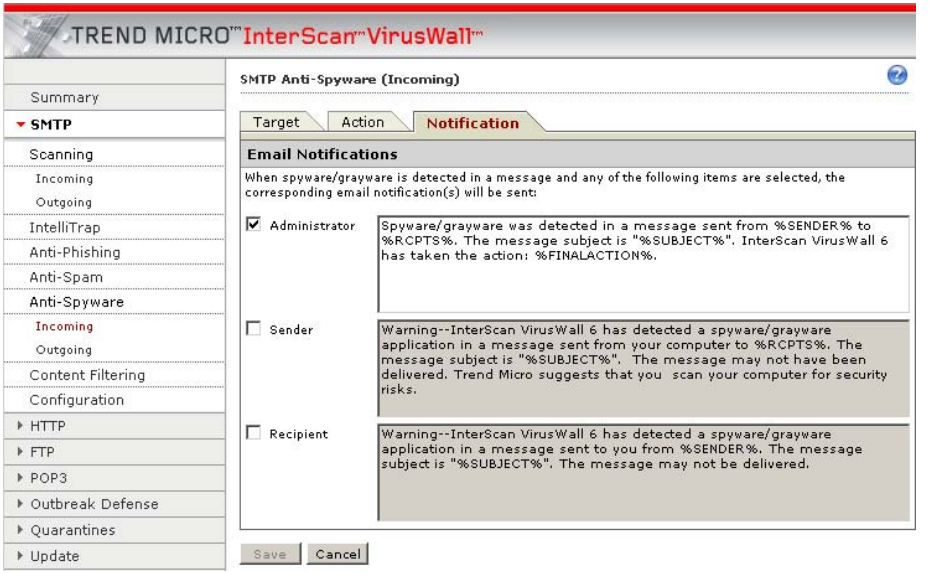


FIGURE 6-3. SMTP Anti-Spyware (Incoming) screen, Notification tab

The notification options for outgoing and incoming SMTP traffic are identical. However, you must set your options for incoming and outgoing traffic independently. Follow the procedure below to select notification options for detection of spyware/grayware in incoming and outgoing SMTP traffic.

To specify notification settings when SMTP VirusWall detects spyware or grayware in incoming or outgoing SMTP traffic:

1. On the left-side menu, select **SMTP** > **Anti-Spyware** > **Incoming** (or **Outgoing**) and click the **Notification** tab. The Notification tab screen appears.
2. Select the recipients of the notification sent when spyware or grayware is detected.
3. Modify the message to send to each recipient or accept the default messages. You can use any of the following tokens or tags to modify the notification messages.

TABLE 6-2. Tokens available for customizing anti-spyware notification messages

Token	Description
%DETECTED%	name of spyware/grayware detected
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%DATETIME%	scan date and time
%MAILID%	mail message ID
%HEADERS%	mail message header
%PROTOCOL%	mail protocol
%FILTERNAME%	name of the filter that performs the action
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	host name of the InterScan VirusWall machine

4. Click **Save**.

Chapter 7

SMTP Content Filtering

InterScan VirusWall provides email content filtering for SMTP. This feature provides real-time monitoring and control of information that enters or leaves the network through the SMTP protocol.

This chapter includes the following topics:

Enabling and Disabling SMTP Content Filtering

When you enable SMTP content filtering, the InterScan VirusWall SMTP scanning feature (SMTP VirusWall) scans all information that enters or leaves the network through SMTP for possible matches with the policies that you have defined. Figure 7-1 shows the content filtering settings. All policies that have been defined to filter content are listed under the Policies section.

