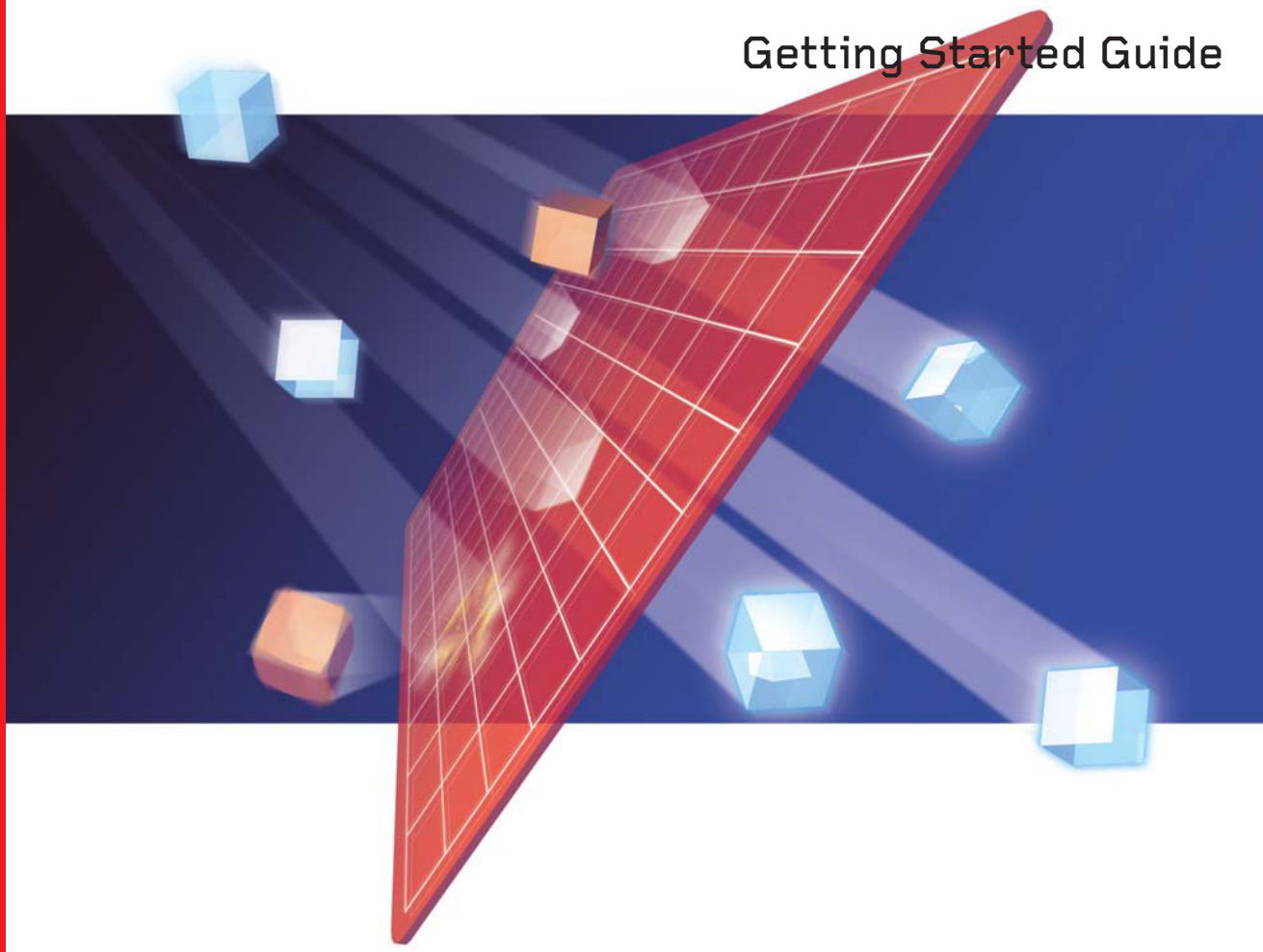
TREND MICRO™
InterScan™ VirusWall™ 6

Integrated virus and spam protection for your Internet gateway

for Linux™

Getting Started Guide



TREND MICRO™

Document Part Number: IVEM62759/60608

Release Date: July 2006

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

The *Trend Micro™ InterScan VirusWall™ 6 Getting Started Guide* is intended to introduce the main features of the software and installation instructions for your production environment. Read it before installing or 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.

To contact Trend Micro Support, please see Obtaining Technical Support on page 5-27 of this document.

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:

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

Contents

Chapter 3: Migrating from Previous Releases

Chapter 4: Getting Started

Chapter 5: Troubleshooting and Support

Tables and Figures

List of Tables

Introduction

Chapter 1: Deployment

Chapter 2: Installation

Chapter 4: Getting Started

Chapter 5: Troubleshooting

List of Figures

Chapter 1: Deployment

Chapter 2: Installation

Chapter 3: Migration from Previous Releases

Chapter 4: Getting Started

Chapter 5. Troubleshooting and Support

Introduction

Welcome to the Getting Started Guide for InterScan™ VirusWall™ 6 for Linux. This document provides the system administrator with the necessary information to set up, configure, and start managing an InterScan VirusWall installation.

About This Guide

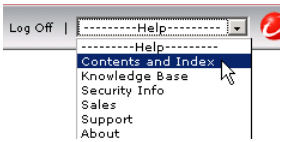
The Getting Started Guide contains the following chapters:

- Chapter 2, *Installation* — includes installation planning, system requirements, installation procedures, and post-installation tasks.
- Chapter 3, *Migrating from Previous Releases* — provides guidance on migrating to InterScan VirusWall 6 from InterScan VirusWall for Unix 3.81, with or without eManager, including how to migrate your configuration settings.
- Chapter 4, *Getting Started* — includes a discussion of the Web management console and the menu options in the console and basic tasks such as starting and stopping InterScan VirusWall services and testing key features.
- Chapter 5, *Troubleshooting and Support* — includes solutions to quick start tasks and how to obtain technical support.

Product Documentation

In addition to this Getting Started Guide, you can obtain relevant information about this software by accessing the following documents:

TABLE 1. InterScan VirusWall manuals, their content, and where to get them

Document	Content	Where to Access
Readme file	System requirements, late-breaking information that may not be included in other documentation, and a list of features	• From the installation folder (you can launch the readme file after installation) • From http://www.trendmicro.com/download/ (the Trend Micro download site)
SMTP Configuration Guide	Guide to setting up and configuring this product to protect SMTP traffic by virus scanning, anti-phishing, anti-spam, anti-spyware/grayware, content filtering, and IntelliTrap	• In the product package • From the Trend Micro download site: http://www.trendmicro.com/download/
HTTP Configuration Guide	Guide to setting up and configuring this product to protect HTTP traffic by virus scanning, anti-phishing, anti-spam, anti-spyware / grayware, URL blocking, and URL filtering	
FTP and POP3 Configuration Guide	Guide to setting up and configuring this product to protect your FTP traffic by scanning for viruses and spyware/grayware and to protect your POP3 mail traffic by virus scanning, anti-phishing, anti-spam, anti-spyware/grayware, content filtering, and IntelliTrap	
Reference Manual	System checklists, migration tables, default values, and information about Outbreak Prevention Services	
Online Help	Information about product features, tasks, frequently asked questions, and troubleshooting commonly encountered problems Context-sensitive information for each page of the user interface and information concerning the purpose of each screen: 	From the Web console:  Click **Contents and Index** in the Help dropdown menu to access the main Online Help.

What's New in Version 6.0?

InterScan VirusWall 6 has new features to protect your network against the latest security threats. The additional features in this release include protection against spam, spyware/grayware, bot threats, and phishing; content-filtering capabilities; HTTP and FTP file blocking based on file type; email notifications for HTTP and FTP scans; ability to specify outbound mail disclaimer through the Web console; and protection through Outbreak Prevention Services (OPS).

TABLE 2. List of New Features for InterScan VirusWall 6 for Linux

New Feature	Descriptions
Migration from InterScan VirusWall 3.8x with the eManager™ 3.8x plug-in	Easy upgrade from version 3.8x to 6 while retaining most configuration settings
SMTP, POP3, FTP and HTTP scanning capabilities	SMTP and POP3 scanning: antivirus, IntelliTrap, spyware/grayware detection, anti-spam, anti-phishing, and content filtering, including notification messages to the administrator, sender, and recipients upon detection of phishing messages FTP scanning: antivirus and spyware/grayware detection and file blocking by file type HTTP scanning: antivirus, spyware/grayware detection, file blocking by file type, and blocking of phishing URLs
Anti-spam configuration	• Can set the spam threshold to high, medium, or low • Can specify approved and blocked senders • Can define certain categories of mail as spam based on company policies
Outbreak Prevention Services (OPS)	OPS updates that come directly from TrendLabs^{SM} and configurable options for automatic deployment
URL blocking and filtering	Can define and configure URL filtering policies Local cache support to reduce network traffic Notifications to users if URL filtering blocks their HTTP requests
Transparent proxy	Support for the HTTP proxy transparency mode, with the ability to inter-operate with an L4 switch
Reverse proxy	Support for the HTTP reverse proxy mode in the HTTP VirusWall to protect the internal Web Server

Chapter 1

Deployment

This chapter includes the following topics:

Installation Topologies

Trend Micro recommends installing InterScan VirusWall directly behind a properly configured firewall or security device that offers network address translation (NAT) and other firewall-type equivalent protection.

You can strategically set up InterScan VirusWall to address multiple topologies, ranging from a single integrated deployment, in which you install InterScan VirusWall on a single server and enable all services on that server, to a completely distributed, server-specific deployment, in which you install one instance of InterScan VirusWall on each kind of server (HTTP, FTP, SMTP, and POP3) and enable only the relevant service on each server.

TABLE 1-1. Possible InterScan VirusWall topology deployments

Single, integrated deployment	Install InterScan VirusWall on one server and enable SMTP VirusWall, POP3 VirusWall, FTP VirusWall and HTTP VirusWall on that server
Messaging/Web deployment	Install InterScan VirusWall on one server and then enable SMTP VirusWall and POP3 VirusWall on that server
	Install InterScan VirusWall on one server and enable FTP VirusWall and HTTP VirusWall on that server
Standalone deployment	Install InterScan VirusWall on four different servers and enable only one service on each server

The following diagrams illustrate the typical network set up before and after installing InterScan VirusWall.

Deploying SMTP VirusWall

The SMTP filtering service of InterScan VirusWall (SMTP VirusWall) checks both inbound and outbound SMTP traffic for viruses. It can be installed on the same machine as your existing SMTP server or on a dedicated machine.

- If the SMTP server is on another machine, specify the hostname (or IP address) and port for InterScan VirusWall. (See figure 1-4, “Topology A: Inbound and outbound mail paths, InterScan VirusWall and SMTP server on different machines,” on page 1-5.)

- If the SMTP server is on the same machine, change the port it uses to listen for incoming SMTP connections, and specify this port and hostname for InterScan VirusWall. (See figure 1-6, “Topology B: After installing InterScan VirusWall (SMTP VirusWall and mail server on the same machine),” on page 1-6.)
- If the SMTP server is Sendmail and on the same machine as InterScan VirusWall, you need to identify the Sendmail path and add the -bs flag. No port configuration is necessary. (See figure 1-5, “The SMTP Configuration Settings screen in the Web console,” on page 1-6.)

Remap the firewall’s SMTP service, port 25, to the newly installed InterScan VirusWall server listening on port 25. Then use mail forwarding (single server environment) or command mode (multi-server environment) to pass scanned mail to an internal mail server or servers.

Using the topology suggestions shown in figure 1-2, “Topology A: Inbound mail path after installing InterScan VirusWall (SMTP VirusWall and SMTP server on different machines),” on page 1-4 and figure 1-3, “Topology A: Outbound mail path after installing InterScan VirusWall (SMTP VirusWall and SMTP server on different machines),” on page 1-4 will require changing the IP address or addresses of internal mail server or servers. No changes to the clients’ outgoing mail settings are required, as they will still connect to their respective outgoing mail server.

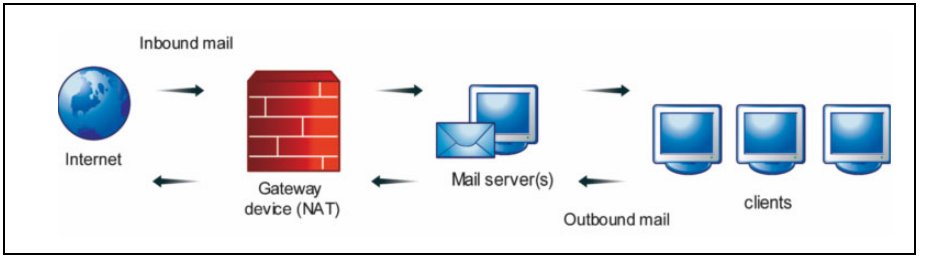


FIGURE 1-1. Topology A: Inbound mail path before installing InterScan VirusWall

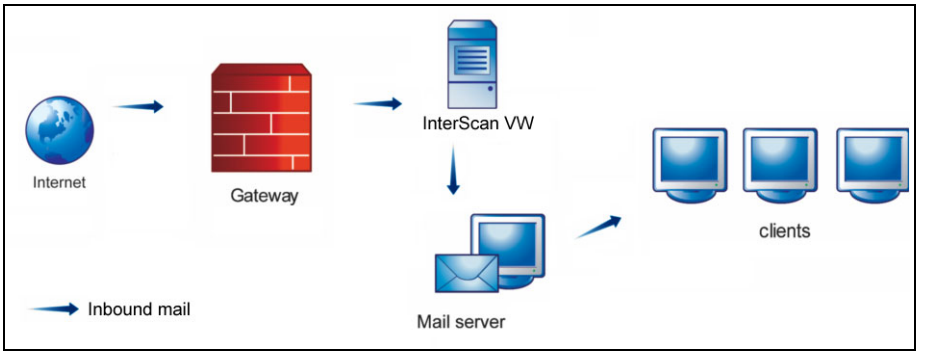


FIGURE 1-2. Topology A: Inbound mail path after installing InterScan VirusWall (SMTP VirusWall and SMTP server on different machines)

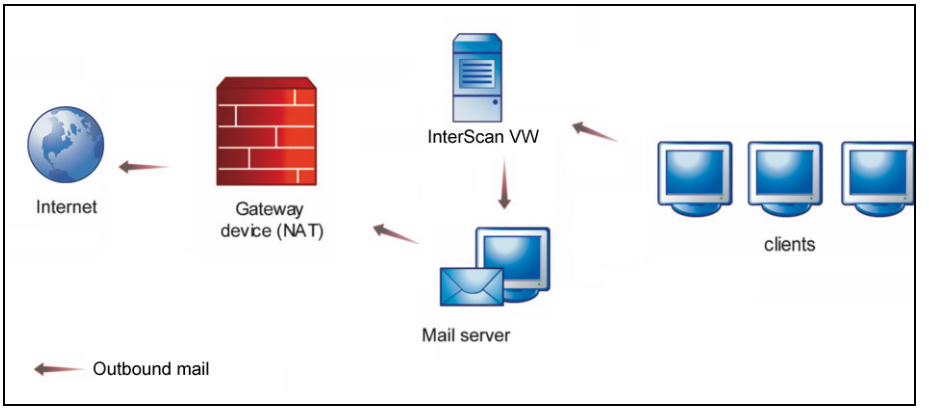


FIGURE 1-3. Topology A: Outbound mail path after installing InterScan VirusWall (SMTP VirusWall and SMTP server on different machines)

When InterScan VirusWall and the SMTP server are not on the same machine, you can replace the original SMTP server with InterScan VirusWall and let InterScan forward mail to the original SMTP server, as shown in figure 1-4, “Topology A: Inbound and outbound mail paths, InterScan VirusWall and SMTP server on different machines,” on page 1-5.

In such a deployment, inbound mail first goes to InterScan VirusWall, which scans it and then forwards it to the original SMTP server. Outbound mail also goes first to InterScan VirusWall, which scans it and forwards it to the original SMTP server, which then sends it out to the Internet.

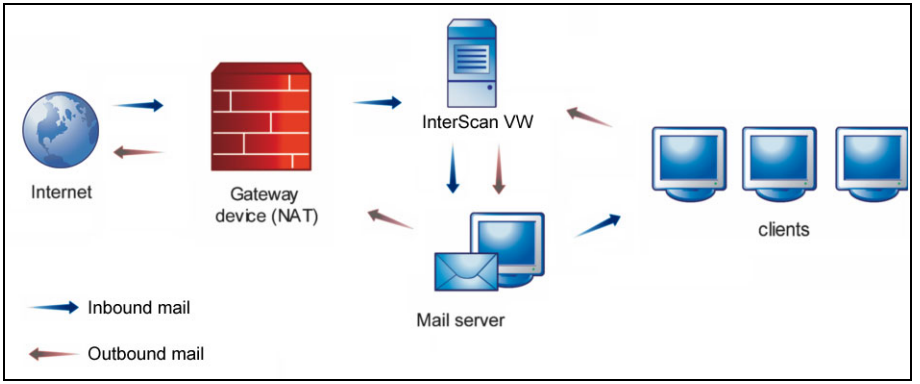


FIGURE 1-4. Topology A: Inbound and outbound mail paths, InterScan VirusWall and SMTP server on different machines

If the SMTP server is Sendmail, and it is on the same machine as InterScan VirusWall, identify the Sendmail path and add the -bs flag. No port configuration is

necessary. (See figure 1-5, “The SMTP Configuration Settings screen in the Web console,” on page 1-6.)

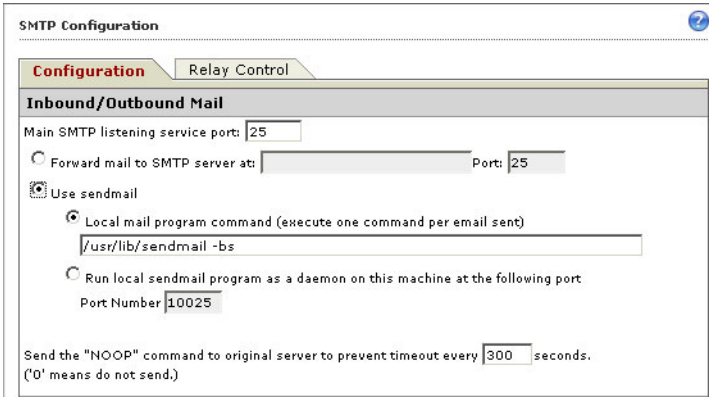


FIGURE 1-5. The SMTP Configuration Settings screen in the Web console

Before selecting **Run local sendmail program as a daemon on this machine at the following port** on the SMTP Configuration Settings screen, first correctly configure the Sendmail or other SMTP mail daemon on that machine.

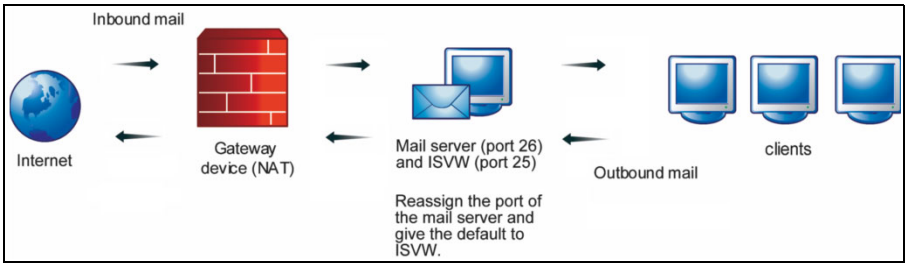


FIGURE 1-6. Topology B: After installing InterScan VirusWall (SMTP VirusWall and mail server on the same machine)

Deploying POP3 VirusWall

The typical POP3 topology requires modifying the client machine POP3 settings so that client receives email directly from InterScan VirusWall. Change the client's mailbox name from *Mailbox_name* to:

```
Mailbox_name#POP3_server[#Port_number]
```

For example, from *joedoe* to:

```
jdoe#externalpop3.com[#110]
```

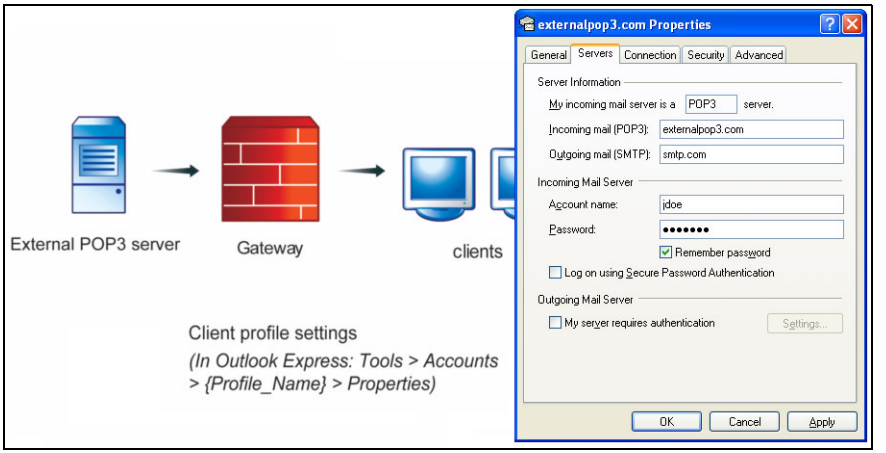


FIGURE 1-7. POP3 topology before installing InterScan VirusWall and POP3 settings

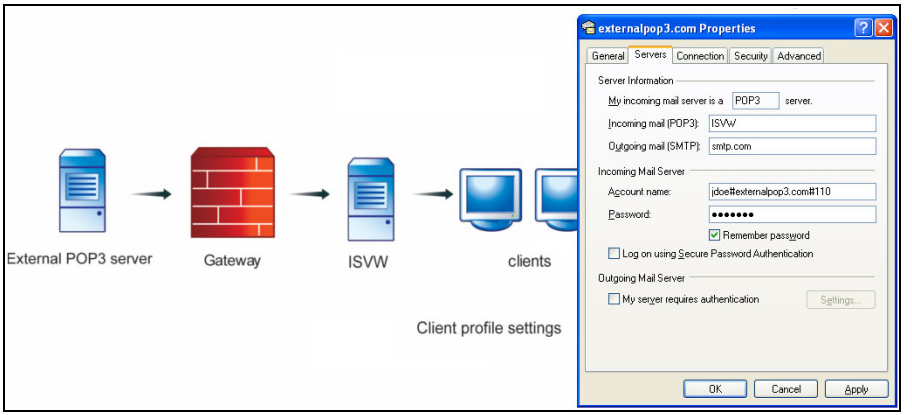


FIGURE 1-8. POP3 topology after installing InterScan VirusWall and POP3 settings

POP3 (Port Mapping)

If InterScan VirusWall acts as a port mapping server, the ports will be mapped to the listening port of InterScan VirusWall and the specific POP3 servers. The required changes for this topology are as follows:

- In the Web management console**, POP3** > **Configuration**, inbound POP3 port should be the port that InterScan VirusWall uses.
- In the POP3 settings on the client machines, incoming mail server name and port should be the InterScan VirusWall server name and port number.

