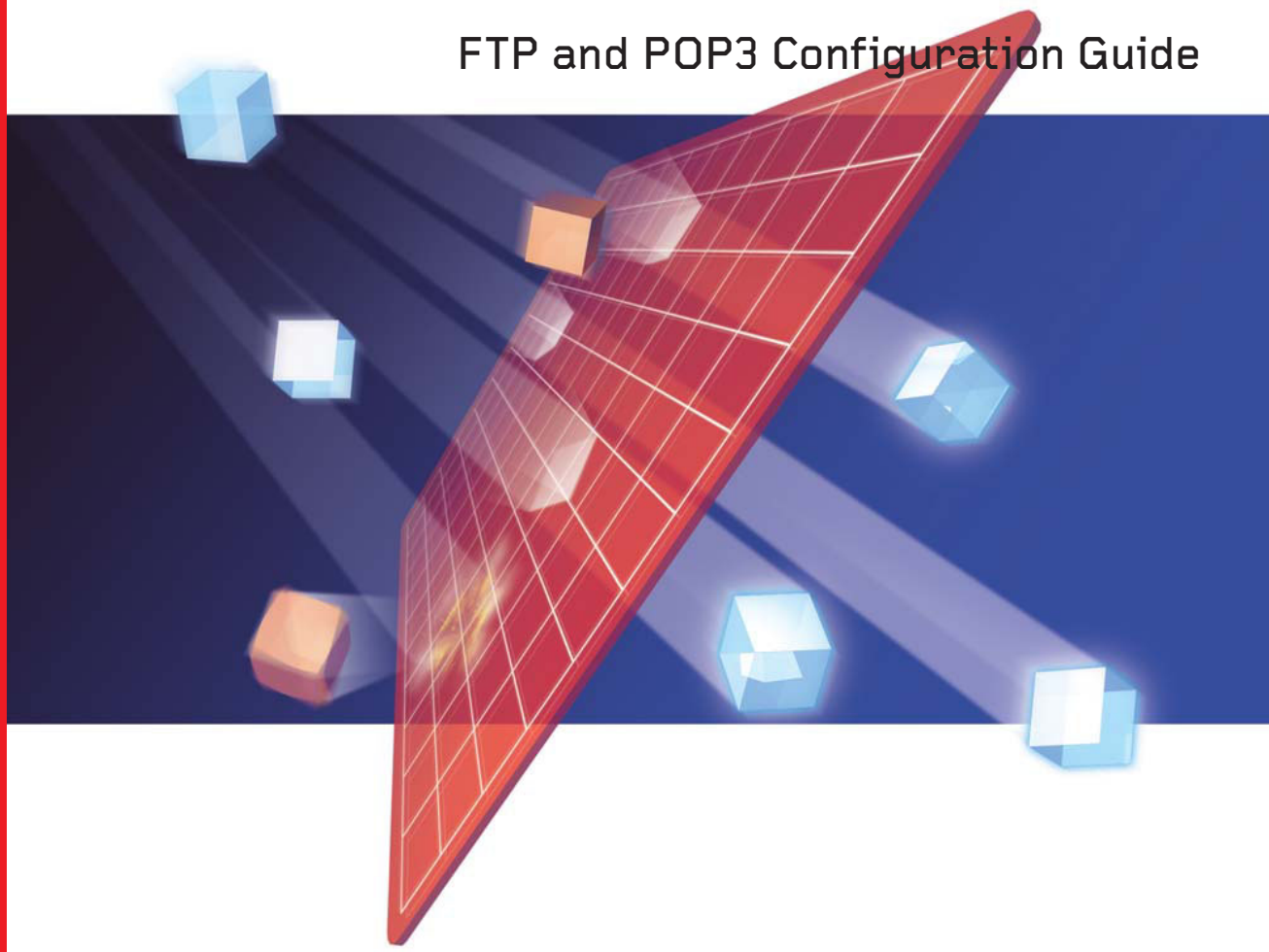
TREND MICRO™

InterScan™ VirusWall™ 6

Integrated virus and spam protection for your Internet gateway

for Linux™

FTP and POP3 Configuration Guide



TREND MICRO™

Before installing and using the software, please review the readme files, release notes and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

http://www.trendmicro.com/download

Document Part No. IVEM62664/60224
Release Date: July 2006
Protected by U.S. Patent Nos. 5,623,600; 5,889,943; 5,951,698 and 6,119,165

The FTP and POP3 Configuration Guide for Trend Micro™ InterScan VirusWall™ is intended to familiarize users with the FTP and POP3 configuration settings and tasks. You should read through it prior to using the software.

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

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any 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 10: Configuring POP3 Content Filtering Settings

List of Figures

Chapter 1

Preparing InterScan VirusWall to Protect FTP Traffic

InterScan VirusWall allows you to monitor FTP traffic to safeguard security at your network gateway. You can enable or disable scanning of FTP traffic during the installation process or at any time thereafter through the Summary page of the InterScan VirusWall Web console.

Available FTP services include:

- Scanning for viruses/malware in uploads and downloads
- Spyware/Grayware detection
- Configuration of the FTP server mode and listening port

The **File Transfer (FTP)** tab on the InterScan VirusWall Summary screen provides statistics concerning the number of security risks that InterScan VirusWall FTP scanning has detected in incoming and outgoing file traffic.

Enabling or Disabling FTP Scanning

To enable or disable scanning of FTP file downloads and uploads, on the **File Transfer (FTP)** tab on the Summary page, select or clear the **Enable FTP traffic** check box.

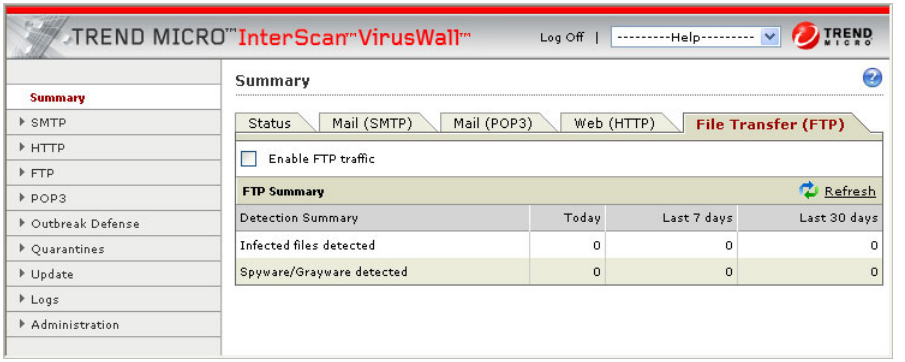


FIGURE 1-1. Summary Screen, File Transfer (FTP) tab

Configuring FTP Server Settings

Before InterScan VirusWall can monitor FTP traffic, you need to configure FTP server settings on the FTP Configuration screen. You can access this screen by selecting **FTP** > **Configuration**. The default values of fields on this screen are already specified.

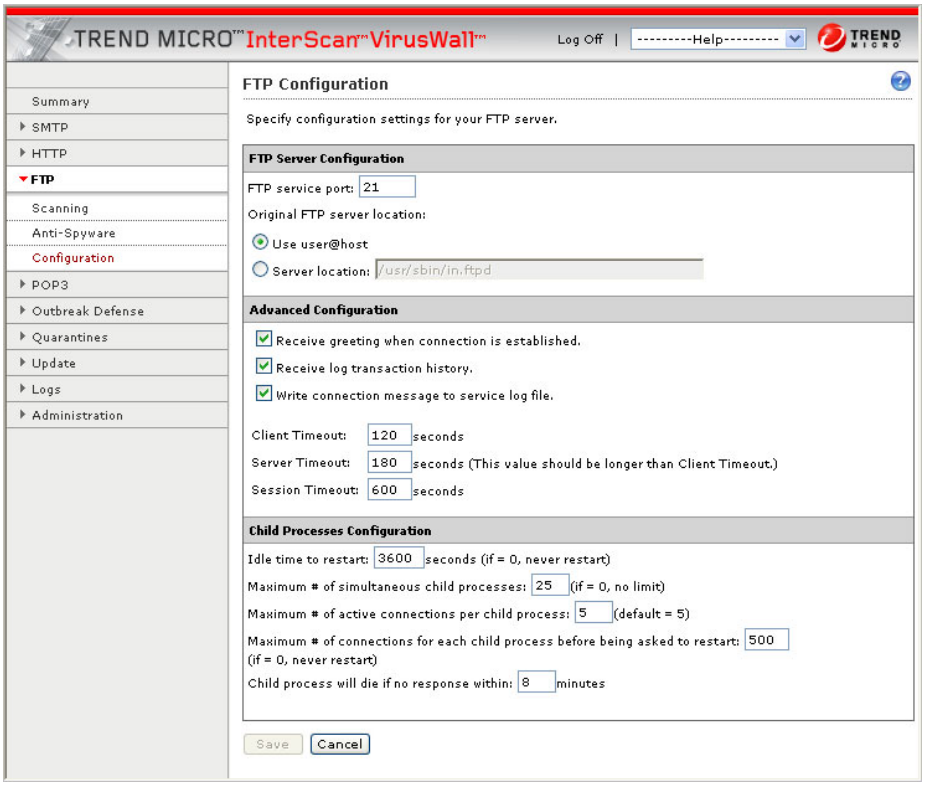


FIGURE 1-2. FTP Configuration screen

To configure FTP server settings:

1. In **FTP service port**, type the listening port for FTP traffic. Make sure the port number is not used by other programs.
2. In **Original FTP server location**, select from two options:
   - **Use user@host**: Select this option if FTP VirusWall will act as a proxy server between the requesting client and the remote site.
   - **Server location**: Select this option if FTP VirusWall will act as a sentry standing guard in front of a specific server within the LAN.

     If you choose this option and the FTP server and FTP VirusWall are on the same machine, type the absolute path of the FTP server in the field; for example, /usr/sbin/in.FTPd.

     If on different machines, type the IP address and port of the original FTP server; for example, 10.0.0.1 21.

   Note: Refer to the online help for more information about the options in the **Server location** field.
3. Select the settings you want to apply when FTP connection is established. You have the option to:
   - Receive a greeting when FTP connection is established.
   - Log your FTP connections.
   - Write the connection message to a service log file.
4. Specify connection timeouts for the FTP client and server, and the FTP session.
5. Specify settings for child processes.
6. Click **Save**.

Chapter 2

Preparing InterScan VirusWall to Protect POP3 Traffic

InterScan VirusWall allows you to monitor incoming POP3 mail traffic. You can enable or disable scanning of POP3 traffic during the installation process or at any time thereafter through the Summary page of the InterScan VirusWall Web console.

Available POP3 services include:

- Scanning for viruses/malware
- Scanning of compressed executable files that could contain potentially malicious code using IntelliTrap
- Phishing site detection
- Spam detection with configurable spam categories and content levels
- Spyware/Grayware detection
- Content filtering
- Size filtering of messages and attachments
- Configuration of the POP3 server port and delivery options for incoming mail

The **Mail (POP3)** tab on the InterScan VirusWall Summary screen provides statistics concerning the number of security risks, spam messages, and phishing messages that InterScan VirusWall POP3 scanning has detected in incoming email communication.