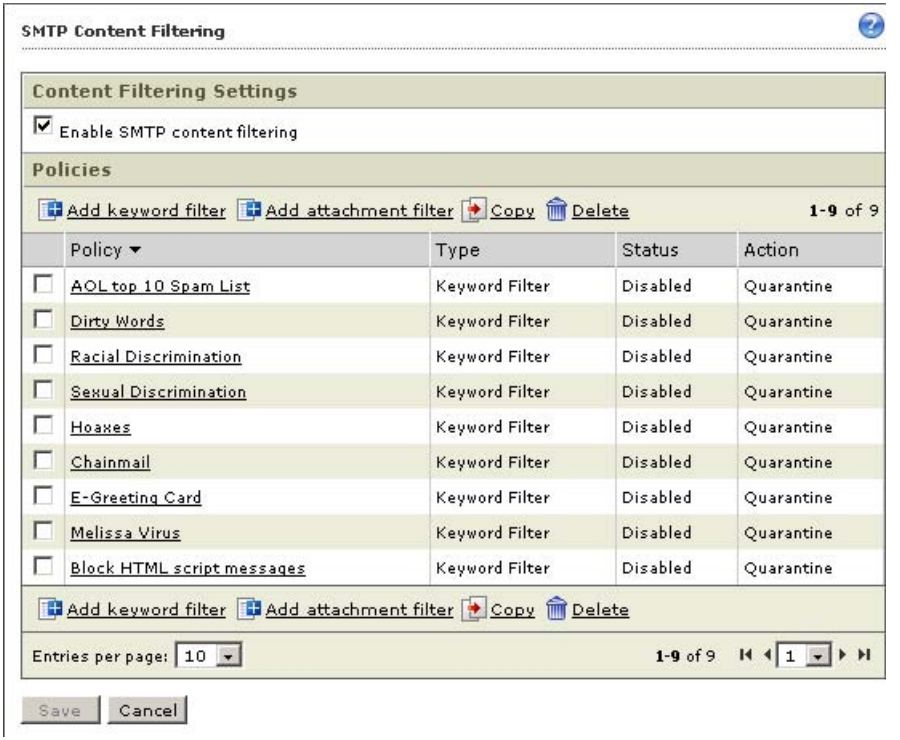


FIGURE 7-1. SMTP Content Filtering screen

Enabling SMTP Content Filtering

To enable SMTP content filtering:

1. On the left side menu, select **SMTP > Content Filtering**.The SMTP Content Filtering screen appears.
2. Under **Content Filtering Settings**, select the **Enable SMTP content filtering** check box.
3. Click **Save**.

Disabling SMTP Content Filtering

If you disable SMTP content filtering, InterScan VirusWall will not monitor the content of SMTP traffic. Any other SMTP scanning features that are enabled will continue to function as specified.

To disable SMTP content filtering:

1. On the left side menu, select **SMTP > Content Filtering**.
2. Under **Content Filtering Settings**, clear the **Enable SMTP content filtering** check box.
3. Click **Save**.

Creating Content-Filtering Policies

SMTP VirusWall uses policies that can use either a keyword filter or an attachment filter.

To create a policy:

1. On the left-side menu, click **SMTP > Content Filtering.** The SMTP Content Filtering screen appears.
2. In the Policies section, click either the Add keyword filter (see Figure 7-6, "SMTP Content Filtering Keyword Filter screen, Target tab," on page 8) or Add attachment filter hyperlink (see Figure 7-11, "SMTP Content Filtering/Attachment Filter screen, Target tab, upper half," on page 15).

The sections below discuss in detail these two different kinds of filters.

Keyword Filters

This section discusses the way in which SMTP VirusWall evaluates keyword lists and provides examples of such lists. For comprehensive guidance in setting up a keyword list using the InterScan VirusWall Web console, see *Adding a Policy Based on a Keyword Filter* on page 7-8.

Keyword filters allow the InterScan VirusWall administrator to evaluate and control the delivery of email messages based on the content of the message. These filters can monitor both inbound and outbound messages to check for sensitive or potentially offensive content. The keyword filter also provides a synonym-checking feature, by which you can extend the reach of your policies. The keyword filter supports scanning of content in double-byte characters, such as messages in Chinese or Japanese.

To access the keyword filter screen, from the SMTP Content Filtering screen, in the Policies section click the hyperlinked words, Add keyword filter. The SMTP Content Filtering Keyword Filter screen appears, displaying the Target tab.

Keyword Lists

The keyword list for a given keyword filter contains the words and phrases matched by the filter to message content. When multiple keywords appear on the same line of a policy, a match occurs only when the message being evaluated contains all of the

keywords on that line. Consider the keyword examples in figure 7-2, *Keyword filter entries, inputted in several lines*:

```
resume, position
resume, job
resume, experience
resume, enclosed
```

FIGURE 7-2. Keyword filter entries, inputted in several lines

In this example, the word *resume* appears with an additional word four times instead of using it just once as a single entry. Using just *resume* would probably produce unreliable results because *resume* can mean either curriculum vitae or to start again. To minimize the chance of such false matches, it is a good idea to qualify the primary word with additional words typically associated with it; in this example, words that are likely to appear in a job-seeking letter include *enclosed*, *position*, *job*, and *experience*. Including several keyword groups increases the reach of the filter.

As configured in the example, messages that contain any of the keyword pairs are considered a match.

Alternatively, the filter could trigger the configured action only when all five words appear in a single outbound message. To do this, include all the keywords on a single line, as shown in figure 7-3.

```
Resume, position, job, experience, enclosed
```

FIGURE 7-3. Keyword filter entries all on one line

Note: For a single-line entry, the criteria you specify are evaluated exactly as entered, including any spaces and punctuation. Phrases delimited by commas are treated as a single unit. Only when each word, space, and so on in the phrase appears in the message, *in the order entered*, will a match occur.

Obviously, the likelihood of detecting every outbound resume on the basis of this filter is much lower than that for a policy that contains several rule sets based upon the word resume, as shown in figure 7-2, *Keyword filter entries, inputted in several lines*.