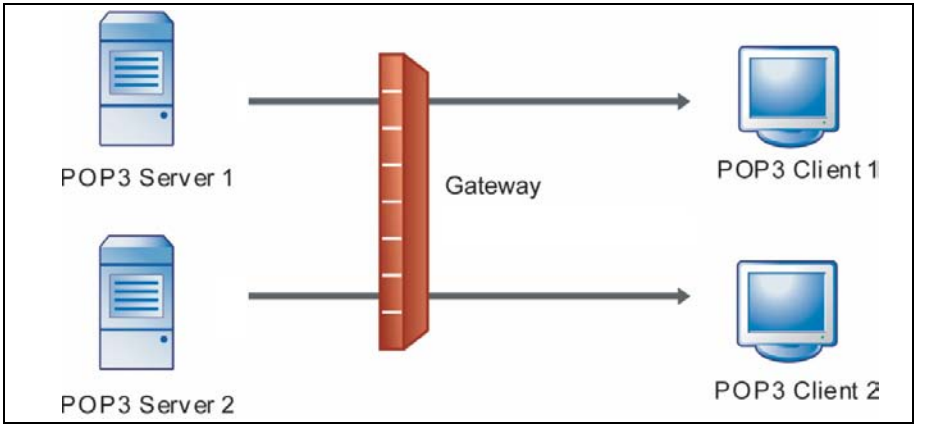


FIGURE 1-9. POP3 topology before installing InterScan VirusWall

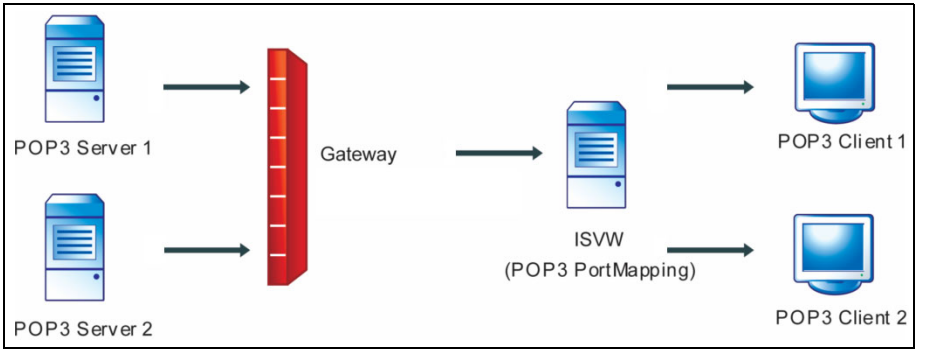


FIGURE 1-10. POP3 topology after installing InterScan VirusWall

Deploying FTP VirusWall

There are two ways to use the FTP scanning feature of InterScan VirusWall (referred to also as the FTP VirusWall):

1. **Standalone mode.—**FTP VirusWall acts as a proxy between the requesting client and the remote site, brokering all transactions, as shown in figure 1-14, “FTP deployment in standalone mode with a separate proxy server,” on page 1-12.
2. **Port-mapping mode.—**FTP VirusWall acts as a sentry standing guard in front of a specific server within the LAN.

In either case, FTP VirusWall checks all transfers for viruses, malicious Java applets, malicious ActiveX controls, and spyware/grayware. FTP VirusWall can be installed on the same machine as an existing FTP server, on a dedicated machine, or as the sole FTP proxy.

When installed and configured to act as a proxy (Figure 1-12), FTP VirusWall does the following:

- Receives all FTP requests originating from within the LAN
- Passes them to the remote FTP server
- Receives the data back using the data port opened by the remote FTP server
- Scans for viruses and spyware/grayware
- Delivers clean files to the requesting client

In Standalone mode, InterScan VirusWall serves as the FTP proxy server. Users connect to the specified FTP server through the FTP VirusWall by typing the following: *username@FTP_Server_IP:Port*.

In Port-mapping mode (using FTP proxy), InterScan VirusWall complements an existing FTP proxy server. If there is no proxy server, clients connecting to the FTP VirusWall will be redirected to the real FTP server specified in the FTP Configuration screen in the Web console.

Note: Every FTP session between the FTP server and the client machine will pass through the FTP VirusWall, but this action is invisible to the end user.

FTP Standalone Mode Deployment

You can deploy FTP VirusWall in a topology that does not have an FTP proxy server, as shown in figure 1-14, “FTP deployment in standalone mode with a separate proxy server,” on page 1-12. In Standalone mode, in which FTP VirusWall resides on a separate machine from the FTP server, select **Use user@host** in the **Original FTP server location** section of the FTP Server Configuration section of the Web console FTP Configuration page (FTP > Configuration). When you have selected **Use user@host**, FTP VirusWall will communicate with your FTP server by its hostname.

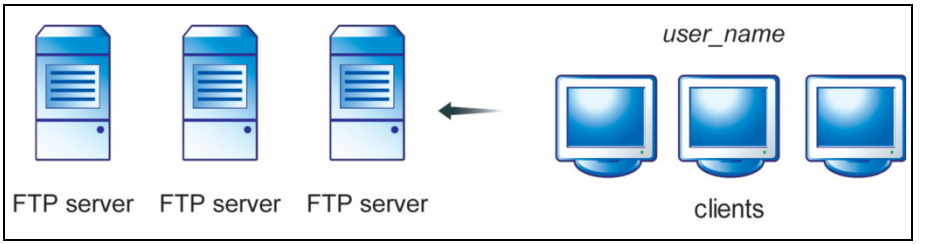


FIGURE 1-11. FTP topology before installing InterScan VirusWall (without proxy server)

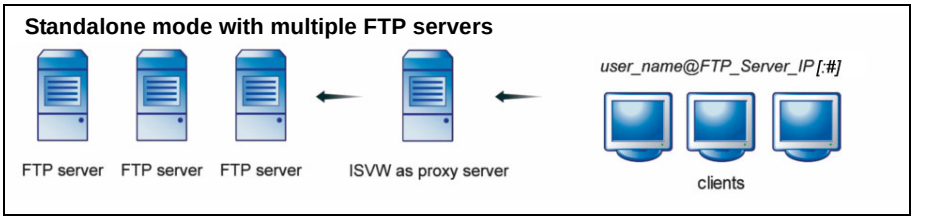


FIGURE 1-12. FTP topology with InterScan VirusWall deployed in standalone mode with multiple FTP servers

You can also opt to deploy FTP VirusWall in standalone mode when your FTP proxy server is a separate, dedicated machine. Just as with the first scenario, in this scenario select **Use user@host** (the default) in the FTP Server Configuration section of the FTP Configuration screen (FTP > Configuration). FTP VirusWall will scan traffic and forward it to the FTP proxy server machine for final delivery.

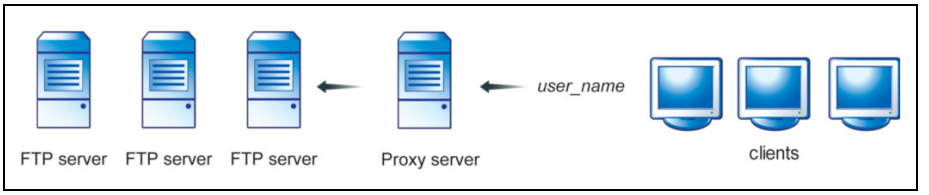


FIGURE 1-13. FTP topology before installing InterScan VirusWall (with proxy server)

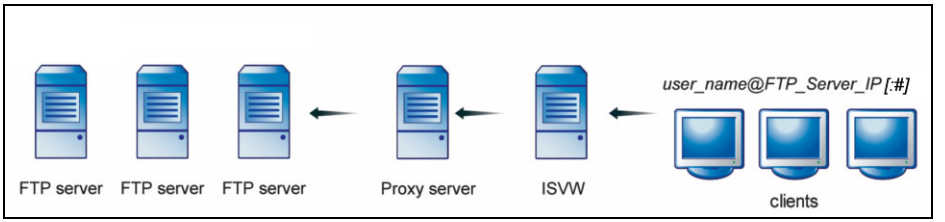


FIGURE 1-14. FTP deployment in standalone mode with a separate proxy server

FTP Port-Mapping Mode Deployment

In Port-mapping mode, set the IP address and port of the original FTP server in the **Server location** field of the FTP Server Configuration section of the Web console FTP Configuration page (FTP > Configuration). (See Figure 1-15.)

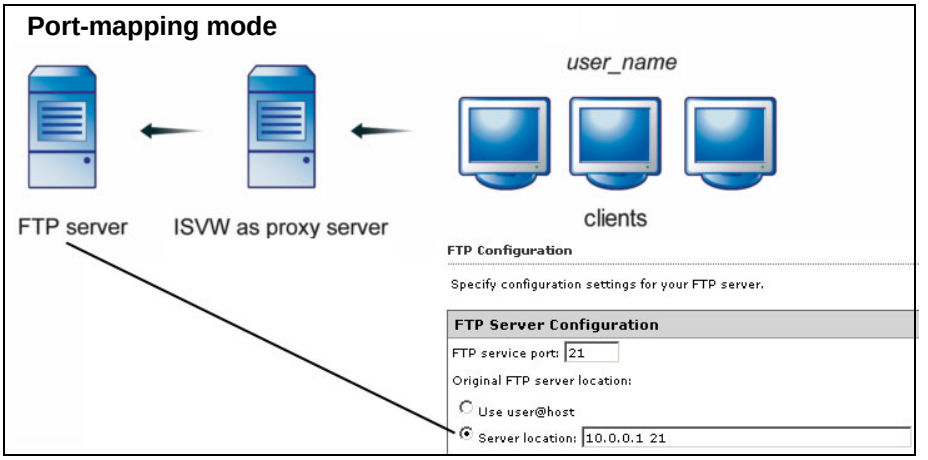


FIGURE 1-15. FTP topology after installing InterScan VirusWall in Port-mapping mode with InterScan VirusWall and FTP server on different machines, showing Web console settings for FTP server

When deploying FTP VirusWall in Port-mapping mode with the FTP server and FTP VirusWall on the same machine, set the absolute path of the FTP server in the **Server location** field of the FTP Server Configuration section of the Web console FTP Configuration page (FTP > Configuration). (See figure 1-17, "FTP topology after installing InterScan VirusWall in Port-Mapping mode (mapped to the real FTP server)," on page 1-14.)

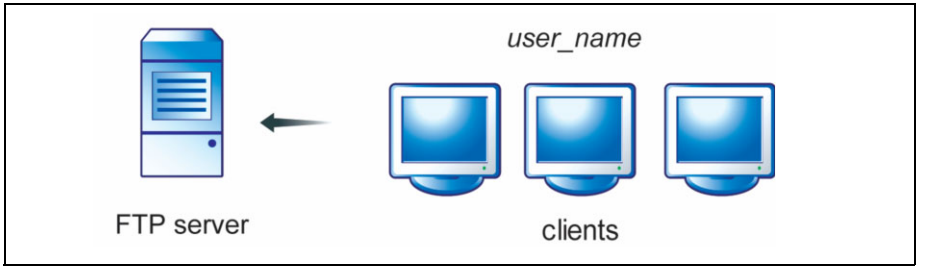


FIGURE 1-16. Simple FTP topology, only one FTP server

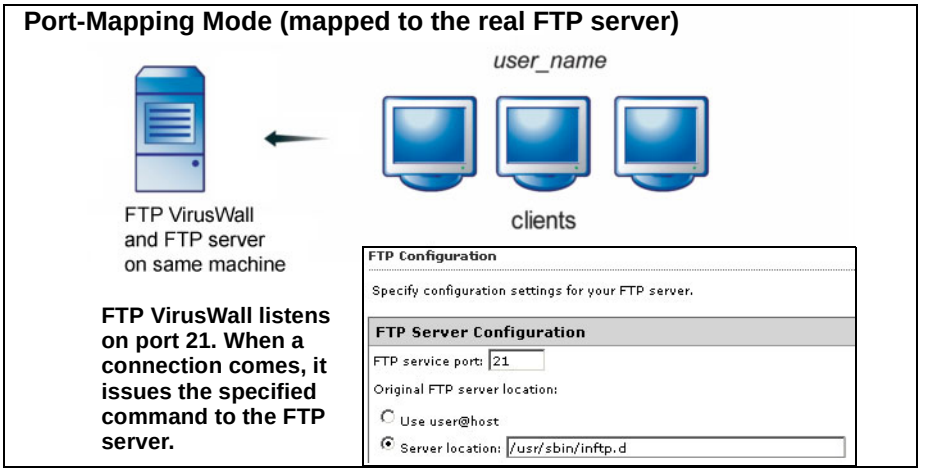


FIGURE 1-17. FTP topology after installing InterScan VirusWall in Port-Mapping mode (mapped to the real FTP server)

Deploying HTTP VirusWall

You can deploy InterScan HTTP VirusWall in three different modes:

- Port-mapping mode
- Dependent mode
- Reverse proxy mode

HTTP VirusWall Standalone Mode

In standalone mode, InterScan VirusWall is directly behind the gateway device, either serving as the HTTP proxy server or receiving HTTP traffic from an existing server.

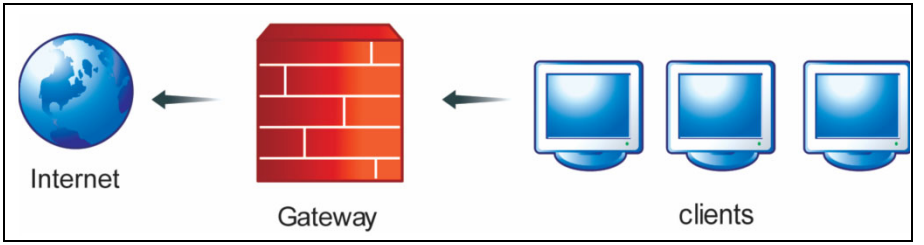


FIGURE 1-18. HTTP topology before installing InterScan VirusWall (without proxy)

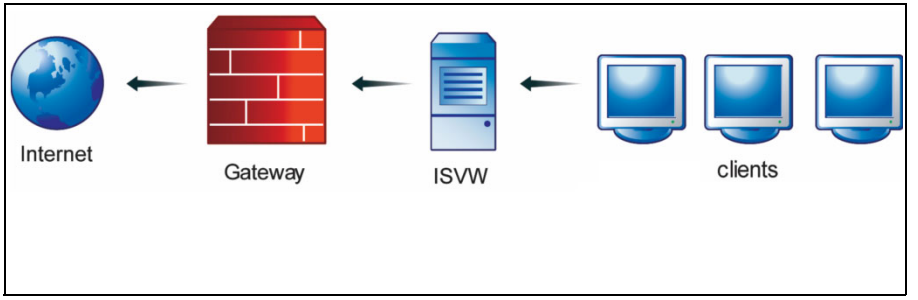


FIGURE 1-19. HTTP topology after installing InterScan VirusWall in standalone mode (without proxy)

HTTP VirusWall Dependent Mode

In dependent mode, InterScan VirusWall is deployed between the client machines and the HTTP proxy server.

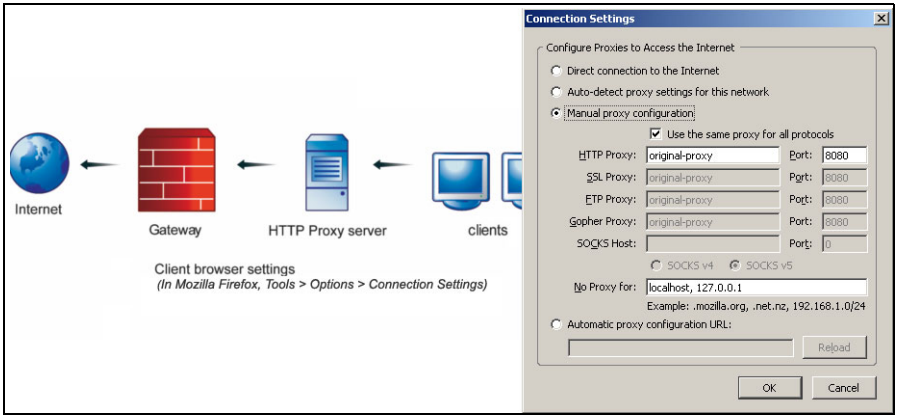


FIGURE 1-20. HTTP topology before installing InterScan VirusWall (with proxy)

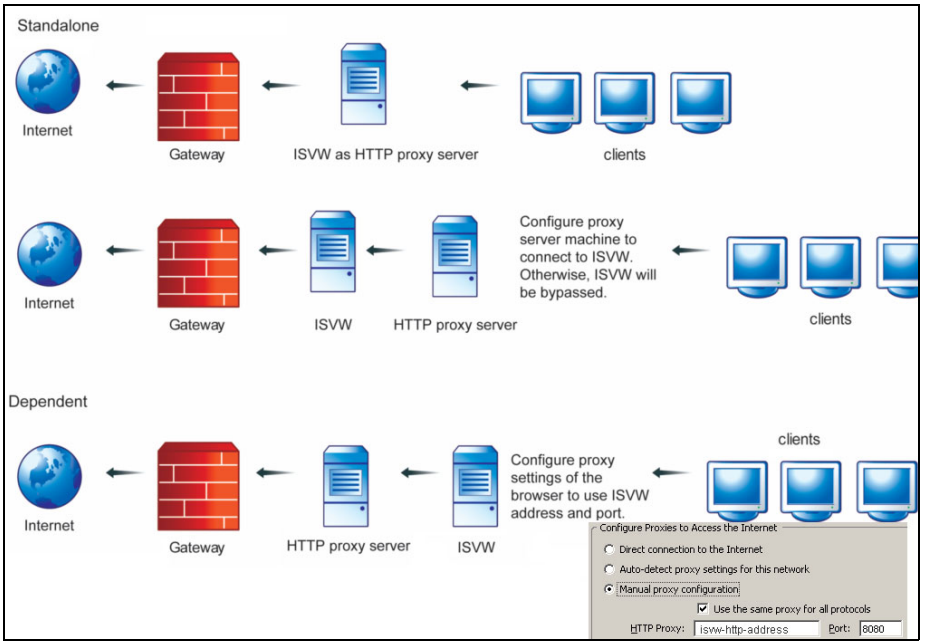


FIGURE 1-21. HTTP topology after installing InterScan VirusWall (with and without proxy)

HTTP Reverse Proxy Mode

In reverse proxy, a content server is made available to outside clients and intranet users but a firewall prevents direct, unmonitored access to the server. This mode is normally used for Web sites involved in e-commerce transactions and distributed applications, which exchange data across the Internet, or for other situations in which clients upload files to the Web server from remote locations. This topology protects the Web server. In this topology, InterScan VirusWall scans HTTP traffic from the content server to the clients within and outside the network.

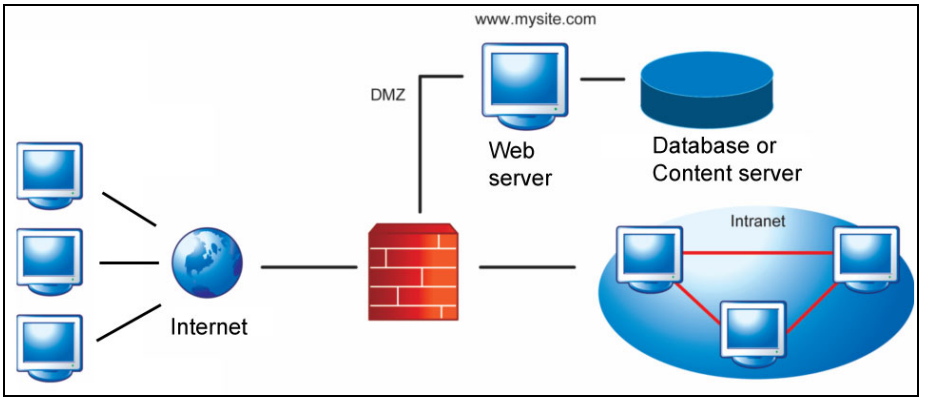
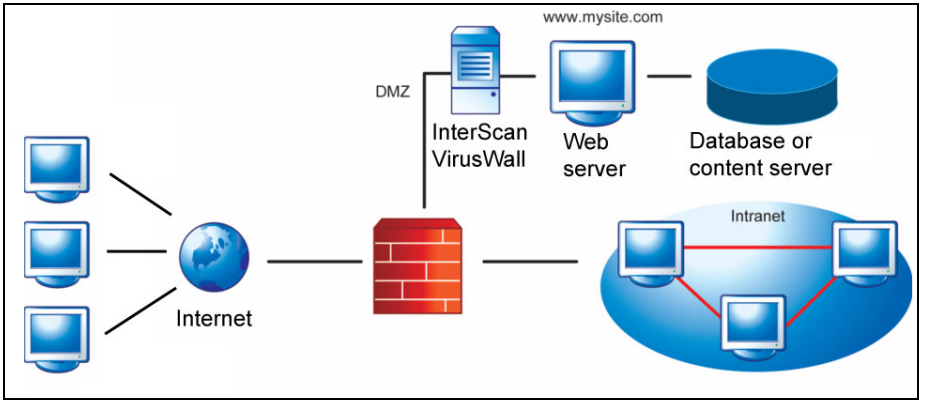


FIGURE 1-22. HTTP reverse proxy mode topology, before installing InterScan VirusWall



HTTP reverse proxy mode topology, after installing InterScan VirusWall

Chapter 2

Installation

This chapter covers the following topics:

Overview

InterScan VirusWall installation takes about 10 minutes and should be performed on the machine where the program(s) will reside. Allow another 10 minutes to configure InterScan VirusWall to work with your existing servers.

InterScan VirusWall provides a migration tool to help existing (InterScan VirusWall for Unix) customers migrate from version 3.81 to version 6.

In this chapter, you will learn about installation planning, the minimum and recommended system requirements, the actual installation process, and key post-installation tasks.

Pre-Installation Checklist

Before installing InterScan VirusWall, complete the following:

☐ **1.** On the machine where you will install InterScan VirusWall, uninstall any version of InterScan VirusWall that is not version 3.8x.