Enabling or Disabling POP3 Services

To enable or disable scanning of POP3 mail traffic, on the **Mail (POP3)** tab on the Summary page, select or clear the **Enable POP3 Traffic** check box.

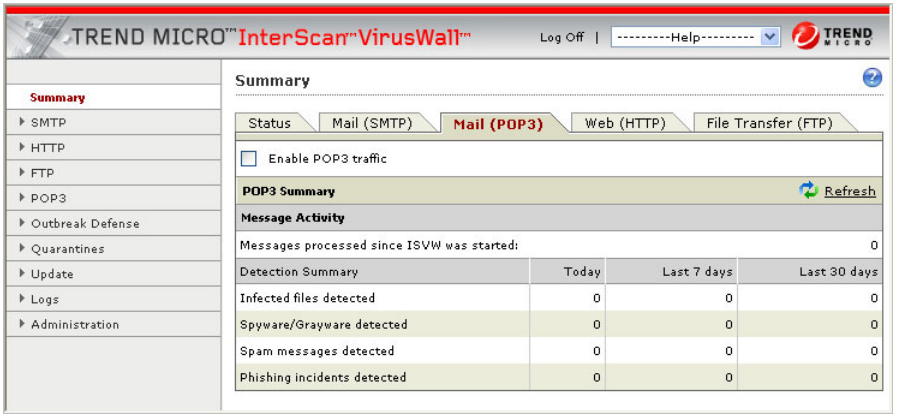


FIGURE 2-1. Summary screen, Mail (POP3) tab

Configuring POP3 Settings

Before InterScan VirusWall can monitor incoming POP3 mail traffic, you need to configure settings on the POP3 Configuration screen. You can access this screen by selecting **POP3 > Configuration**. The default values for some of the fields on this screen are already specified.

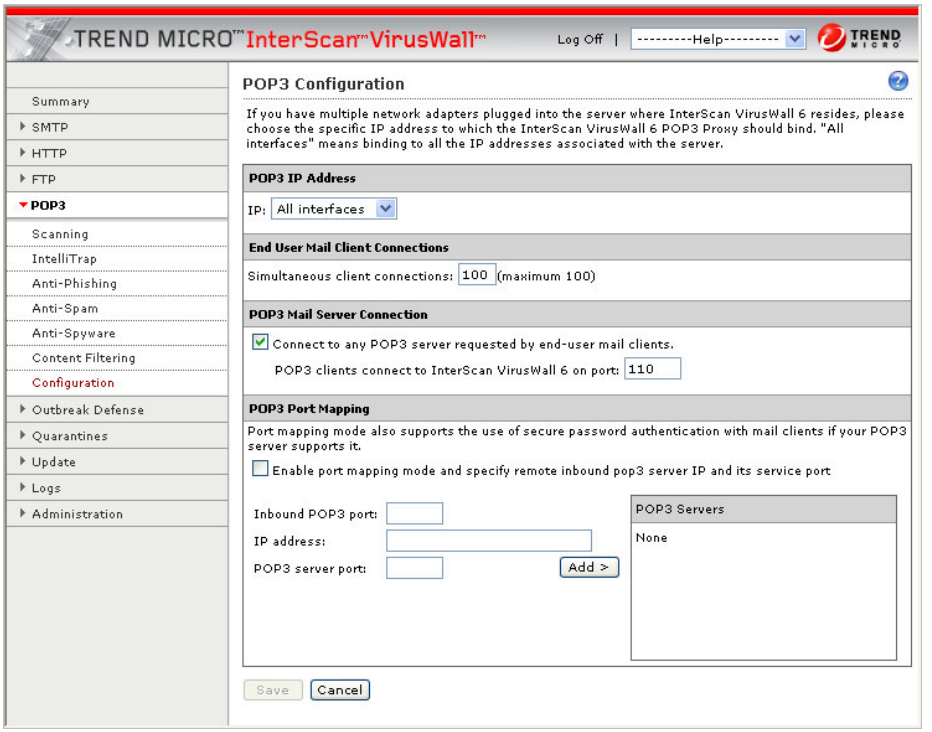


FIGURE 2-2. POP3 Configuration Screen

This screen also allows you to enable port mapping mode. In port mapping mode, InterScan VirusWall acts as a port mapping server, listening for POP3 client connections, then searching for the actual POP3 server address and port number in the port mapping list, before finally connecting the client to the actual server. In the

POP3 settings on the client machines, incoming mail server name and port should be the InterScan VirusWall server name and port number.

To configure POP3 settings:

1. From the **IP** drop-down list, select the IP address where the InterScan VirusWall POP3 service will bind and listen.
   - **All interfaces**: Sets the POP3 service to listen on all IP addresses assigned to the machine where InterScan VirusWall is installed.
   - **127.0.0.1**: Configures the service to listen on the local host, leaving it inaccessible to other machines.
   - **{Specific IP address}**: Other machines will access the POP3 service through this IP address.
2. Specify the maximum number of simultaneous client connections allowed.
3. Specify the following settings for POP3 mail server connections:
   - If InterScan VirusWall will connect to any POP3 server requested by clients.
   - The port number clients will use to connect to InterScan VirusWall.

4. Specify port mapping mode settings.

   a. Select the check box for enabling port mapping mode.

   b. Add tuples by specifying the following information for each tuple to add:

   - **Inbound POP3 port**: The port on which the InterScan VirusWall POP3 service listens. This port number should not be used by other programs, and cannot be the same as the proxy server's port number.
   - **IP address**: The IP address of the specific POP3 server, which can either be its domain name or its numeric IP address.
   - **POP3 server port**

   c. Click **Add** to add each tuple to the list on the right. To delete a specific tuple, click the trash bin icon.

5. Click **Save**.

Note: Do not allow other programs to use the IP addresses and the ports that you specify because the InterScan VirusWall POP3 service will fail to bind to and listen on those ports if the ports are being used.

Chapter 3

Configuring FTP Virus/Malware Scan Settings

InterScan VirusWall scans FTP uploads and downloads for virus/malware. By default, InterScan VirusWall will scan all scannable and compressed files, clean files with detected virus/malware (if cleanable), and then send users and the administrator predefined notification messages about the virus/malware detection.

FTP virus/malware scanning is highly configurable. The following are procedures for configuring scanning settings:

Enabling FTP Virus/Malware Scanning

To enable FTP virus/malware scanning:

1. On the main menu, select **FTP > Scanning**. The **Target** tab displays.

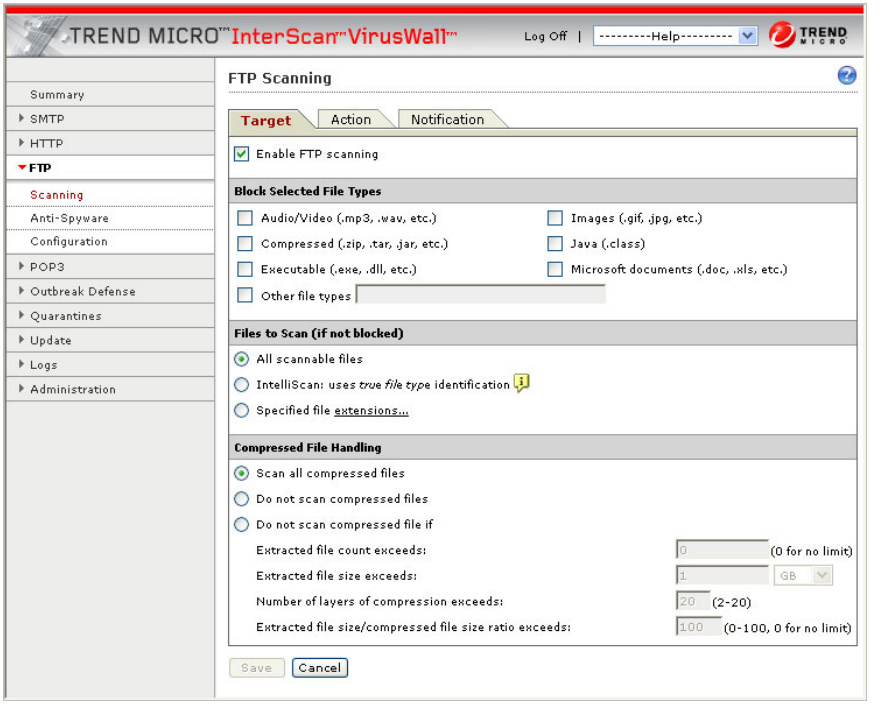


FIGURE 3-1. FTP Scanning screen, Target tab

2. Select the **Enable FTP scanning** check box.
3. Click **Save**.

Specifying File Types to Block

To specify file types to block:

1. On the main menu, select **FTP > Scanning**. The **Target** tab displays.
2. Under **Block Selected File Types,** select one or more file types from the predefined lists.
3. To block a file type not included in the list, select the **Other file types** check box and type the file type extension in the **Other file types** field.
4. Click **Save**.

Specifying File Types to Scan

To specify file types to scan:

1. On the main menu, select **FTP > Scanning**. The **Target** tab displays.
2. Under **Files to Scan (if not blocked)**, select from the following options:
   - **All scannable files**: Scans all files regardless of file type. This is the most secure setting.
   - **IntelliScan: uses "true file type" identification**: Allows the product to intelligently identify the files to scan.

     Note: This option will pass some file types, which will result in higher performance, but will be less secure than when scanning all files.

   - **Specified file extensions**: Scans only certain file extensions.

     To find out which file extensions will be scanned by default, or to enter additional file extensions you want scanned, click the **extensions...** link. In the new window that opens, enter additional file extensions under **Additional Extensions**, and then click **OK**.
3. Click **Save**.

Handling Compressed Files

To specify how InterScan VirusWall will handle compressed files:

1. On the main menu, select **FTP > Scanning**. The **Target** tab displays.
2. Under **Compressed File Handling**, select from the following options:
   - **Scan all compressed files**: The most secure configuration.
   - **Do not scan compressed files**: Skips scanning of all compressed files.
   - **Do not scan compressed files if**: Skips scanning of compressed files when user-specified limits are exceeded. Scanning will proceed if the limits are not exceeded.
     - **Extracted file count exceeds**: The maximum number of files within the compressed file (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. For example, if a ZIP file contains a RAR file, and that file contains another compressed file, the number of compression layers is three.
     - **Extracted file size/compressed file size ratio exceeds**: The maximum size ratio before and after compression.
3. Click **Save**.