Figure 7-4, “Keyword list with single keywords in multiple lines,” on page 6 shows a policy wherein the occurrence of any one of the five words in figure 7-3 triggers a match.

```
job
resume
enclosed
position
experience
```

FIGURE 7-4. Keyword list with single keywords in multiple lines

Generally speaking, keywords linked by the AND operator should not include more than four or five words or the policy risks being overly restrictive. On the other hand, if only one keyword is included on any given line (OR operator), the policy risks being too permissive—too many email messages will be found to match. Of course, as shown above, a lot depends upon what you are filtering.

One possible alternative to clarifying keywords for *resume* may be to include one entry with the correct spelling of the word, including its diacritical marks, as shown in figure 7-5:

```
job
resume
résumé
enclosed
position
experience
```

FIGURE 7-5. Keyword list for résumé, including both its common spelling and its proper spelling, with correct diacritical marks

Operators on Keyword Lists

Consider the following cases for keywords and the logical operators that apply to them based on the position of the keywords, as shown in

TABLE 7-1. Keyword list showing logical operators and sample matching results

Case	*Result*
Case 1. Keywords appear on a single line Apple Juice, [AND] Pear, [AND] Orange	Only messages containing all items, Apple Juice, Pear, and Orange (in any order, anywhere in the message text) are considered a match.
Case 2. Keywords each appear on their own individual lines Apple Juice [OR] Pear [OR] Orange	All messages containing the phrase *Apple Juice* are considered a match, all messages that contain the word Pear are considered a match, and all messages that contain the word Orange are considered a match.
Case 3. Keywords appear on a single line and synonym checking is enabled for the word Orange Apple Juice, [AND] Pear, [AND] Orange [OR] orangish [OR] red [OR] yellow* (*where the words *orangish, red,* and *yellow* are included in the synonyms list)	With synonym checking on, messages that contain the phrase *Apple Juice,* the word *Pear,* and any of the words *Orange, orangish, red,* or *yellow* are considered a match.

Other Keyword Notes

Note that *Apple Juice* is a phrase because the words *Apple* and *Juice* are not delimited by a comma; even if the words *Apple* and *Juice* both appear somewhere in the message, no match occurs unless they occur together as *Apple Juice.*

The capitalization and exact-match properties of synonyms are consistent with those defined for the keyword itself. In other words, if the word red appears in the synonyms list, it will trigger a match with the word Red if Exact Match is not checked; likewise, the word red will trigger a match with the word Red in the message text if Match Case comparison is not checked.

If a user adds multiple keywords in a single line separated by commas, the policy will be triggered only when all the keywords at that line appear in the same part of the mail. For example, if a user adds the keywords apple, pear, if apple appears in the subject of the message and pear appears in the body, the policy will not be triggered.

Adding a Policy Based on a Keyword Filter

To create a policy that uses keywords as the criteria to filter SMTP content, use the SMTP Content Filtering Keyword Filter Target tab shown in figure 7-6 to specify the policy rules.

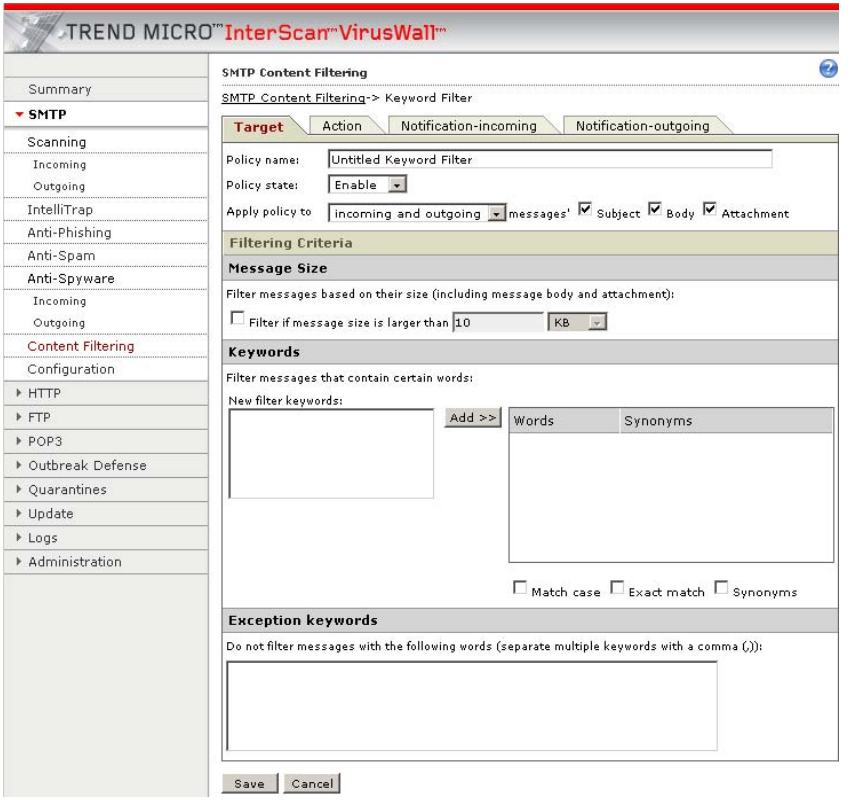


FIGURE 7-6. SMTP Content Filtering Keyword Filter screen, Target tab

To add a policy based on a keyword filter:

1. On the left-side menu, select **SMTP > Content Filtering**. The main SMTP Content Filtering screen appears.
2. Directly under the Policies section title, click the Add keyword filter hyperlink. The SMTP Content Filtering > Keyword Filter screen opens, displaying the Target tab.
3. In the **Policy name** text box, type a policy name.
4. For **Policy status**, select **Enable** to apply the policy or **Disable** if you do not want to apply it at this time.
5. In **Apply policy to**, select the type of messages (incoming, outgoing, or both) and the sections of the messages to which this policy will apply (Subject, Body, or Attachment).
6. If you want the policy to block messages whose total size (message size + attachment size) is larger than a specified size, in the Filtering Criteria/Message Size section, select **Filter if message size is larger than** and specify the size limit (choose from bytes, kilobytes, or megabytes).
7. In the Keywords section, type the keywords that you want SMTP VirusWall to scan messages for in the **New filter keywords** text box and click **Add>>** (

). The keywords move to the Words/Synonyms text box on the right.
8. If desired, select any of the **Match case**, **Exact match**, and **Synonyms** check boxes.
9. Click **Save.**

Creating or Modifying a Keyword Synonym List

The SMTP VirusWall Content Filtering feature offers the option of including synonyms for each of your keywords. After you have moved at least one keyword to the Words/Synonyms text box, you can specify synonyms for each keyword using the procedure below.

To add a list of synonyms for each keyword:

1. Follow the instructions for adding a keyword as laid out in *To add a policy based on a keyword filter:* on page 7-9.
2. Click a hyperlinked word in the **Synonyms** column (the default synonym is [none]). The Edit Synonyms screen appears showing a prepopulated list of synonyms for your selected keyword. (If you have entered multiple keywords

that you separated with commas, all the keywords will appear in the Keyword drop-down box.)

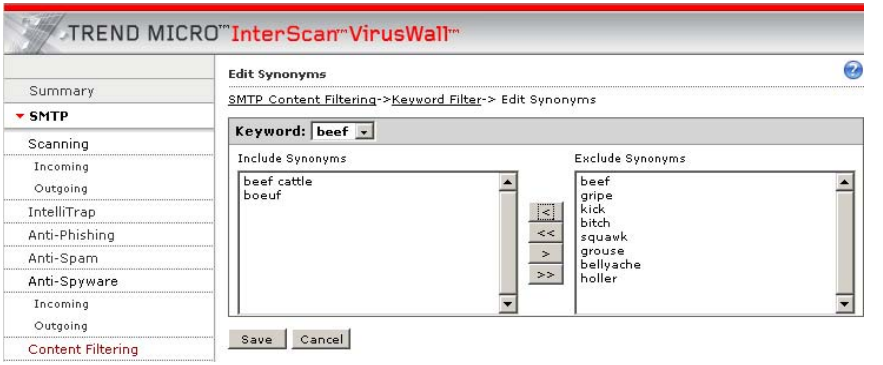


FIGURE 7-7. SMTP Content Filtering > Keyword Filter > Edit Synonyms screen

---

Note: The predefined list is not editable. You cannot modify or add to the predefined list of synonyms.

---

3. To add a synonym to the list for the keyword shown in the Keyword field, select the synonym in the Exclude Synonyms box and click the left arrow button (<). The synonym moves over to the Include Synonyms box. You can add two or more synonyms using multiple select (Ctrl-c).
4. To exclude a synonym that is already associated with your keyword, select it and click the right arrow button (>).

Tip: You can move all of the items in either box to the other box by clicking the double left arrow button (<<) or the double right arrow button (>>), respectively.

---

5. Click **Save**.

Adding Exception Keywords

Use the **Exception keywords** section to reduce the chances that SMTP VirusWall will block messages that it should pass (false positives).

To set up a keyword exception list:

1. Click SMTP > Content Filtering (Target tab) and click the Add keyword filter hyperlink. The SMTP Content Filtering > Keyword Filter screen appears displaying the Target tab.
2. Under the **Exception keywords** section, type keywords that will identify messages that you do not wish to block. The policy will allow through messages that contain these keywords even when a keyword filter matches the message.
3. Click **Save.**

Setting the Action on Messages That Match the Keyword-Filtering Policy

When an SMTP message meets the filtering criteria that you have specified, SMTP VirusWall can take one of three actions on the message, as shown in Figure 7-8.

FIGURE 7-8. SMTP Content Filtering Keyword Filter screen, Action tab

To set the action on messages that match the content filtering policy:

1. On the left side menu, select **SMTP > Content Filtering**. The SMTP Content Filtering screen appears.
2. Under **Policies**, click the Add keyword filter hyperlink. The SMTP Content Filtering screen appears, displaying the Target tab.
3. Click the **Action** tab. A message appears asking if you want to save your changes.