☐ **2.** Either remove any real-time scanning product or add the following items to the product's scanning exclusion list:

- InterScan VirusWall destination path
- Quarantine paths for each of the four protocols (each path must be unique)

☐ **3.** Log on as *root*.

4. Make sure that the following default port numbers are not in use. (Issue `# netstat -an` command to see all ports in use)

- FTP: 21 ☐
- SMTP: 25 ☐
- POP3: 110 ☐
- HTTP: 8080 ☐

Note: For the Web management console, the default port numbers are 9240 for HTTP and 9241 for HTTPS. You can, however, specify different port numbers during installation.

☐ **5.** If you are installing this product for the first time, prepare a list of domains that SMTP VirusWall will recognize as valid domains. SMTP will deliver only inbound emails addressed to these domains.

☐ **6.** If you are upgrading from InterScan VirusWall 3.81 with eManager 3.8 to InterScan VirusWall, enable the following before installation to enable content filter settings after the upgrade:

InterScan eManager Content Management service in InterScan VirusWall for Unix 3.8x **Attachment Filter > Enable attachment filter** option in eManager 3.8

System Requirements

TABLE 2-1. Minimum and recommended system requirements

Requirement	Minimum	Recommended
CPU	1 CPU with Intel™ Pentium™ 4, 1.6 GHz or higher	2 or 4 CPUs with Intel Pentium 4 with Hyper-Threading Technology™, 3.0GHz or higher
Memory	• 512MB RAM, without enabling HTTP VirusWall URL filtering • 1GB RAM, with HTTP VirusWall URL filtering enabled	1GB RAM or higher
Available hard disk space	2GB for the target program drive **Note**: The InterScan VirusWall installation program checks the free disk space on the system and target drives. If your server lacks the minimum disk space, the installation process will not proceed.	20GB for the target program drive for quarantine files and log files
Network interface	10/100/1000 Full Duplex NIC	10/100/1000 Full Duplex NIC
Monitor/Display	1024 x 768 resolution or higher with high color (16 bit)	1024 x 768 resolution or higher with high color (16 bit)
Internet browser to access the Web management console	• Firefox for Linux 1.0 • Firefox for Windows 1.5 • Mozilla 1.7.12 • Netscape browser 8.0.2 • Microsoft™ Internet Explorer 6.0	n/a

TABLE 2-1. Minimum and recommended system requirements (Continued)

Requirement	Minimum	Recommended
Operating system	**Red Hat™ Enterprise Linux (AS, ES, WS) 3.0** with update package 4 • kernel 2.4.21 up • kernel 2.4.21 smp **Red Hat Enterprise Linux (AS, ES, WS) 4.0** with update package 2 • kernel 2.6.9 up • kernel 2.6.9 smp **SuSE™ Linux Professional 9.0** • kernel 2.4.21-99 up • kernel 2.4.21-99 smp **SuSE Linux Professional 9.2** • kernel 2.6.8-24 up • kernel 2.6.8-24 smp **SuSE Linux Enterprise server 9** • kernel 2.6.5-7.97 up • kernel 2.6.5-7.97 smp • kernel 2.6.5-7.139 up (SP1) • kernel 2.6.5-7.139 smp (SP1) • kernel 2.6.5-7.191 up (SP2) • kernel 2.6.5-7.191 smp (SP2) • kernel 2.6.5-7.244 up (SP3) • kernel 2.6.5-7.244 smp (SP3) **SuSE Linux Professional 10.0** • kernel 2.6.13-15 up • kernel 2.6.13-15 smp **SuSE Linux Professional 10.1** • kernel 2.6.16-13-4 up • kernel 2.6.16-13-4 smp **Turbo™ Linux Enterprise Server 8.0** • kernel 2.4.18-5 up • kernel 2.4.18-5 smp **Turbo Linux Enterprise Server 10.0** • kernel 2.6.8-1 up • kernel 2.6.8-1 smp	(n/a)

TABLE 2-1. Minimum and recommended system requirements (Continued)

Requirement	Minimum	Recommended

Libraries	Glibc-2.3.4
	Libstdc++-3.4.4
	Libstdc++-2-libc6.1-1*
	
	The Libstdc++-2-libc6.1-1, resides in different package files for different Linux distributions:
	
	SuSE 10.0 and 10.0 and 9.0 and 9.2
	`compat-2006.1.25-9.i586.rpm`
	(where *2006.1.25-9* is the release version and it varies by distribution)
	
	Turbo Linux 8.0 and 10.0
	`libstdc++-compat-2.10.0-3.i586.rpm`
	(where *2.10.03* is the release version and it varies by distribution)
	
	Red Hat Enterprise Linux 3 and 4
	`compat-lib-stdc++-296-2.96-132.7.2.i386.rpm`
	(where *296-2.96-132.7.2* is the release version and it varies by distribution)
		(N/A)

Installing InterScan VirusWall

There are three installation scenarios. This section addresses only fresh installation. For guidance on upgrading from previous versions, please see Chapter 3, *Migrating from Previous Releases*.

Fresh Install

Use this procedure if you are installing InterScan VirusWall 6 for Linux on a machine with no previous versions and you do not wish to import settings. (See *Performing a Fresh Install* on page 2-7**)**

Upgrade from Version 3.8x on the Same Machine

Use this procedure if you are installing InterScan VirusWall for Linux on a computer that has InterScan VirusWall for Unix 3.81 installed on it and you wish to import settings from version 3.81. (See *Upgrading from Version 3.8x on the Same Machine* starting on page 3-2.)

Upgrade from Version 3.8x on a Different Machine

Use this procedure if you are installing InterScan VirusWall for Linux on a new computer, and migrating settings from another machine that has InterScan VirusWall for Unix 3.81 installed on it. You will use a migration tool to migrate version 3.81 settings and import them during installation. (See *Upgrading from Version 3.8x on a Different Machine* starting on page 3-4.)

Performing a Fresh Install

To perform a fresh installation of InterScan VirusWall:

1. Log on as ***root***.
2. After downloading the tar.gz file, uncompress and un-archive the file by issuing the following command (where #### is the build number of the release):

```
tar xvzf ISVW6_lnx_GM_####.tar.gz
```

3. Tar extracts the following directories and files:

```
./setup.tar.gz
./setup.sh
./isvw.tar.gz
./README.txt
./tool/
./tool/isvw-migration
./ISVW6_lnx_getting_started_guide.pdf
./ISVW6_lnx_ftp_and_pop3_configuration_guide.pdf
./ISVW6_lnx_http_configuration_guide.pdf
./ISVW6_lnx_smtp_configuration_guide.pdf
./ISVW6_lnx_reference_manual.pdf
```

4. Begin the installation by issuing the following command:

```
$ ./setup.sh
```

The following screen appears:

```
      InterScan VirusWall 6 Installer - Main Menu
------------------------------------------------------------------
Welcome to the Trend Micro InterScan VirusWall Installer

Your current system configuration:

InterScan VirusWall -------- [Not installed]

1. Install InterScan VirusWall
2. Exit installation

Enter option number [1]:
```

FIGURE 2-1. Installer main menu

5. To view and approve the license agreement type *1* and press **ENTER** or just press **ENTER**. The following screen appears:

```
       InterScan VirusWall 6 Installer - License Agreement
------------------------------------------------------------------
Trend Micro License Agreement

NOTICE: Trend Micro licenses its products in accordance with
certain terms and conditions. By breaking the seal on the CD
jacket in the Software package or entering a serial number,
registration key or activation code, You already accepted a Trend
Micro license agreement. A courtesy copy of a representative
Trend Micro License Agreement is included for reference below.
The language and terms of the actual Trend Micro license
agreement that you accepted may vary. By clicking "I Accept"
below or using the Software, You confirm Your agreement to the
terms and conditions of the original Trend Micro license
agreement you accepted.

Trend Micro License Agreement (Release Build Version
0403Nov03D021004)

         [Space] = Next screen    [Y|y] = Accept   [N|n] = Decline
```

FIGURE 2-2. InterScan VirusWall 6 license agreement, screen 1

6. After reading the license agreement, select *y* to accept it.

7. Choose what kind of installation you would like to do. Since this topic addresses "fresh install" only, select option *1* from the screen below. (For information on migrating configuration settings, see *Upgrading from Version 3.8x on the Same Machine* on page 3-2 and *Upgrading from Version 3.8x on a Different Machine* on page 3-4).

```
       InterScan VirusWall 6 Installer - Installation Type
------------------------------------------------------------------

Please select an installation type:

1. Install as a fresh installation
2. Install using configuration settings of previously installed
version
3. Exit installation

Enter option number: 1
```

FIGURE 2-3. Installation: Installation Type screen

After you select Fresh Installation, the installer performs a system check:

```
       InterScan VirusWall 6 Installer - System Check
-----------------------------------------------------------------
Checking the system . . .
The Linux kernel verion is [2.6.9-5.EL].

System check completed successfully.

[Enter] = Continue installation   [Ctrl+c] = Exit installation

:
```

FIGURE 2-4. Installation: System Check screen

Activating the Product

InterScan VirusWall can only protect your network fully if you activate the product. Activation is required before the product can receive scan engine and pattern updates and outbreak alerts. You can activate InterScan VirusWall during installation or afterwards, from the InterScan VirusWall Web management console.

Tip: Trend Micro recommends that you activate InterScan VirusWall during installation, so that you get the full protection from this product immediately after it is installed and configured.

To activate InterScan VirusWall during installation:

1. Press Enter at the System Check screen (see figure 2-4, "Installation: System Check screen," on page 2-10). The following screen appears:

```
       InterScan VirusWall 6 Installer - Product Activation
------------------------------------------------------------------

InterScan VirusWall must be activated in order to receive pattern
and engine updates as well as Outbreak Alerts.
Do you have the Activation Code for this product?

[Y|y] = Yes      [N|n] = No      [Ctrl+c] = Exit installation

:
```

FIGURE 2-5. Installation: Product Activation screen

2. If you have your activation code and would like to enter it during installation, type *y* and press **ENTER**. The **`Please enter the Activation Code`** prompt appears.

```
       InterScan VirusWall 6 Installer - Product Activation
------------------------------------------------------------------
Please enter the Activation Code
(Activation Code format: xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx)

[Enter] = Continue installation   [Ctrl+c] = Exit installation

:
```

FIGURE 2-6. Installation: Product Activation screen with prompt to enter Activation Code

3. Type your valid activation code at the command prompt (**:**) and press **ENTER**. The Activation Success screen appears (figure 2-7, "Installation: Activation Success screen," on page 2-12).

```
       InterScan VirusWall 6 Installer - Activation Success
-------------------------------------------------------------------

InterScan VirusWall has been successfully activated. The product
can now receive pattern and engine updates and Outbreak Prevention
Policy alerts.

[Enter] = Continue installation  [Ctrl+c] = Exit installation

:
```

FIGURE 2-7. Installation: Activation Success screen

4. Press **ENTER** to continue. If the password is null, the Administrator Password screen appears (figure 2-8, *Installation: Administrator Password input screen*).

Note: If you do not activate the product during installation, the installer defaults to installing an evaluation version. You can enter the activation code later, through the Web management console (**Administration > Product License**).

Setting an Administrator Password

Before you can use the InterScan VirusWall Web console, you must set an administrator password for it. You can do so at the Administrator Password screen, shown below.

```
 InterScan VirusWall 6 Installer - Administrator Password
-------------------------------------------------------------------

    An administrator password is required to access the InterScan
    VirusWall Web console.


    New password:

    Confirm new password:
```

FIGURE 2-8. Installation: Administrator Password input screen

Preconfiguration Settings

After you enter an administrator password for the Web console, the Installation List screen appears:

```
       InterScan VirusWall 6 Installer - Installation List
-----------------------------------------------------------------

                Web Console addresses:
                   -    HTTP address:   All Interfaces
                   -    HTTP port:      9240
                   -    HTTPS address:  All Interfaces
                   -    HTTPS port:     9241

                Installation path:      /opt/trend

                Administrator password: ********

1. Modify Web console addresses
2. Modify installation path
3. Modify administrator password
4. Continue with installation
5. Exit installation

Enter option number [4]:
```

FIGURE 2-9. Installation: Installation List screen

This screen displays the ports and interfaces that you have chosen for HTTP and HTTPS protocols and the default InterScan VirusWall installation path. As shown in figure 2-9, “Installation: Installation List screen,” on page 2-13, this screen displays the InterScan VirusWall installation path and following information about the Web console:

- HTTP address
- HTTP port
- HTTPS address
- HTTPS port

From this screen you can choose to do the following:

1. Modify Web console addresses
2. Modify installation path
3. Modify administrator password
4. Continue with installation
5. Exit installation

Tip: You can change the administrator password later, from the Web console, but this screen is your last chance within this installation to modify the installation path or the Web console address. To change them later, you would need to re-install.

After you have made any changes to the above settings or have entered *4* to continue with the installation, a screen appears that asks you to select the InterScan VirusWall scanning services. Type *y* and press **ENTER** or just press **ENTER** to enable each of the services that you want this installation of InterScan VirusWall to scan. The screen below shows all four protocol options.

```
       InterScan VirusWall 6 Installer - Preconfiguration
------------------------------------------------------------------
Services Configuration

Type y or n to select the services to enable. (You can also
do this after installation, from the Web console.)

[Ctrl+c] = Exit installation

Enable SMTP scanning? (y/n) [y]:
Enable HTTP scanning? (y/n) [y]:
Enable FTP scanning? (y/n) [y]:
Enable POP3 scanning? (y/n) [y]:
```

FIGURE 2-10. Installation Preconfiguration screen 1, Services Configuration

The next installation screen presents information about relay settings and prompts you to enter a list of domains in your network. InterScan VirusWall will limit incoming mail to only those messages addressed to the domains that you input.

```
       InterScan VirusWall 6 Installer - Preconfiguration
-----------------------------------------------------------------
Relay Settings

This software can act as an SMTP proxy, relaying incoming mail
from any domain to any other.However, leaving inbound and outbound
mail relay settings wide open can allow open-relay abuse by spam-
mers. To prevent this abuse, set InterScan VirusWall to accept
only inbound mail addressed to the domains in your network.
(separate each domain with a semicolon ";")

You can modify this information here or in the Web console,
under SMTP Configuration.

                         [Ctrl+c] = Exit installation

Domains:
```

FIGURE 2-11. Installation: Preconfiguration screen 2, Relay Settings

Tip: Trend Micro strongly recommends that you use the relay control settings, to help prevent spammers from making use of your email server.

Notification Settings

After you enter your internal domains for the anti-relay settings, the following screen appears:

```
      InterScan VirusWall 6 Installer - Preconfiguration
-----------------------------------------------------------------
Notification Settings

InterScan VirusWall requires the following information in order to
send the notification messages by email. You can also modify this
information after installation, in the Web console, under
Administration > Notification Settings.

                         [Ctrl+c] = Exit installation

SMTP server:
```

FIGURE 2-12. Installation: Preconfiguration screen 3, Notification Settings

At the **SMTP server:** prompt, type the address of your SMTP server (for example, *smtp1.mydomain.com* or *11.4.121.121*) and press **ENTER.** The installer records the address and prompts you for the SMTP port and the administrator email address:

```
Port[25]:
Administrator email address (separate multiple entries with a
semicolon (;))
: isvw_administrator@isvw
Sender email address(isvw@mail_sample)
:
```

FIGURE 2-13. Installation: The lower part of the Notification Settings screen, showing prompts for SMTP server port and administrator and sender email addresses

Starting the Installation

After you enter the SMTP port and the administrator email address, a screen appears that asks you to confirm all previous input and start the installation:

```
       InterScan VirusWall 6 Installer - Confirmation
------------------------------------------------------------------

Installer is ready to install InterScan VirusWall.

1. Return to Main Menu
2. Start installation
3. Exit Installation

Enter option number [2]:
```

FIGURE 2-14. Installation: Confirmation screen

Type *2* and press **ENTER** or just press **ENTER** to start the installation. The installer begins copying files and the following screen appears, displaying the percent complete as the installer copies files.

```
 Copying files...

        100%


Starting ISVW6 services:
                                                        [  OK  ]
```

FIGURE 2-15. Installation: Copying files screen

The installer installs InterScan VirusWall using the settings you have entered. After installation completes, the following screen displays:

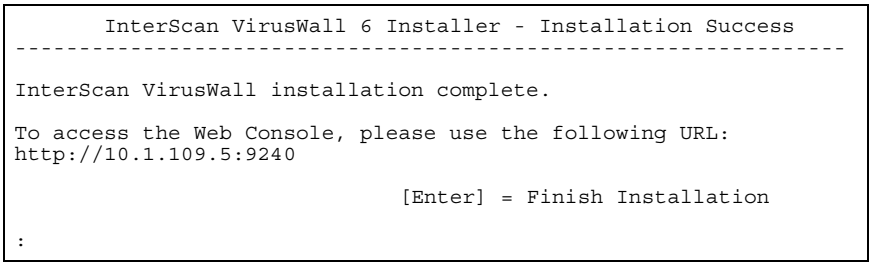


FIGURE 2-16. Installation: Installation Success screen

The URL of the InterScan VirusWall Web management console displays in the Install Success screen. Copy this URL into the address field of a supported Web browser (see *System Requirements* on page 2-4) to view the InterScan VirusWall Web management console.

Tip: Trend Micro recommends that you record the InterScan VirusWall Web console URL for later use before exiting the installation.

Now that InterScan VirusWall is installed, there are several tasks that you need to do through the Web console. The following section discusses those tasks.

Post-Installation Tasks

After installing InterScan VirusWall, you can immediately perform a number of tasks to ensure that everything is set up and working properly.

Note: For instructions on how to accomplish these tasks, refer to the online help or the respective configuration guide (see *table 1, InterScan VirusWall manuals, their content, and where to get them,* on page xi for list of configuration guides).

Post-Installation Checklist

- ☐ **Activate the product** (if not activated during installation)
- ☐ **Enable services** (virus scanning, spam detection, content filtering)
- ☐ **Update components** (pattern files, scan engine) and set update schedule
- ☐ **Configure notifications** (notification server, port, administrator email, and character set)
- ☐ **Configure proxy settings** (depends on which services you are running) See *Configure Proxy Server Settings* on page 2-19 for details.
- ☐ **Configure Outbreak Prevention Policy** (See *Configure Outbreak Alerts* on page 2-20)
- ☐ **Configure Scanning by Protocol** (See *Configure Scanning by Protocol* on page 2-20)
- ☐ **Test Your Installation** (obtain the EICAR test virus and test it on all enabled protocols. See *Testing InterScan VirusWall* on page 4-21)
- ☐ **Add More Instances** (optional) See *Install More Instances* on page 2-21 for details.

Activate the Product

If InterScan VirusWall was not activated during installation, register and activate it now, or begin the 30-day evaluation period.

Enable Services

Enable and then begin virus scanning, spam detection, and content filtering. See the respective configuration guide for the protocol you are configuring:

- *InterScan VirusWall 6 for Linux SMTP Configuration Guide*
- *InterScan VirusWall 6 for Linux HTTP Configuration Guide*
- *InterScan VirusWall 6 for Linux FTP/POP3 Configuration Guide*

All of these manuals are available in Adobe Acrobat™ format (PDF) either on the Solutions CD that came with InterScan VirusWall or from the Trend Micro product download site:

`http://www.trendmicro.com/en/home/us/smb.htm`

Update Components

Update the pattern files and scan engine and set up an update schedule for the virus pattern file, scan engine, and anti-spam rules and engine. (See *Updating InterScan VirusWall Components* on page 4-27 for more information.)

Configure Notifications

Set the notification settings, including the notification server, port, administrator email address, and preferred character set. (See *Notification Settings* on page 4-36 for more information.)

Configure Proxy Server Settings

Adjust the default configuration of the product to meet the needs of your organization. Depending on the services installed and the proxy servers on the system, the following information may be needed when you configure InterScan VirusWall after installation:

- IP address and port number of the current SMTP server
- IP address and port number of the current POP3 server
- IP address and port number of the current HTTP proxy server
- Port that InterScan VirusWall will use if it is set up as the HTTP proxy server
- IP address and port number of the current FTP proxy server
- Port that InterScan VirusWall will use if it is set up as the FTP proxy server

If you need a proxy to connect to the Internet, configure the proxy information for Registration/Activation and ActiveUpdate services. (See *Administration Menu* on page 4-18 for more information.)

Configure Outbreak Alerts

To enable Outbreak Prevention Services (OPS):

1. On the left menu, select **Outbreak Defense** > **Current Status**.
2. Select the **Enable Outbreak Prevention Services (OPS)** check box.
3. Click **Save.**

Configure Scanning by Protocol

If the SMTP protocol is enabled:

- Configure inbound and outbound SMTP traffic.
- Configure policies and notifications for SMTP scanning, IntelliTrap, anti-phishing, anti-spam, anti-spyware, and content filtering.

If the HTTP protocol is enabled:

- Configure your HTTP working mode.
- Configure policies and notifications for HTTP scanning, anti-phishing, anti-spyware, URL blocking and URL filtering settings.

If the FTP protocol is enabled:

- Configure your FTP working mode.
- Configure policies and notifications for FTP scanning and anti-spyware.

If the POP3 protocol is enabled:

- Configure POP3 IP addresses and connections.
- Configure policies and notifications for POP3 scanning, IntelliTrap, anti-phishing, anti-spam, anti-spyware, and content filtering.

Test Your Installation

Obtain the EICAR test file to determine if your installation is working properly.

- If the SMTP protocol is enabled:
  - Test SMTP inbound and outbound scanning.
  - Test SMTP inbound and outbound content filtering.
- If the POP3 protocol is enabled, test POP3 scanning and content-filtering settings.
- If the HTTP protocol is enabled:
  - Test HTTP download and upload scanning.
  - Test HTTP URL blocking and URL filtering.
- If the FTP protocol is enabled, test FTP download and upload scanning.

Install More Instances

Install additional instances of InterScan VirusWall 6 to the network if desired.

A common deployment strategy is to deploy one instance of InterScan VirusWall on the server for each protocol and enable only the relevant scanning service on each server. For example, install one instance of InterScan VirusWall on your:

- SMTP server
- POP3 server
- FTP server
- HTTP server

This approach makes it easier to manage the deployment and conserves the bandwidth of each server.

Chapter 3

Migrating from Previous Releases

This chapter includes the following topics:

Migration Path

There is only one release of this product that can be upgraded to InterScan VirusWall 6. That release is InterScan VirusWall for Unix 3.8x. There is no migration path from InterScan VirusWall 5 for SMB or any other previous release.

Two Methods of Migrating

There are two ways of migrating from version 3.8x to version 6.0. One way is to simply directly install version 6.0 on the same machine on which version 3.8x is installed. (See *Upgrading from Version 3.8x on the Same Machine* on page 3-2.)