Specifying the Action to Take When Virus/Malware Is Detected

To specify the action to take when virus/malware is detected:

1. On the main menu, select **FTP > Scanning**, and then click the **Action** tab.

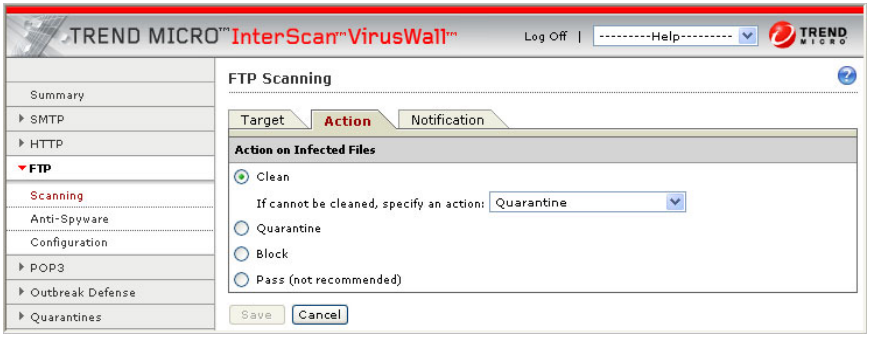


FIGURE 3-2. FTP Scanning screen, Action tab

2. Under **Action on Infected Files**, select from the following options:
   - **Clean**: A file with virus/malware will first be cleaned before delivering it to the recipient. If the file is uncleanable, select from the following actions:
     - **Quarantine**: Removes and quarantines infected files.
     - **Block**: Removes infected files without quarantining them.
     - **Pass (not recommended)**: Delivers the infected file.
   - **Quarantine**: Moves, without cleaning, the infected file to the quarantine directory. The recipient will not receive the infected file.
   - **Block**: Deletes the infected file. The recipient will not receive the infected file.
   - **Pass (not recommended)**: Delivers the infected file to the recipient.
3. Click **Save**.

Note: The default quarantine folder for FTP scanning is quarantine/ftp.

Configuring Notification Settings

To configure notification settings:

1. On the main menu, select **FTP > Scanning**, and then click the **Notification** tab.

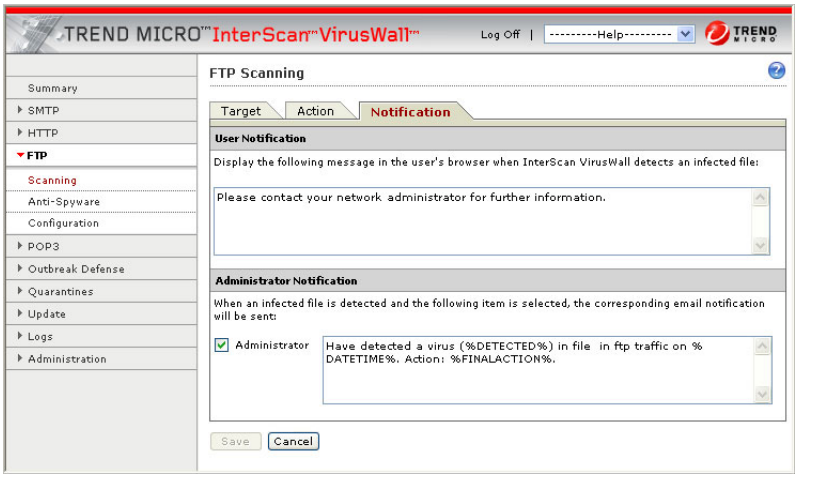


FIGURE 3-3. FTP Scanning screen, Notification tab

2. Under **User Notification**, modify the user notification message as desired.
3. To send notifications to the administrator, select **Administrator**, and then modify the message as desired. The following tokens are supported in administrator notification for FTP scanning:

Token	Description
%DATETIME%	scan date and time
%PROTOCOL%	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**.

Chapter 4

Configuring FTP Anti-Spyware/Grayware Settings

Spyware/Grayware comes in many forms and often appears to be a legitimate software program.

By default, InterScan VirusWall will scan for all the types of spyware/grayware listed in Table 4-1, block file transfer upon spyware/grayware detection, and then send users predefined notification messages about the spyware/grayware detection.

FTP spyware/grayware scanning is highly configurable. The following are procedures for configuring scanning settings:

TABLE 4-1. Types of Spyware/Grayware

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 FTP Spyware/Grayware Scanning

To enable FTP spyware/grayware scanning:

1. On the main menu, select **FTP > Anti-Spyware**. The **Target** tab displays.

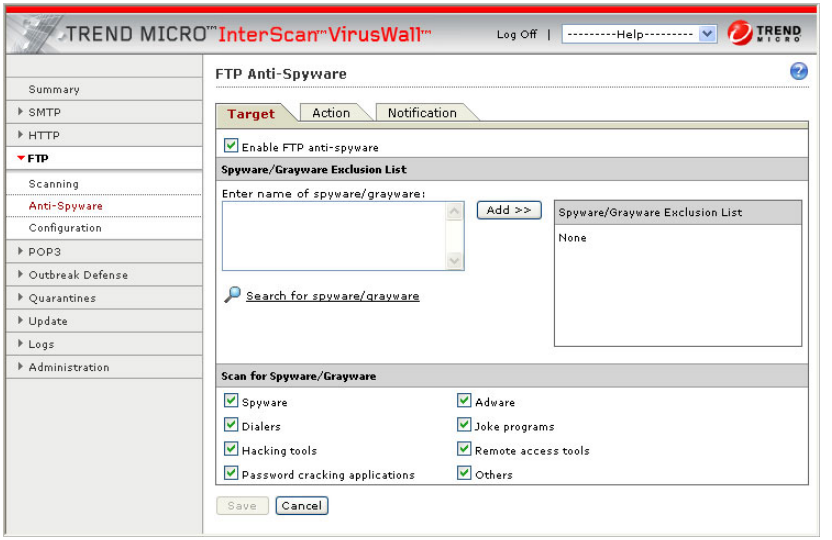


FIGURE 4-1. FTP Anti-Spyware screen, Target tab

2. Select the **Enable FTP anti-spyware** check box.
3. Click **Save**.

Setting the Spyware/Grayware Scanning Exclusion List

To set the spyware/grayware scanning exclusion list:

1. On the main menu, select **FTP** > **Anti-Spyware**. The **Target** tab displays.
2. In **Enter name of spyware/grayware**, type the file names or the file extensions to exclude from spyware/grayware scanning. For extension names, use the asterisk (*) as a wildcard character. For example, to exclude .bmp files, type *.bmp.
3. Click **Add**, and then click **Save**.

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

Specifying Spyware/Grayware Types to Scan

To specify the types of spyware/grayware to scan:

1. On the main menu, select **FTP** > **Anti-Spyware**. The **Target** tab displays.
2. Under **Scan for Spyware/Grayware**, select the types of spyware/grayware InterScan VirusWall will scan.
3. Click **Save**.

Specifying the Action to Take When Spyware/Grayware Is Detected

To specify the action to take when spyware/grayware is detected:

1. On the main menu, select **FTP** > **Anti-Spyware**, and then click the **Action** tab.

FIGURE 4-2. FTP Anti-Spyware screen, Action tab

2. Under **Action on Spyware/Grayware**, select from the following options:
   - **Quarantine**: Moves the file with spyware/grayware to the quarantine directory. The recipient will not receive the file.
   - **Block**: Prevents the file transfer of spyware/grayware programs. The recipient will not receive the file.
   - **Allow download (not recommended)**: Delivers the file to the recipient.
3. Click **Save**.

Note: The default quarantine folder for FTP scanning is quarantine/ftp.

Configuring Notification Settings

To configure notification settings:

1. On the main menu, select **FTP > Anti-Spyware**, and then click the **Notification** tab.

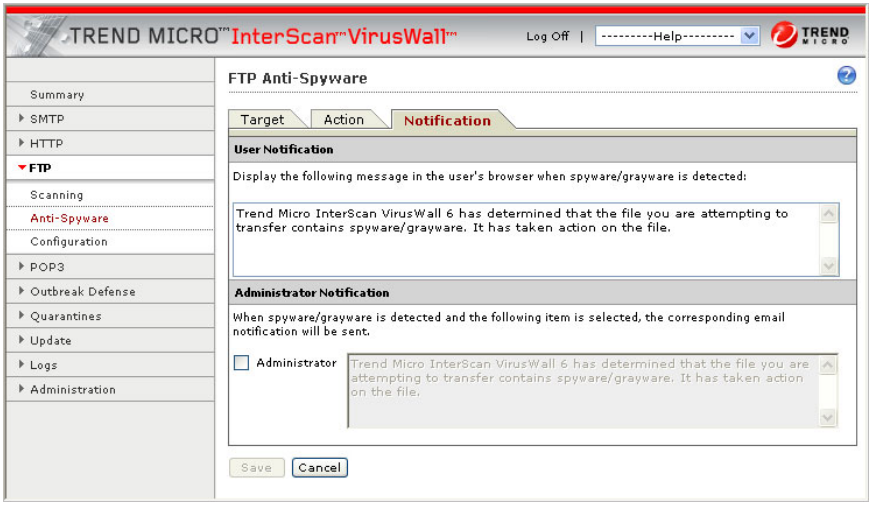


FIGURE 4-3. FTP Anti-Spyware screen, Notification tab

2. Under **User Notification**, modify the user notification message as desired.
3. To send notifications to the administrator, select **Administrator**, and then modify the message as desired.
4. Click **Save**.

Chapter 5

Configuring POP3 Virus/Malware Scan Settings

InterScan VirusWall scans POP3 mail for virus/malware. By default, InterScan VirusWall will scan all scannable and compressed files, clean infected items (if cleanable), and then send the administrator a predefined notification message about the virus/malware detection.

Note: Infected items could be the email's message body or the files attached to the email.

POP3 virus/malware scanning is highly configurable. The following are procedures for configuring scanning settings:

Enabling POP3 Virus/Malware Scanning

To enable POP3 virus/malware scanning:

1. On the main menu, select **POP3 > Scanning**. The **Target** tab displays.

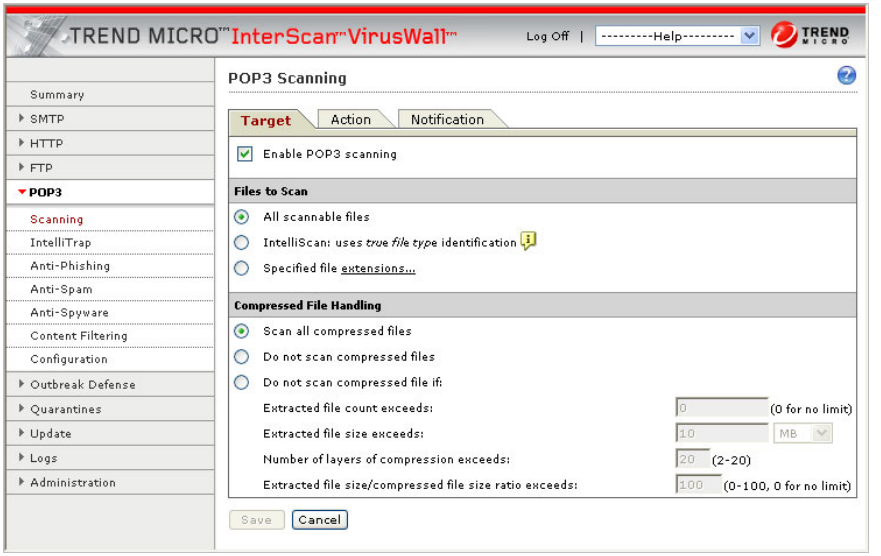


FIGURE 5-1. POP3 Scanning screen, Target tab

2. Select the **Enable POP3 scanning** check box.
3. Click **Save**.

Specifying File Types to Scan

To specify file types to scan:

1. On the main menu, select **POP3 > Scanning**. The **Target** tab displays.
2. Under **Files to Scan**, select from the following options:
   - **All scannable files**: Scans all files regardless of file type. This is the most secure setting.
   - **IntelliScan: uses "true file type" identification**: Allows the product to intelligently identify the files to scan.