4. Click **OK** to close the message. The Action tab screen appears.
5. Under **Action on Messages Matching the Filtering Criteria**, select one of the following options:
   - To quarantine messages, select **Quarantine**.
   - To delete the message, select **Delete**; messages will not be delivered.
   - To deliver the message, select **Pass**. Users will receive the message.
6. Click **Save**.

Specifying Notifications to Send When a Keyword Matches a Message

You can send a notification to the administrator and the message recipients when SMTP VirusWall detects prohibited content in an incoming (Figure 7-9) or outgoing (Figure 7-10) mail message.

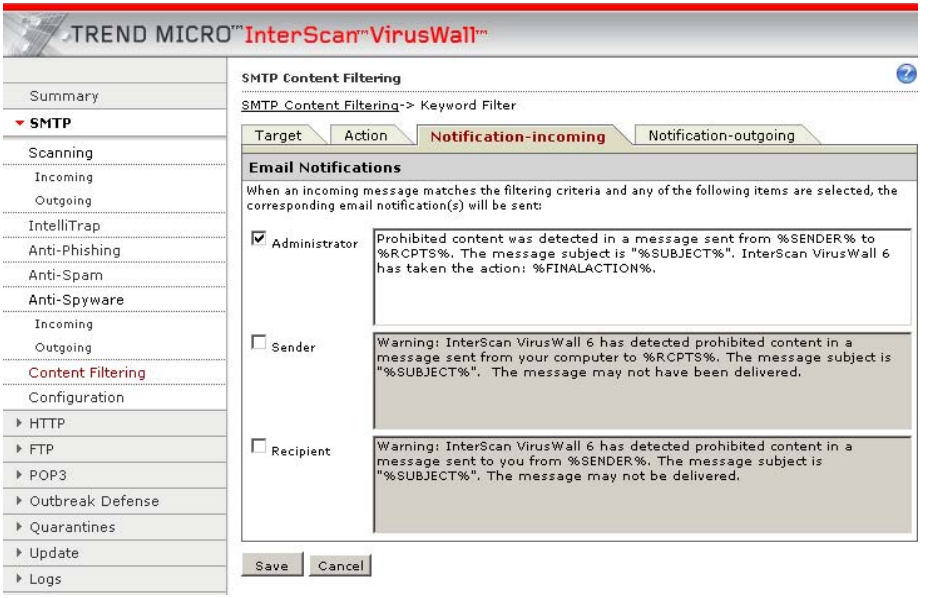


FIGURE 7-9. SMTP Content Filtering/Keyword Filter screen, Notification–incoming tab

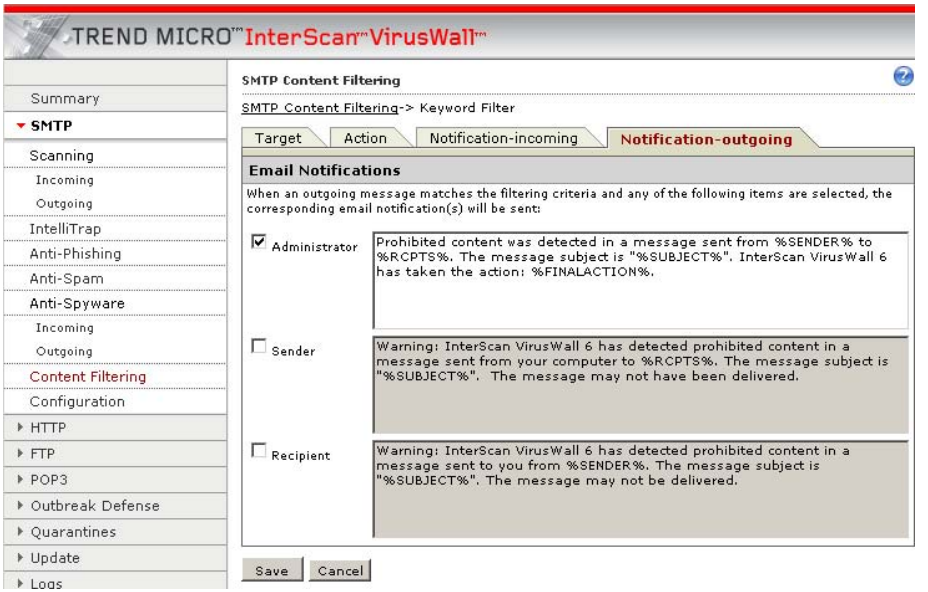


FIGURE 7-10. SMTP Content Filtering/Keyword Filter screen, Notification–outgoing tab

The steps for setting notifications for incoming and outgoing traffic are identical, however you must set notifications for incoming and outgoing traffic separately.