However, if you want to install version 6.0 on a machine other than the one on which version 3.8x resides, you can use the migration tool included in this release. The migration tool retrieves the version 3.8x settings and stores them in a settings file for use when installing version 6.0 on another machine. For guidance on using this migration tool, see *Upgrading from Version 3.8x on a Different Machine* on page 3-4.

Upgrading from Version 3.8x on the Same Machine

For this installation type, the first steps are identical to those of a fresh install, as outlined in *Performing a Fresh Install* starting on page 2-7. Follow those instructions to un-tar the binary file, execute the setup command, and view and accept the license agreement. After you have completed those steps, and have issued the `./setup.sh` command, the InterScan VirusWall 6 installation program senses the existence of the previous installation and displays the following screen:

```
      InterScan VirusWall 6 Installer - Upgrade
-----------------------------------------------------------------

An earlier version of InterScan VirusWall is installed on this
system.

Migrate configuration settings from previous version? (y/n) [y]:
```

FIGURE 3-1. Installation: Upgrade screen

Note: If you enter *y*, the old installation (InterScan VirusWall for Unix 3.81) will be completely removed.

Type *y* and press **ENTER** or just press **ENTER** to upgrade from a version 3.8x installation on the same machine.The installation script gets the configuration options from the version 3.8x install and alerts you when it has completed this task:

```
      InterScan VirusWall 6 Installer - Upgrade
------------------------------------------------------------------

An earlier version of InterScan VirusWall is installed on this
system.

Migrate configuration settings from previous version? (y/n) [y]:y
INF: The collection of ISUX 3.x options are done.
```

FIGURE 3-2. Installation: Collecting options from version 3.8x installation

The installer removes the old installation (InterScan VirusWall 3.8x) and then continues as if it were a fresh installation, except that it uses the configuration settings from the previous version. For details of a fresh installation, see *Installing InterScan VirusWall* on page 2-7

Using the Migration Tool for 3.8x

The migration provided enables you to preserve some settings from InterScan VirusWall for Unix 3.8x, as outlined below.

Category	*Settings for*
Protocol settings	FTP, HTTP, and SMTP
Virus scan settings	FTP, HTTP, and SMTP*
eManager	Content filtering, specialized filtering, and notifications
* Except file blocking by file type and outbound mail blocking.	

Protocol Settings Migration

The tool migrates SMTP, FTP and HTTP protocol settings, from ***intscan.ini*** of version 3.8x to ***config.xml*** of version 6.0.

Note: Performance setting is not migrated.

Virus Scan Settings

The migration tool migrates virus scanning settings for SMTP, FTP and HTTP

Note: For SMTP scanning, file blocking by file type and outbound mail blocking cannot be migrated

eManager Settings

The InterScan eManager 3.8 policy will also be migrated if you have installed eManager along with the InterScan VirusWall 3.8x installation.

Note: The only settings that migrate from eManager are those for content filtering, specialized filtering, and notifications.

Migration Tables

For a detailed list of settings that the tool can migrate from version 3.8x, see XREF ("Migration tables" in the *InterScan VirusWall 6 Reference Manual*.) and eManager migration tables.

Upgrading from Version 3.8x on a Different Machine

If you have a previous installation (version 3.8x) installed on another machine, you can use the migration tool that comes with InterScan VirusWall 6 to import many settings from your version 3.8x configuration.

In order to locate the tool, first un-tar the program binary on the target machine for the new installation, as shown below:

```
$ tar xvzf ISVW6_lnx_GM_####.tar.gz
```

The migration tool file name is ***isvw-migration***, and it resides in the ***tool*** directory as shown below:

```
{installation directory}/tool/isvw-migration
```

To migrate version 3.8x settings using the migration tool:

1. Copy the isvw-migration tool (***isvw-migration***) from your target machine to the machine on which InterScan VirusWall 3.8x resides.
2. Log on to the version 3.8x machine as *root.*
3. From that machine, issue the following command:

   ```
   isvw-migration {export_file_name}
   ```

   ...where ***export_file_name*** is the name of a file that the migration tool will create to hold the InterScan VirusWall 3.8x settings temporarily. The tool imports the InterScan VirusWall for Unix 3.8x settings into a file with the name you have provided and displays the following message:

   ```
   # ./isvw-migration export_my_ISVW_3.8_settings.out

   INF: The collection of ISUX 3.x options are done.
   ```

   FIGURE 3-3. Migration tool displays this message upon successful extraction of InterScan VirusWall 3.8x settings

4. Copy this new file on to your target machine for installing InterScan VirusWall 6.0.
5. While logged on to the target machine as *root* start the installation as if it were a fresh install:

   ```
   $ ./setup.sh
   ```

   The following screen appears:

   ```
         InterScan VirusWall 6 Installer - Main Menu
   ------------------------------------------------------------------
   Welcome to Trend Micro InterScan VirusWall Install Script

   Your Current System Configuration:

   InterScan VirusWall ---------- [Not installed]

   1. Install InterScan VirusWall
   2. Exit installation

   Enter option number [default: 1]:
   ```

   FIGURE 3-4. Install script Main Menu

6. To view and approve the license agreement type *1* and press **ENTER** or just press **ENTER**. The following screen appears:

```
      InterScan VirusWall 6 Install Script - License Agreement
------------------------------------------------------------------
Trend Micro License Agreement

NOTICE: Trend Micro licenses its products in accordance with
certain terms and conditions. By breaking the seal on the CD
jacket in the Software package or entering a serial number,
registration key or activation code, You already accepted a Trend
Micro license agreement. A courtesy copy of a representative
Trend Micro License Agreement is included for reference below.
The language and terms of the actual Trend Micro license
agreement that you accepted may vary. By clicking "I Accept"
below or using the Software, You confirm Your agreement to the
terms and conditions of the original Trend Micro license
agreement you accepted.

Trend Micro License Agreement (Release Build Version
0403Nov03D021004)



        [Space]=Continue         [Y|y]=Accept     [N|n]=Decline
        :
```

FIGURE 3-5. InterScan VirusWall 6 license agreement, screen 1

7. After reading the license agreement, select *y* to accept it. The following screen appears:

```
      InterScan VirusWall 6 Install Script - Setup Type
------------------------------------------------------------------

Please select a setup type.

1. Fresh Installation
2. Migrate from configuration settings of previous version
3. Exit installation

Enter option number:
```

FIGURE 3-6. Installation: Setup Type screen

8. Select option `2. Migrate from configuration settings of previous version.` The following screen appears:

```
   InterScan VirusWall 6 Install Script - Migration File
------------------------------------------------------------------
Please input the configuration file
:
```

FIGURE 3-7. Migration File screen

9. Type the full, absolute path and file name of the file that the migration tool created when you ran it on your machine with InterScan VirusWall 3.8x installed, for example:

   `/root/Desktop/export_my_ISVW_3.8_settings.out`

   Press **ENTER** and then press **ENTER** again to continue. The installer imports your settings, performs a system check, and continues the installation using your newly imported settings. (For information on the remaining installation screens, see *Installing InterScan VirusWall* starting on page 2-7.)

Chapter 4

Getting Started

This chapter includes the following topics:

The InterScan VirusWall Web Console

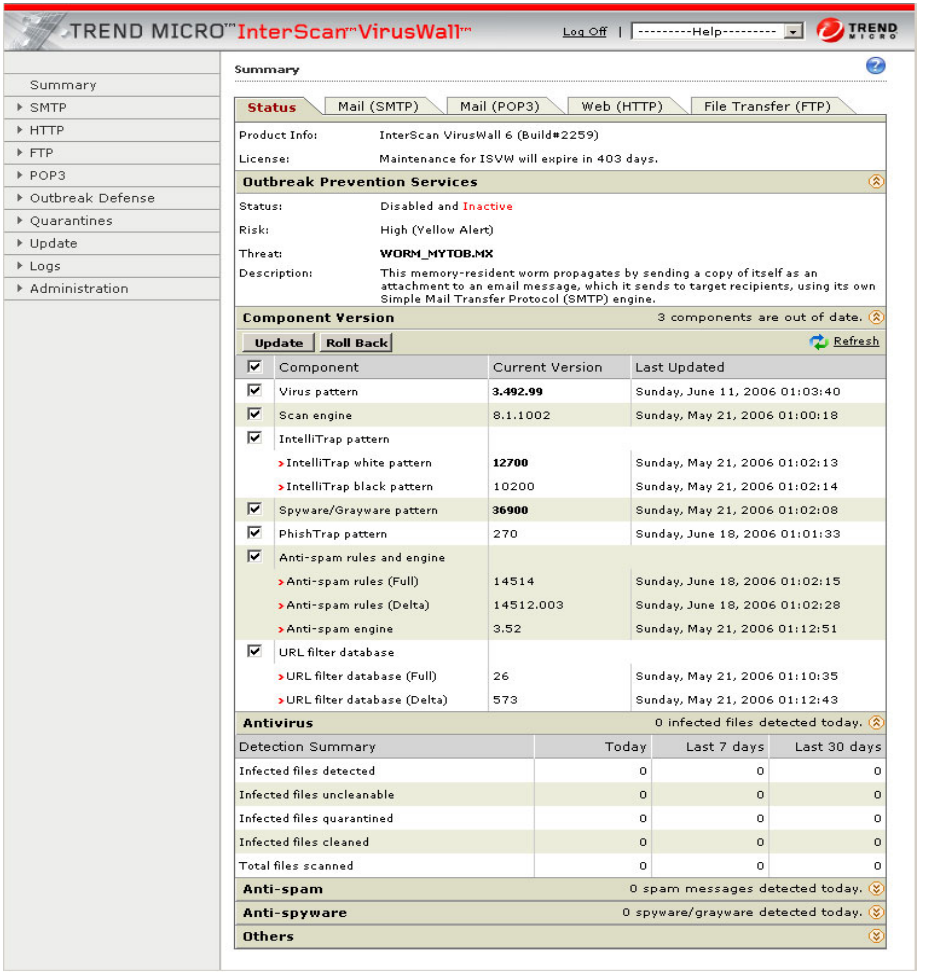


FIGURE 4-1. The InterScan VirusWall Web console Summary screen with the Component Version and Antivirus sections open

The main menu of the Web console consists of 10 menu items. Except for Summary, each of the console's menu items has several submenu items. However, the Summary screen has five tabs—one for each protocol and one status tab. The default Summary screen (Status tab) has six expandable/collapsible horizontal sections:

- Outbreak Prevention Services
- Component Version
- Antivirus
- Anti-spam
- Anti-spyware
- Others

See *Navigating Through the Web Console* on page 4-4 for an overview of the different menu items and the various tasks that you can perform on each submenu screen.

Accessing the Web Console

After installation, InterScan VirusWall automatically starts the basic services and the services that you enabled during installation.

Tip: Although InterScan VirusWall is configured to run on a robust set of default values, Trend Micro recommends that you open the InterScan VirusWall console and confirm the settings the first time you access the Web console for a newly installed instance of the software.

Use any of the following browsers to access the console:

- Firefox for Linux 1.0
- Firefox for Windows 1.5
- Mozilla 1.7.12
- Netscape browser 8.0.2
- Microsoft™ Internet Explorer 6.0

To access the Web console:

1. Open a Web browser, then type the InterScan VirusWall URL followed by the port number that you set during the installation. The default port numbers are 9240 (HTTP) and 9241 (HTTPS).
   - ***http://{your ISVW server IP address}:port number***
   - ***https://{your ISVW server IP address:}port number***

Note: The URL is determined by the IP address and port number that you bound to the Web management console during installation.

2. Type the administrator password that you specified during installation and click **Log On**. The Summary screen of the Web console appears.

Navigating Through the Web Console

This section describes the different menu items in the Web Management console and highlights the tasks that you can perform while navigating the different screens. Refer to the InterScan VirusWall configuration guides for detailed information about how to perform the tasks. The three configuration guides are:

- SMTP Configuration Guide
- HTTP Configuration Guide
- FTP and POP3 Configuration Guide

Summary Screen

The Summary menu item provides a quick overview of the status of InterScan VirusWall and its four services. Clicking Summary opens the Summary screen, with the Status tab preselected. The Summary screen opens by default when you log on to the console.

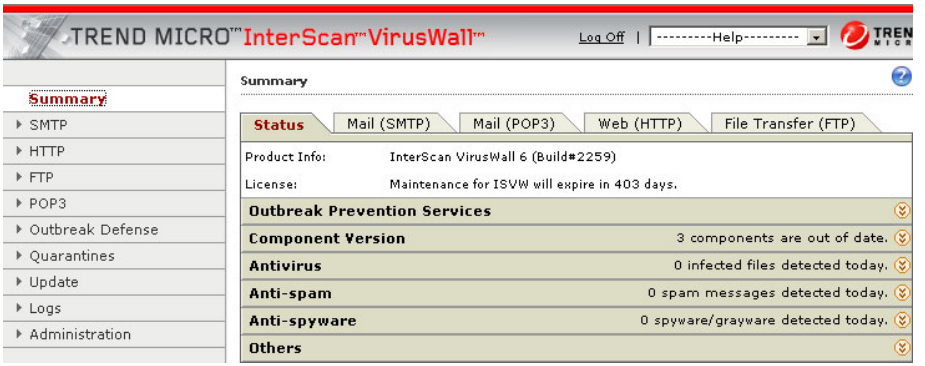


FIGURE 4-2. The Summary screen with all subsections closed

TABLE 4-1. The Summary screen tabs

Tab	Available Information	Tasks
Status	Your product and license information Outbreak Prevention Services status Current versions of pattern files and engines The following statistics: • Files scanned for viruses, spam, spyware/grayware • URLs and content filtered • Files infected with viruses (includes files detected by IntelliTrap) • Spam messages • Spyware/Grayware files • Phishing incidents	Update to the latest versions of InterScan VirusWall components Roll back to the previous versions of pattern files
Mail (SMTP)	Number of viruses, spyware, spam messages, and phishing messages SMTP scanning detected in incoming and outgoing email communication	Enable or disable scanning of SMTP traffic
Mail (POP3)	Number of viruses, spyware, spam messages, and phishing messages POP3 scanning detected in incoming email communication	Enable or disable scanning of POP3 traffic
Web (HTTP)	The following HTTP scanning statistics: • Virus/malware detection • Spyware/Grayware detection • URL blocking/anti-phishing • URL filtering	Enable or disable scannning of HTTP traffic
File Transfer (FTP)	FTP scanning statistics for virus/malware and spyware/grayware detection	Enable or disable scanning of FTP traffic

SMTP

The SMTP menu item allows you to configure SMTP security settings and rules.

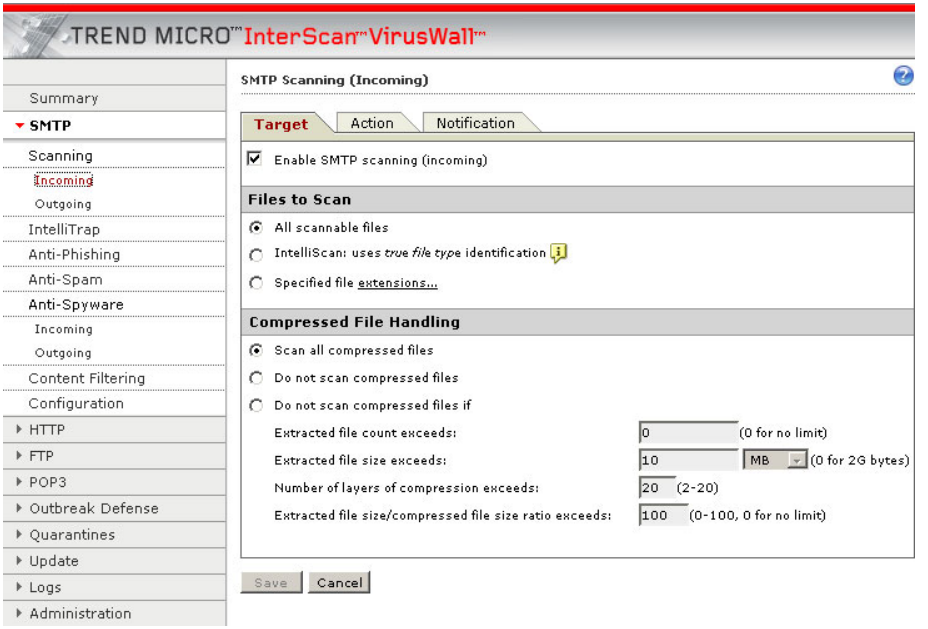


FIGURE 4-3. The SMTP Scanning screen, Target tab

Tip: Note that for malware scanning and anti-spyware scanning there are separate submenus for incoming and outgoing SMTP traffic.

In the SMTP menus, you can select targets, actions, and notifications for malware scanning, anti-phishing scanning, anti-spam scanning, and anti-spyware scanning, and content-filtering of SMTP traffic. You can also fine-tune IntelliTrap compressed-file-scanning and configure how InterScan VirusWall works with your SMTP server.

Tip: For details about using all of the options on these screens, consult the *Trend Micro InterScan™ VirusWall™ SMTP Configuration Guide* (an Adobe Acrobat™ document that comes with this software) or the InterScan VirusWall Online Help.

TABLE 4-2. The submenu items under SMTP

Submenu	Description	Tasks
Scanning (that is, virus/malware scanning)	Provides real-time virus/malware scanning of incoming and outgoing SMTP traffic	Enable or disable SMTP virus/malware scanning Target the attachment types to scan Determine the action to take for infected files (clean, delete, move, or block) For both incoming and outgoing mail, customize the notification sent to specific individuals (administrator, sender, or recipient) or the inline stamp on an email when a virus is detected
IntelliTrap	Detects potentially malicious code in compressed files that can execute automatically	Enable or disable SMTP IntelliTrap Determine the action to take against Bots detected by IntelliTrap (quarantine, delete, or pass) Customize the notification message an administrator, sender, or recipient receives when a heuristic scan detects a security risk in a compressed file
Anti-phishing	Detects phishing attempts in SMTP mail	Enable or disable SMTP anti-phishing Define the action to take for all messages containing links to known phishing sites (quarantine, delete, or deliver message) Customize the notification message the administrator or recipient receives when a phishing message is detected Report a potential phishing URL to TrendLabs

TABLE 4-2. The submenu items under SMTP (Continued)

Submenu	Description	Tasks
Anti-spam	Detects spam messages sent through your SMTP email server	Enable or disable SMTP anti-spam Tune the spam detection rate to Low, Medium, or High, or by category (Commercial, Health, Religion, and so on) Define keyword exceptions (messages containing identified keywords will not be considered spam) or Approved or Blocked Senders by email address or domain names Specify the action to take for spam messages based on their confidence level Customize the notification message an administrator or recipient receives when spam is detected
Anti-spyware	Detects spyware and allows you to perform specific actions upon it	Enable or disable SMTP anti-spyware Specify filenames or filename extensions that will be excluded from spyware search Search for spyware/grayware Target the kind of spyware/grayware you wish to scan Determine the action to take against spyware (Quarantine, Delete, or Pass) Automatically notify selected recipients whenever spyware is detected during SMTP scanning
Content Filtering	Provides real-time monitoring and control of information that enters or leaves the network via the SMTP server	Enable or disable SMTP Content Filtering Specify keyword and attachment filters to evaluate and control the delivery of email messages on the basis of the message content itself

TABLE 4-2. The submenu items under SMTP (Continued)

Submenu	Description	Tasks
Configuration	Allows you to configure the way the InterScan VirusWall server—as a proxy server—routes incoming and outgoing mail through your SMTP server, while defining certain limits and constraints	Specify the main service port Specify how InterScan VirusWall forwards inbound mail and delivers outbound mail Track processed messages Queue inbound or outbound mails Configure the number of simultaneous client connections, size of inbound/outbound messages, frequency of message sending attempts, and other advance settings

HTTP Menu

The HTTP menu item provides you with features to help maintain HTTP gateway security.

In the HTTP menus, you can select targets, actions, and notifications for malware scanning, anti-phishing scanning, anti-spyware scanning of HTTP traffic. You can also set up URL blocking and filtering rules and policies and configure how InterScan VirusWall works with your HTTP server. For details about using all of the options on these screens, consult the *InterScan™ VirusWall™ HTTP Configuration*

Guide (an Adobe Acrobat™ document that comes with this software) or the InterScan VirusWall Online Help.

TABLE 4-3. The submenu items under HTTP

Submenu	Description	Tasks
Scanning	Lets you determine how InterScan VirusWall scans HTTP traffic for viruses and other security risks in uploads and downloads	Enable or disable HTTP scanning Target the types of files to scan List MIME Type Exceptions Specify how InterScan VirusWall handles large files to prevent performance issues and browser timeouts Determine actions for infected files (Clean, Quarantine, Block, or Pass) Customize the message in the user's browser when InterScan VirusWall detects an infected file
Anti-phishing	Lets you determine how InterScan VirusWall handles phishing attempts initiated while browsing the Internet	Enable or disable HTTP anti-phishing Set categories to block URLs (for example, phishing, spyware, virus accomplice, and disease vector sites) Define actions for all known phishing sites (block or allow) Customize the message in the user's browser when a known phishing site is detected Submit a potential phishing URL to TrendLabs
Anti-spyware	Scans HTTP traffic to detect many types of malware uploads and downloads	Enable or disable HTTP anti-spyware Create exclusion lists for spyware/grayware Search for spyware/grayware Target the kind of spyware/grayware to scan Set the action to take when spyware/grayware is detected (block, quarantine, or allow) Customize the message in the user's browser when spyware/grayware is detected

TABLE 4-3. The submenu items under HTTP (Continued)

Submenu	Description	Tasks
URL Blocking	Blocks access to Web sites with undesirable content via a user-configured list Allows access to certain URLs by adding them to an exception list	Enable or disable HTTP URL blocking Define "matching" URL lists (defined via Web site, URL keyword, IP address, or string), one for URLs that will be blocked, and another for URLs excluded from blocking Import lists of blocked or exempted sites Customize the message in the user's browser when a blocked URL is accessed
URL Filtering Rules	Lets you set the rules by which URL categories are filtered	Enable or disable HTTP URL filtering Set the time when the rules apply (during work time, during leisure time)
URL Filtering Settings	Defines how URL filtering is applied across the URL Categories in the InterScan VirusWall database.	Move a URL subcategory to another category (for example, Adult/Mature Content from "Company Prohibited Sites" to "Not Work Related") Create or import URL Filtering Exception lists matched by Web site, URL keyword, or string, even though the URL is classified in a prohibited content category Designate the day and time the settings apply Submit a URL to TrendLabs for reclassification
Configuration	Configures settings for your HTTP scanning service	Determine if you want InterScan VirusWall to operate in standalone, dependent, or reverse proxy mode Specify the HTTP listening port Specify anonymous FTP over a specified HTTP logon email Allow logging of HTTP requests

FTP Menu

The FTP menu item provides you with features to help secure file transfers to and from your FTP server.