     Note: This option will pass some file types, which will result in higher performance, but will be less secure than when scanning all files.

   - **Specified file extensions**: Scans only certain file extensions.

     To find out which file extensions will be scanned by default, or to enter additional file extensions you want scanned, click the **extensions...** link. In the new window that opens, enter additional file extensions under **Additional Extensions**, and then click **OK**.
3. Click **Save**.

Handling Compressed Files

To specify how InterScan VirusWall will handle compressed files:

1. On the main menu, select **POP3 > Scanning**. The **Target** tab displays.
2. Under **Compressed File Handling**, select from the following options:
   - **Scan all compressed files**: The most secure configuration.
   - **Do not scan compressed files**: Skips scanning of all compressed files.
   - **Do not scan compressed files if**: Skips scanning of compressed files when user-specified limits are exceeded. Scanning will proceed if the limits are not exceeded.
     - **Extracted file count exceeds**: The maximum number of files within the compressed file (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. For example, if a ZIP file contains a RAR file, and that file contains another compressed file, the number of compression layers is three.
     - **Extracted file size/compressed file size ratio exceeds**: The maximum size ratio before and after compression.
3. Click **Save**.

Specifying the Action to Take When Virus/Malware Is Detected

To specify the action to take when virus/malware is detected:

1. On the main menu, select **POP3** > **Scanning**, and then click the **Action** tab.

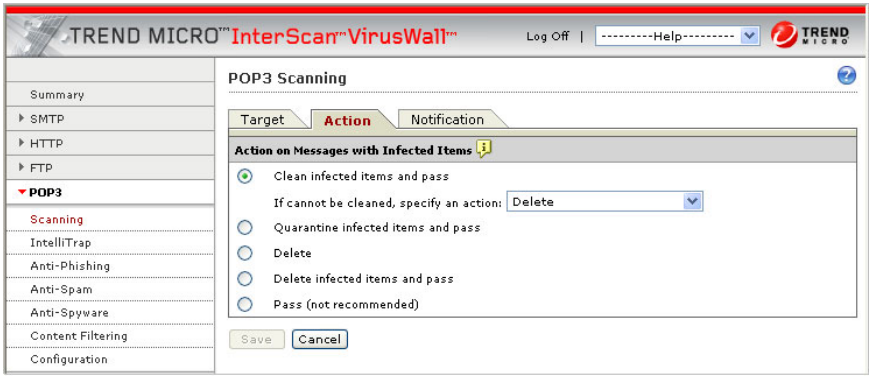


FIGURE 5-2. POP3 Scanning screen, Action tab

2. Under **Action on Messages with Infected Items**, select from the following options:

   - **Clean infected items and pass**: Cleans infected items before delivering the email to the recipient. If the infected item is uncleanable, select from the following actions:
     - **Quarantine**: Removes and quarantines infected items.
     - **Delete**: Removes infected items without quarantining them.
     - **Pass (not recommended)**: Delivers the email with the infected items.
   - **Quarantine infected items and pass**: Automatically moves the infected items to the quarantine directory, then sends the email.

Note: The default quarantine folder for POP3 scanning is quarantine/POP3.

- **Delete**: Automatically deletes the email with infected items.
- **Delete infected items and pass**: Deletes infected items before delivering the email to the recipient.
- **Pass (not recommended)**: Delivers the email with infected items.

3. Click **Save**.

Configuring Notification Settings

To configure notification settings:

1. On the main menu, select **POP3 > Scanning**, and then click the **Notification** tab.

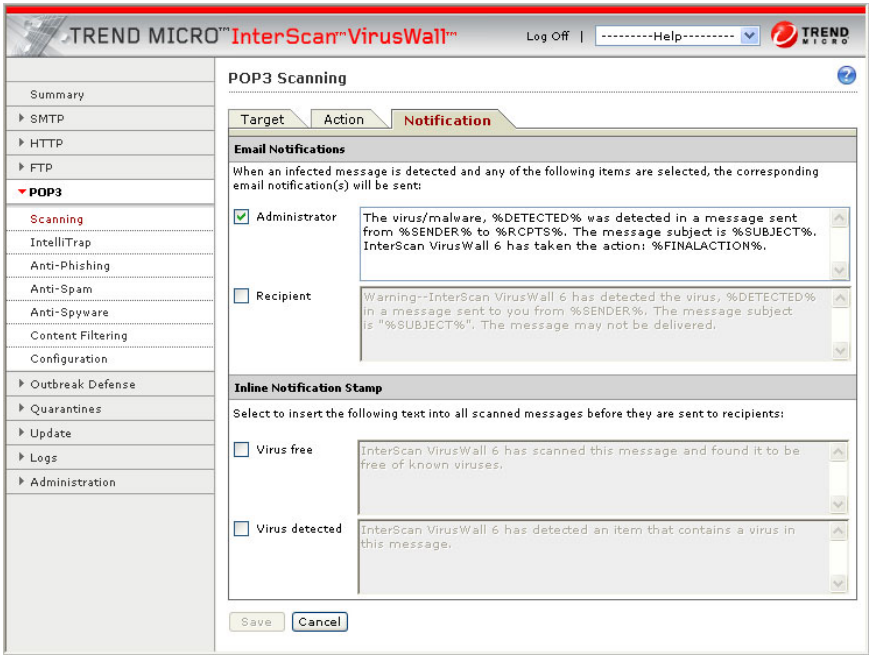


FIGURE 5-3. POP3 Scanning screen, Notification tab

2. Under **Email Notifications**, modify the administrator notification message as desired. You can unselect the **Administrator** check box if you do not want to send the notification.

3. To send email notifications to recipients, select the **Recipient** check box, and modify the message as desired.
   The following tokens are supported in both administrator and recipient notifications for POP3 scanning:

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 on the message
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the InterScan VirusWall machine

4. If you want InterScan VirusWall to insert inline notifications into the message body of an incoming email message, do the following:
   - Select **Virus free** to add inline notifications to emails not infected with virus/malware, then modify the inline notification as desired.
   - Select **Virus detected** to add inline notifications to emails with infected items, then modify the inline notification as desired.

You can use the following tokens when modifying the inline notification:

Token	Description
%VIRUSNAME%	name of the virus/malware 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

5. Click **Save**.

Chapter 6

Configuring POP3 IntelliTrap Settings

IntelliTrap detects in real-time potentially malicious code in compressed executable files that arrive as email attachments. By default, IntelliTrap will quarantine infected attachments, send the email to the recipient, and then send the administrator a predefined notification message about the threat detected.

IntelliTrap scanning is highly configurable. The following are procedures for configuring scanning settings:

Enabling POP3 IntelliTrap Scanning

To enable POP3 IntelliTrap scanning:

1. On the main menu, select **POP3 > IntelliTrap**. The **Target** tab displays.

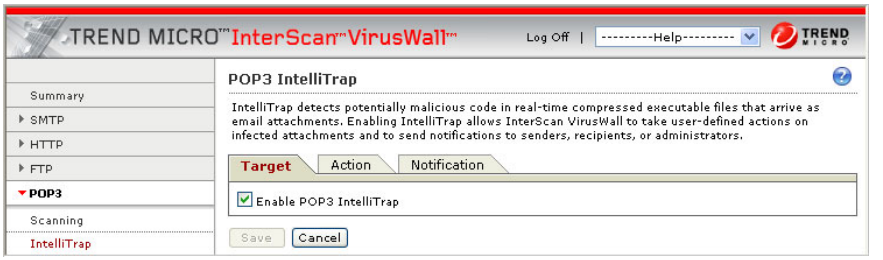


FIGURE 6-1. POP3 IntelliTrap screen, Target tab

2. Select the **Enable POP3 IntelliTrap** check box.
3. Click **Save**.

Specifying the Action to Take When Potentially Malicious Code Is Detected

To specify the action to take when potentially malicious code is detected:

1. On the main menu, select **POP3 > IntelliTrap**, and then click the **Action** tab.

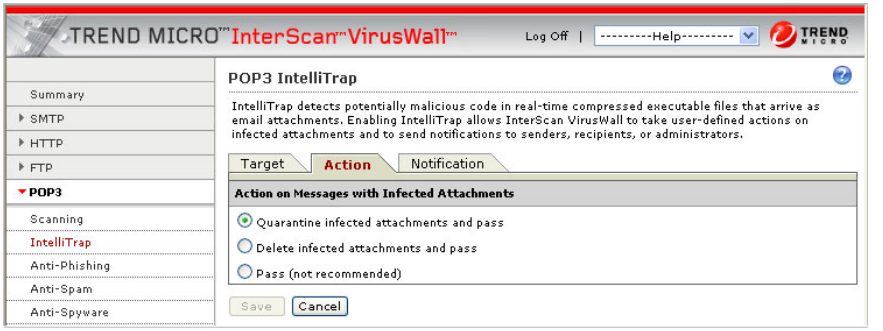


FIGURE 6-2. POP3 IntelliTrap screen, Action tab

2. Under **Action on Messages with Infected Attachments**, select from the following options:
   - **Quarantine infected attachments and pass**: Moves attachments to the quarantine folder and then delivers the email without the attachments.

     Note: The default quarantine folder for POP3 scanning is quarantine/POP3.

   - **Delete infected attachments and pass**: Permanently deletes attachments and then delivers the email.
   - **Pass (not recommended)**: Delivers the email with the infected attachments and an inline warning.
3. Click **Save**.