To specify notification settings for outgoing or incoming SMTP traffic when an email message triggers a keyword-filtering policy:

1. On the left side menu, select **SMTP > Content Filtering**.The SMTP Content Filtering screen appears.
2. Under **Policies**, click the Add keyword filter hyperlink. The SMTP Content Filtering screen appears, displaying the Target tab.
3. Click the **Notification-incoming** (or **-outgoing**) tab. The tab displays.

4. Select the recipients of the notification from the following options:
   - **Administrator**.—You or your network administrator
   - **Sender**.—The person who sent the message that contains prohibited content
   - **Recipient**.—The person who received the message that contains prohibited content
5. Modify the message to send to each recipient or accept the default messages. You can use the following tokens or tags to modify the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	always MailContentScan
%DETECTED%	name of policy that is triggered
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	host name of the InterScan VirusWall machine

6. Click **Save**.

Attachment Filters

Creating an SMTP Attachment Filter Policy for Content Filtering

To create a policy that uses attachments or message headers as the criteria to filter SMTP content, use the SMTP Content Filtering Attachment Filter Target tab shown in figure 7-11 and figure 7-12 to specify the policy rules.

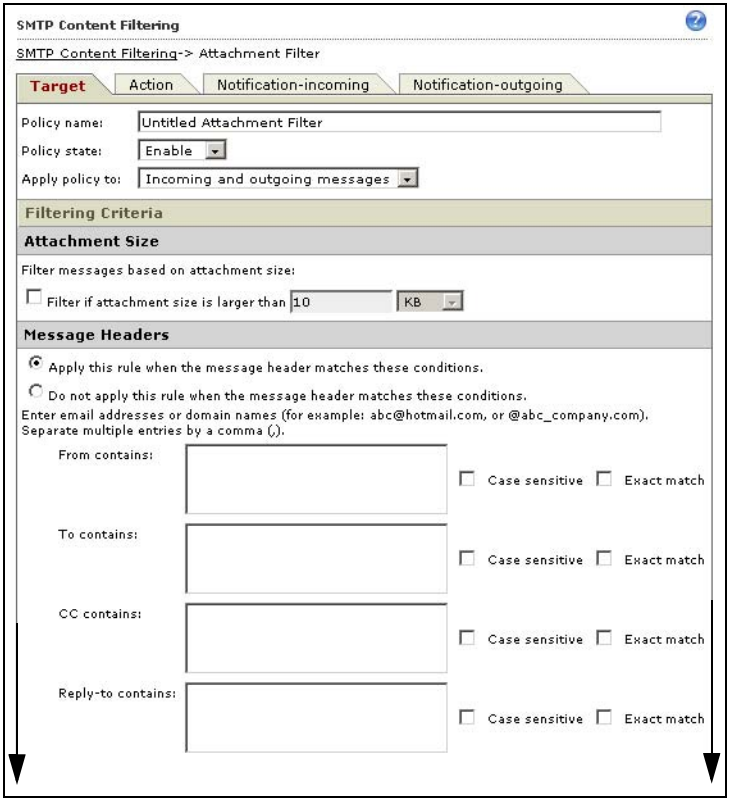


FIGURE 7-11. SMTP Content Filtering/Attachment Filter screen, Target tab, upper half

To add a policy based on filtering message headers:

1. On the left side menu, select **SMTP > Content Filtering**. The SMTP Content Filtering screen appears.
2. In the Policies section, click the Add attachment filter hyperlink. The SMTP Content/Attachment Filter screen appears, displaying the Target tab. (See figure 7-11, *SMTP Content Filtering/Attachment Filter screen, Target tab, upper half*.)
3. In the **Policy name** text box, type a policy name.
4. For **Policy state**, select **Enable** to apply the policy or **Disable** if you do not want to apply it.
5. In **Apply policy to**, select the type of messages (incoming, outgoing, or both) to which this policy applies.
6. In the Message Headers section, the primary choice that you must make is whether you want:
   - Take the specified action (Action tab) on any message that matches the filter or
   - Allow any message that matches the filter to pass through.

   To choose the first option, select **Apply this rule when the message header matches these conditions** (the default choice).

   To choose the second option, select **Do not apply this rule when the message header matches these conditions.**
7. Continuing in the Message Headers section, specify the matching conditions for message headers. Fields in the message header that you can filter are *From*, *To*, *CC*, and *Reply-to*. To select any of these fields for filtering, type entries in the message header text boxes, separating multiple entries in each box with a comma. For example: `user1@isvw.com,user2@isvw.com.`
8. For each of the four message header fields mentioned above, choose whether or not to make the match case sensitive, an exact match, or both by checking the respective check boxes.
9. Click **Save.**

You can also filter message based on the characteristics of their attachments.