In the FTP menus, you can select targets, actions, and notifications for malware scanning and anti-spyware scanning of FTP traffic. You can also configure how InterScan VirusWall works with your FTP server. For details about using all of the options on these screens, consult the *InterScan™ VirusWall™ FTP/POP3 Configuration Guide* (an Adobe Acrobat™ document that comes with this software) or the InterScan VirusWall Online Help.

TABLE 4-4. The submenu items under FTP

Submenu	Description	Tasks
Scanning	Checks all or specified types of files for viruses and other malware, including individual files within a compressed volume	Enable or disable FTP scanning Determine the files you want to scan Designate if and how attached compressed files are scanned Specify the action to take on infected files (clean, quarantine, block, or pass) Customize the notification message an administrator or user receives when an infected file is detected
Anti-spyware	Records settings for the scanning of spyware/grayware during FTP file transfers	Enable or disable FTP anti-spyware Create an Exclusion list for spyware/grayware Search for spyware/grayware Scan for spyware/grayware according to specific categories Determine the action to take when spyware/grayware is detected (block, quarantine, allow) Customize the message to display in the user's browser when FTP VirusWall detects spyware/grayware.

TABLE 4-4. The submenu items under FTP (Continued)

Submenu	Description	Tasks
Configuration	Configures FTP VirusWall to work with your FTP server	Choose between standalone or FTP proxy mode • Choose standalone mode if there is no FTP proxy server on the network and you want FTP VirusWall to serve as the system's FTP proxy server. • Choose FTP proxy if there is an existing FTP proxy server that you want to continue using. Enable PASV mode and specify the FTP service port Determine the maximum connections allowed Designate the number of bytes to send versus those received (to prevent browser timeouts) Customize the greeting to send when connection is established

POP3 Menu

The POP3 menus are similar to the SMTP menu items, except that for POP3, the Scanning and Anti-Spyware submenus are not subdivided into incoming and outgoing.

In the POP3 menus, you can select targets, actions, and notifications for malware scanning, anti-phishing scanning, anti-spam scanning, anti-spyware scanning, and content-filtering of POP3 traffic. You can also fine-tune IntelliTrap true file type matching and configure how InterScan VirusWall works with your POP3 server. For details about using all of the options on these screens, consult the *InterScan*™

VirusWall™ FTP/POP3 Configuration Guide (an Adobe Acrobat™ document that comes with this software) or the InterScan VirusWall Online Help.

TABLE 4-5. The submenu items under POP3

Submenu	Description	Tasks
Scanning (that is, virus/malware scanning)	Provides real-time virus/malware scanning of POP3 traffic	Enable or disable POP3 virus/malware scanning Determine the attachments to scan Designate if and how attached compressed files are scanned Determine the action to take for infected files (clean, delete, move, or block) Customize the notification sent to specific individuals (administrator or recipient) or the inline stamp on an email when a virus is detected
IntelliTrap	Detects potentially malicious code in compressed files that can execute automatically	Enable or disable POP3 IntelliTrap Take action on Bots detected by IntelliTrap (quarantine, delete, or pass) Determine the action to take against Bots detected by IntelliTrap (quarantine, delete, or pass) Customize the notification message an administrator or recipient receives when a heuristic scan detects a security risk in a compressed file
Anti-phishing	Detects phishing attempts in POP3 mail	Enable or disable POP3 anti-phishing Define the action to take for all messages containing links to known phishing sites (quarantine, delete, or deliver message) Customize the notification message the administrator or recipient receives when a phishing message is detected Report a potential phishing URL to TrendLabs

TABLE 4-5. The submenu items under POP3 (Continued)

Submenu	Description	Tasks
Anti-spam	Detects spam messages sent through your POP3 email server	Enable or disable POP3 anti-spam Tune the spam detection rate to Low, Medium, or High, or by category (Commercial, Health, Religion, and so on) Define keyword exceptions (messages containing identified keywords will not be considered spam) or Approved or Blocked Senders by email address or domain names Customize the notification message an administrator or recipient receives when spam is detected
Anti-spyware	Detects incoming spyware and allows you to perform specific actions upon it	Enable or disable POP3 Anti-spyware Specify filenames or filename extensions that will be excluded from spyware search Search for spyware/grayware Target the kind of spyware/grayware you wish to scan Determine the action to take against spyware (quarantine, delete, or pass) Automatically notify selected recipients whenever spyware is detected during POP3 scanning
Content Filtering	Provides real-time monitoring and control of information that enters or leaves the network via the POP3 server	Enable or disable POP3 Content Filtering Specify keyword and attachment filters to evaluate and control the delivery of email messages on the basis of the message content itself
Configuration	Allows you to configure the way the InterScan VirusWall's POP3 proxy server handles POP3 traffic	Specify the POP3 IP address that the InterScan VirusWall POP3 proxy server binds to Specify the number of simultaneous local connections allowed, the port POP3 clients will use to connect to InterScan VirusWall (the default port is 110), and the settings for secure password authentication

Outbreak Defense

Trend Micro provides Outbreak Prevention Services (OPS) to help you contain a threat while TrendLabs is developing a solution.

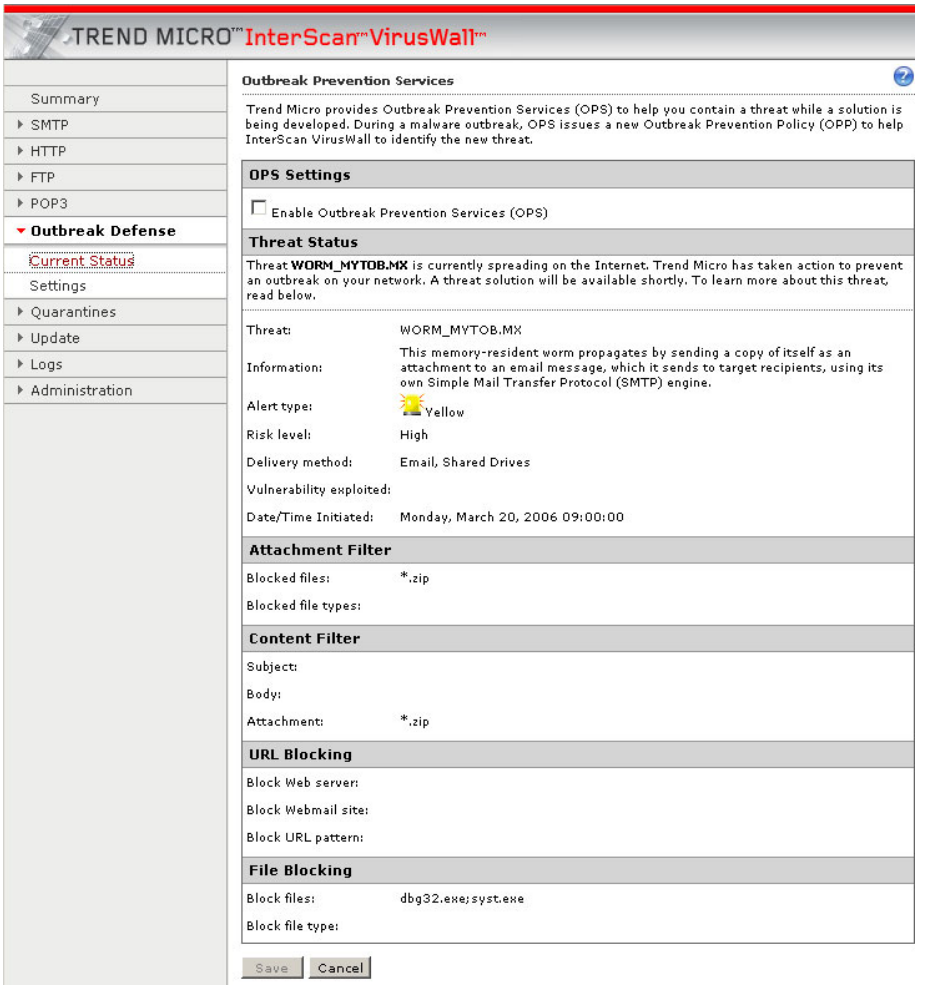


FIGURE 4-4. The Outbreak Defense Current Status screen

TABLE 4-6. The submenu items under Outbreak Defense

Submenu	Description	Tasks
Current Status	Informs you of the active OPS policies being enforced	Enable or disable OPS View the OPS status
Settings	Lets you view and modify OPS settings	Manually change the default expiration time of OPS policies

For a more thorough discussion of Outbreak Prevention Services, see the *Trend Micro InterScan VirusWall 6 for Linux Reference Manual*.

Administration Menu

Use the Administration menu to manage the notification settings, password, license, and proxy settings of your InterScan VirusWall installation.

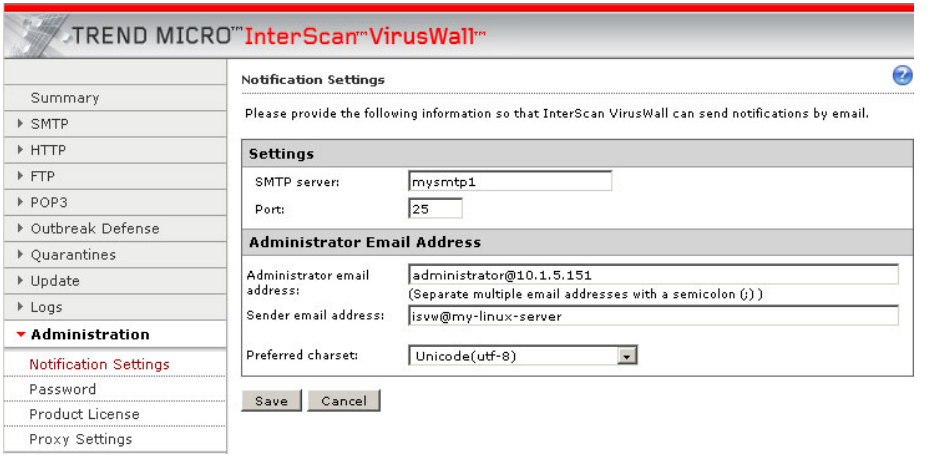


FIGURE 4-5. The Administration >Notification Settings screen

Use the submenus of the Administration menu for a variety of purposes, including:

- Supplying mail server and email address information so that InterScan VirusWall can send out administrator notifications
- Changing the administrator password
- Activating the product or renewing the product license
- Modifying proxy settings

TABLE 4-7. The submenu items under Administration

Submenu	Description	Tasks
Notification Settings	Determines the settings that will be used when sending email notifications from InterScan VirusWall	Specify the following settings: • SMTP server • Port • Administrator email address • Preferred character set for receiving notifications
Password	Allows you to change the password you use to log on to InterScan VirusWall	Specify the old password, the new password, and a new password confirmation to change your current password
Product License	Displays information about your maintenance agreement and product license for InterScan VirusWall	View license upgrade instructions View license online Enter a new Activation Code Update the information on the screen
Proxy Settings	If using a proxy server to connect to the Internet, lets you specify the settings used to update the pattern file, engine, and license	Enable or disable the proxy server Determine the proxy settings Test your connection

Starting and Stopping InterScan VirusWall

By default, all InterScan VirusWall services that you selected during installation are automatically started following installation. You can enable or disable each service individually through the Summary screen of the Web console.

In certain circumstances—such as when you have made a change to a configuration file and you want for the change to take effect so that you can observe the result—you may wish to restart all services simultaneously.

To restart all services:

1. Log on as ***root*** on the computer on which your instance of InterScan VirusWall resides.
2. Issue the following command:

   ```
   # /etc/init.d/isvw6 restart
   ```

   The Linux machine stops and restarts all InterScan VirusWall services.

You can also stop the main InterScan VirusWall service from the command line.

To stop the InterScan VirusWall service:

1. Log on as ***root*** on the computer on which your instance of InterScan VirusWall resides.
2. Issue the following command:

   ```
   # /etc/init.d/isvw6 stop
   ```

   The InterScan VirusWall service stops.

WARNING! *If you stop the InterScan VirusWall service, InterScan VirusWall will no longer be scanning network traffic.*

Testing InterScan VirusWall

After installation, test your InterScan VirusWall installation to become familiar with the configuration and see how the program works. This section provides instructions for testing the antivirus and content-filtering features.

Antivirus Testing Using the EICAR Test Virus

The European Institute for Computer Antivirus Research (EICAR) has developed a test "virus" that you can use to test your InterScan VirusWall installation and configuration. The test virus is an inert text file whose binary pattern is included in the virus pattern file of most antivirus vendors. It is *not* a virus and does not contain any program code. It will cause no harm and will not replicate.

Once the EICAR test virus is on your machine, you can use the test virus to simulate a virus infection. You can then observe the virus clean/deletion features of InterScan VirusWall. InterScan VirusWall will take action on the EICAR test file, a zipped EICAR test file, and an EICAR test file that is zipped twice. The incident will be logged in the SMTP Virus Log.

In the following section, you will test the antivirus capability of the SMTP VirusWall. Once familiar with SMTP VirusWall testing, you can proceed and test the scanning services of the other protocols (HTTP VirusWall, FTP VirusWall, and POP3 VirusWall).

To obtain the test virus, do either of the following:

- Download the file from the following URLs:
  - http://www.trendmicro.com/vinfo/testfiles/
  - www.eicar.org/anti_virus_test_file.htm

  Note: You can also download a zipped EICAR test file (eicar_com.zip), and an EICAR test file zipped twice (eicarcom2.zip) from the EICAR Web site.

  - OR -

- Create your own EICAR test virus by typing the following into a text file and then naming the file `eicar.com`:

  ```
  X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FI
  LE!$H+H*
  ```

To test InterScan VirusWall using the EICAR test virus:

1. Send an email message with the eicar.com, eicar_com.zip, and eicarcom2.zip files enclosed. Use the email client you designated to send email.
2. Receive the email. Use the email client (or its equivalent) that you designated to receive email.

   When you open an attachment, you will get a message indicating that it is not cleanable and was therefore deleted.
3. Check the SMTP Virus Log.

   a. Open the Web console and click **Logs** > **Query**. The Log Query screen appears.

   b. Select the following drop-down menu settings:

   - Protocol: SMTP
   - Log type: Virus/Malware
   - Time period: All

   c. Click **Display Log**. The SMTP Virus Log screen appears.

   d. Review the details for the test virus log entries.

Testing Content Filtering

Test the SMTP content-filtering feature by sending an email message whose subject and message body contain a keyword that you have set as a trigger for blocking. SMTP VirusWall will quarantine the message and will log the incident in the SMTP Keyword Filter Log.

Note: After testing SMTP content filtering, you can test the POP3 content-filtering feature by using the same method.

To test the content-filtering feature:

1. In the Web console, click **SMTP > Content Filtering**. On the **Target** tab, go to the Keywords section, type "sex", and click **Add**. InterScan VirusWall adds the keyword "sex" to the list on the right.
2. Send an email message with the word "sex" in the **Subject** and **Message** fields. Use the email client you designated to send email, or its equivalent.

   For example:

   To: jane@trendsmb.com

   Subject: Sex in "Last Tango in Paris"

   Message field:
   Hello Jane,
   "Last Tango in Paris" is a sexually explicit film.

   Best regards,
   John

3. Receive the email message. Use the email client you designated to receive email, or its equivalent.

   The email will not appear because it has been filtered.

4. Check the SMTP Keyword Filter Log.

   a. Open the Web management console and click **Logs > Query**. The Log Query screen appears.

   b. Select from the following popup menu settings:

      - Protocol: SMTP
      - Log type: Keyword Filter
      - Time period: All

   c. Click **Display Log**. The SMTP Keyword Filter Log screen appears.

   d. Review the details for the content-filtering log entries, specifically entries in the Subject column with the term "sex".

5. Query the InterScan VirusWall quarantine.

   a. In the Web management console, click **Quarantines** > **Query**. The Quarantine Query screen appears.

   b. Under Criteria, narrow down your query by typing the date you sent the test email, the email address of the sender in step 1, the email address of the recipient in step 2, and "sex" as the subject.

   c. Click **Query**.

      The Quarantine Query Results panel shows the date and time the email was quarantined, the sender and recipient email addresses, the subject of the email, and the reason it was quarantined.

Using the Real-Time Performance Monitor

InterScan VirusWall comes with a command-line performance monitoring tool. You can use it to view the number of processes, threads, connections, process start time, and requests per minute for SMTP, HTTP, and POP3 protocols. For FTP, you can use the performance monitor to view the master process ID, number of child processes, start time, and the following information for each child process:

- Number of active connections
- Number of available connections
- Scanned files per minute
- Start time (of the child process)

To start the performance monitor:

1. Log in as ***root*** on the computer on which your instance of InterScan VirusWall is installed.
2. Navigate to the `/perform/` subdirectory in the InterScan VirusWall installation directory. For example, if you used the default installation path, the path would be the one shown below:

   ```
   /opt/trend/isvw6/perform
   ```

3. Verify that you are in the correct directory by issuing an **ls** command. If the file ***isvw-perform*** appears in the file list, you are in the correct directory.
4. Issue the following command to start the performance monitor:

   ```
   # watch "./isvw-perform"
   ```

5. Press **CTRL-C** to stop the performance monitor.

The performance monitor loads. Figure 4-6. shows sample output of the performance monitor.

```
               *** InterScan VirusWall 6 - Performance Monitor ***

*** SMTP/POP3/HTTP Services ***

Service    Process    Threads    Connections     Requests        Start Time
           ID                                    (per min.)
================================================================================
SMTP(on)   4267       20         0               0               06/27/06 18:09:03
POP3(on)   4268       20         0               0               06/27/06 18:09:03
HTTP(on)   4289       14         -               0               06/27/06 18:09:03


*** FTP Service ***

Service              Master               Child                Start Time
                     Process ID           Processes
================================================================================
FTP(on)              4303                 2                    06/27/06 18:09:02

Child           Active          Available       Scanned         Start Time
Process ID      Connections     Connections     Files(per min.)
================================================================================
14276           1               5               4               06/27/06 18:09:02
14277           1               5               0               06/27/06 18:10:48
--------------------------------------------------------------------------------
Total:          2               10              4
```

FIGURE 4-6. Sample Performance Monitor output

Updating InterScan VirusWall Components

Because new malicious programs and potentially offensive Web sites are developed and launched daily, InterScan VirusWall provides both on-demand and automated methods to keep your software updated with the latest pattern files, scan engines, and URL filtering database, without interrupting your network services or requiring you to reboot your computers. InterScan VirusWall does this by polling the InterScan VirusWall ActiveUpdate server directly, and then downloading the updates either manually or on a schedule.

Note: You can only update components if you have activated InterScan VirusWall or if the product is within its 30-day evaluation period.

As new viruses and other Internet threats are written, released to the public, and discovered, Trend Micro collects their tell-tale signatures and incorporates the information into the virus and other pattern files.

Trend Micro updates the file as often as several times a week, and sometimes several times a day when people release multiple variants of a widespread threat. By default, InterScan VirusWall checks for updates at least once a week. If a particularly damaging virus is discovered “in the wild,” or actively circulating, Trend Micro releases a new pattern file as soon as a detection routine for the threat is available (usually within a few hours).

Update Submenu Items

In the left-side menu there are two submenus under Update. Use the Manual Update screen to update InterScan VirusWall components immediately after you install the product or any time on demand. Use the Scheduled Update screen to set a schedule for automatic updates of InterScan VirusWall components.

TABLE 4-8. The submenus under Update

Submenu	Description	Tasks
Manual	Update your components on demand	Select the components to update Roll back selected components to the previous update
Scheduled	Schedule a regular interval for updating InterScan VirusWall components	Enable or disable the scheduled update function Select the components to update Set an update schedule

Components That You Can Update

Table 4-9 lists and describes the seven kinds of InterScan VirusWall components that you can update.

TABLE 4-9. Components that InterScan VirusWall can update, their descriptions, and example files

Component	Description	Example file
Virus pattern	The collection of the latest patterns of virus/malware that Trend Micro knows of.	lpt$vpn.755
Scan engine	The (virus) scan engine is the component that performs virus/malware scans. The rollback function does not apply to scan engines.	libvsapi.so
Spyware pattern	The collection of the latest patterns of spyware/grayware programs that Trend Micro knows of.	tmaptn.275
IntelliTrap pattern		
white list (IntelliTrap pattern)	The latest list of patterns of malware in compressed files.	tmwhite.101
black list (IntelliTrap exception pattern)	The latest list of compressed files known to not contain malware. (An exception list.)	tmblack.102
PhishTrap pattern	The latest list of phish sites known to Trend Micro	PhishB.ini

TABLE 4-9. Components that InterScan VirusWall can update, their descriptions, and example files (Continued)

Component	Description	Example file
Anti-spam rules and engine		
rule, full	The latest full list of anti-spam rules file	tm013974.rul tm013974.sig tm013974.phi tm013974.hsh tm013974.exp
rule, delta (incremental update)	The latest incremental update of the anti-spam rules file. (see *Incremental and Full Updates* on page 4-30)	tm013972.sig tm013972.phi tm013972-000001.hsh tm013972.exp
engine	The latest anti-spam rules and engine.	libtmaseng.so
URL filter database		
full database	The latest full database of URLs associated with potential filtering categories	ratings.rat
delta database (incremental update)	The latest incremental update of the database of URLs associated with potential filtering categories	ratings.tst

Incremental and Full Updates

ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update Web site, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, and program files via the Internet or the Trend Micro Total Solution CD.

ActiveUpdate supports incremental (delta) updates of anti-spam rules and engines and the URL filter database. Rather than download the entire file each time, ActiveUpdate can download only the portion of the file that is new and append it to the existing component file. This efficient update method can substantially reduce the bandwidth needed to update your deployment of InterScan VirusWall and deploy pattern files throughout your environment.

Note: You cannot configure or roll back incremental (delta) updates. The time, date, and pattern number information for those updates are listed only for your reference.

Updating Components Manually

There are two ways to update components manually:

- From the Manual Update screen
- From the Summary screen

Using the Manual Update Feature

From the left-side menu, click **Update > Manual** to display the Manual Update screen. The Web console displays the pattern number of an outdated pattern in bold red, as shown in figure 4-7 below.