Configuring Notification Settings

To configure notification settings:

1. On the main menu, select **POP3 > IntelliTrap**, and then click the **Notification** tab.

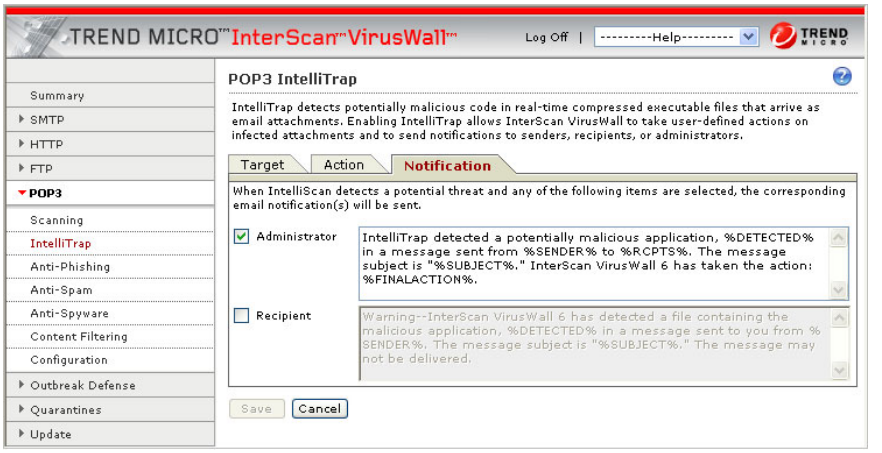


FIGURE 6-3. POP3 IntelliTrap screen, Notification tab

2. Modify the administrator notification message as desired. You can unselect the **Administrator** check box if you do not want to send the notification.
3. To send email notifications to recipients, select the **Recipient** check box, and modify the message as desired.
   Use any of the following tokens or tags on 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%	name of the filter that performs the action
%DETECTED%	name of the security risk found
%FINALACTION%	action taken on the message
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the InterScan VirusWall machine

4. Click **Save.**

Chapter 7

Configuring POP3 Anti-Phishing Settings

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 a legitimate established organization. The messages typically encourage recipients to click 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 the account will be closed. The email will include a URL to a Web site that looks exactly like the real thing (it is relatively simple to copy a legitimate email and a legitimate Web site but then change the back end—where the collected data is actually sent).

By default, InterScan VirusWall will quarantine phishing messages, and then send the administrator a predefined notification message about the phishing message.

IntelliTrap scanning is highly configurable. The following are procedures for configuring anti-phishing settings:

- *Specifying the Action to Take When a Phishing Message Is Detected* on page 7-3
- *Configuring Notification Settings* on page 7-4

Enabling POP3 Anti-Phishing

To enable POP3 anti-phishing:

1. On the main menu, select **POP3 > Anti-phishing**. The **Target** tab displays.

FIGURE 7-1. POP3 Anti-Phishing screen, Target tab

2. Select the **Enable POP3 anti-phishing** check box.
3. Click **Save**.

Specifying the Action to Take When a Phishing Message Is Detected

To specify the action to take when a phishing message is detected:

1. On the main menu, select **POP3** > **Anti-Phishing**, and then click the **Action** tab.

FIGURE 7-2. POP3 Anti-Phishing screen, Action tab

2. Under **Action on Messages with Phishing Sites**, select from the following options:
   - **Quarantine**: Moves the message to the quarantine folder.
   - **Delete**: Automatically deletes the message without delivering it.
   - **Pass (not recommended)**: Delivers the phishing message.
3. Click **Save**.

Configuring Notification Settings

To configure notification settings:

1. On the main menu, select **POP3 > Anti-phishing**, and then click the **Notification** tab.

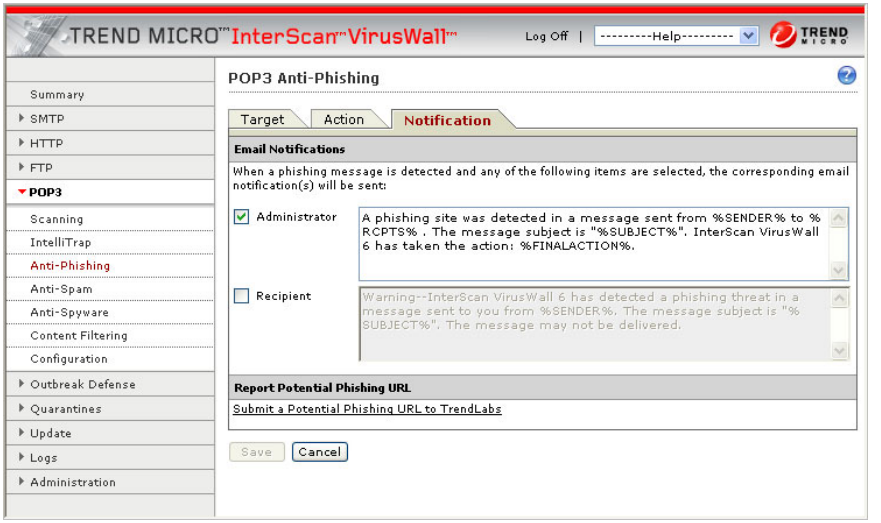


FIGURE 7-3. POP3 Anti-Phishing screen, Notification tab

2. Modify the administrator notification message as desired. You can unselect the **Administrator** check box if you do not want to send the notification.

3. To send email notifications to recipients, select the **Recipient** check box, and modify the message as desired.

   Use any of the following tokens or tags on 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%	name of the filter that performs the action
%DETECTED%	name of the security risk found
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the InterScan VirusWall machine

4. To report suspected or known phishing sites to TrendLabs, click **Submit a Potential Phishing URL to TrendLabs** and provide the URL in an email that you will send to antifraud@support.trendmicro.com.

   TrendLabs monitors sites that obtain information for fraudulent purposes and distributes known phishing site information as part of the automatic updates that Trend Micro makes available to InterScan VirusWall customers.

   Note: To view a list of phishing emails, go to http://www.trendmicro.com/en/security/phishing/overview.htm.

5. Click **Save**.

Chapter 8

Configuring POP3 Anti-Spam Settings

InterScan VirusWall uses the following basic features to filter spam in POP3 email communication:

- **Approved and Blocked Senders lists**: These lists filter on the sender's email address rather than on content.
  - The Approved Senders list contains trusted email addresses. InterScan VirusWall does not filter messages arriving from these addresses, except when POP3 anti-phishing is enabled.
  - The Blocked Senders list contains email addresses that cannot be trusted. InterScan 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.

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

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

- **Spam filter**: Administrators set a spam detection level to filter out spam. The higher the detection level, the more messages are classified as spam. Administrators can set a global detection level for all messages or set one detection level for each spam category.
  The detection level determines how tolerant InterScan VirusWall will be toward suspect email messages. InterScan VirusWall uses the following detection levels:

Detection Level	Filtering Criteria
Low	InterScan 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 most lenient level of spam detection.
Medium	InterScan VirusWall monitors at a high level of spam detection with a moderate chance of filtering false positives. This is the default setting.
High	InterScan VirusWall monitors all email messages for suspicious files or text, but there is 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, InterScan VirusWall determines whether the item is spam.

The predefined threshold settings are:

	Low Confidence	Medium Confidence	High Confidence
Low detection level	6	7	10
Medium detection level	4.5	6	10
High detection level	4	5	7

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

Categories of Spam

InterScan 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 POP3 Anti-Spam

To enable POP3 anti-spam:

1. On the main menu, select **POP3 > Anti-Spam**. The **Target** tab displays.

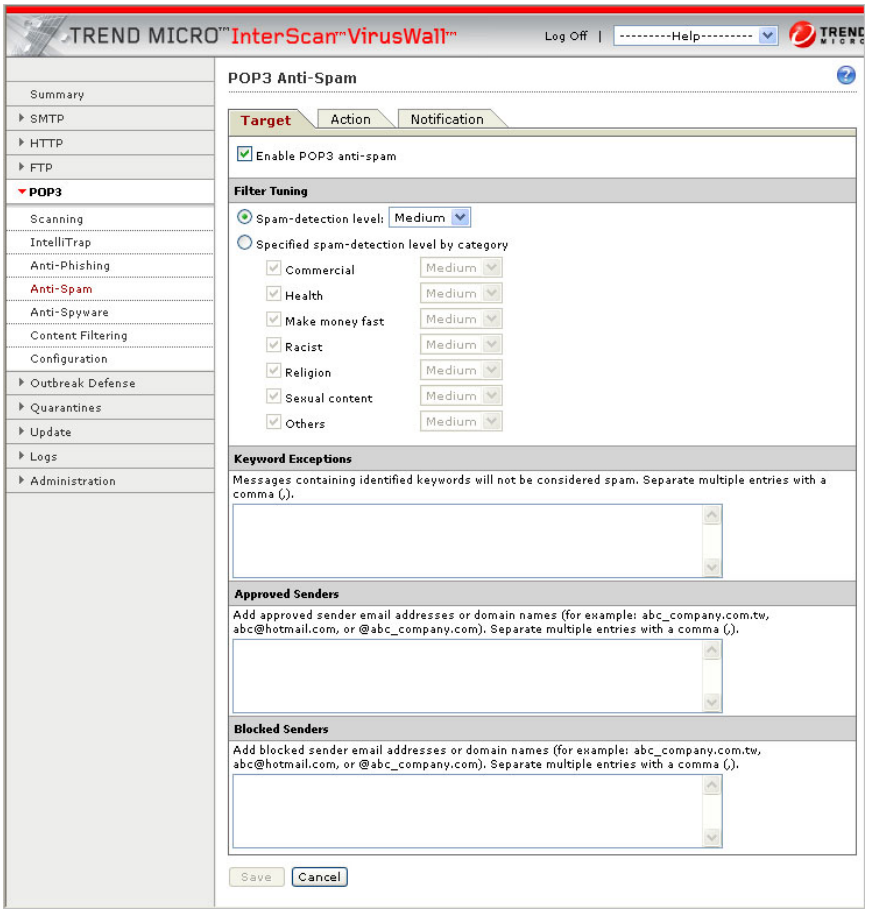


FIGURE 8-1. POP3 Anti-Spam screen, Target tab

2. Select the **Enable POP3 anti-spam** check box.
3. Click **Save**.

Setting the Spam Detection Level (Filter Tuning)

To specify the spam detection level:

1. On the main menu, select **POP3 > Anti-Spam**. The **Target** tab displays.
2. Under **Filter Tuning**, select from the following options:
   - **Spam-detection level**: Uses one detection level for all spam categories.
     - **High**: InterScan VirusWall is very confident that the mail message is spam.
     - **Medium**: InterScan VirusWall is fairly confident that the mail message is spam.
     - **Low**: InterScan VirusWall is fairly confident that the mail message is not spam.
   - **Specified spam-detection level by category**: Uses any of the detection levels for each spam category.

Tip: 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, go to http://subwiz.trendmicro.com/SubWiz/spam_mail-Form.asp.

---

3. Click **Save**.

Specifying Keyword Exceptions

To specify keyword exceptions:

1. On the main menu, select **POP3 > Anti-Spam**. The **Target** tab displays.
2. Type keywords that should ***not*** be considered spam in the **Keyword Exceptions** text box. Separate keywords in the exception lists with a comma.
3. Click **Save**.