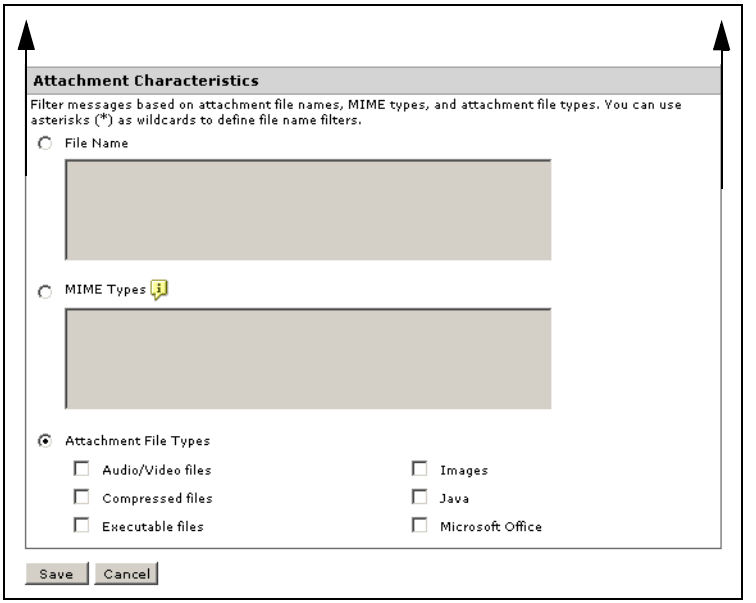


FIGURE 7-12. SMTP Content Filtering/Attachment Filter screen, Target tab, lower half

To filter messages based on the characteristics of their attachments:

1. On the left side menu, select **SMTP > Content Filtering**. The SMTP Content Filtering screen appears.
2. In the Policies section, click the Add attachment filter hyperlink. The SMTP Content/Attachment Filter screen appears, displaying the Target tab.
3. If you want the policy to block attachments of messages larger than a specified size, select **Filter if attachment size is larger than**, and specify the size limit, in bytes, kilobytes, or megabytes. (See figure 7-11, *SMTP Content Filtering/Attachment Filter screen, Target tab, upper half*.)
4. Under **Attachment Characteristics**, select the filtering criteria for message attachments. Choose from one of the three following options:

- **File Name**—specify a file name or a string using a wildcard (*). SMTP VirusWall will filter all attachments with file names that match the names or the strings.
- **MIME Types**—specify the MIME types to filter. For more information on MIME types, place your mouse cursor over the yellow tooltip icon. The following text appears:

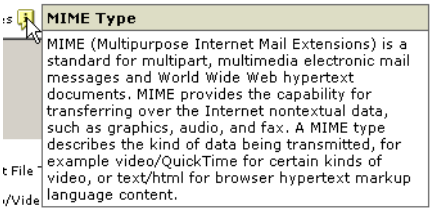


FIGURE 7-13. MIME Type tooltip mouseover text

- **Attachment File Types**—specify the file type categories to block. SMTP VirusWall will block all attachments that are in the specified categories.

Note: To specify multiple entries in the File Name and MIME Types text boxes, separate each entry with a comma; for example, ***.jpg,*.txt** or **text/plain,image/jpeg**.

---

5. Click **Save**.

Setting the Action for an SMTP Content-Filtering Policy

When an SMTP message meets the filtering criteria that you have specified, SMTP VirusWall can take one of three actions on the message, as shown in Figure 7-14.

FIGURE 7-14. SMTP Content Filtering/Attachment Filter screen, Action tab

To set the action on messages that match the policy for attachments:

1. On the left side menu, select **SMTP > Content Filtering**. The SMTP Content Filtering screen appears.
2. In the Policies section, click the Add attachment filter hyperlink. The SMTP Content/Attachment Filter screen appears, displaying the Target tab.
3. Click the **Action** tab. The Action tab displays.
4. Under **Action on Messages Matching the Filtering Criteria**, select one of the following options:
   - To quarantine messages, select **Quarantine**.
   - To deliver the message, select **Pass**. Users will receive the message.
   - To remove the attachment, select **Delete attachment and pass**. Users will receive the message without the attachment.

5. To insert a notification into the body of the message, select **Insert the following notification in the message**. You can accept the default message or modify the text of the message that you insert and use the following tokens:
   - %FILENAME%: the name of the removed attachment
   - %RULENAME%: the name of the policy
6. Click **Save**.

Specifying Notifications to Send When Filtering Criteria Match a Message Attachment

You can notify the administrator and the message recipients when prohibited content has been detected in an incoming (Figure 7-15) or outgoing (Figure 7-16) mail message attachment.