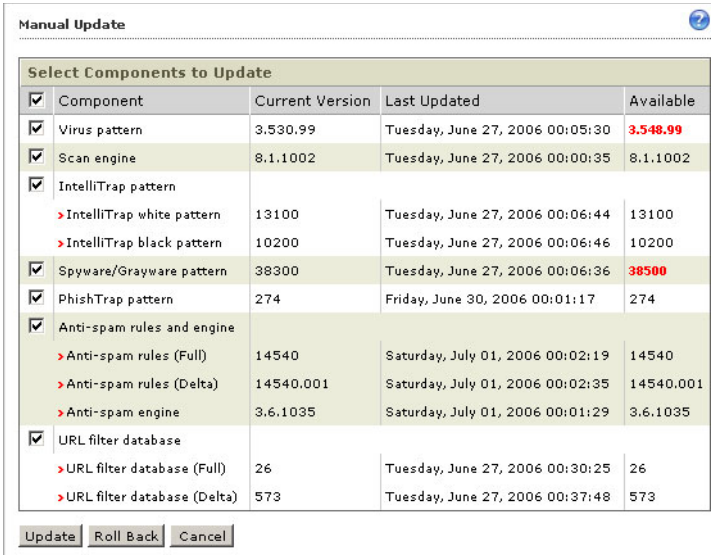


FIGURE 4-7. Manual Update screen detail showing two out-of-date components

Update All Outdated Components

By default, all component check boxes contain a check mark when the Manual Update page loads. To update any component that is out of date (that is, any component whose last column contains a pattern version number in bold, red font), simply click **Update**. There is no need to deselect check boxes.

Rolling Back Patterns

From the Manual Update screen you can also roll back any pattern in the unlikely event that it may be causing some kind of problem. Note that you can roll back only one pattern at a time.

Note: Only pattern files can be rolled back. Engines cannot.

To roll back a pattern to its previous version:

1. From the left-side menu, click **Update > Manual.** The Manual Update screen appears.
2. Deselect all components except for the pattern to roll back. (You can deselect the check box at the top of the table, to the left of the Component column head, to deselect all components simultaneously.)
3. After verifying that only the one pattern to roll back remains selected, click **Roll Back.** InterScan VirusWall rolls back the pattern to the previous version.

Using the Summary Screen to View and Update Components

The second way to manually update components is to do so from the Summary screen. The steps are very similar to those described above for updating from the Manual Update screen. As on the Manual Update screen, there is both an update function and a rollback function on the Summary screen, however the buttons for these functions appear at the top of the section. The main differences are the appearance of the tables on the two screens and how the screens are structured, as illustrated by figure 4-8, *Summary (top) and Manual Update (bottom) screens comparing component update sections*.

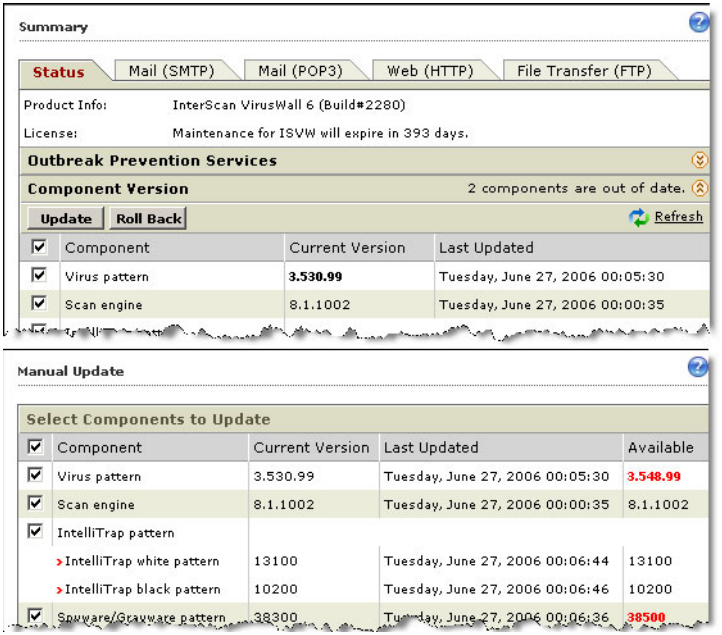


FIGURE 4-8. Summary (top) and Manual Update (bottom) screens comparing component update sections

To manually update components from the Summary screen:

1. On the left-side menu, click **Summary.** The Summary screen appears.
2. If the Component Version section is not already open, then click the expand/collapse icon () for that section. The Component Version section opens, showing in black boldface font the version number of any component in need of updating.
3. Select the components to update and then click **Update.** InterScan VirusWall performs the manual update.

The procedure for rolling back a pattern in the Summary screen is identical to that for the Manual Update screen (see *Rolling Back Patterns* on page 4-32). The main difference in appearance between the two screens is the location of the **Roll Back** button.

Scheduling Updates

The second method of updating components is to set a schedule for automatic updates. More precisely, automatic *checking for* updates. That is, InterScan VirusWall can regular contact the ActiveUpdate server to see if any components are in need of updating (that is, out of date). If any component needs updating, the scheduled update feature performs the update.

To schedule automatic updates:

1. On the left-side menu, click **Update > Scheduled.** The Scheduled Update screen appears.
2. Select the **Enable Scheduled Updates** check box.
3. Select the components to automatically update.

Tip: Trend Micro recommends selecting all seven kinds of updates.

---

4. In the Update Schedule section, select the frequency and time of automatic update checking. Options for frequency are:

   - Minute(s)
   - Hour(s)
   - Day(s)
   - Week, on

   The field to the right of these options is dynamic. It changes to reflect the appropriate option to match the choice you make on the left side. Table 4-10 shows the appearance of the right-side options for each of the various options for frequency.

TABLE 4-10. Scheduled update options for frequency and time of update

Frequency option	Right-side options
Minute(s)	15 minute(s)
Hour(s)	1 hour(s)
Day(s)	1 day(s) at 00 : 00 (hh:mm)
Week, on	Sunday at 00 : 00 (hh:mm)

5. Click **Save.**

Tip: Trend Micro recommends that you set your automatic updates to run during periods of low demand for bandwidth.

Setting Up InterScan VirusWall for Use with ActiveUpdate

You can configure scheduled updates to communicate with the main Trend Micro ActiveUpdate server or through a proxy server. If you use a proxy server, follow the procedure below to set up InterScan VirusWall for automatic updates through that server.

To set up InterScan VirusWall to access updates through a proxy server:

1. On the left-side menu, click **Administration > Proxy Settings.** The Proxy screen appears.
2. Select the check box next to **Use a proxy server for pattern, engine, and license updates.** The remaining fields become active.

3. Choose your proxy protocol from the following options:
   - HTTP
   - SOCKS4
   - SOCKS5
4. In the **Server name or IP address** field, type the host name or IP address of your proxy server.
5. Modify the port in the port field or accept the default of 8080.
6. If your proxy server uses authentication, type the user ID and password in their respective fields in the **Proxy server authentication** section.
7. Click **Test Connection** to test the authentication to ensure that InterScan VirusWall has all the necessary credentials. InterScan VirusWall verifies that it can contact the server using authentication.
8. Click **Save.**

Notification Settings

Before InterScan VirusWall can sends notifications of any type, it must have enough information about your mail server in order to use it. You can provide this necessary information in two ways:

- During installation (see *Notification Settings* on page 2-15)
- Through the Web console

To provide mail server information for notifications in the Web console:

1. On the left-side menu, click **Administration > Notification Settings.** The Notification Settings screen appears.
2. In the Settings section, type the host name or IP address of your mail server.
3. In the Administrator Email Address section, type the email addresses of the person or persons who will receive administrative notifications. (Separate multiple entries with a semicolon (;).)
4. In the **Sender email address** field, type the email address for InterScan VirusWall to use as the sender of notifications. (For example, interscan_viruswall@<your_domain>.)

5. Finally, choose your preferred characters set from the **Preferred charset** drop-down menu. InterScan VirusWall uses this character set for HTML-based email.
6. Click **Save.**

Password Maintenance

It is a good idea to change passwords at least once every 90 days. You can change the administrator password (the password necessary for logging on the Web console) from within the Web console.

To change administrator password:

1. On the left-side menu, click **Administration > Password.** The Change Password screen appears.
2. Type your old (current) password in the **Old password** field.
3. Type the new password in the **New password** field and retype it in the **Confirm password** field.
4. Click **Save.** InterScan VirusWall evaluates the password to ensure that—
   - The password in the **Old password** field is the correct, current password
   - The passwords typed in the **New password** and **Confirm password** fields match
   - The new password is at least 4 alphanumeric characters long but no more than 32 characters

   If the new password does not meet the above conditions or any other InterScan VirusWall security conditions, an error message appears. If all conditions are met, a confirmation message appears.

Chapter 5

Troubleshooting and Support

This chapter provides useful information to solve problems that you may encounter while installing, configuring or starting to use this software.

This chapter includes the following topics:

Overview

If your problem is not included in the list of issues provided in this chapter, refer to the configuration guide for the protocol you are using. The configuration guides are:

- *InterScan VirusWall SMTP Configuration Guide*
- *InterScan VirusWall HTTP Configuration Guide*
- *InterScan VirusWall FTP/POP3 Configuration guide*

If you need further assistance, see *Obtaining Technical Support* on page 5-27.

Troubleshooting

Consult the tables below for troubleshooting guidance on installation and migration, licensing and activation, and the user interface.

Installation and Migration

TABLE 5-1. Troubleshooting installation and migration

Issue	Explanations, Possible Causes, and Solutions

Unsuccessful installation	• System requirements are not satisfied. See *System Requirements* on page 2-4.
	  ◦ If the operating system version or service pack is not satisfied, installation will not proceed.
	  ◦ There is insufficient space on the target disk. You need at least 2GB of hard disk space to install InterScan VirusWall. Free up some disk space or install InterScan VirusWall on a server with sufficient disk space.
	• A previous version of InterScan VirusWall other than version 3.8x may already be installed. Uninstall InterScan VirusWall first, and then run Setup again.
	• You do not have sufficient privileges to install InterScan VirusWall. Log on with administrator privileges to install.
	• Other applications are using needed ports. Issue `netstat -an` command to see all ports in use.
	• If you have satisfied the above requirements and installation still fails, contact Trend Micro Support.

TABLE 5-1. Troubleshooting installation and migration (Continued)

Issue	Explanations, Possible Causes, and Solutions

Postfix Issue
I would like to continue taking advantage of some of the advanced features of Postfix (for example, RBL [Real-time Blackhole List]), but I am having trouble using Postfix on the same machine as InterScan VirusWall.
	Assuming your environment is:
	`Internet > ISVW > Exchange server > Client (Inbound)`
	`Client > Exchange server > ISVW > Internet (Outbound)`
	1. Start two instances of Postfix on the machine on which SMTP VirusWall resides. One of them is before SMTP VirusWall; the other is after SMTP VirusWall.
	2. The topology in the machine that has SMTP VirusWall installed on it should be:
	`Postfix > ISVW > Postfix`
	3. The user environment after installation of SMTP VirusWall with this solution is:
	Inbound:
	`Internet > Postfix (localhost/25) [plus RBL+] > ISVW (localhost/10025) > Postfix (localhost/10026) > Exchange server > Client`
	Outbound:
	`Clients > Exchange (with SmartHost to ISVW Port 10025) > ISVW (localhost/10025) > Postfix (localhost/10026) > Internet`
	(Red = InterScan VirusWall server in a DMZ)

TABLE 5-1. Troubleshooting installation and migration (Continued)

Issue	Explanations, Possible Causes, and Solutions

Unable to migrate configuration settings during installation	• A corrupt was used when trying to migrate settings from InterScan VirusWall for Unix 3.81 when installing InterScan VirusWall on a new computer.
	  • On the machine where InterScan VirusWall for Unix 3.8x is installed, generate a new configuration settings file. For the procedure, see steps 1 to 4 of *Upgrading from Version 3.8x on a Different Machine* on page 3-4.
	  • Install InterScan VirusWall again on the new computer. Continue with steps 5 to 18 of the above topic.
	• The machine on which you are installing InterScan VirusWall has an improperly installed instance of InterScan VirusWall 3.8x on it.
	  • Generate a configuration settings file on the computer on which you wish to install InterScan VirusWall 6. See steps 1 to 3 of *Upgrading from Version 3.8x on a Different Machine on page 3-4*.
	  • Install InterScan VirusWall again on the machine. To re-install InterScan VirusWall, see *Upgrading from Version 3.8x on the Same Machine on page 3-2*.
	• If you have followed the above steps and migration still fails, contact Trend Micro Support.

100% CPU utilization right after installation	This normally happens because InterScan VirusWall needs to initialize components such as the scan engine, anti-spam engine, configuration file, log file, and loading pattern before it can run normally. Initialization will take no more than a few minutes on the recommended environment (see *System Requirements on page 2-4*). After that, CPU usage will normalize.

TABLE 5-1. Troubleshooting installation and migration (Continued)

Issue	Explanations, Possible Causes, and Solutions

eManager upgrading
The eManager 3.8 plug-in may still be installed after upgrading
	• The eManager 3.8 plug-in may still be installed after upgrading because other machines with InterScan VirusWall for Unix 3.8x are still using the plug-in. It is possible for several InterScan VirusWall for Unix 3.8x installations to share the same eManager 3.8 plug-in.
	• All content filter settings were migrated but all of them may be disabled upon upgrade because:
	  • In version 3.8x, the service “InterScan eManager Content Management” is disabled while doing migration.
	  • In eManager 3.8, the “Attachment Filter > Enable attachment filter” option is disabled while doing migration.

eManager rules migration Unable to import email management rules	• InterScan VirusWall 6 does not support the migration of email management rules. You need to define these rules again. • Migration of anti-spam rules is not supported. InterScan VirusWall uses eManager 6 to support the content-filtering feature, and the anti-spam feature is provided by Trend Micro Anti-spam Engine 3.8x.
eManager folders still exist after upgrade	• Some folders under the installation folder of eManager 3.8 still exist after the upgrade. • Manually delete these folders.
Cannot stop or start a service	If you cannot stop a service, follow the procedure in *Starting and Stopping InterScan VirusWall* on page 4-20. If you cannot start or stop a service after following this procedure, call Trend Micro Technical Support.

TABLE 5-1. Troubleshooting installation and migration (Continued)

Issue	Explanations, Possible Causes, and Solutions
Compatibility issue with ServerProtect on the same machine	If you have ServerProtect for Linux installed on the same machine on which you wish to install an instance of InterScan VirusWall, you need to add InterScan VirusWall to the ServerProtect real-time scan exclusion list so that ServerProtect does not block InterScan VirusWall. **To add InterScan VirusWall to the ServerProtect real-time scan exclusion list:** 1. Open the Trend Micro Server Protect 2.5 for Linux Web console. 2. On the left-side menu of the ServerProtect 2.5 Web console, click **Scan Options > Exclusion List.** The Exclusion List - Real-time Scan screen appears. (See figure 5-1, below.) 3. In the **Input directory path** field, type the installed directory of your InterScan VirusWall installation. 4. Click **add** (>>). The InterScan VirusWall installation directory path appears in the **Directories to exclude** field on the right. 5. Click **Save** at the bottom of the screen.

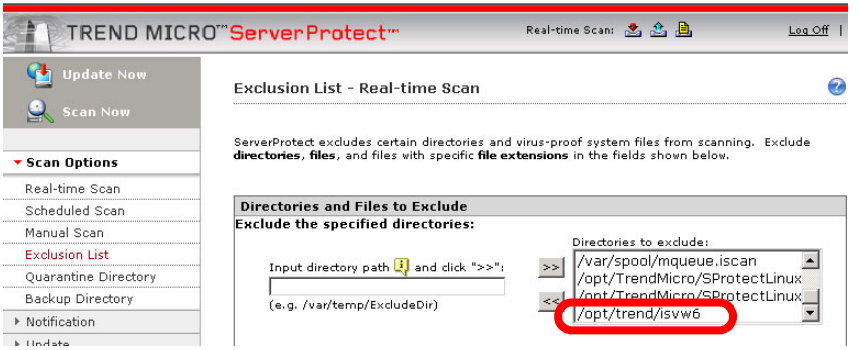


FIGURE 5-1. ServerProtect 2.5 Real-Time Scan Exclusion List screen showing where to add the installed directory for InterScan VirusWall

Licensing and Activation

TABLE 5-2. Troubleshooting licensing and activation

Issue	Explanations, Possible Causes, and Solutions
Cannot update license	• Activate your product before you update your license. • Do not use an evaluation-version of InterScan VirusWall to update your license. • If you encounter a system or program exception error in the backend online update license server, please wait a few minutes and then try again. If you are still experiencing problems, contact Trend Micro Technical Support. • If you cannot update your license because of an incorrect server URL restored in Config.xml\Common\ProductRegistration\OnLineUpdate\Server\Source, check your configuration and try again. • If the Activation Code used is not found in the online update license server, type a valid activation code and try again. • If you cannot update your license online, check the network status. If you are using a proxy server, check if the server can connect to the Product Registration server. If you are still experiencing problems, contact Trend Micro Technical Support.

Problems with activation	• The Activation Code used is invalid because:
	  • You may have already used your full-version or evaluation-version Activation Code to activate the product.
	  • The evaluation-version or full-version Activation Code that you used has expired.
	  • You may have used an evaluation-version Activation Code if you installed a full version, or vice versa.
	• If activation still fails, contact Trend Micro Support.

The User Interface

TABLE 5-3. Troubleshooting the user interface

Issue	Explanations, Possible Causes, and Solutions
Web console does not display normally after typing some Chinese/Japanese characters in a text box	Check the encoding of the browser. For Mozilla Firefox, go to **View > Character Encoding** and select **Unicode (UTF-8)** so that Web console can display double-byte characters (such as Chinese/Japanese) correctly.
Web console does not open	Check the machine on which InterScan VirusWall is installed. Make sure that there is enough space for query cache files.
I forgot my Web console administrator password	• Contact Trend Micro Technical Support and ask for assistance in resetting your password. • Please note that only registered InterScan VirusWall installations are eligible for technical support. If your InterScan VirusWall is not registered, there is no way to recover your password.

TABLE 5-3. Troubleshooting the user interface (Continued)

Issue	Explanations, Possible Causes, and Solutions

URL blocking issue relating to IP translation	• By default, if you block a site by its domain name (for example, www.badsite.com), InterScan VirusWall translates the domain into its IP address and stores that information so that users cannot access the site by its IP address. However, this feature may increase the load on your network.
	• If you want to block sites by domain name only, you can change one option in the config file (`Config.xml`).
	• `Config.xml` resides in your installation directory, for example: `/opt/trend/isvw6/Config.xml`
	• To disable the domain-to-IP-translation feature, edit this line of `Config.xml`:
	`<Value Name="ip_translate" string="yes" type="string" int="0" />`
	...changing it to the following:
	`<Value Name="ip_translate" string="no" type="string" int="0" />`

HTTP scanning issue relating to a change in DNS on the InterScan VirusWall machine	If an administrator changes DNS settings on the machine on which InterScan VirusWall is installed, the HTTP VirusWall services stop working. **To restart the service:** 1. On the left-side menu, click **Summary.** The Summary screen appears. 2. On the Web (HTTP) tab of the Summary screen, clear the **Enable HTTP Traffic** check box and then reselect it.

TABLE 5-3. Troubleshooting the user interface (Continued)

Issue	Explanations, Possible Causes, and Solutions
Delay in changing HTTP listening port	• For SMTP, if you change its listening port, the setting immediately applies. However, for HTTP, there is a slight delay. • For HTTP, if you change its listening port, the http scanning task requests that InterScan VirusWall kill the http scanning task and restart it. Upon restart of that task, the port change applies. This process takes a few seconds, but under no circumstances will it take longer than 1 minute.
HTTP can accept connections only after update is finished	• When InterScan VirusWall conducts an update of the scan engine (or the URL-filtering database), this process can take a few minutes. • During that time, the HTTP process will not be able to accept connections. • After the update is complete, the HTTP process can again accept connections For this reason, Trend Micro strongly recommends that you schedule updates of these two components during periods when Web traffic is at its absolute lowest, to minimize any inconvenience to users.

Frequently Asked Questions

Installation

Q. Can I install InterScan VirusWall remotely?

A. No, this release of InterScan VirusWall for Linux supports local installation only.

Q. Does InterScan VirusWall 6 support silent install or component install?

A. No, this release does not support silent install or component install.

Quarantines

Using the screens in the Quarantines menu, you can manage files quarantined by InterScan VirusWall. You can use these screens to query the quarantine folders for email messages and files (Query menu), to modify the quarantine directory paths (Settings menu), and to set the conditions for deleting older files in the quarantine (Maintenance menu).

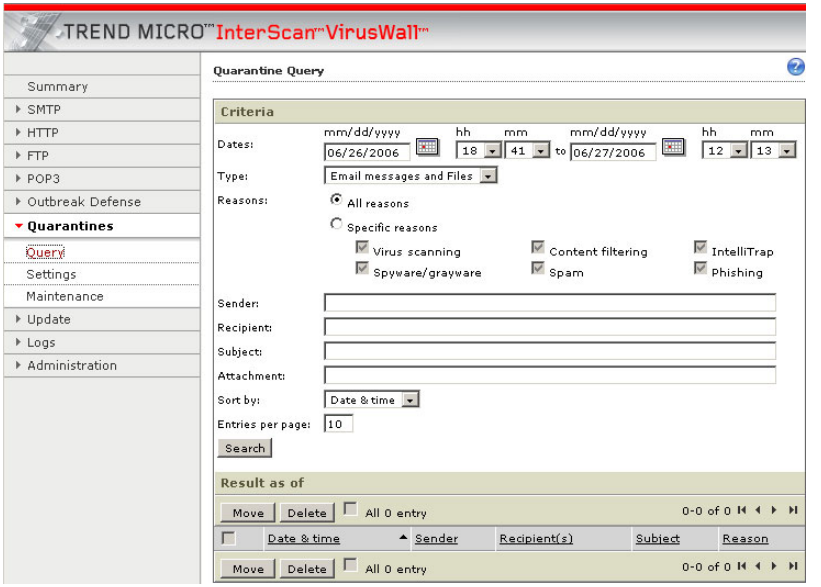


FIGURE 5-2. The Quarantine Query screen

The table below lists the quarantine submenus and the tasks that you can perform using each.