Maintaining Approved and Blocked Senders Lists

To maintain approved and blocked senders lists:

1. On the main menu, select **POP3 > Anti-Spam**. The **Target** tab displays.
2. Type all email addresses in the appropriate list, separating them with a comma.

   InterScan VirusWall supports wildcard (*) matching for the Approved and Blocked Senders lists. Sample patterns are shown in Table 8-1.

TABLE 8-1. 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.	

3. Click **Save**.

Specifying Actions on Messages Identified as Spam

To specify actions on messages identified as spam:

1. On the main menu, select **POP3** > **Anti-Spam**, and then click the **Action** tab.

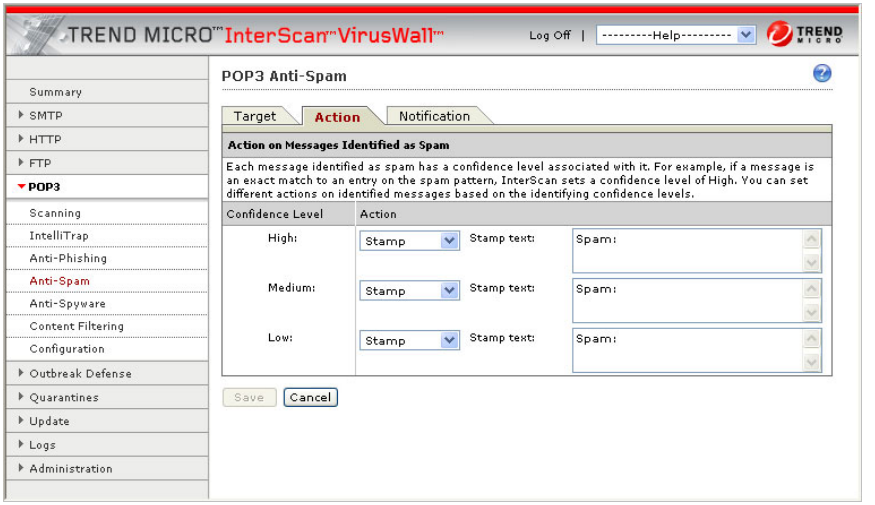


FIGURE 8-2. POP3 Anti-Spam screen, Action tab

2. Under **Action on Messages Identified as Spam**, specify the action to take based on the detection confidence levels:
   - **Delete**: Deletes the whole message.
   - **Quarantine**: Quarantines the message.
   - **Stamp**: Inserts a notification content stamp into the subject line of the message. If you choose this option, type the notification message in the provided text box.
   - **Pass**: InterScan VirusWall does nothing to the message and it is processed normally.
3. Click **Save**.

Configuring Notification Settings

To configure notification settings:

1. On the main menu, select **POP3 > Anti-Spam**, and then click the **Notification** tab.

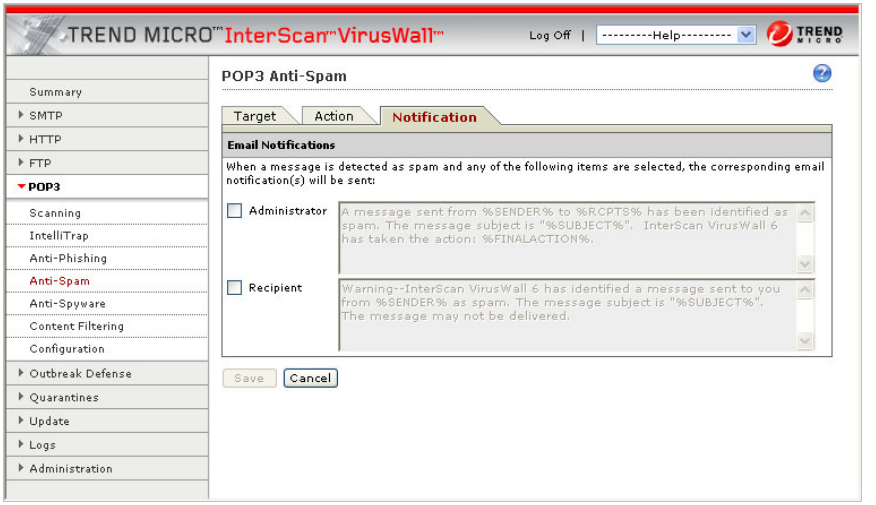


FIGURE 8-3. POP3 Anti-Spam screen, Notification tab

2. To send email notifications to the administrator, select the **Administrator** text box, and modify the administrator notification message as desired.
3. To send email notifications to recipients, select the **Recipient** check box, and modify the message as desired.

Use any of the following tokens or tags on 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%	name of the filter that performs the action
%DETECTED%	name of the security risk found
%FINALACTION%	action taken
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the InterScan VirusWall machine

4. Click **Save**.

Chapter 9

Configuring POP3 Anti-Spyware/Grayware Settings

Spyware/Grayware comes in many forms and often appears to be a legitimate software program.

POP3 spyware/grayware scanning is highly configurable. The following are procedures for configuring scanning settings:

By default, InterScan VirusWall will scan for all the types of spyware/grayware listed in Table 9-1, delete attachments with spyware/grayware and deliver the emails, and then send the administrator a predefined notification message about the spyware/grayware detection.

TABLE 9-1. Types of Spyware/Grayware

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 POP3 Spyware/Grayware Scanning

To enable POP3 spyware/grayware scanning:

1. On the main menu, select **POP3 > Anti-Spyware**. The **Target** tab displays.

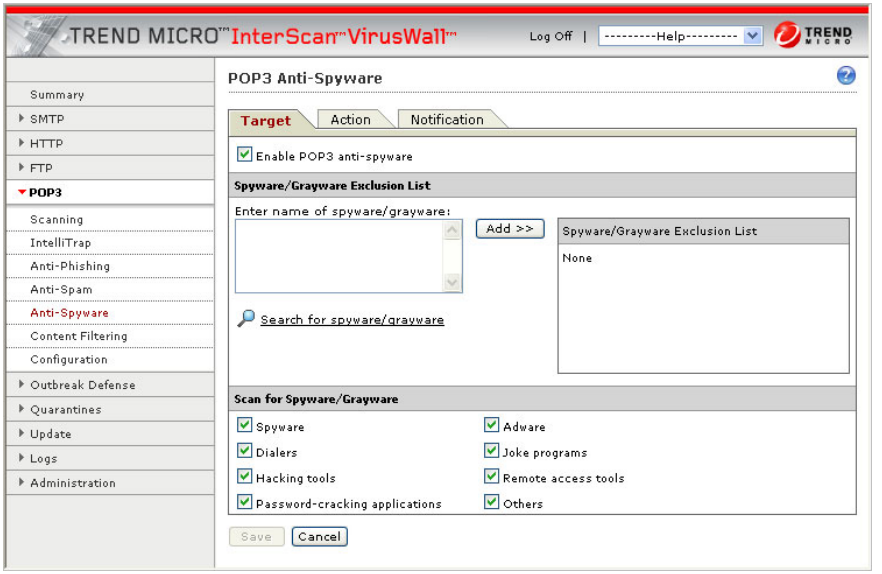


FIGURE 9-1. POP3 Anti-Spyware screen, Target tab

2. Select the **Enable POP3 anti-spyware** check box.
3. Click **Save**.

Setting the Spyware/Grayware Scanning Exclusion List

To set the spyware/grayware scanning exclusion list:

1. On the main menu, select **POP3 > Anti-Spyware**. The **Target** tab displays.
2. In **Enter name of spyware/grayware**, type the file names or the file extensions to exclude from spyware/grayware scanning. For extension names, use the asterisk (*) as a wildcard character. For example, to exclude .bmp files, type *.bmp.
3. Click **Add**, and then click **Save**.

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

Specifying Spyware/Grayware Types to Scan

To specify the types of spyware/grayware to scan:

1. On the main menu, select **POP3 > Anti-Spyware**. The **Target** tab displays.
2. Under **Scan for Spyware/Grayware**, select the types of spyware/grayware InterScan VirusWall will scan.
3. Click **Save**.

Specifying the Action to Take When Spyware/Grayware Is Detected

To specify the action to take when spyware/grayware is detected:

1. On the main menu, select **POP3** > **Anti-Spyware**, and then click the **Action** tab.

FIGURE 9-2. POP3 Anti-Spyware screen, Action tab

2. Under **Action on Spyware/Grayware**, select from the following options:
   - **Quarantine spyware/grayware and pass**: Moves the attachment with spyware/grayware to the quarantine directory. The recipient will receive the email without the attachment.
   - **Delete spyware/grayware and pass**: Permanently deletes the attachment and delivers the email without the attachment.
   - **Pass (not recommended)**: Delivers the email with the attachment.
3. Click **Save**.

Configuring Notification Settings

To configure notification settings:

1. On the main menu, select **POP3 > Anti-Spyware**, and then click the **Notification** tab.

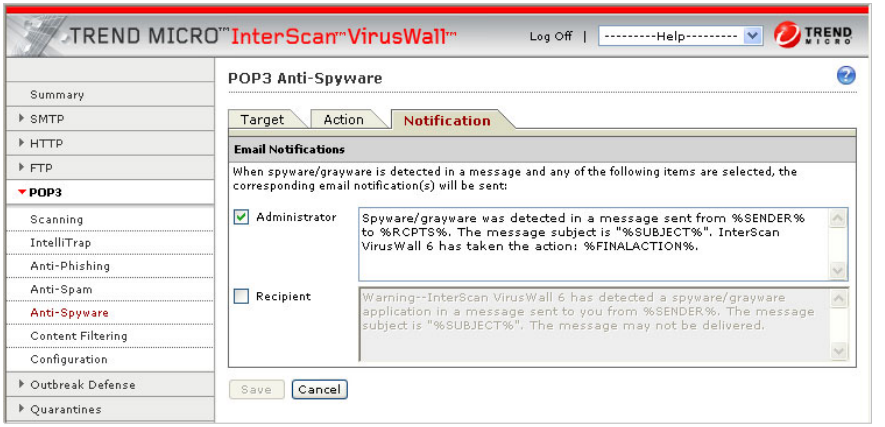


FIGURE 9-3. POP3 Anti-Spyware screen, Notification tab

2. Under **Email Notifications**, modify the administrator notification message as desired. You can unselect the **Administrator** check box if you do not want to send the notification.
3. To send email notifications to recipients, select the **Recipient** check box, and modify the message as desired.

Use any of the following tokens or tags on 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%	name of the filter that performs the action
%DETECTED%	name of the security risk found
%FINALACTION%	action taken on the message
%QUARANTINE_AREA%	quarantine location
%MACHINENAME%	hostname of the InterScan VirusWall machine

4. Click **Save**.

Chapter 10

Configuring POP3 Content Filtering Settings

InterScan VirusWall provides real-time email content filtering for POP3. When you enable POP3 content filtering, all information that enters or leaves the network through POP3 is scanned for possible matches with the content filtering policies you have defined. InterScan VirusWall uses policies based on either a keyword filter or an attachment filter.