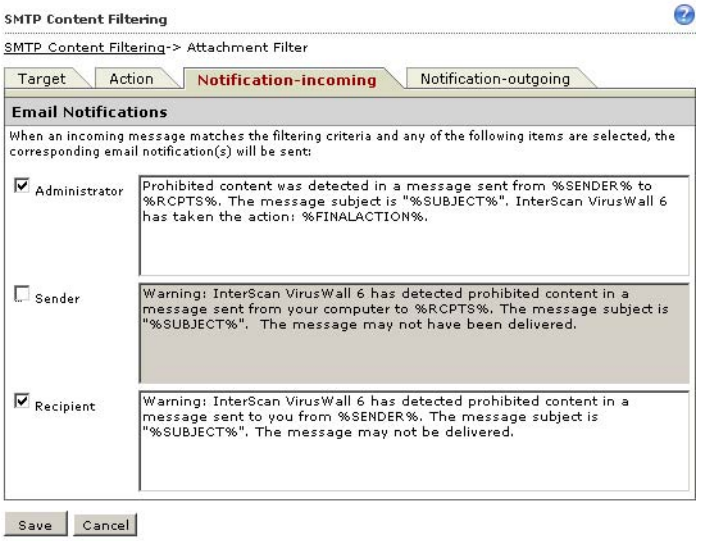


FIGURE 7-15. SMTP Content Filtering/Attachment Filter screen, Notification–incoming tab

The Notification-incoming and Notification-outgoing tabs are identical, however you must set them separately for incoming and outgoing SMTP traffic, respectively.

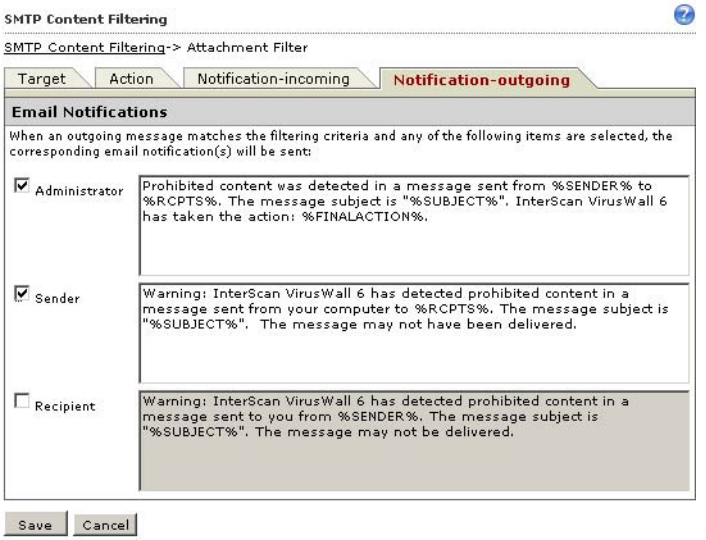


FIGURE 7-16. SMTP Content Filtering/Attachment Filter screen, Notification–outgoing tab

To specify to send when filtering criteria match a message attachment in incoming (or outgoing) SMTP traffic:

1. On the left side menu, select **SMTP > Content Filtering**. The SMTP Content Filtering screen appears.
2. In the Policies section, click the Add attachment filter hyperlink. The SMTP Content/Attachment Filter screen appears, displaying the Target tab.
3. Click the **Notification-incoming** or **Notification-outgoing** tab as appropriate.

4. Select the recipients of the notification from the following options:
   - **Administrator**.—You or your network administrator
   - **Sender**.—The person who sent the message that contains prohibited attachment.
   - **Recipient**.—The person who received the message that contains prohibited attachment.
5. Modify the message to send to each recipient or accept the default messages. You can use the following tokens or tags to modify the message:

Token	Description
%SENDER%	sender address
%RCPTS%	recipient address
%SUBJECT%	mail subject
%HEADERS%	mail headers
%DATETIME%	scan date and time
%MAILID%	mail message ID
%PROTOCOL%	mail protocol
%FILTERNAME%	always MailContentScan
%DETECTED%	name of policy that is triggered
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	host name of the InterScan VirusWall machine

6. Click **Save**.

Copying or Deleting a Content-Filtering Policy

Instead of creating several similar policies from the beginning, you can use an existing policy to create a slightly modified version. To use one policy as the basis for modifying into another, follow the procedure below.

To copy an existing SMTP content filtering policy :

1. On the left side menu, select **SMTP > Content Filtering**. The SMTP Content Filtering screen appears.
2. Under Policies, select the check box next to one or more policies and click the Copy hyperlink either in the row of icons/links above the table of polices or in the row beneath it.
3. Click **OK** on the pop-up message box to finalize changes. A copy of the policy appears as the last item in the list of policies.
4. Click the policy name of the copied policy and modify at as needed, including changing its name to something that clearly distinguishes the new policy from the policy from which it was cloned.
5. Click **Save.**

Note: If there is more than one page of policies listed, go to the last page to find your newly copied policy. Use the page navigation tools at the bottom right of the screen.

FIGURE 7-17. Policy page navigation tools at the bottom of the SMTP Content Filtering screen

To delete an SMTP content-filtering policy:

1. On the left-side menu, select **SMTP > Content Filtering**. The SMTP Content Filtering screen appears.
2. Under Policies, select the check box next to one or more policies and click the Delete hyperlink either in the row of icons/links above the table of polices or in the row beneath it.
3. Click **OK** on the pop-up message box to finalize changes. The SMTP Content Filtering screen refreshes, displaying a list of policies that does not include the deleted policy or policies.

Index

D

E

F

T

U

V