TABLE 5-4. The submenu items under Quarantines

Submenu	Description	Tasks
Query	Provides details regarding SMTP/POP3 quarantined email messages and attachments	Specify the query criteria by dates, type, reasons, sender, recipient, subject, and attachment Order the sort result by any of the above criteria, while limiting the number of entries per page **Note:** InterScan VirusWall 6 supports queries of the SMTP and POP3 quarantines only.
Settings	Enables you to modify the quarantine directories	Modify the quarantine directories for SMTP, HTTP, POP3, and FTP quarantined items
Maintenance	Enables you to determine how long to store infected files in the Quarantine directory before deleting them	Delete quarantined files Schedule automatic deletion times **Note:** InterScan VirusWall 6 supports query maintenance of the SMTP and POP3 quarantines only.

Querying SMTP and POP3 Quarantines

Based on the settings you choose when configuring actions in the individual protocols, InterScan VirusWall can move some email messages or files to quarantine directories for later consideration. You can query the SMTP and POP3 quarantines from the Web console and can also maintain those two quarantines.

Tip: This release does not support querying and maintaining the HTTP and FTP quarantine directories from the Web console. However, you can manually access those quarantines and manage their contents from the command line.

Table 5-5 lists the default quarantine directories, by quarantine type.

TABLE 5-5. Default quarantine directory paths, by quarantine type

Quarantine Type	Default directory path
SMTP scanning	/opt/trend/isvw6/quarantine/smtp
HTTP scanning	/opt/trend/isvw6/quarantine/http
FTP scanning	/opt/trend/isvw6/quarantine/ftp
POP3 scanning	/opt/trend/isvw6/quarantine/pop3

Available Query Criteria for SMTP and POP3 Quarantines

Using the query definition fields on the Quarantine Query screen, you can specify the following criteria for your query:

- Beginning and ending date and time (accurate to the minute)
- Type:
  - Email messages
  - Email messages and Files
  - Files
- Reasons (that is, the reason why InterScan VirusWall quarantined the item):
  - Virus scanning
  - Content filtering
  - IntelliTrap
  - Spyware/grayware
  - Spam
  - Phishing

The following criteria apply only if the quarantined item is an email message or attachment:

- Sender
- Recipient
- Subject
- Attachment

In addition to the above criteria, you can specify the sort order of the results, choosing from the following:

- Date & time
- Sender
- Recipient
- Subject
- Reason

You can also specify the number of entries per page to display (default is 10).

To query the contents of the SMTP and POP3 quarantine directories:

1. On the left-side menu, click **Quarantine > Query.** The Quarantine Query screen appears.
2. Select from any of the criteria fields listed above and fill in the criteria for the query.
3. Click **Search.** InterScan VirusWall queries the quarantine using the specified criteria and returns a page of query results in the **Result as of** section at the bottom of the screen.

If there is more than one page of results, paging information displays at the top and bottom of the list. Click the arrows to navigate through multiple pages. You can sort the results in the results table by clicking on any of the column heads.

Moving or Deleting Quarantined SMTP and POP3 Items

From the results list, you can select one or more items and delete or move them. You can also select all items in the results list and delete or move them.

To delete one or more items in the SMTP/POP3 quarantine results list:

1. Run a quarantine query as shown in *To query the contents of the SMTP and POP3 quarantine directories:* on page 5-15.
2. Select one or more items to delete by selecting the check box next to each of those items. (You can also select all items in the results list by clicking the **All x entry** check box in the top or bottom navigation bar of the results list.)
3. Click **Delete.** InterScan VirusWall deletes all selected items from the quarantine.

To move one or more items in the SMTP/POP3 quarantine results list:

1. Run a quarantine query as shown in *To query the contents of the SMTP and POP3 quarantine directories:* on page 5-15.
2. Select one or more items to move by selecting the check box next to each of those items. (You can also select all items in the results list by clicking the **All x entry** check box in the top or bottom navigation bar of the results list.)
3. Click **Move.** The Move Quarantined Items screen appears, showing a default move directory.
4. Replace the default move directory with your preferred directory or accept the default.
5. Click **Move.** InterScan VirusWall moves the selected items to the location that you have specified. (To return to the results list, click **Back.**)

Modifying Quarantine Directory Paths

You can change the paths of any of the four quarantine directories on the Quarantine Settings screen.

Note: This feature supports only absolute—and not relative—paths.

To modify paths for one or more quarantine directories:

1. On the left-side menu, click **Quarantine > Settings.** The Quarantine Settings screen appears, displaying the current paths to each of the four quarantine directories (SMTP, POP3, HTTP, and FTP).
2. Edit any of the the paths in the fields shown using an absolute path.
3. Click **Save.**

Purging Older Quarantined SMTP and POP3 Items

Using the Quarantine Maintenance screen, you can manually purge older SMTP and POP3 quarantined items or set up an automatic purge of those quarantines based on the age (in days) of such quarantined items.

To manually purge older SMTP and POP3 quarantined items:

1. On the left-side menu, click **Quarantine > Maintenance.** The Quarantine Maintenance screen appears, displaying the Manual tab.
2. Edit the number of days in the **Delete files older than** check box or accept the default of 7 days.
3. Click **Delete Now.** InterScan VirusWall purges all quarantined SMTP and POP3 items that are older than the number of days that you specified.

From the Automatic tab, you can set up an automatic purge of quarantined SMTP and POP3 items. Follow the procedures below to do so.

To set up automatic purges based on age of quarantined SMTP and POP3 items:

1. On the left-side menu, click **Quarantine > Maintenance.** The Quarantine Maintenance screen appears, displaying the Manual tab.
2. Click the **Automatic** tab.
3. In the Automatic tab, select the **Enable Automatic Purge** check box if it is not already selected.
4. In the Action section, edit the number of days in the **Delete files older than** check box or accept the default of 7 days.
5. Click **Save.** InterScan VirusWall will regularly delete quarantined SMTP and POP3 items that are older than the number of days that you specified.

Analyze Your Security Incidents Using Logs

Use the Logs menu to query incidents of security threats that InterScan VirusWall has detected.

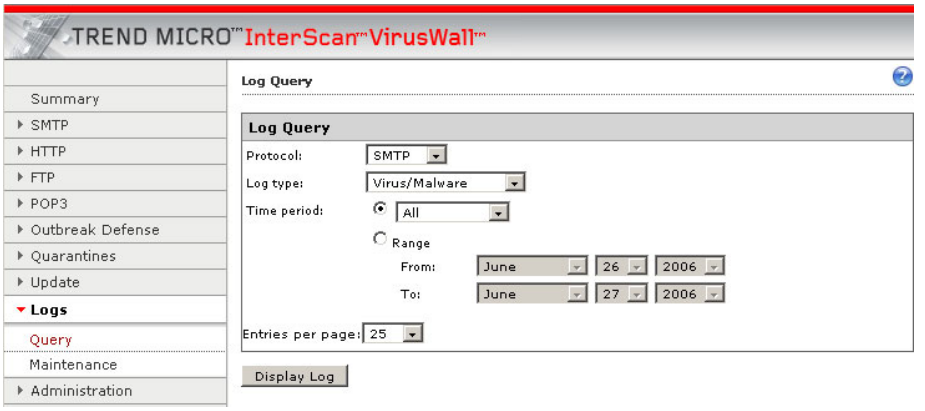


FIGURE 5-3. The Log Query screen

Click the Logs menu to open its submenus, Query and Maintenance. Use the Log Query screen to query any of the six available types of InterScan VirusWall logs available:

- Virus/malware logs
- Spyware/grayware logs
- Attachment filter logs
- Keyword filter logs
- Anti-spam logs
- Anti-phishing logs

TABLE 5-6. The submenu items under Logs

Submenu	Description	Tasks
Query	Query the automatic logging feature in InterScan VirusWall **Note:** This release does not support query of the system log, connect log, or debug log from the Web console.	Query by protocol, log type, and time period Designate the number of entries per page that will be displayed Browse the log using a paging tool and re-specify how many items (10, 25, 50, 100) will be listed on a page Export the log query result as a text, CSV (comma-separated values) or XML file
Maintenance	Delete old logs according to specific criteria **Note:** This release does not support maintenance of the system log, event log, or connect log from the Web console.	Specify the target logs that you want to delete Delete logs older than *n* days Enable or disable automatic purging of target logs

Querying Logs

Using the query definition fields on the Log Query screen, you can specify the following criteria for your query:

- Protocol:
  - SMTP
    - Log type:
      - Virus/malware
      - Spyware/grayware
      - Attachment filter
      - Keyword filter
      - Anti-spam
      - Anti-phishing
  - POP3
    - Log type:
      - Virus/malware
      - Spyware/grayware
      - Attachment filter
      - Keyword filter
      - Anti-spam
      - Anti-phishing
  - HTTP
    - Log type:
      - Virus/malware
      - Spyware/grayware
      - URL blocking
      - URL filtering
      - URL accessing

    - FTP
        - Log type:
            - Virus/malware
            - Spyware/grayware
    - Others (Event log only)
- Time period:
    - All
    - Today
    - Yesterday
    - Last week
    - Last month
    - Last year
    - Date range

You can also specify the number of entries per page to display (default is 25 and options are 10, 25, 50, or 100).

To query the contents of the logs:

1. On the left-side menu, click **Logs > Query.** The Log Query screen appears.
2. Select from any of the criteria fields listed above and fill in the criteria for the query.
3. Click **Display Log.** InterScan VirusWall queries the selected log(s) using the specified criteria and returns a page of query results as a separate screen.

If there is more than one page of results, paging information displays at the top of the list. Click the arrow icons or select the page number from the drop-down menu to navigate through multiple pages, as shown in figure 5-4, *Log query results for a query of the event log based on a time range of a single day*. You can sort the results in the results table by clicking on any of the column heads that are all hyperlinked.

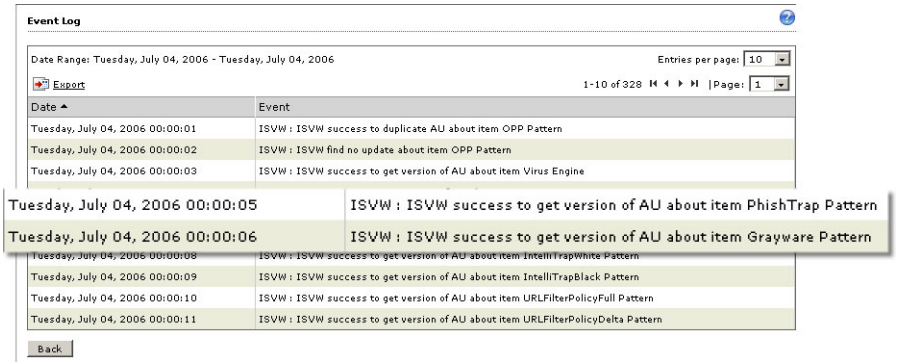


FIGURE 5-4. Log query results for a query of the event log based on a time range of a single day

Query Result Tables

The columns displayed in a query result vary based on what kind of log you have queried. The query result table for the event log, for example, contains only two columns: Date and Event, as shown in figure 5-4, above.

Other log types display different information, as shown in Table 5-7, “Information displayed upon log query, by log type,” on page 5-24.

TABLE 5-7. Information displayed upon log query, by log type

Log type	Columns displayed						
SMTP or POP3 virus/ malware	Date	Virus/ Malware Name	Type	Sender	Recipient	Subject	Content Action
SMTP or POP3 spyware	Date	Spyware/ Grayware name	Type	Sender	Recipient	Subject	Content Action
SMTP or POP3 Attachment Filter (and Keyword Filter)	Date	Sender	Recipient		Subject		Action
SMTP or POP3 Anti-Spam and Anti-Phishing	Date	Sender	Recipient		Subject	Message Action	
HTTP Virus/ Malware	Date	Virus/ Malware Name		Type	File Name	Client IP	Action
HTTP Spyware	Date	Spyware/Grayware Name		Type	File Name	Client IP	Action
HTTP URL Blocking and URL Filtering	Date	Client IP	URL		Blocking Rule		
HTTP URL Accessing	Date	Client IP	Domain name		Path		
FTP Virus	Date	Virus/Malware Name		Type	File Name	User ID	Action
FTP Spyware	Date	Spyware/Grayware Name		Type	File Name	User ID	Action
Event	Date	Event					

Exporting Query Results

You can export log query results in plain text, XML, or CSV format for use in a variety of programs, such as spreadsheet or Web-based applications.

To export log query results:

1. Create and run a query, as explained in *To query the contents of the logs:* on page 5-22.
2. Click the Export hyperlink at the top of the log query results table. An Export Log File popup window opens.
3. Select a file type from the **Export file type** drop-down menu, choosing from:
   - Text
   - XML
   - CSV
4. Click **Export.** Your browser takes its default action upon downloading a file. For example, the browser may open a dialog box asking if you want to save the file to your computer.

Purging Logs

Using the Log Maintenance screen, you can manually purge all logs, all logs of one or more types, or logs older than a select number of days. From that screen you can also set up an automatic purge of logs based on the same criteria.

To manually purge logs:

1. On the left-side menu, click **Logs > Maintenance.** The Log Maintenance screen appears, displaying the Manual tab.
2. In the Target section, select the type of logs to purge (or select **All** to select all types).
3. In the Action section, choose one of the following options:
   - **Delete all logs selected above**
   - **Delete logs selected above older than *n* days**
4. If you selected the time-based option, type the number of days to use as the deletion trigger or accept the default value of 30 days.

5. Click **Delete Now.** InterScan VirusWall deletes all logs matching the criteria that you have set up and displays a Done message box confirming this action. (Click **Back** to return to the Log Maintenance screen.)

Note: You cannot purge the following log types from the Web console: system log, event log, connection log, or debug log.

Setting up automatic log maintenance (purging) is very similar to manually purging logs.

To set up automatic log maintenance:

1. On the left-side menu, click **Logs > Maintenance.** The Log Maintenance screen appears, displaying the Manual tab.
2. Click the **Automatic** tab.
3. In the Automatic tab, select the **Enable Automatic Purge** check box.
4. Select the purging criteria (see *To manually purge logs:* on page 5-25).
5. Click **Save.** InterScan VirusWall records your criteria for automatic log maintenance and will regularly purge logs accordingly.

Other Logs

In addition to logs that you can maintain from the Web console, InterScan VirusWall keeps the following logs:

- **System log.**—Information about services starts and stops, system errors, exceptions, and so on. Log file name: ***systemlog.yyyymmdd.nnnn***
- **Debug log** (if enabled).—Debugging information for use only upon request by Trend Micro Technical Support. Log file name: ***debuglog.yyyymmdd.nnnn***
- **Connection log.**—SMTP connection/disconnection log. Log file name: ***connectlog.yyyymmdd.nnnn***.

Tip: Trend Micro strongly recommends that you do not turn on the debug log unless Trend Micro Technical Support asks you to do so, for a specific troubleshooting purpose.

Obtaining Technical Support

There are several ways to obtain technical support.

- The Trend Micro Knowledge Base, maintained at the Trend Micro Web site, has the most up-to-date answers to product questions. You can also use Knowledge Base to submit a question if you cannot find the answer in the product documentation. Access the Knowledge Base at:
  http://esupport.trendmicro.com
- If you are not able to find an answer in the documentation or the Knowledge Base, you can email your question to Trend Micro technical support.
  support@support.trendmicro.com
- For a list of the worldwide support offices, go to:
  http://kb.trendmicro.com/solutions/includes2/ContactTechSupport.asp
  In the United States, you can reach Trend Micro representatives via phone or fax:

  Toll free: +1 (800) 228-5651 (sales)

  Voice: +1 (408) 257-1500 (main)

  Fax: +1 (408) 257-2003

To speed up the resolution of your product issue, provide the following information when you send an email or call Trend Micro:

- Program version and number (Click **About** on the main console's footer menu to learn about the program version and build number.)
- Serial number
- Exact text of the error message, if any
- Steps to reproduce the issue

Glossary of Terms

This glossary describes special terms as used in this document or the online help.

Term	Explanation
action (*Also see* target and notification)	The operation to be performed when: • A virus has been detected • Spam has been detected • A content violation has occurred • An attempt was made to access a blocked URL, • File blocking has been triggered. Actions typically include clean and deliver, quarantine, delete, or deliver/transfer anyway. Delivering/transferring anyway is not recommended—delivering a virus-infected message or transferring a virus-infected file can compromise your network.
activate	To enable your software after completion of the registration process. Trend Micro products will not be operable until product activation is complete. Activate during installation or after installation (in the management console) on the Product License screen.
Activation Code	A 37-character code, including hyphens, that is used to activate Trend Micro products. Here is an example of an Activation Code: SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 *Also see* Registration Key.

Term	Explanation
ActiveUpdate	ActiveUpdate is a function common to many Trend Micro products. Connected to the Trend Micro update Web site, ActiveUpdate provides up-to-date downloads of virus pattern files, scan engines, and program files via the Internet or the Trend Micro Total Solution CD.
address	Refers to a networking address (*see* IP address) or an email address, which is the string of characters that specify the source or destination of an email message.
administrator	Refers to the “system administrator"—the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.
administrator account	A user name and password that has administrator-level privileges.
administrator email address	The address used by the administrator of your Trend Micro product to manage notifications and alerts.
adware	Advertising-supported software in which advertising banners display while the program is running. Adware that installs a “backdoor”; tracking mechanism on the user's computer without the user's knowledge is called “spyware.”
anti-relay	Mechanisms to prevent hosts from “piggybacking” through another host’s network.
anti-spam	Refers to a filtering mechanism, designed to identify and prevent delivery of advertisements, pornography, and other “nuisance” mail.
anti-spam rules and engine	The Trend Micro tools used to detect and filter spam.
antivirus	Computer programs designed to detect and clean computer viruses.
approved sender	A sender whose messages are always allowed into your network.
archive	A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program, such as a .zip file.

Term	Explanation
attachment	A file attached to an email message.
audio/video file	A file containing sounds, such as music, or video footage.
authentication	The verification of the identity of a person or a process. Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver that the message and its source are secure. The simplest form of authentication requires a user name and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption, such as the Data Encryption Standard (DES) algorithm, or on public-key systems using digital signatures. *Also see* public-key encryption *and* digital signature.
block	To prevent entry into your network.
blocked sender	A sender whose messages are never allowed to enter your network.
boot sector virus	A boot sector virus is a virus targeted at the boot sector (the operating system) of a computer. Computer systems are most likely to be attacked by boot sector viruses when you boot the system with an infected disk from the floppy drive. The boot attempt does not have to be successful for the virus to infect the hard drive. Also, there are a few viruses that can infect the boot sector from executable programs. These are known as multi-partite viruses and they are relatively rare. Once the system is infected, the boot sector virus will attempt to infect every disk that is accessed by that computer. Boot sector viruses can usually be successfully removed.
browser	A program which allows a person to read hypertext, such as Internet Explorer. The browser gives some means of viewing the contents of nodes (or "pages") and of navigating from one node to another. A browser acts as a client to a remote Web server.
cache	A small fast memory, holding recently accessed data, designed to speed up subsequent access to the same data. The term is most often applied to processor-memory access, but also applies to a local copy of data accessible over a network etc.

Term	Explanation
case-matching	Scanning for text that matches both words and case. For example, if "dog" is added to the content-filter, with case-matching enabled, messages containing "Dog" will pass through the filter; messages containing "dog" will not.
clean	To remove virus code from a file or message.
client	A computer system or process that requests a service of another computer system or process (a "server") using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture.
compressed file	A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.
configuration	Selecting options for how your Trend Micro product will function, for example, selecting whether to quarantine or delete a virus-infected email message.
content filtering	Scanning email messages for content (words or phrases) prohibited by your organization's Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.
content violation	An event that has triggered the content filtering policy.
cookie	A mechanism for storing information about an Internet user, such as name, preferences, and interests, which is stored in your Web browser for later use. The next time you access a Web site for which your browser has a cookie, your browser sends the cookie to the Web server, which the Web server can then use to present you with customized Web pages. For example, you might enter a Web site that welcomes you by name.
daemon	A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The perpetrator of the condition need not be aware that a daemon is lurking.
De-Militarized Zone (DMZ)	From the military term for an area between two opponents where fighting is prevented. DMZ Ethernets connect networks and computers controlled by different bodies. They may be external or internal. External DMZ Ethernets link regional networks with routers.

Term	Explanation
dialer	A type of Trojan that when executed, connects the user's system to a pay-per-call location in which the unsuspecting user is billed for the call without his or her knowledge.
digital signature	Extra data appended to a message which identifies and authenticates the sender and message data using a technique called public-key encryption. *Also see* public-key encryption *and* authentication.
disclaimer	A statement appended to the beginning or end of an email message, that states certain terms of legality and confidentiality regarding the message, To see an example, click the online help for the **SMTP Configuration - Disclaimer** screen.
DNS	Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses.
DNS resolution	When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.
(administrative) domain	A group of computers sharing a common database and security policy.
domain name	The full name of a system, consisting of its local host name and its domain name, for example, tellsitall.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called "name resolution", uses the Domain Name System (DNS).
DoS (Denial of Service) attack	Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped.
DOS virus	Also referred to as “COM” and “EXE file infectors.” DOS viruses infect DOS executable programs- files that have the extensions *.COM or *.EXE. Unless they have overwritten or inadvertently destroyed part of the original program's code, most DOS viruses try to replicate and spread by infecting other host programs.

Term	Explanation
encryption	Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (Data Encryption Standard) are two of the most popular public-key encryption schemes.
End User License Agreement (EULA)	An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking "I accept" during installation. Clicking "I do not accept" will, of course, end the installation of the software product. Many users inadvertently agree to the installation of spyware and adware into their computers when they click "I accept" on EULA prompts displayed during the installation of certain free software.
Ethernet	A local area network (LAN) technology invented at the Xerox Corporation, Palo Alto Research Center. Ethernet is a best-effort delivery system that uses CSMA/CD technology. Ethernet can be run over a variety of cable schemes, including thick coaxial, thin coaxial, twisted pair, and fiber optic cable. Ethernet is a standard for connecting computers into a local area network. The most common form of Ethernet is called 10BaseT, which denotes a peak transmission speed of 10 Mbps using copper twisted-pair cable.
executable file	A binary file containing a program in machine language which is ready to be executed (run).
exploit	An exploit is code that takes advantage of a software vulnerability or security hole. Exploits are able to propagate into and run intricate routines on vulnerable computers.
false positive	An email message that was "caught" by the spam filter and identified as spam, but is actually not spam.
FAQ	Frequently Asked Questions—A list of questions and answers about a specific topic.