Content Filtering Policy Based on Keywords

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

Keyword Lists

The keyword list for a given keyword filter contains the words and phrases matched to the message content. When multiple keywords are included on the same line of a policy, a match occurs only when the message being evaluated contains all of the keywords on that line. For example, you can use the following keywords to a list:

Example 1:

resume, position

resume, job

resume, experience

resume, enclosed

In this example, the word ‘resume’ appears with an additional word four times instead of using it just once as a single entry. Using only ‘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 will increase 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.

Example 2:

Resume, position, job, experience, enclosed

Obviously, the likelihood of detecting every outbound resume on the basis of this filter is much less than for a policy that contains several rule sets based upon the word ‘resume’, as shown in Example 1.

Example 3 shows a policy wherein the occurrence of any one of the four words in Example 2 triggers a match.

Example 3:

job

resume

enclosed

position

experience

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 appears on any given line (OR operator), the policy risks being too permissive—too many email messages will match. Of course, as shown above, a lot depends upon what you are filtering.

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.

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:

Case 1. Keywords appear on a single line

Apple Juice, [and] Pear, [and] Orange

Case 2. Keywords each appear on their own individual lines

Apple Juice [or]

Pear [or]

Orange [or]

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.

Results

In Case 1, only messages containing all items, Apple Juice, Pear, and Orange (in any order, anywhere in the message text) are considered a match.

In Case 2, 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.

In Case 3, with synonym checking on, messages that contain the phrase Apple Juice, the word Pear, and any of the word(s) Orange, orangish, red, or yellow are considered a match.

Synonym List for Keywords

InterScan VirusWall has a predefined list of synonyms for certain keywords. You cannot modify or add to the predefined list of synonyms.

Other Keyword Notes

Note that Apple Juice is a phrase because the words Apple and Juice are not delimited with a comma; even if the words Apple and Juice both appear somewhere in the message, no match will be triggered 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.

Enabling POP3 Content Filtering

To enable POP3 content filtering:

1. On the main menu, select **POP3 > Content Filtering**.

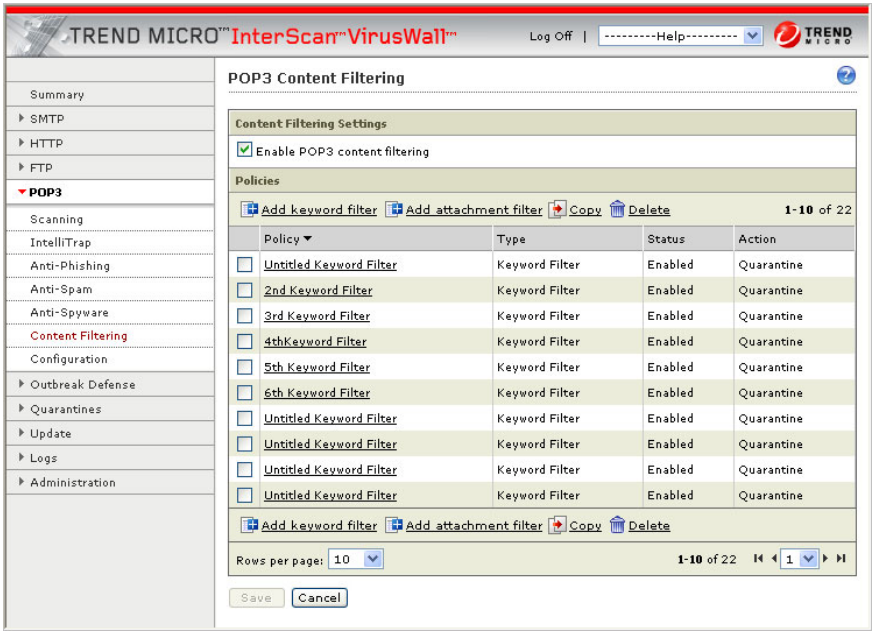


FIGURE 10-1. POP3 Content Filtering screen

2. Under **Content Filtering Settings**, select the **Enable POP3 content filtering** check box.
3. Click **Save**.

Note: If you disable POP3 content filtering, InterScan VirusWall will not monitor the content of POP3 traffic. Any other POP3 scanning features that are enabled will continue to function as specified.

Creating a Policy Based on a Keyword Filter

To create a policy based on a keyword filter:

1. On the main menu, select **POP3 > Content Filtering**.
2. Under **Policies**, select **Add keyword filter**. The Keyword Filter screen opens, displaying the **Target** tab.

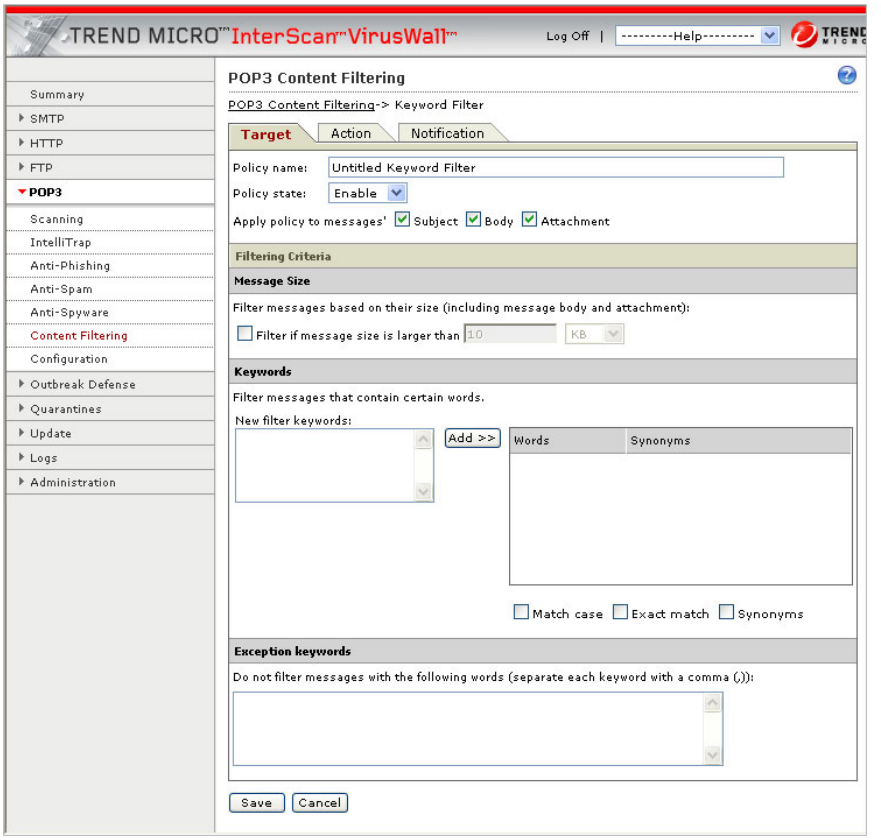


FIGURE 10-2. Keyword Filter screen, Target tab

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 messages'**, select the sections of the messages (Subject, Body, or Attachment) to which this policy applies.
6. If you want the policy to block messages with attachments larger than a specified size, select **Filter if message size is larger than**, and then specify the size limit.
7. Under **Keywords**, type the keywords for which you want InterScan VirusWall to scan messages and click **Add**.
8. To specify synonyms for each keyword, do the following:

   a. Click the link under the **Synonyms** column (default is [none]). The Edit Synonyms screen opens.

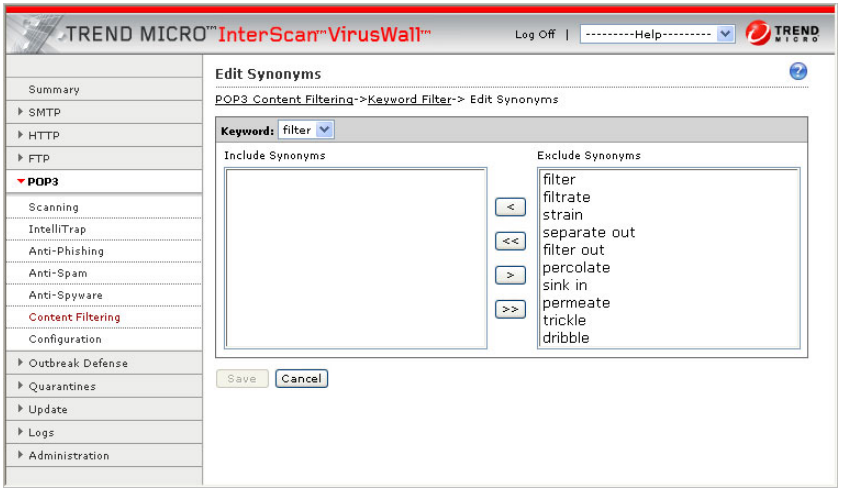


FIGURE 10-3. Edit Synonyms screen

   b. If you have entered multiple keywords that you separated with commas, all the keywords will appear in a drop-down box. Select the one keyword for which you want synonyms to be displayed.

   c. Select the synonyms you want to use for the keyword from the list of synonyms in the **Exclude Synonyms** column, and click < to move the synonyms into the **Include Synonyms** column.

d. Click **Save**. The Keyword Filter screen opens again.

9. If desired, enable any of the options **Match case**, **Exact match**, and **Synonyms**.

Note: For more information in creating a keyword list for your policy, see *Creating a Policy Based on a Keyword Filter* on page 10-6.

---

10. To reduce the chances of InterScan VirusWall blocking messages that should be allowed to pass, in **Exception keywords**, type keywords that will identify these messages. Messages that contain these keywords will not be blocked by the policy even when a match with a keyword filter is made.

11. Click **Save**.

Specifying the Action on Messages That Match the Keyword Filtering Policy

To specify the action on messages that match the keyword filtering policy:

1. On the main menu, select **POP3 > Content Filtering**.

2. Under **Policies**, select **Add keyword filter**.

3. When the Keyword Filter screen opens, click the **Action** tab.

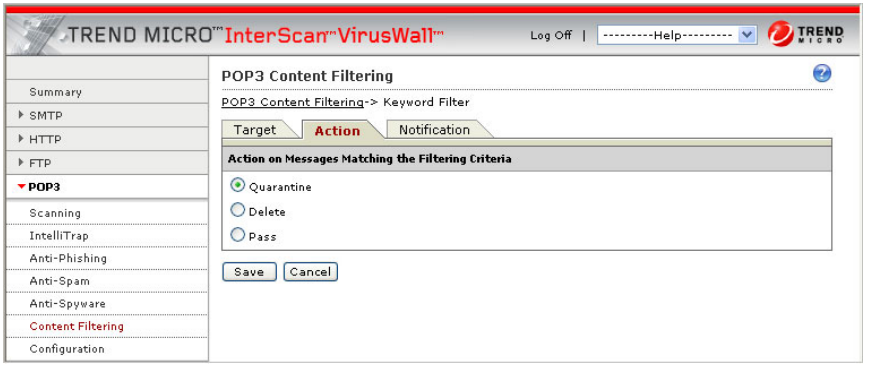


FIGURE 10-4. Keyword Filter screen, Action tab

4. Under **Action on Messages Matching the Filtering Criteria**, select one of the following options:
   - **Quarantine**: Quarantines the message.
   - **Delete**: Deletes the entire message.
   - **Pass**: Delivers the message.
5. Click **Save**.

Configuring Notification Settings When a Message Triggers a Keyword Filtering Policy

To specify notification settings when a message triggers a keyword filtering policy:

1. On the main menu, select **POP3 > Content Filtering**.
2. Under **Policies**, select **Add keyword filter**.
3. When the Keyword Filter screen opens, select the **Notification** tab.

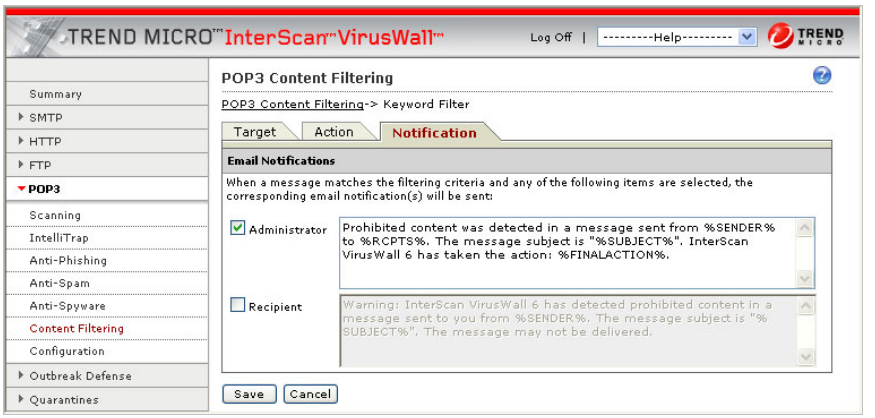


FIGURE 10-5. Keyword Filter screen, Notification tab

4. Modify the administrator notification message as desired. You can unselect the **Administrator** check box if you do not want to send the notification.

5. To send email notifications to recipients, select the **Recipient** check box, and modify the message as desired.

   Use any of the following tokens or tags on 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%	hostname of the InterScan VirusWall machine

6. Click **Save**.

Creating a Policy based on an Attachment Filter

To create a policy based on an attachment filter:

1. On the main menu, select **POP3 > Content Filtering**.
2. Under **Policies**, select **Add attachment filter**. When the Attachment Filter screen opens, click the **Target** tab.

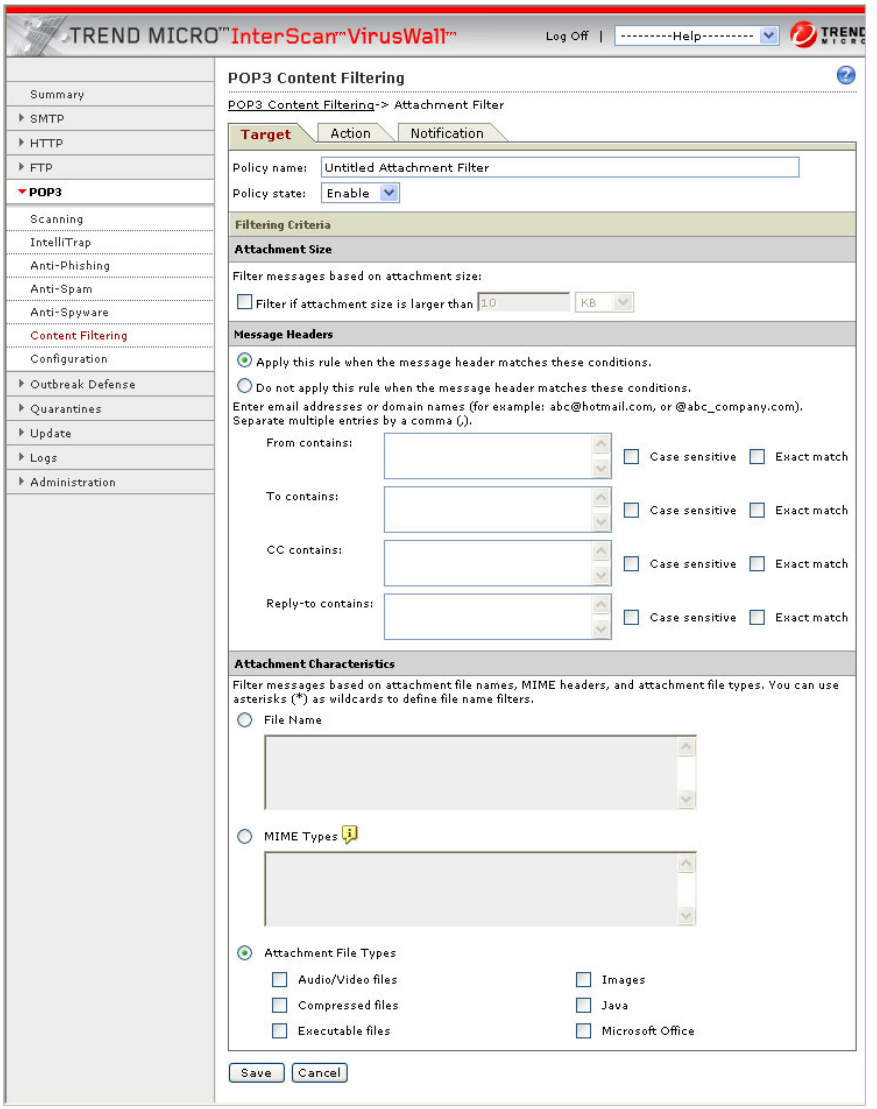


FIGURE 10-6. Attachment Filter screen, Target tab

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. 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.
6. Under **Message Headers**, choose from the following options:
   - **Apply this rule when the message header matches these conditions**: Applies the settings under **Attachment Characteristics** to message headers that match the header strings you specified.
   - **Do not apply this rule when the message header matches these conditions**: When message headers match the header settings you specified, the policy will not be applied to the message.
7. Specify whether you want to apply the header rule when strings in the message header match certain conditions, including the **From**, **To**, **CC**, **and Reply-to** fields.

Note: You can specify multiple entries in the message header text boxes and separate each entry with a comma. For example, user1@isvw.com,user2@isvw.com.

---

8. Under **Attachment Characteristics**, select the filtering criteria for message attachments.
   - **File Name**: Specify a file name or a string using a wildcard (*). InterScan VirusWall will filter all attachments with file names that match the names or the strings.
   - **MIME Types**: Specify the MIME types to filter.
   - **Attachment File Types**: Specify file type categories that you want to block. InterScan VirusWall will block all attachments in the specified file type 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**.

---

9. Click **Save**.

Specifying the Action on Messages That Match the Attachment Filtering Policy

To specify the action on messages that match the attachment filtering policy:

1. On the main menu, select **POP3 > Content Filtering**.
2. Under **Policies**, select **Add attachment filter**.
3. When the Attachment Filter screen opens, click the **Action** tab.

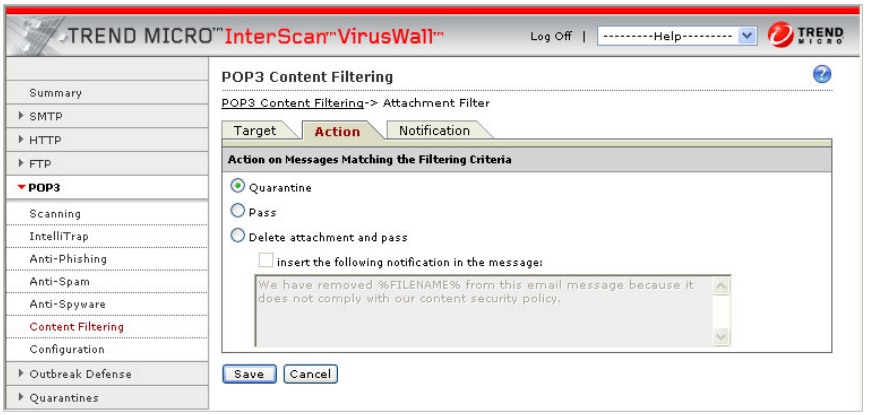


FIGURE 10-7. Attachment Filter screen, Action tab

4. Under **Action on Messages Matching the Filtering Criteria**, select one of the following options:
   - **Quarantine**: Quarantines the message.
   - **Pass**: Delivers the message
   - **Delete attachment and pass**: Removes the attachment and delivers the message.

5. To insert a notification into the body of the message, select **Insert the following notification in the message:**. You can 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**.

Configuring Notification Settings When a Message Triggers an Attachment Filtering Policy

To specify notification settings when a message trigger an attachment filtering policy:

1. On the main menu, select **POP3 > Content Filtering**.
2. Under **Policies**, select **Add attachment filter**.
3. When the Attachment Filter screen opens, select the **Notification** tab.

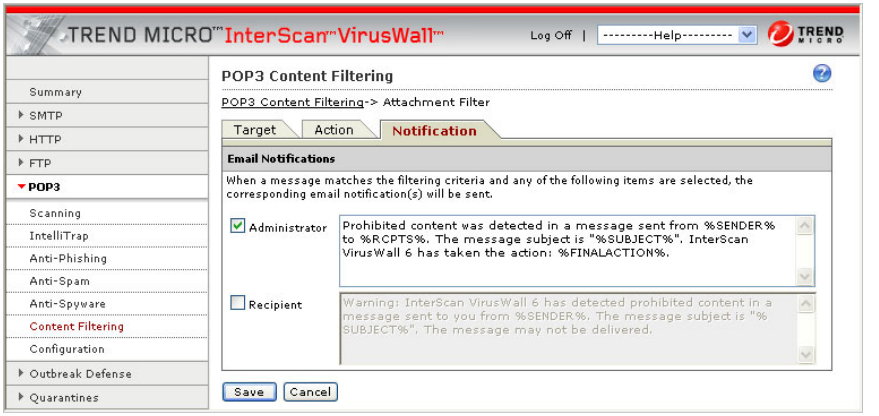


FIGURE 10-8. Attachment Filter screen, Notification tab

4. Modify the administrator notification message as desired. You can unselect the **Administrator** check box if you do not want to send the notification.
5. To send email notifications to recipients, select the **Recipient** check box, and modify the message as desired.

Use any of the following tokens or tags on 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%	hostname of the InterScan VirusWall machine

6. Click **Save**.

Copying or Deleting a POP3 Content Filtering Policy

To copy or delete a POP3 content filtering policy:

1. On the main menu, select **POP3 > Content Filtering**.
2. Under **Policies**, select a policy and click **Copy** or **Delete**.
3. Click **OK** on the message box to finalize changes.