Term	Explanation
file-infecting virus	File-infecting viruses infect executable programs (generally, files that have extensions of .com or .exe). Most such viruses simply try to replicate and spread by infecting other host programs, but some inadvertently destroy the program they infect by overwriting a portion of the original code. A minority of these viruses are very destructive and attempt to format the hard drive at a pre-determined time or perform some other malicious action. In many cases, a file-infecting virus can be successfully removed from the infected file. However, if the virus has overwritten part of the program's code, the original file will be unrecoverable
file type	The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.
file name extension	The portion of a file name (such as .dll or .xml) which indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run.
filter criteria	User-specified guidelines for determining whether a message and attachment(s), if any, will be delivered, such as: - size of the message body and attachment - presence of words or text strings in the message subject - presence of words or text strings in the message body - presence of words or text strings in the attachment subject - file type of the attachment
firewall	A gateway machine with special security precautions on it, used to service outside network (especially Internet) connections and dial-in lines.
FTP	A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also refers to the client program the user executes to transfer files.
gateway	An interface between an information source and a Web server.

Term	Explanation
grayware	A category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.
group file type	Types of files that have a common theme, for example: - Audio/Video - Compressed - Executable - Images - Java - Microsoft Office
hacker	*See* virus writer.
hacking tool	Tools such as hardware and software that enables penetration testing of a computer system or network for the purpose of finding security vulnerabilities that can be exploited.
hard disk (or hard drive)	One or more rigid magnetic disks rotating about a central axle with associated read/write heads and electronics, used to read and write hard disks or floppy disks, and to store data. Most hard disks are permanently connected to the drive (fixed disks) though there are also removable disks.
HTML virus	A virus targeted at HTML (Hyper Text Markup Language), the authoring language used to create information in a Web page. The virus resides in a Web page and downloads via a user's browser.
HTTP	Hypertext Transfer Protocol—The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.
HTTPS	Hypertext Transfer Protocol Secure—A variant of HTTP used for handling secure transactions.
host	A computer connected to a network.

Term	Explanation
hub	This hardware is used to network computers together (usually over an Ethernet connection). It serves as a common wiring point so that information can flow through one central location to any other computer on the network thus enabling centralized management. A hub is a hardware device that repeats signals at the physical Ethernet layer. A hub retains the behavior of a standard bus type network (such as Thinnet), but produces a star topology with the hub at the center of the star. This configuration enables centralized management.
IMAP	Internet Message Access Protocol—A protocol allowing a client to access and manipulate electronic mail messages on a server. It permits manipulation of remote message folders (mailboxes), in a way that is functionally equivalent to local mailboxes.
incoming	Email messages or other data routed *into* your network.
installation script	The installation screens used to install Unix versions of Trend Micro products.
IntelliScan	IntelliScan is a Trend Micro scanning technology that 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 be disguised by a harmless extension name.
Internet Control Message Protocol (ICMP)	Occasionally a gateway or destination host will communicate with a source host, for example, to report an error in datagram processing. For such purposes the protocol, the Internet Control Message Protocol (ICMP), is used. ICMP uses the basic support of IP as if it were a higher level protocol, however, ICMP is actually an integral part of IP, and must be implemented by every IP module. ICMP messages are sent in several situations: for example, when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. The Internet Protocol is not designed to be absolutely reliable. The purpose of these control messages is to provide feedback about problems in the communication environment, not to make IP reliable.
Internet Protocol (IP)	An Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet.

Term	Explanation
“in the wild”	Describes known viruses that are actively circulating. *Also see* “in the zoo.”
intranet	Any network which provides similar services within an organization to those provided by the Internet outside it, but which is not necessarily connected to the Internet.
IP	Internet Protocol—*See* IP address.
IP address	Internet address for a device on a network, typically expressed using dot notation such as 123.123.123.123.
IP gateway	Also called a router, a gateway is a program or a special-purpose device that transfers IP datagrams from one network to another until the final destination is reached.
IP Security (IPSec)	Security standard produced by the Internet Engineering Task Force (IETF). It is a protocol suite that provides everything you need for secure communications—authentication, integrity, and confidentiality—and makes key exchange practical even in larger networks. *Also see* DES-CBC, ESP/AH.
Java applets	Java applets are small, portable Java programs embedded in HTML pages that can run automatically when the pages are viewed. Java applets allow Web developers to create interactive, dynamic Web pages with broader functionality. Authors of malicious code have used Java applets as a vehicle for attack. Most Web browsers, however, can be configured so that these applets do not execute - sometimes by simply changing browser security settings to "high."
Java file	Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets." (An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet’s code is transferred to your system and is executed by the browser’s Java Virtual Machine.)
Java malicious code	Virus code written or embedded in Java. *Also see* Java file.

Term	Explanation
JavaScript virus	JavaScript is a simple programming language developed by Netscape that allows Web developers to add dynamic content to HTML pages displayed in a browser using scripts. Javascript shares some features of Sun Microsystems Java programming language, but was developed independently. A JavaScript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user's desktop through the user's browser. *Also see* VBscript virus.
joke program	An executable program that is annoying or causes users undue alarm. Unlike viruses, joke programs do not self-propagate and should simply be removed from your system.
keylogger	Keyloggers are programs that catch and store all keyboard activity. There are legitimate keylogging programs that are used by corporations to monitor employees and by parents to monitor their children. However, criminals also use keystroke logs to sort for valuable information such as logon credentials and credit card numbers.
LHA file format	LHA is a free data compression utility, popular mainly in Japan. Files that are compressed using LHA have the file extension .lha or .lzh.
license	Authorization by law to use a Trend Micro product.
license certificate	A document that proves you are an authorized user of a Trend Micro product.
link (also called hyperlink)	A reference from some point in one hypertext document to some point in another document or another place in the same document. Links are usually distinguished by a different color or style of text, such as underlined blue text. When you activate the link, for example, by clicking on it with a mouse, the browser displays the target of the link.
listening port	A port utilized for client connection requests for data exchange.
load balancing	Load balancing is the mapping (or re-mapping) of work to processors, with the intent of improving the efficiency of a concurrent computation.

Term	Explanation
local area network (LAN)	Any network technology that interconnects resources within an office environment, usually at high speeds, such as Ethernet. A local area network is a short-distance network used to link a group of computers together within a building. 10BaseT Ethernet is the most commonly used form of LAN. A hardware device called a hub serves as the common wiring point, enabling data to be sent from one machine to another over the network. LANs are typically limited to distances of less than 500 meters and provide low-cost, high-bandwidth networking capabilities within a small geographical area.
logic bomb	Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met.
macro	A command used to automate certain functions within an application.
MacroTrap	A Trend Micro utility that performs a rule-based examination of all macro code that is saved in association with a document. macro virus code is typically contained in part of the invisible template that travels with many documents (.dot, for example, in Microsoft Word documents). MacroTrap checks the template for signs of a macro virus by seeking out key instructions that perform virus-like activity—instructions such as copying parts of the template to other templates (replication), or instructions to execute potentially harmful commands (destruction).
macro virus	Macro viruses are often encoded as an application macro and included in a document. Unlike other virus types, macro viruses aren't specific to an operating system and can spread via email attachments, Web downloads, file transfers, and cooperative applications.
malware (malicious software)	Programming or files that are developed for the purpose of doing harm, such as viruses, worms, and Trojans.
mass mailer (also known as a Worm)	A malicious program that has high damage potential, because it causes large amounts of network traffic.
match case	*See* case-matching.
Mbps	Millions of bits per second—a measure of bandwidth in data communications.

Term	Explanation
Media Access Control (MAC) address	An address that uniquely identifies the network interface card, such as an Ethernet adapter. For Ethernet, the MAC address is a 6 octet address assigned by IEEE. On a LAN or other network, the MAC address is a computer's unique hardware number. (On an Ethernet LAN, it's the same as the Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN. The MAC address is used by the Media Access Control sublayer of the Data-Link Control (DLC) layer of telecommunication protocols. There is a different MAC sublayer for each physical device type.
message	An email message, which includes the message subject in the message header and the message body.
message body	The content of an email message.
message queue	The number of messages waiting to be scanned.
message size	The number of KB or MB occupied by a message and its attachments.
message subject	The title or topic of an email message, such as “Third Quarter Results” or “Lunch on Friday.”
Microsoft Office file	Files created with Microsoft Office tools such as Excel or Microsoft Word.
mixed threat attack	Complex attacks that take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the “Nimda” or “Code Red” threats.
MTA (Mail Transport Agent)	The program responsible for delivering email messages. *Also see* SMTP server.
multi-partite virus	A virus that has characteristics of both boot sector viruses and file-infecting viruses.
MX record	A DNS resource record type indicating which host can handle electronic mail for a particular domain.

Term	Explanation
Network Address Translation (NAT)	A standard for translating secure IP addresses to temporary, external, registered IP address from the address pool. This allows Trusted networks with privately assigned IP addresses to have access to the Internet. This also means that you don't have to get a registered IP address for every machine in your network.
NetBIOS (Network Basic Input Output System)	An application program interface (API) that adds functionality such as network capabilities to DOS (disk operating system) BIOS (basic input/output system).
NetScreen Redundancy Protocol (NSRP)	A proprietary protocol that provides configuration and run time object (RTO) redundancy and a device failover mechanism for GateLock units in a high availability (HA) cluster.
network virus	A type of virus that uses network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. Network viruses often do not alter system files or modify the boot sectors of hard disks. Instead, they infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns or even complete network failure.
notification (*Also see* action and target)	A message that is forwarded to one or more of the following: - system administrator - sender of a message - recipient of a message, file download, or file transfer The purpose of the notification is to communicate that a prohibited action has taken place, or was attempted, such as a virus being detected in an attempted HTTP file download.
offensive content	Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.
online help	Documentation that is bundled with the GUI.
open source	Programming code that is available to the general public for use or modification free of charge and without license restrictions.
OSPF (Open Shortest Path First)	A link-state routing protocol that is one of the Internet standard interior gateway protocols. OSPF routers send data using the shortest path to each node in the Internet topography.
outgoing	Email messages or other data *leaving* your network, routed out to the Internet.

Term	Explanation
parameter	A variable, such as a range of values (a number from 1 to 10).
partition	A logical portion of a disk. (*Also see* sector, which is a physical portion of a disk.)
passive FTP	Configuration of FTP protocol that allows clients within your local area network to initiate the file transfer, using random upper port numbers (1024 and above).
password cracker	An application program that is used to recover a lost or forgotten password. These applications can also be used by an intruder to gain unauthorized access to a computer or network resources.
pattern file (also known as Official Pattern Release)	The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.
payload	Payload refers to an action that a virus performs on the infected computer. This can be something relatively harmless, such as displaying messages or ejecting the CD drive, or something destructive, such as deleting the entire hard drive.
POP3	Post Office Protocol, version 3—A messaging protocol that allows a client computer to retrieve electronic mail from a server via a temporary connection, for example, a mobile computer without a permanent network connection.
POP3 server	A server which hosts POP3 email, from which clients in your network will retrieve POP3 messages.
port	A logical channel or channel endpoint in a communications system, used to distinguish between different logical channels on the same network interface on the same computer. Each application program has a unique port number associated with it.
protected network	A network protected by Network VirusWall.
proxy	A process providing a cache of items available on other servers which are presumably slower or more expensive to access.

Term	Explanation
proxy server	A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.
public-key encryption	An encryption scheme where each person gets a pair of “keys,” called the public key and the private key. Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his or her private key. *Also see* authentication *and* digital signature.
purge	To delete all, as in getting rid of old entries in the logs.
quarantine	To place infected data such as email messages, infected attachments, infected HTTP downloads, or infected FTP files in an isolated directory (the Quarantine Directory) on your server.
queue	A data structure used to sequence multiple demands for a resource when mail is being received faster than it can be processed. Messages are added at the end of the queue, and are taken from the beginning of the queue, using a FIFO (first-in, first-out) approach.
recipient	The person or entity to whom an email message is addressed.
registration	The process of identifying yourself as a Trend Micro customer, using a product Registration Key, on the Trend Micro Online Registration screen. *https://olr.trendmicro.com/registration*
Registration Key	A 22-character code, including hyphens, that is used to register in the Trend Micro customer database. Here is an example of a Registration Key: SM-27RT-UY4Z-39HB-MNW8 *Also see* Activation Code
relay	To convey by means of passing through various other points.
remote access tool (RAT)	Hardware and software that allow a legitimate system administrator to manage a network remotely. However, these same tools can also be used by intruders to attempt a breach of your system security.
replicate	To self-reproduce. As used in this documentation, the term refers to viruses or worms that can self-reproduce.

Term	Explanation
router	This hardware device routes data from a local area network (LAN) to a phone line's long distance line. Routers also act as traffic cops, allowing only authorized machines to transmit data into the local network so that private information can remain secure. In addition to supporting these dial-in and leased connections, routers also handle errors, keep network usage statistics, and handle security issues.
rule-based spam detection	Spam detection based on heuristic evaluation of message characteristics for determining whether an email message should be considered spam. When the anti-spam engine examines an email message, it searches for matches between the mail contents and the entries in the rules files. Rule-based spam detection has a higher catch rate than signature-based spam detection, but it also has a higher false positive rate as well. *Also see* signature-based spam detection. *Also see* false positive.
scan	To examine items in a file in sequence to find those that meet a particular criteria.
scan engine	The module that performs antivirus scanning and detection in the host product to which it is integrated.
script	A set of programming commands that, once invoked, can be executed together. Other terms used synonymously with “script” are “macro” or “batch file.”
seat	A license for one person to use a Trend Micro product.
Secure Socket Layer (SSL)	Secure Socket Layer (SSL), is a protocol designed by Netscape for providing data security layered between application protocols (such as HTTP, Telnet, or FTP) and TCP/IP. This security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection.
security association	The combination of a Security Parameters Index and a destination address. Required for both Authentication Header and Encapsulating Security Payload protocols. *Also see* Security Parameters Index.
Security Parameters Index (SPI)	(SPI) is a hexadecimal value which uniquely identifies each tunnel. It also tells Trend Micro GateLock which key to use to decrypt packets.

Term	Explanation
security zone	A security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic via access policies.
sender	The person who is sending an email message to another person or entity.
server	A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. The server may run continuously (as a daemon), waiting for requests to arrive, or it may be invoked by some higher-level daemon which controls a number of specific servers.
server farm	A server farm is a network where clients install their own computers to run Web servers, e-mail, or any other TCP/IP based services they require, making use of leased permanent Internet connections with 24-hour worldwide access. Instead of expensive dedicated-line connections to various offices, servers can be placed on server farm networks to have them connected to the Internet at high-speed for a fraction of the cost of a leased line.
shared drive	A computer peripheral device that is used by more than one person, thus increasing the risk of exposure to viruses.
signature	*See* virus signature.
signature-based spam detection	A method of determining whether an email message is spam by comparing the message contents to entries in a spam database. An exact match must be found for the message to be identified as spam. Signature-based spam detection has a nearly zero false positive rate, but does not detect “new” spam that isn’t an exact match for text in the spam signature file. *Also see* rule-based spam detection. *Also see* false positive.
SMTP	Simple Mail Transfer Protocol—A protocol used to transfer electronic mail between computers, usually over Ethernet. It is a server-to-server protocol, so other protocols are used to access the messages.
SMTP server	A server that relays email messages to their destinations.

Term	Explanation
SNMP	Simple Network Management Protocol—A protocol that supports monitoring of devices attached to a network for conditions that merit administrative attention.
SNMP trap	A trap is a programming mechanism that handles errors or other problems in a computer program. An SNMP trap handles errors related to network device monitoring. *See* SNMP.
SOCKS4	A protocol that relays TCP (transmission control protocol) sessions at a firewall host to allow application users transparent access across the firewall.
spam	Unsolicited email messages meant to promote a product or service.
spyware	Advertising-supported software that typically installs tracking software on your system, capable of sending information about you to another party. The danger is that users cannot control what data is being collected, or how it is used.
stamp	To place an identifier, such as “Spam,” in the subject field of an email message.
status bar	A feature of the user interface, that displays the status or progress of a particular activity, such as loading of files on your machine.
subnet mask	In larger networks, the subnet mask lets you define subnetworks. For example, if you have a class B network, a subnet mask of 255.255.255.0 specifies that the first two portions of the decimal dot format are the network number, while the third portion is a subnet number. The fourth portion is the host number. If you do not want to have a subnet on a class B network, you would use a subnet mask of 255.255.0.0. A network can be subnetted into one or more physical networks which form a subset of the main network. The subnet mask is the part of the IP address which is used to represent a subnetwork within a network. Using subnet masks allows you to use network address space which is normally unavailable and ensures that network traffic does not get sent to the whole network unless intended. Subnet masks are a complex feature, so great care should be taken when using them. *Also see* IP address.

Term	Explanation
target (*Also see* action and notification)	The scope of activity to be monitored for a violating event, such as a virus being detected in an email message. For example, you could target virus scanning of all files passing into and out of your network, or just files with a certain file name extension.
TCP	Transmission Control Protocol—TCP is a networking protocol, most commonly use in combination with IP (Internet Protocol), to govern connection of computer systems to the Internet.
Telnet	The Internet standard protocol for remote login that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). This term can also refer to networking software that acts as a terminal emulator for a remote login session.
Total Solution CD	A CD containing the latest product versions and all the patches that have been applied during the previous quarter. The Total Solution CD is available to all Trend Micro Premium Support customers.
traffic	Data flowing between the Internet and your network, both incoming and outgoing.
Transmission Control Protocol/Internet Protocol (TCP/IP)	A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks. A communications protocol which allows computers with different operating systems to communicate with each other. Controls how data is transferred between computers on the Internet.
trigger	An event that causes an action to take place. For example, your Trend Micro product detects a virus in an email message. This may *trigger* the message to be placed in quarantine, and a notification to be sent to the system administrator, message sender, and message recipient.
Trojan Horse	A malicious program that is disguised as something benign. A Trojan is an executable program that does not replicate, but instead, resides on a system to perform malicious acts, such as opening a port for an intruder.
true file type	Used by IntelliScan, a virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).

Term	Explanation
trusted domain	A domain from which your Trend Micro product will always accept messages, without considering whether the message is spam. For example, a company called Dominion, Inc. has a subsidiary called Dominion-Japan, Inc. Messages from dominion-japan.com are always accepted into the dominion.com network, without checking for spam, since the messages are from a known and trusted source.
trusted host	A server that is allowed to relay mail through your network because they are trusted to act appropriately and not, for example, relay spam through your network.
UDP	User Datagram Protocol—A protocol used mainly for broadcasting messages over a network. Like TCP, UDP is layered over IP (Internet Protocol), but UDP is not as reliable as TCP.
URL	Universal Resource Locator—A standard way of specifying the location of an object, typically a Web page, on the Internet, for example, *www.trendmicro.com*. The URL maps to an IP address using DNS.
User Datagram Protocol (UDP)	A protocol in the TCP/IP protocol suite, the User Datagram Protocol or UDP allows an application program to send datagrams to other application programs on a remote machine. Basically UDP is a protocol that provides an unreliable and connectionless datagram service where delivery and duplicate detection are not guaranteed. It does not use acknowledgments, or control the order of arrival.
VBscript virus	VBscript (Microsoft Visual Basic scripting language) is a simple programming language that allows Web developers to add interactive functionality to HTML pages displayed in a browser. For example, developers might use VBscript to add a “Click Here for More Information” button on a Web page. A VBscript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user’s desktop through the user’s browser. *Also see* JavaScript virus.
virtual IP address (VIP address)	A VIP address maps traffic received at one IP address to another address based on the destination port number in the packet header.

Term	Explanation
Virtual Local Area Network (VLAN)	A logical (rather than physical) grouping of devices that constitute a single broadcast domain. VLAN members are not identified by their location on a physical subnetwork but through the use of tags in the frame headers of their transmitted data. VLANs are described in the IEEE 802.1Q standard.
Virtual Private Network (VPN)	A VPN is an easy, cost-effective and secure way for corporations to provide telecommuters and mobile professionals local dial-up access to their corporate network or to another Internet Service Provider (ISP). Secure private connections over the Internet are more cost-effective than dedicated private lines. VPNs are possible because of technologies and standards such as tunneling and encryption.
virtual router	A virtual router is the component of Screen OS that performs routing functions. By default, Trend Micro GateLock supports two virtual routers: Untrust-VR and Trust-VR.
Virtual Security Device (VSD)	A single logical device composed by a set of physical Trend Micro GateLock remote appliances.
Virtual Security Interface (VSI)	A logical entity at layer 3 that is linked to multiple layer 2 physical interfaces in a VSD group. The VSI binds to the physical interface of the device acting as master of the VSD group. The VSI shifts to the physical interface of another device in the VSD group if there is a failover and it becomes the new master.
virtual system	A virtual system is a subdivision of the main system that appears to the user to be a stand-alone entity. Virtual systems reside separately from each other in the same Trend Micro GateLock remote appliance; each one can be managed by its own virtual system administrator.
virus	A computer virus is a program – a piece of executable code – that has the unique ability to infect. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate. In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.
virus kit	A template of source code for building and executing a virus, available from the Internet.

Term	Explanation
virus signature	A virus signature is a unique string of bits that identifies a specific virus. Virus signatures are stored in the Trend Micro virus pattern file. The Trend Micro scan engine compares code in files, such as the body of an email message, or the content of an HTTP download, to the signatures in the pattern file. If a match is found, the virus is detected, and is acted upon (for example, cleaned, deleted, or quarantined) according to your security policy.
virus trap	Software that helps you capture a sample of virus code for analysis.
virus writer	Another name for a computer hacker, someone who writes virus code.
Web	The World Wide Web, also called the Web or the Internet.
Web server	A server process running at a Web site which sends out Web pages in response to HTTP requests from remote browsers.
wildcard	A term used in reference to content filtering, where an asterisk (*) represents any characters. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on. The term originates from card games, in which a specific card, identified as a "wildcard," can be used for any number or suit in the card deck.
Windows Internet Naming Service (WINS)	WINS is a service for mapping IP addresses to NetBIOS computer names on Windows NT server-based networks. A WINS server maps a NetBIOS name used in a Windows network environment to an IP address used on an IP-based network.
working directory	The destination directory in which the main application files are stored, such as C:\Program Files\Trend Micro\ISVW.
workstation (also known as client)	A general-purpose computer designed to be used by one person at a time and which offers higher performance than normally found in a personal computer, especially with respect to graphics, processing power and the ability to carry out several tasks at the same time.
worm	A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems.
zip file	A compressed archive (in other words, “zip file") from one or more files using an archiving program such as WinZip.

Term	Explanation
"Zip of Death"	A zip (or archive) file of a type that when decompressed, expands enormously (for example 1000%) or a zip file with thousands of attachments. Compressed files must be decompressed during scanning. Huge files can slow or stop your network.
zone	A zone can be a segment of network space to which security measures are applied (a security zone), a logical segment to which a VPN tunnel interface is bound (a tunnel zone), or a physical or logical entity that performs a specific function (a function zone).